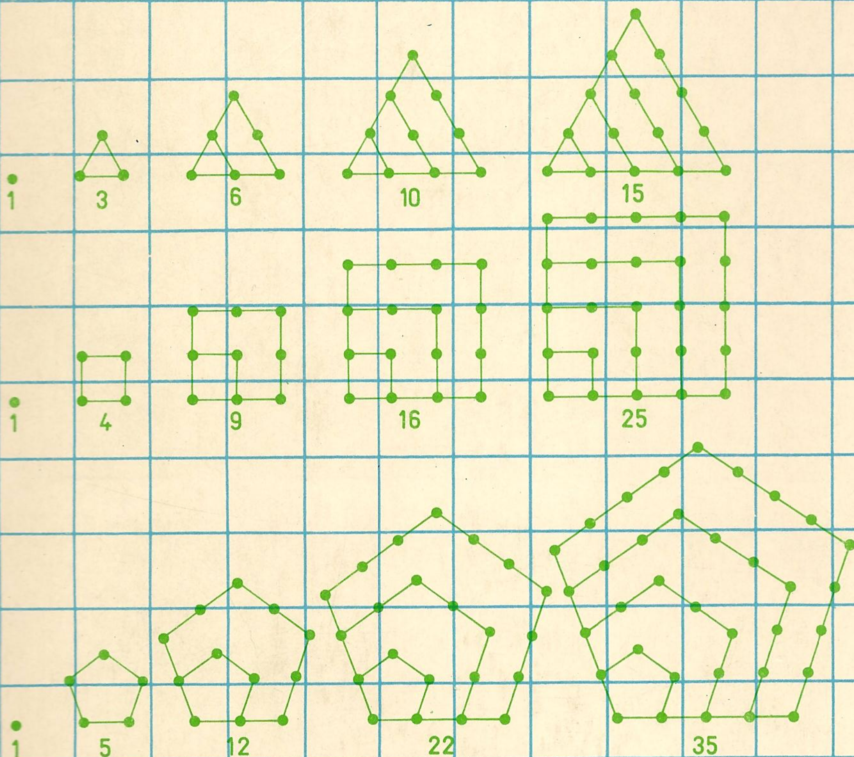
نظریهٔ تحلیلی اعداد

نوشتهٔ

تام م. اپوستل

ترجمهٔ

علی اکبر عالم زاده، علی اکبر رحیم زاده



$$\omega(n) = \sum_{k=0}^{n-1} (3k+1) = \frac{3n(n-1)}{2} + n = \frac{3n^2 - n}{2}$$

نظریه اعداد

تام. م. آپوستل

ترجمه علی اکبر عالم زاده، علی اکبر رحیم زاده

انتشارات شباهنگ

پیشگفتار مترجمان

نظریهٔ اعداد جالب‌ترین شاخهٔ ریاضیات است. این مبحث، که زمانی پراکنده و منزوی بود، اینک به علمی منجسم، فعال، با اصولی پیچیده بدل شده است. توان اعجاب‌آورش را ناشی از روشهای تحلیلی آن می‌دانند. از اینروست که بخش تحلیلی این نظریه زیباترین تجلیات فکری ریاضی بشر محسوب می‌شود.

چون در نظریهٔ تحلیلی اعداد کتابی به فارسی وجود نداشت، بر آن شدیم تا جلد اول کتاب بی‌نظیر اپوستل را ترجمه و تقدیم شیفتگان این نظریه نماییم. باشد که این خدمت مقبول ریاضی دوستان فارسی زبان قرار گیرد.

علی‌اکبر عالم‌زاده   علی‌اکبر رحیم‌زاده
گروه آموزشی ریاضی
دانشگاه تربیت معلم

پیشگفتار مؤلف

این کتاب جلد اول یک کتاب درسی دوجلدی است[1] که از درسی (ریاضیات ۱۶۰) که ۲۵ سال است در موسسهٔ فنی کالیفرنیا ارائه می‌شود ناشی شده است. کتاب مقدمه‌ای است بر نظریهٔ تحلیلی اعداد که برای دانشجویان لیسانس که قدری حساب دیفرانسیل وانتگرال پیشرفته می‌دانند، ولو هیچ معرفتی از نظریهٔ اعداد ندارند، مناسب است. درواقع، بخش وسیعی از کتاب به حساب دیفرانسیل و انتگرال نیاز ندارد، و شاگردان خوب دبیرستانی نیز می‌توانند آن را مطالعه کرده از آن سود ببرند.

نظریهٔ اعداد چنان رشتهٔ وسیع و پرباری است که در یک درس یکساله نمی‌توان به همهٔ جنبه‌های آن پرداخت. مطالب این کتاب به این قصد که تنوعی باشد و عمقی ببخشد انتخاب شده‌اند. همچنین، مسائلی که نسلهای مختلف ریاضیدانان حرفه‌ای و آماتور را مجذوب خود ساخته‌اند همراه با روشهایی برای حلشان مورد بحث قرار گرفته‌اند.

از هدفهای این درس پرورش علاقهٔ ذاتی است که بسیاری از دانشجویان جوان ریاضی به نظریهٔ اعداد دارند و باز کردن درهای مجلات تحقیقی جاری به روی آنهاست. جای خوشوقتی است که می‌بینیم بسیاری از دانشجویانی که این درس را در ۲۵ سال گذشته گرفته‌اند ریاضیدانانی حرفه‌ای شده‌اند، و برخی از آنها خدمات شایسته‌ای به نظریهٔ اعداد کرده‌اند. کتاب را به همهٔ آنها تقدیم می‌دارم.

تام م. اپوستل

---

۱. عنوان جلد دوم این کتاب عبارت است از:

Modular Functions and Dirichlet Series in Number Theory.

فهرست مطالب

مقدمهٔ تاریخی

نظریهٔ اعداد شاخه‌ای است از ریاضیات که از خواص اعداد درست، یعنی

$$1, 2, 3, 4, 5, \ldots$$

که ***اعداد شمار*** یا ***اعداد صحیح مثبت*** نیز نام دارند، سخن می‌گوید.

شک نیست که اعداد صحیح مثبت نخستین اختراع ریاضی بشر است. بسختی می‌توان انسانی را مجسم کرد که، لااقل در سطحی محدود، قدرت شمارش نداشته باشد. یادداشتهای تاریخی نشان می‌دهند که سومریان باستان حدود ۵۷۰۰ ق م تقویم داشته‌اند؛ و از اینرو، باید نوعی حساب می‌داشته‌اند.

حدود ۲۵۰۰ ق م، سومریها، با استفاده از عدد 60 به عنوان پایه، دستگاه اعدادی ابداع کردند. این دستگاه نصیب بابلیها شد، که به مهارتهای والایی در حساب رسیدند. لوحهای گلی بدست آمده از بابلیها شامل جداول ریاضی کاملی هستند و قدمتشان به ۲۰۰۰ ق م می‌رسد.

وقتی تمدنهای باستان به سطحی رسیدند که اوقات فراغت برای تدقیق در اشیاء بدست آمد، برخی به تفکر در سرشت و خواص اعداد پرداختند. این کنجکاوی به‌نوعی تصوف یا علم معانی رمزی اعداد منجر شد، و حتی امروزه نیز اعدادی نظیر 3، 7، 11، و 13 نشانهٔ خوش شانسی یا بدشانسی هستند.

بیش از ۵۰۰۰ سال، قبل از آنکه کسی به فکر بررسی خود اعداد به‌طور اصولی باشد، اعداد برای حفظ محاسبات و معاملات تجاری بکار رفته‌اند. اولین روش علمی برای بررسی اعداد صحیح، یعنی مبداء اصلی نظریهٔ اعداد، را عموماً به یونانیان نسبت می‌دهند. حدود ۶۰۰ ق م، فیثاغورس[1] و پیروانش بررسی نسبتاً جامعی از اعداد صحیح کردند.

1. Pythagoras

آنان اولین کسانی بودند که اعداد صحیح را به طرق مختلف رده‌بندی کردند :

اعداد زوج : 2, 4, 6, 8, 10, 12, 14, 16, ...

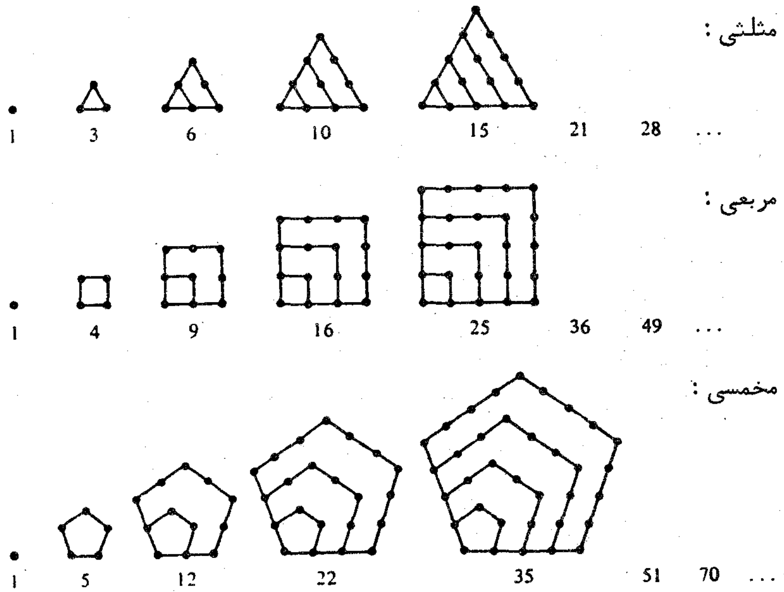
اعداد فرد : 1, 3, 5, 7, 9, 11, 13, 15, ...

اعداد اول : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

اعداد مرکب : 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, ...

یک **عدد *اول*** عددی است بزرگتر از 1 که تنها مقسوم علیه‌های آن 1 و خود عدد باشند. اعدادی‌که اول نباشند نام دارند **مرکب**، جز عدد 1 که نه اول گرفته می‌شود نه مرکب.

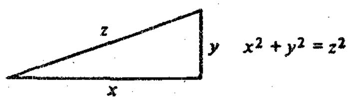
فیثاغوریان اعداد را به هندسه نیز مربوط ساختند. آنان مفهوم **اعداد چند ضلعی** را معرفی کردند : اعداد مثلثی، اعداد مربعی، اعداد مخمسی، و غیره. دلیل این



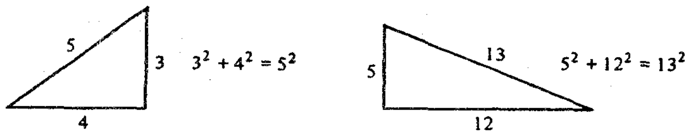
شکل م ۱۰

نامگذاری هندسی با نمایش اعداد به وسیلهٔ نقاط به شکل مثلث، مربع، مخمس، و غیره، بصورتی که در شکل م ۱۰ نموده شده، مشخص می‌شود.

رابطهٔ دیگر اعداد با هندسه ناشی از قضیهٔ معروف فیثاغورس است، که می‌گوید: در هر مثلث قائم الزاویه مربع وتر مساوی مجموع مربعات دوضلع دیگر است (ر.ک. شکل م ۲۰). فیثاغوریان بـه مثلثهای قائمی نظر داشتند که، همانند شکل م ۳۰، اضلاعشان



شکل م ۲۰



شکل م ۳۰

اعدادی صحیح باشند. این نوع مثلثها را امروزه ***مثلثهای فیثاغوری*** می‌نامند. سه‌تایی (x, y, z) نظیر که نمایشگر طول اضلاع است یک ***سه‌تایی فیثاغوری*** نام دارد.

یک لوح بابلی، متعلق به حدود ۱۷۰۰ ق م، پیدا شده که شامل صورت مبسوطی از سه‌تاییهای فیثاغوری است و بعضی از اعداد آن نسبتا" بزرگ می‌باشند. فیثاغوریان نخستین کسانی بودند که روشی برای تعیین بی‌نهایت سه‌تایی عرضه کردند. این روش را می‌توان با نمادهای جـدید چنین بیان کرد: فرض کنیم n یک عدد فرد بزرگتر از 1 باشد، و

$$x = n, \qquad y = \tfrac{1}{2}(n^2 - 1), \qquad z = \tfrac{1}{2}(n^2 + 1).$$

سه‌تایی (x, y, z) حاصل همیشه یک سه‌تایی فیثاغوری است، که درآن $z = y + 1$. چند نمونه از آن عبارتند از

x	3	5	7	9	11	13	15	17	19
y	4	12	24	40	60	84	112	144	180
z	5	13	25	41	61	85	113	145	181

علاوه براینها، سه‌تاییهای فیثاغوری دیگری نیز وجود دارند؛ به‌عنوان مثال،

x	8	12	16	20
y	15	35	63	99
z	17	37	65	101

دراین مثالها داریم $z = y + 2$. افلاطون[1] (۳۴۹ – ۴۳۰ ق م) روشی برای تعیین همهٔ این سه‌تاییها بدست آورد؛ این سه‌تاییها در نمادگذاری جدید با فرمولهای زیر بیان می‌شوند :

$$x = 4n, \qquad y = 4n^2 - 1, \qquad z = 4n^2 + 1.$$

حدود ۳۰۰ ق م واقعهٔ مهمی در تاریخ ریاضیات رخ داد . ظهور *اصول* آقلیدس[2]، مجموعه‌ای مرکب از ۱۳ کتاب ، ریاضیات را از علم معانی رمزی اعداد به یک علم استنتاجی بدل ساخت . اقلیدس اولین کسی بود که حقایق ریاضی را همراه با برهانهای دقیق آنها عرضه کرد . سه کتاب از سیزده کتاب (کتابهای **VII** ، **IX** ، و **X**) به‌نظریهٔ اعداد اختصاص دارند . در کتاب **IX** ، اقلیدس وجود بی‌نهایت عدد اول را ثابت می‌کند . اثباتش هنوز درکلاسهای درسی تدریس می‌شود . او در کتاب **X** روشی برای بدست آوردن همهٔ سه‌تاییهای فیثاغوری ارائه می‌دهد ، اما دلیلی براینکه روشش جمیع آنها را بدست می‌دهد نمی‌آورد . این روش را می‌توان در فرمولهای زیر خلاصه کرد :

$$x = t(a^2 - b^2), \qquad y = 2tab, \qquad z = t(a^2 + b^2),$$

که‌درآنها t ، a ، و b اعداد صحیح مثبت دلخواهی هستند بطوری‌که $a > b$ ، a و b عامل اول مشترک ندارند ، و یکی از a و b فرد و دیگری زوج است .

همچنین ، اقلیدس در مسئلهٔ دیگری که فیثاغوریان طرح کرده بودند ــ و آن یافتن همهٔ اعداد تام بود ــ تحقیقات مهمی انجام داد . عدد 6 را یک عدد تام می‌گفتند زیرا $6 = 1 + 2 + 3$، یعنی مساوی مجموع تمام مقسوم علیه‌های واقعی خود (یعنی ، مجموع تمام مقسوم علیه‌های کوچکتر از 6) بود . مثالی دیگر از اعداد تام 28 است ، زیرا $28 = 1 + 2 + 4 + 7 + 14$، و 1 ، 2 ، 4 ، 7 ، و 14 مقسوم علیه‌های 28 هستند که از 28 کوچکترند . یونانیان مقسوم علیه‌های واقعی یک عدد را "فرازهای" آن عدد می‌خواندند . آنان 6 و 28 را اعداد تام می‌گفتند ، از آنجهت که هریک مساوی مجموع تمام فرازهای خود می‌باشد .

در کتاب IX ، اقلیدس همهٔ اعداد تام **زوج** را بدست می‌دهد . وی ثابت کرده

1. Plato 2. Euclid

است که یک عدد زوج تام است اگر به شکل

$$2^{p-1}(2^p - 1)$$

بوده و درآن p و $2^p - 1$ هر دو اول باشند.

دو هزار سال بعد، اویلر[1] عکس قضیهٔ اقلیدس را ثابت کرد. یعنی، ثابت کرد هر عدد تام زوج باید از نوع اقلیدس باشد. مثلاً، برای 6 و 28 داریم

$$6 = 2^{2-1}(2^2 - 1) = 2 \cdot 3 \quad \text{و} \quad 28 = 2^{3-1}(2^3 - 1) = 4 \cdot 7.$$

اولین پنج عدد تام زوج عبارتند از

$$6، 28، 496، 8128 \quad \text{و} \quad 33،550،336.$$

در واقع، اعداد تام بسیار نادرند. تا امروز (۱۹۷۵) فقط ۲۴ عدد تام شناخته شده است. اینها در فرمول اقلیدس نظیر به مقادیر زیر از p اند:

$$2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281,$$
$$3217, 4253, 4423, 9689, 9941, 11{,}213, 19{,}937.$$

اعداد به شکل $2^p - 1$، که درآن p اول است، به افتخار مرسن[2]، که آنها را در ۱۶۴۴ مطالعه کرد، **اعداد مرسن** نام یافته‌اند و با M_p نموده می‌شوند. ثابت شده‌است که M_p به‌ازای ۲۴ عدد اول مذکور در بالا اول، و به‌ازای مقادیر دیگر از $p \le 257$، جز احتمالاً

$$p = 157, 167, 193, 199, 227, 229,$$

مرکب است. در مورد این اعداد هنوز معلوم نشده که M_p اول است یا مرکب.

تاکنون هیچ عدد تام **فرد** بدست نیامده است؛ حتی از وجود آنها نیز اطلاعی در دست نیست. اما، اگر وجود داشته باشند، باید خیلی بزرگ باشند؛ درواقع، بزرگتر از 10^{50} (ر.ک. هگیس[3] [۲۹]).

حال به شرح مختصر تاریخ نظریهٔ اعداد از زمان اقلیدس تا امروز می‌پردازیم.

بعد از اقلیدس در ۳۰۰ ق م پیشرفت چشمگیری در نظریهٔ اعداد صورت نگرفت تا حدود ۲۵۰ ب‍ م که ریاضیدان دیگر یونانی، دیوفانتوس[4] اهل اسکندریه، ۱۳ کتاب منتشر کرد، که فقط شش‌تای آنها بجا مانده است. این اولین اثر یونانی است که درآن از علایم جبری به‌نحو اصولی استفاده شده است. با اینکه نمادهای جبریش در مقایسه با نمادهای فعلی خامند، دیوفانتوس توانسته بعضی از معادلات جبری دو یا سه متغیره را حل نماید. بسیاری از مسائل آن از نظریهٔ اعداد مایه گرفته‌اند و، درنتیجه، جستجوی جوابهای

---

1. Euler 2. Mersenne 3. Hagis 4. Diophantus

صحیح معادلات برایش امری طبیعی بوده‌است. امروزه معادلاتی که حلشان مستلزم یافتن جوابهای صحیح است **معادلات دیوفانتینی** نام داشته، و بررسی این معادلات به **آنالیز دیوفانتینی** شهرت دارد. معادلهٔ $x^2 + y^2 = z^2$ در مورد سه‌تاییهای فیثاغوری نمونه‌ای از یک معادلهٔ دیوفانتینی است.

بعد از دیوفانتوس تا قرن هفده پیشرفت چندانی در نظریهٔ اعداد حاصل نشد، اگرچه شواهدی وجود دارند که نشان می‌دهند این مبحث در شرق دور — بویژه در هندوستان — در فاصله زمانی ۵۰۰ ب.م و ۱۲۰۰ ب.م شروع به شکوفایی کرده است.

این مبحث در قرن هفده در اروپای غربی جان گرفت، و آن بیشتر بخاطر مساعی ریاضیدان برجستهٔ فرانسوی، پیردوفرما[1] (۱۶۶۵ — ۱۶۰۱)، بود، که عموم وی را پدر نظریهٔ جدید اعداد می‌دانند. فرما بسیاری از الهامات خود را از آثار دیوفانتوس گرفت. وی نخستین کسی بود که خواص عمیق اعداد صحیح را کشف کرد. مثلاً، فرما قضایای حیرت انگیز زیر را اثبات کرد:

هر عدد صحیح یک عدد مثلثی است یا مجموع 2 یا 3 عدد مثلثی؛ هر عدد صحیح یک عدد مربعی است یا مجموع 2، 3، یا 4 عدد مربعی؛ هر عدد صحیح یک عدد مخمسی است یا مجموع 2، 3، 4، یا 5 عدد مخمسی، و غیره.

همچنین، فرما کشف کرد که هر عدد اول به شکل $4n + 1$، نظیر 5، 13، 17، 29، 37، 41، و غیره، مجموع دو عدد مربعی است. مثلاً،

$$5 = 1^2 + 2^2, \qquad 13 = 2^2 + 3^2, \qquad 17 = 1^2 + 4^2, \qquad 29 = 2^2 + 5^2,$$
$$37 = 1^2 + 6^2, \qquad 41 = 4^2 + 5^2.$$

اندکی پس از فرما، نامهایی چون اویلر (۱۷۸۳—۱۷۰۷)، لاگرانژ[2] (۱۸۱۳—۱۷۳۶)، لژاندر[3] (۱۸۳۳ — ۱۷۵۲)، گاوس[4] (۱۸۵۵ — ۱۷۷۷)، و دیریکله[5] (۱۸۵۹ — ۱۸۰۵) بخاطر بسط بیشتر این نظریه به شهرت رسیدند. اولین کتاب درسی در نظریهٔ اعداد به‌وسیلهٔ لژاندر در ۱۷۹۸ منتشر شد. سه سال بعد، گاوس *Disquisitiones Arithmeticae* را انتشار داد، کتابی که نظریهٔ اعداد را به یک علم اصولی و زیبا بدل کرد. گاوس با آنکه در رشته‌های دیگر ریاضیات، و نیز در سایر علوم، کارهای باارزشی کرده بود، کتاب نظریهٔ اعداد خود را بزرگترین اثر خویش می‌دانست.

درصد سال اخیر، یا بیشتر، از زمان گاوس، این مبحث پیشرفتهای زیادی درجهات

---

1. Pierre de Fermat 2. Lagrange 3. Legendre 4. Gauss
5. Dirichlet

مختلف داشته است. شرح انواع مسائلی که در نظریهٔ اعداد بررسی شده‌اند در چند صفحه ممکن نیست. این مبحث بسیار وسیع است و در بعضی قسمتها نیاز به معرفت عمیقی از ریاضیات عالی دارد. با اینحال، مسائل زیادی در نظریهٔ اعداد وجود دارند که به آسانی قابل بیانند. برخی از آنها به اعداد اول مربوط می‌شوند، و ما بقیهٔ این مقدمه‌را به این مسائل اختصاص می‌دهیم.

اعداد اول کوچکتر از 100 در بالا ذکر شده‌اند. جدول همهٔ اعداد اول کوچکتر از 10 میلیون در ۱۹۱۴ توسط ریاضیدان امریکایی، دی. ان. لمر[1] [۴۳] منتشر شد. درست 664,579، یا حدوداً $6\frac{1}{2}\%$، عدد اول کوچکتر از 10 میلیون وجود دارد. اخیراً، دی. اچ. لمر[2] (پسر دی. ان. لمر) تعداد اعداد اول کوچکتر از 10 بیلیون را حساب کرده است؛ درست 455,052,512، یا حدوداً $4\frac{1}{2}\%$، از این اعداد وجود دارد، اگرچه تک تک آنها شناخته شده نیستند (ر.ک. لمر [۴۱]).

بررسی دقیق جدول اعداد اول نشان می‌دهد که توزیع آنها بسیار نامنظم است. این جداول شکافهای عریض را بین آنها نشان می‌دهند. مثلاً، بعد از عدد اول 370,261، 111 عدد مرکب می‌آیند. هیچ عدد اولی بین 20,831,323 و 20,831,533 وجود ندارد. به‌آسانی ثابت می‌شود که شکافهای عریض دلخواه بین اعداد اول مآلاً رخ خواهند داد.

از آن‌سو، این جدولها نشان می‌دهند که اعداد اول متوالی، نظیر 3 و 5، یا 101 و 103، همین‌طور تکرار می‌شوند. جفتهایی از اعداد اول که تفاضلشان 2 باشد ***دوقلوهای اول*** نام دارند. بیش از 1000 تا از این جفتها زیر 100,000 و بیش از 8000 جفت زیر 1,000,000 وجود دارد. بزرگترین جفتی که تابحال شناخته شده (ر.ک. ویلیامز[3] و زارنکه[4] [۷۶]) $76 \cdot 3^{139} - 1$ و $76 \cdot 3^{139} + 1$ است. به‌نظر بسیاری از ریاضیدانان، تعداد این جفتها بی‌نهایت است، اما کسی تاکنون قادر به‌اثباتش نبوده است.

یکی از علل این بی‌نظمی در توزیع اعداد اول عدم وجود فرمولی ساده برای تولید همهٔ این اعداد است. بعضی فرمولها اعداد اول بسیاری را به‌ما می‌دهند. مثلاً، عبارت

$$x^2 - x + 41$$

به‌ازای $x = 0, 1, 2, \ldots, 40$ اول است، و نیز

$$x^2 - 79x + 1601$$

به‌ازای $x = 0, 1, 2, \ldots, 79$ اول می‌باشد. لیکن، هیچ فرمول ساده‌ای از این نوع، حتی

---

1. D. N. Lehmer 2. D. H. Lehmer 3. Williams 4. Zarnke

اگر مکعب و توانهای بالاتر بکار روند، نمی‌تواند به‌ازای هر x اول باشد. درواقع، در سال ۱۷۵۲، گلدباخ[1] ثابت کرد که هیچ چند جمله‌ای از x با ضرایب صحیح نمی‌تواند به‌ازای هر x، یا حتی x های به‌قدر کافی بزرگ، اول باشد.

بعضی از چند جمله‌ایها بی‌نهایت عدد اول‌را نمایش می‌دهند. مثلاً، وقتی x اعداد صحیح $0, 1, 2, 3, \ldots$ را بگیرد، چندجمله‌ای خطی

$$2x + 1$$

همهٔ اعداد فرد و، درنتیجه، بی‌نهایت عدد اول بدست می‌دهد. همچنین، هریک از چندجمله‌ایهای

$$4x + 3 \quad \text{و} \quad 4x + 1$$

نمایش بی‌نهایت عدد اول است. دیریکله در یک مقالهٔ مشهور ([۱۵])، که به‌سال ۱۸۳۷ منتشر شد، ثابت کرد که، اگر a و b اعداد صحیح مثبتی بدون عامل مشترک باشند، چندجمله‌ای

$$ax + b$$

وقتی x همهٔ اعداد صحیح مثبت را بگیرد، بی‌نهایت عدد اول بدست می‌دهد. این نتیجه امروزه به قضیهٔ دیریکله در باب وجود اعداد اول در یک تصاعد عددی معروف است.

برای اثبات این قضیه، دیریکله از حیطهٔ اعداد صحیح بیرون رفت و ابزارهایی از آنالیز نظیر حدود و پیوستگی را معرفی کرد. با این‌کار، پایه‌های شاخهٔ جدیدی از ریاضیات به‌نام ***نظریهٔ تحلیلی اعداد*** ریخته شد، که درآن مفاهیم و روشهای آنالیز حقیقی و مختلط برای حل مسائل مربوط به اعداد صحیح بکار برده می‌شوند.

معلوم نیست آیا چندجمله‌ای درجهٔ دومی مانند $ax^2 + bx + c$ با $a \neq 0$ وجود دارد که بی‌نهایت عدد اول را نمایش دهد. دیریکله [۱۶] با استفاده از روشهای قوی تحلیلی خود ثابت کرد که، اگر a، $2b$، و c عامل اول مشترک نداشته باشند، چندجمله‌ای درجهٔ دوم دومتغیرهٔ

$$ax^2 + 2bxy + cy^2$$

وقتی x و y اعداد صحیح مثبت را بگیرند، بی‌نهایت عدد اول را نمایش می‌دهد.

فرما می‌پنداشت که فرمول $2^{2^n} + 1$ همیشه، به‌ازای $n = 0, 1, 2, \ldots$، اول است. این اعداد را ***اعداد فرما*** می‌نامند و با F_n نشان می‌دهند. اولین پنج عدد فرما عبارتند از

---

1. Goldbach

$F_0 = 3$ ، $F_1 = 5$ ، $F_2 = 17$ ، $F_3 = 257$ ، و $F_4 = 65,537$ ،
و همهٔ آنها اولند . لیکن، اویلر در ۱۷۳۲ دریافت که F_5 مرکب است ؛ در واقع ،

$$F_5 = 2^{32} + 1 = (641)(6,700,417).$$

این اعداد درهندسهٔ مسطحه نیز مورد توجه‌اند . گاوس ثابت کرد که اگر F_n اول باشد ، مثلا" $F_n = p$ ، به‌کمک خط‌کش و پرگار می‌توان p ضلعی منتظم را ساخت .

هیچ عدد فرمای اولی بزرگتر از F_5 یافت نشده است .

درواقع ، به‌ازای $5 \leq n \leq 16$ ، هر عدد فرمای F_n مرکب است . همچنین، معلوم شده که F_n به‌ازای مقادیر زیر از n مرکب است :

$$n = 18, 19, 21, 23, 25, 26, 27, 30, 32, 36, 38, 39, 42, 52, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 452, 1945.$$

بزرگترین عدد فرمای مرکب شناخته شده ، یعنی F_{1945} ، بیش از 10^{582} رقم دارد ، عددی بزرگتر از تعداد حروف راهنماهای تلفن لوس آنجلس و نیویورک (ر.ک. رابینسون[1] [۵۹] وراتهال[2] [۷۷]) .

قبلا" گفتیم که برای همهٔ اعداد اول فرمول ساده‌ای وجود ندارد . دراین رابطه، لازم است نتیجه‌ای که در ۱۹۴۷ به‌وسیلهٔ ریاضیدان امریکایی ، دبلیو . اچ . میلز[3] [۵۰]، کشف شد را ذکر کنیم . وی ثابت کرد که عددی مانند A ، بزرگتر از 1 ولی نه عددی صحیح ، وجود دارد بطوری که

$[A^{3^x}]$ به‌ازای هر $x = 1, 2, 3, \ldots$ اول است .

دراینجا $[A^{3^x}]$ یعنی بزرگترین عدد صحیح نابیشتر از A^{3^x} . متاسفانه ، هیچکس نمی‌داند A مساوی چیست .

نتایج پیشگفته بی‌نظمی توزیع اعداد اول رانشان می‌دهند . لیکن، با بررسی دسته‌های بزرگی از اعداد اول، درمی‌یابیم که توزیع متوسط آنها نسبتا" منظم است . با اینکه اعداد اول پایان ندارند ، ولی همین‌طور که در جدول پیش می‌رویم ، به‌طور متوسط، از هم فاصله می‌گیرند . کاهش فراوانی اعداد اول موضوع تحقیقات بسیاری در آغاز قرن نوزدهم بوده است . برای مطالعهٔ این توزیع ، تابع $\pi(x)$ را درنظر می‌گیریم که تعداد اعداد اول نابیشتر از x را می‌شمارد ؛ یعنی ،

$\pi(x) =$ تعداد اعداد اول p صادق در $2 \leq p \leq x$.

---

1. Robinson 2. Wrathall 3. W. H. Mills

ذیلا" جدول مختصری از این‌تابع و مقایسه‌اش با $x/\log x$ ذکر شده است، که در آن $\log x$ لگاریتم طبیعی x است.

x	$\pi(x)$	$x/\log x$	$\pi(x)\Big/\dfrac{x}{\log x}$
10	4	4.3	0.93
10^2	25	21.7	1.15
10^3	168	144.9	1.16
10^4	1,229	1,086	1.11
10^5	9,592	8,686	1.10
10^6	78,498	72,464	1.08
10^7	664,579	621,118	1.07
10^8	5,761,455	5,434,780	1.06
10^9	50,847,534	48,309,180	1.05
10^{10}	455,052,512	434,294,482	1.048

گاوس [۲۴] و لژاندر [۴۰] با بررسی‌جدولی مانند فوق به‌ازای $x \leq 10^6$ مستقلا" دریافتند که، به‌ازای x های بزرگ، نسبت

$$\pi(x)\Big/\frac{x}{\log x}$$

نزدیک به 1 است، وحدس‌زدند که‌این‌نسبت، وقتی x به ∞ نزدیک شود، به 1 نزدیک می‌شود. گاوس و لژاندر هر دو در اثبات آن کوشیدند اما موفق نشدند. مسئلهٔ درست یا نادرست بودن این حدس قریب به ۱۰۰ سال نظر ریاضیدانان برجسته را به‌خود جلب کرده بود.

درسال ۱۸۵۱، ریاضیدان روسی چبیشف[1] [۹]، با اثبات اینکه "اگر این نسبت به‌حدی میل کند، این حد باید 1 باشد"، قدم مهمی به‌جلو برداشت. لیکن، قادر به اثبات اینکه این نسبت به‌حدی میل **می‌کند** نبود.

درسال ۱۸۵۹، ریمان[۲] [۵۸] به‌روشهای تحلیلی، و با استفاده از فرمولی که‌توسط اویلر در ۱۸۳۷ کشف شده بود و اعداد اول را به‌تابع

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

به‌ازای $s > 1$ حقیقی مربوط می‌کرد، به‌مسئله حمله برد. ریمان مقادیر مختلط s را در

1. Chebyshev 2. Riemann

نظرگرفت و روشی ابتکاری برای ربط توزیع اعداد اول به خواص تابع $\zeta(s)$ را طرح ریخت. هنوز ریاضیات لازم برای توجیه کامل روش او بدست نیامده بود، و ریمان نتوانست مسئله را پیش از مرگش در ۱۸۶۶ کاملاً سامان دهد.

سی سال بعد ابزارهای تحلیلی لازم در دست بودند و در سال ۱۸۹۶، ج. هادامار[1] [۲۸] و سی. ج. دولاواله‌پوسن[2] [۷۱] مستقلاً و تقریباً همزمان به اثبات

$$\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1$$

موفق شدند. این نتیجهٔ قابل توجه ***قضیهٔ اعداد اول*** نام دارد، و اثباتش یکی از عالی‌ترین کارها در نظریهٔ تحلیلی اعداد است.

در سال ۱۹۴۹، دو ریاضیدان معاصر، اتل سلبرگ[3] [۶۲] و پل اردوش[4] [۱۹]، با کشف یک برهان مقدماتی قضیهٔ اعداد اول هیجانی در ریاضیات آفریدند. در این برهان، با همهٔ پیچیدگی، نه از $\zeta(s)$ استفاده می‌شد نه از نظریهٔ توابع مختلط، و اصولش برای هر فرد آشنا با حساب دیفرانسیل و انتگرال مقدماتی قابل درک بود.

یکی از معروفترین مسائل اعداد اول ***حدس گلدباخ*** است. در سال ۱۷۴۲، گلدباخ [۲۶] در نامه‌ای به اویلر نوشت که هر عدد زوج ناکمتر از 4 مجموع دو عدد اول است. مثلاً،

$$4=2+2,\qquad 6=3+3,\qquad 8=3+5,$$
$$10=3+7=5+5,\qquad 12=5+7.$$

این حدس تاکنون بلاتکلیف مانده است، گرچه در سالهای اخیر پیشرفتهایی صورت گرفته که صحت احتمالی آن را نشان می‌دهند. اما چرا ریاضیدانان حدس را ***احتمالاً*** "درست می‌دانند درحالی که قادر به اثباتش نیستند؟ قبل از همه، حدس به‌ازای تمام اعداد زوج کوچکتر از 33×10^6 با محاسبه تحقیق شده است. معلوم شده که هر عدد زوج بزرگتر از 6 و کوچکتر از 33×10^6 نه فقط مجموع دو عدد اول فرد است بلکه مجموع دو عدد اول فرد ***متمایز*** می‌باشد (ر.ک. شن[5] [۶۶]). اما، در نظریهٔ اعداد، تحقیق چند هزار حالت برای متقاعد کردن ریاضیدانان که چیزی احتمالاً "**درست** است کافی نیست. مثلاً"، همهٔ اعداد اول به دو رسته تقسیم می‌شوند، یک رسته به شکل $4n+1$ و رستهٔ دیگر به شکل $4n+3$. فرض کنیم $\pi_1(x)$ تعداد اعداد اول نابیشتر از x و به‌شکل $4n+1$، و $\pi_3(x)$ تعداد اعداد اول نابیشتر از x و به‌شکل $4n+3$ باشد. معلوم شده که بی‌نهایت

---

1. J. Hadamard 2. C. J. de la Vallée Poussin 3. Atle Selberg
4. Paul Erdös 5. Shen

عدد اول از هر دو نوع وجود دارند. با محاسبه معلوم شده است که، به‌ازای هر $x < 26,861$، $\pi_1(x) \le \pi_3(x)$. اما، درسال ۱۹۵۷، ج. لیچ[1] [۳۹] دریافت که، به‌ازای $x = 26,861$، داریم $\pi_1(x) = 1473$ و $\pi_3(x) = 1472$؛ درنتیجه، عکس نامساوی فوق برقرار است. در سال ۱۹۱۴، لیتلوود[2] [۴۹] ثابت کرد که این نامساوی بی‌نهایت بار پس و پیش می‌شود. یعنی، بی‌نهایت x وجود دارد که به‌ازای آنها $\pi_1(x) < \pi_3(x)$، و بی‌نهایت x وجود دارد که به‌ازای آنها $\pi_3(x) < \pi_1(x)$. بنابراین، حدسهای مربوط به اعداد اول، حتی اگر درچند هزار حالت با محاسبه تحقیق شوند، ممکن است خطا باشند.

لذا، این امر که حدس گلدباخ به‌ازای همهٔ اعداد زوج کوچکتر از 33×10^6 تحقیق شده گواه ضعیفی در جهت اعتبار آن بیش نیست.

راه دیگری که ریاضیدانان برای صحت یک حدس خاص گواه جمع می‌کنند اثبات قضایایی است که با آن حدس شباهت دارند. مثلاً، درسال ۱۹۳۰، ریاضیدان روسی، اشنیرلمان[3] [۶۱]، ثابت کرد عددی مانند M هست بطوری که هر عدد n از مرتبه‌ای به بعد مجموع M عدد اول یا کمتر است:

$$n = p_1 + p_2 + \cdots + p_M \qquad (\text{به‌ازای } n \text{ به‌قدر کافی بزرگ})$$

اگر M به‌ازای هر n زوج مساوی 2 می‌بود، حدس گلدباخ به‌ازای هر n به‌قدر کافی بزرگ ثابت می‌شد. درسال ۱۹۵۶، ریاضیدان چینی، یین ون ــ لین[4] [۷۸]، ثابت کرد که $M \le 18$. یعنی، هر عدد n از مرتبه‌ای به بعد مجموع 18 عدد اول یا کمتر است. نتیجهٔ اشنیرلمان را گام بلندی درجهت اثبات حدس گلدباخ می‌دانند. این نتیجه اولین پیشرفت واقعی درحل این مسئله بعد از قریب به ۲۰۰ سال بوده است.

درسال ۱۹۳۷، ریاضیدان دیگر روس، آی. ام. وینوگرادف[5] [۷۳]، به‌حل مسئلهٔ گلدباخ خیلی نزدیکتر شد، و ثابت کرد که، از مرتبه‌ای به‌بعد، هر عدد **فرد** مجموع **سه** عدد اول است:

$$n = p_1 + p_2 + p_3 \qquad (n \text{ فرد و به‌قدر کافی بزرگ})$$

در واقع، این مطلب برای هر n فرد بزرگتر از $3^{3^{15}}$ درست است (ر.ک. برودزکین[6] [۵]). تاکنون، این قویترین شاهد در تایید حدس گلدباخ بوده است. به یک دلیل، و آن این است که قضیهٔ وینوگرادف به‌آسانی از حکم گلدباخ نتیجه می‌شود. یعنی، اگر حدس گلدباخ درست باشد، به‌آسانی حکم وینوگرادف بدست می‌آید. کار عظیم وینوگرادف

---

1. J. Leech 2. Littlewood 3. Schnirelmann 4. Yin Wen-Lin
5. I. M. Vinogradov 6. Borodzkin

این بود که توانست نتیجه‌اش را بی‌استفاده از حکم گلدباخ ثابت کند. متاسفانه، کسی نتوانسته عکس آن را ثابت کند و حکم گلدباخ را از حکم وینوگرادف نتیجه بگیرد.

گواه دیگر در تایید حدس گلدباخ را ریاضیدان مجار، رنی[1] [۵۷]، به‌سال ۱۹۴۸ بدست‌آورد، و ثابت کرد عددی مانند M هست بطوری که هر عدد زوج به‌قدر کافی بزرگ را می‌توان به‌صورت یک عدد اول بعلاوهٔ عددی دیگر که بیش از M عامل اول ندارد نوشت:

$$n = p + A,$$

که درآن A بیش از M عامل اول ندارد (n زوج و به‌قدر کافی بزرگ). اگر می‌دانستیم که $M = 1$، حدس گلدباخ به‌ازای هر n به‌قدر کافی بزرگ درست می‌بود. درسال ۱۹۶۵، ا.ا. بوشتاب[2] [۶] و ا.آی. وینوگرادف[3] [۷۲] ثابت‌کردندکه $M \leq 3$، ودرسال ۱۹۶۶، چن‌جینگ ــ رون[4] [۱۰] ثابت‌کرد که $M \leq 2$.

مقدمه را با ذکر مختصری از چند مسئلهٔ مهم حل نشده درباب اعداد اول خاتمه می‌دهیم.

۱. (مسئلهٔ گلدباخ). آیا عددزوجی بزرگتر از 2 هست که مجموع دوعدد اول نباشد؟

۲. آیا عدد زوجی بزرگتر از 2 هست که تفاضل دو عدد اول نباشد؟

۳. آیا بی‌نهایت دوقلوی اول وجود دارد؟

۴. آیا بی‌نهایت عدد مرسن اول وجود دارد؛ یعنی، اعداد اولی به شکل $2^p - 1$ که درآن p اول است؟

۵. آیا بی‌نهایت عدد مرسن مرکب وجود دارد؟

۶. آیا بی‌نهایت عدد فرمای اول وجود دارد؛ یعنی، اعداد اولی به‌شکل $2^{2^n} + 1$؟

۷. آیابی‌نهایت عدد فرمای مرکب وجود دارد؟

۸. آیا بی‌نهایت عدد اول به‌شکل $x^2 + 1$، که درآن x صحیح است‌وجود دارد؟ (ثابت شده که بی‌نهایت عدد اول به اشکال $x^2 + y^2$، $x^2 + y^2 + 1$، و $x^2 + y^2 + z^2 + 1$ وجود دارد).

۹. آیا بی‌نهایت عدد اول به‌شکل $x^2 + k$ (به‌ازای k ی مفروض) وجود دارد؟

۱۰. آیا همیشه دست‌کم یک عدد اول بین n^2 و $(n+1)^2$ به‌ازای هر عدد صحیح $n \geq 1$ وجود دارد؟

۱۱. آیا همیشه دست کم یک عدد اول بین n^2 و $n^2 + n$ به‌ازای هر عدد صحیح

1. Rényi 2. A. A. Buhštab 3. A. I. Vinogradov 4. Chen Jing-run

$n > 1$ وجود دارد؟

۱۲ . آیا بی‌نهایت عدد اول که ارقامشان (در پایهٔ 10) همه یک‌اند وجود دارد؟ (دو نمونه عبارت است از 11 و 11,111,111,111,111,111,111,111) .

ریاضیدانان حرفه‌ای مجذوب نظریهٔ اعداد بوده‌اند از آنروکه می‌توان همهٔ سلاحهای ریاضیات جدید را به‌سوی مسائل آن نشانه رفت . درواقع ، بسیاری از شاخه‌های مهم ریاضیات ریشه در نظریهٔ اعداد دارند . مثلا" ، تلاشهای اولیه در اثبات قضیهٔ اعداد اول موجب پیدایش نظریهٔ توابع مختلط، بویژه نظریهٔ توابع تمام ، شدند . تلاش برای اثبات اینکه معادلهٔ دیوفانتینی $x^n + y^n = z^n$ به‌ازای $n \geq 3$ جواب نابدیهی ندارد (حدس فرما) به‌پیدایش نظریهٔ جبری اعداد منجر شد ،که یکی از فعالترین زمینهٔ تحقیق در ریاضیات جدید است . با اینکه حدس فرما هنوز بلاتکلیف است ، این حدس در مقایسه با نتایج بسیار گرانبهای حاصل از کار روی آن بی‌اهمیت است . مثال دیگر نظریهٔ افرازها است که در بسط آنالیز ترکیباتی و در مطالعهٔ توابع هنگی عامل مهمی بوده است .

در نظریهٔ اعداد صدها مسئله وجود دارند که حل نشده‌اند . سرعت پیدایش مسائل جدید از حل مسائل قدیم بیشتر است ، و بسیاری از مسائل قدیم قرنهاست بی‌حل مانده‌اند . همانطور که سیرپینسکی [1] ریاضیدان زمانی گفت : " . . . زیادی معرفت ما از اعداد بخاطر آنچه از آنها می‌دانیم نیست ، بلکه بخاطر درک آنچه هنوز از آنها نمی‌دانیم نیز می‌باشد . "

تذکر. هر دانشجوی جدی نظریهٔ اعداد باید با سه جلد کتاب دیکسون [2] (*History of the Theory of Numbers* [13]) ، و شش جلد کتاب لووک [3] (*Reviews in Number Theory* [45]) آشنا باشد . کتاب تاریخ دیکسون شرح دایره‌المعارف گونه‌ای است از آثار مربوط به نظریهٔ اعداد تا ۱۹۱۸ . کتابهای لووک مرور مطالبی است از مجلدهای ۱ تا ۴۴ (۱۹۷۲ — ۱۹۴۰) *Mathematical Reviews* که معمولا" بخشی از نظریهٔ اعداد محسوب می‌شوند . این دو گردآیهٔ با ارزش تاریخ همهٔ کشفیات مهم در نظریهٔ اعداد از دوران قدیم تا ۱۹۷۲ را بدست می‌دهند .

---

1. Sierpinski 2. Dickson 3. LeVeque

۱ قضیهٔ اساسی حساب

۱۰۱ مقدمه

در این فصل مفاهیم اساسی نظریهٔ مقدماتی اعداد نظیر بخشپذیری ، بزرگترین مقسوم علیه مشترک ، واعداد اول و اعداد مرکب معرفی می شوند . نتایج عمده عبارتند از قضیهٔ ۲۰۱ ، که وجود بزرگترین مقسوم علیه مشترک هر دو عدد صحیح را ثابت می‌کند ، و قضیهٔ ۱۰۰۱ (قضیهٔ اساسی حساب) ، که نشان می دهد هر عدد صحیح بزرگتر از 1 را می‌توان (صرف‌نظر از ترتیب عـوامل) فقط به یک طریق به صورت حاصل ضرب عواملی اول نمایش داد . در بسیاری از برهانها از خاصیت زیر از اعداد صحیح استفاده می شود .

اصل استقرا . *هرگاه Q مجموعه‌ای از اعداد صحیح باشد بطوری که*

(آ) $1 \in Q$ ،

(ب) $n \in Q$ *ایجاب کند که* $n+1 \in Q$ ،

آنگاه

(پ) *هر* $s \geq 1$ *متعلق به* Q *خواهد بود .*

البته ،این اصل به صور دیگر نیز تنظیم شده است . مثلا" ، در عبارت (آ) ، عدد صحیح 1 را می‌توان بـا هـر عدد صحیح k عوض کرد ، مشروط براینکه نامساوی ≥ 1 در (پ) با $\geq k$ عوض‌شود . همچنین ، (ب) را می‌توان با عبارت " $1, 2, 3, \ldots, n \in Q$ ایجاب می‌کند که $(n+1) \in Q$ " عوض کرد .

فرض می‌کنیم خواننده با این اصل و نحوهٔ بکارگیری آن در اثبات قضایا به استقرا آشنا باشد . همچنین ، فرض می‌کنیم با اصل زیر ، که با اصل استقرا معادل منطقی است ، آشنا باشد .

اصل خوش ترتیبی. *هرگاه A یک مجموعهٔ ناتهی از اعداد صحیح مثبت باشد، A شامل کوچکترین عضو است.*

ایـن اصل نیـز دارای صورتهای معادلی می‌باشد. مثلاً "، "اعداد صحیح مثبت" را می‌توان با "اعداد صحیح ناکمتر از k به‌ازای k ای"عوض کرد.

۱٫۲ بخشپذیری

نمادگذاری. دراین فصل، حروف کوچک لاتینی a ، b ، c ، d ، n ، و غیره نمایش اعداد صحیح‌اند؛ آنها می‌توانند مثبت، منفی، یا صفر باشند.

تعریف بخشپذیری. گوییم d ، n را **عاد می‌کند** و می‌نویسیم $d|n$ در صورتی که، به ازای c ای، $n = cd$. همچنین، گوییم n یک مضرب d است، d یک مقسوم علیه n است، یا d یک عامل n می‌باشد. اگر d ، n را عاد نکند، می‌نویسیم $d \nmid n$.

بخشپذیری بین هر دو عدد صحیح رابطه‌ای برقرار می‌کند با خواص مقدماتی زیر که اثباتشان بـه‌عنوان تمـرین به خواننده محول می‌شود. (حروف a, b, d, m, n در قضیهٔ ۱٫۱ نمایش اعداد صحیح دلخواهند مگر آنکه خلافش تصریح شود.)

قضیهٔ ۱٫۱ . *بخشپذیری از خواص زیر برخوردار است:*

(آ) $n|n$ *(خاصیت انعکاسی)*؛

(ب) $d|n$ و $n|m$ *ایجاب می‌کنند که* $d|m$ *(خاصیت تعدی)*؛

(پ) $d|n$ و $d|m$ *ایجاب می‌کنند که* $d|(an + bm)$ *(خاصیت خطی)*؛

(ت) $d|n$ *ایجاب می‌کند که* $ad|an$ *(خاصیت ضرب)*؛

(ث) $ad|an$ و $a \neq 0$ *ایجاب می‌کنندکه* $d|n$ *(قانون حذف)*؛

(ج) $1|n$ *(1 هر عدد صحیح را عاد می‌کند)*؛

(چ) $n|0$ *(هر عدد صحیح صفر را عاد می‌کند)*؛

(ح) $0|n$ *ایجاب می‌کند که* $n = 0$ *(صفر فقط صفر را عاد می‌کند)*؛

(خ) $d|n$ و $n \neq 0$ *ایجاب می‌کنند که* $|d| \leq |n|$ *(خاصیت مقایسه‌ای)*؛

(د) $d|n$ و $n|d$ *ایجاب می‌کنند که* $|d| = |n|$ ؛

(ذ) $d|n$ و $d \neq 0$ *ایجاب می‌کنند که* $(n/d)|n$.

تذکر. اگر $d|n$ ، n/d مقسوم علیه مزدوج d نام دارد .

۳۰۱ بزرگترین مقسوم علیه مشترک

اگر d دو عدد صحیح a و b را عـاد کنـد ، d یک **مقسوم علیـه مشترک** a و b نامیده می‌شود . مثـلا" ، 1 مقسوم علیه مشترک هر جفت عدد صحیح مانند a و b است . حال ثابت می‌کنیم هرجفت عدد صحیح a و b دارای یک مقسوم علیه مشترک است که می‌توان آن را به صورت ترکیبی خطی از a و b نمایش داد .

قضیهٔ ۲۰۱ . ***هر دو عدد صحیح a و b مقسوم علیه مشترکی مانند d به شکل***

$$d = ax + by$$

دارند ، که در آن x و y اعدادی صحیح می‌باشند . بعلاوه ، هر مقسوم علیه مشترک a و b این d را عاد می‌کند .

برهان . ابتدا فرض می‌کنیم $a \geq 0$ و $b \geq 0$. به‌استقرا روی n ، که $n = a + b$ ، عمل می‌کنیم . هرگاه $n = 0$ ، آنگاه $a = b = 0$ و می‌توان $d = 0$ را با $x = y = 0$ اختیار کرد . پس فرض کنیم قضیه برای $0, 1, 2, \ldots, n - 1$ ثابت شده باشد . بنابر تقارن ، می‌توان فرض کرد $a \geq b$. اگر $b = 0$ ، اختیار می‌کنیم $d = a, x = 1, y = 0$. اگر $b \geq 1$ ، قضیه را درمورد $a - b$ و b بکار می‌بریم . چون $(a - b) + b = a = n - b \leq n - 1$ ، فرض استقـرا قـابل بکار بـردن است و مقسوم علیه مشترک d از $a - b$ و b به شکـل $d = (a - b)x + by$ وجود دارد . این d ، $(a - b) + b = a$ را نیـز عاد می‌کند ؛ درنتیجه ، d یک مقسوم علیه مشترک a و b است و داریم $d = ax + (y - x)b$ ، که یک ترکیب خطی a و b است . برای تکمیل برهان ، باید نشان دهیم که هر مقسوم علیه مشترک d را عاد می‌کند . اما یک مقسوم علیه مشترک a و b ، و درنتیجه ، بنابر خاصیت خطی ، d را عاد می‌نماید .

اگر $a < 0$ یا $b < 0$ (یاهردو) ، می‌توان نتیجهٔ فوق را درمورد $|a|$ و $|b|$ بکار برد . پس مقسوم علیه مشترکی مانند d از $|a|$ و $|b|$ به شکل

$$d = |a|x + |b|y$$

وجـــود دارد . اگـــر $a < 0$ ، $|a|x = -ax = a(-x)$. بـهمیـن نحو، اگر $b < 0$ ، $|b|y = b(-y)$. بنابراین، d مجددا" یک ترکیب خطی از a و b خواهد بود .

قضیهٔ ۳۰۱ . به‌ازای‌هردو عدد صحیح a و b ، یک و فقط یک عدد مانند d باخواص زیر وجود دارد :

(آ) $d \geq 0$ (**d نامنفی است)؛**

(ب) $d|a$ و $d|b$ (**d یک مقسوم علیه مشترک a و b است)؛**

(پ) $e|a$ و $e|b$ **ایجاب می‌کنندکه** $e|d$ (**هرمقسوم‌علیه مشترک d را عاد می‌کند).**

برهان . بنابرقضیهٔ ۲۰۱ ، دست کم یک d صادق در شرایط (ب) و (پ) وجود دارد . همچنین، $-d$ نیز دراین شرایط صدق می‌کند . اما، اگر d' در (ب) و (پ) صدق کند، $d|d'$ و $d'|d$ ؛ در نتیجه، $|d| = |d'|$. بنابراین، دقیقا" یک $d \geq 0$ وجود دارد که در (ب) و (پ) صدق می‌کند .

تذکر . در قضیهٔ ۳۰۱، $d = 0$ اگر و فقط اگر $a = b = 0$. درغیر این‌صورت، $d \geq 1$.

تعریف . عدد d در قضیهٔ ۳۰۱ **بزرگترین مقسوم‌علیه مشترک** (بمعم) a و b نامیده وبا (a, b) یا aDb نموده مـی‌شود . هرگاه $(a, b) = 1$ ، گوییم a و b **نسبت بهم اول** می‌باشند .

نماد aDb از تعبیربمعم به عنوان عملی بر a و b ناشی می‌شود . اما، متداولترین نماد (a, b) است و ، باآنکه در قضیهٔ بعدی از نماد aDb برای تاکیدبرخواص جبری عمل D استفاده شده، مورد قبول ما می‌باشد .

قضیهٔ ۴۰۱ . بمعم از خواص زیر برخوردار است :

(آ) $(a, b) = (b, a)$

$aDb = bDa$ **(قانون تعویضپذیری)؛**

(ب) $(a, (b, c)) = ((a, b), c)$

$aD(bDc) = (aDb)Dc$ **(قانون شرکتپذیری)؛**

(پ) $(ac, bc) = |c|(a, b)$

$(ca)D(cb) = |c|(aDb)$ **(قانون پخشپذیری)؛**

(ت) $(a, 1) = (1, a) = 1, \quad (a, 0) = (0, a) = |a|.$
$$aD1 = 1Da = 1, \quad aD0 = 0Da = |a|.$$

برهان. ما فقط (پ) را ثابت می‌کنیم. اثبات سایر احکام به‌عنوان تمرین به خواننده واگذار می‌شود.

فرض‌کنیم $d = (a, b)$ و $e = (ac, bc)$. می‌خواهیم ثابت کنیم $e = |c|d$. می‌نویسیم $d = ax + by$. دراین صورت، داریم

$$cd = acx + bcy. \tag{1}$$

بنابراین، $cd|e$، زیرا cd هم ac وهم bc را عاد می‌کند. همچنین، معادلهٔ (۱) نشان می‌دهد که $e|cd$، زیرا $e|ac$ و $e|bc$. بنابراین، $|e| = |cd|$، یا $e = |c|d$.

قضیهٔ ۵.۱ (لم اقلیدس). هرگاه $a|bc$ و $(a, b) = 1$، آنگاه $a|c$.

برهان. چون $(a, b) = 1$، می‌توان نوشت $1 = ax + by$. لذا، $c = acx + bcy$. اما $a|acx$ و $a|bcy$؛ درنتیجه، $a|c$.

۴.۱ اعداد اول

تعریف. عدد صحیح n را اول نامیم اگر $n > 1$ و تنها مقسوم علیه مثبت آن 1 و n باشند. اگر $n > 1$ و n اول نباشد، n مرکب نامیده می‌شود.

چند مثال. اعداد اول کوچکتر از 100 عبارتند از 2، 3، 5، 7، 11، 13، 17، 19، 23، 29، 31، 37، 41، 43، 47، 53، 59، 61، 67، 71، 73، 79، 83، 89 و 97.

نمادگذاری. اعداد اول معمولاً با p, p', p_i, q, q', q_i نشان داده می‌شوند.

قضیهٔ ۶.۱. *هر عدد صحیح $n > 1$ یا یک عدد اول است یا حاصل ضربی از اعداد اول.*

برهان. از استقرا روی n استفاده می‌کنیم. واضح است که قضیه برای $n = 2$ درست است.

فرض کنیم برای هر عدد صحیح کوچکتر از n درست باشد. دراین صورت، اگر n اول نباشد، دارای مقسوم علیه مثبتی مانند d است که $d \neq 1, d \neq n$. بنابراین، $n = cd$، که درآن $c \neq n$. اما c و d کوچکتر از n و بزرگتر از 1 هستند؛ درنتیجه، هریک از c و d حاصل ضربی از اعداد اول است، بنابراین، n نیز چنین می‌باشد.

قضیهٔ ۷.۱ (اقلیدس). *بی‌نهایت عدد اول وجود دارند.*

برهان اقلیدس. فرض کنیم فقط تعدادی متناهی عدد اول، مثلاً $p_1, p_2, \ldots, p_n$، وجود داشته باشند. قرار می‌دهیم $N = 1 + p_1 p_2 \cdots p_n$. داریم $N > 1$؛ درنتیجه، یا N اول است یا حاصل ضربی از اعداد اول است. البته، N اول نیست، زیرا از هر p_i بزرگتراست. بعلاوه، هیچ p_i ی N را عاد نمی‌کند (هرگاه $p_i | N$، آنگاه p_i تفاضل $N - p_1 p_2 \cdots p_n = 1$ را عاد می‌کند). این با قضیهٔ ۶.۱ متناقض می‌باشد.

قضیهٔ ۸.۱. *هرگاه عدد اول p، a را عاد نکند، آنگاه $(p, a) = 1$.*

برهان. فرض‌کنیم $d = (p, a)$. پس $d | p$؛ درنتیجه، $d = 1$ یا $d = p$. اما $d | a$؛ درنتیجه، $d \neq p$ زیرا $p \nmid a$. بنابراین، $d = 1$.

قضیهٔ ۹.۱. *هرگاه عدد اول p، ab را عاد کند، آنگاه $p | a$ یا $p | b$. بطور کلی، هرگاه عدد اول p حاصل ضرب $a_1 \ldots a_n$ را عاد کند، آنگاه p دست کم یکی از عاملها را عاد می‌نماید.*

برهان. فرض‌کنیم $p | ab$ و $p \nmid a$. ثابت می‌کنیم $p | b$. بنابرقضیهٔ ۸.۱، $(p, a) = 1$؛ درنتیجه، طبق لم اقلیدس، $p | b$.

برای اثبات حکم کلی، از استقرا روی n، یعنی تعداد عاملها، استفاده می‌کنیم. جزئیات کار به خواننده محول می‌شود.

۵.۱ قضیهٔ اساسی حساب

قضیهٔ ۱۰.۱ (قضیهٔ اساسی حساب). *هر عدد صحیح $n > 1$ را می‌توان (صرف نظر از*

ترتیب عوامل) فقط به یک طریق به‌صورت حاصل ضربی از عوامل اول نمایش داد.

برهان. از استقــرا روی n استفاده می‌کنیم. قضیه برای $n = 2$ درست است. پس فرض کنیم برای هــر عدد صحیح بزرگتر از 1 و کوچکتر از n درست‌باشد. ثابت می‌کنیم قضیه برای n نیزدرست می‌باشد. اگر n اول باشد، چیزی برای اثبات وجود ندارد. پس فرض کنیم n مرکب بوده و n دو تجزیه، مثلاً

$$n = p_1p_2\cdots p_s = q_1q_2\cdots q_t \tag{۲}$$

داشته باشد. می‌خواهیم نشان دهیم $s = t$ و هر p مساوی q ای است. چون p_1 حاصل ضرب $q_1q_2\cdots q_t$ را عاد می‌کند، باید دست کم یکی از عاملها را عاد کند. $q_1, q_2, \ldots, q_t$ را طوری اندیسگذاری می‌کنیم که $p_1|q_1$. دراین صورت، $p_1 = q_1$، زیرا p_1 و q_1 هردو اولند. در (۲) می‌توان با حذف p_1 از طرفین بدست آورد

$$n/p_1 = p_2\cdots p_s = q_2\cdots q_t.$$

هرگاه $s > 1$ یا $t > 1$، آنگاه $1 < n/p_1 < n$. پس، بنا بــه فرض استقرا، دو تجزیهٔ n/p_1، صرف‌نظر از تــرتیب عوامل، باید یکی باشند. بنابراین، $s = t$ و تجزیه‌های (۲) نیز، صرف نظر از ترتیب، یکی می‌باشند. این برهان را تمام خواهد کرد.

تذکر. درتجزیهٔ عدد صحیح n، عدد اول خاص p ممکن است بیش از یکبار بیاید. هرگاه عوامل اول متمایز n، $p_1, \ldots, p_r$ بوده و p_i به عنوان یک عامل a_i بار بیاید، می‌توانیم بنویسیم

$$n = p_1^{a_1}\cdots p_r^{a_r}$$

یا، مختصرتر،

$$n = \prod_{i=1}^{r} p_i^{a_i}.$$

این را تجزیهٔ n به عوامل اول می‌نــامند. همچنین، می‌توان 1 را با اختیار هر نمای a_i مساوی 0 به این صورت بیان کرد.

قضیهٔ ۱۱.۱. *هرگاه $n = \prod_{i=1}^{r} p_i^{a_i}$، مجموعهٔ مقســوم علیه‌های مثبت n مجموعهٔ اعدادی است به شکل $\prod_{i=1}^{r} p_i^{c_i}$، که در آن، به‌ازای $i = 1, 2, \ldots, r$، $0 \le c_i \le a_i$.*

برهان. تمرین.

تذکر. اگر اعداد اول را به ترتیب صعودی اندیسگذاری کنیم، مثلاً

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \ldots, \quad p_n = n\text{امین عدد اول}$$

هر عدد صحیح و مثبت n (به انضمام 1) را می‌توان به شکل

$$n = \prod_{i=1}^{\infty} p_i^{a_i}$$

بیان کرد ، که درآن هر نمای a_i نامنفی می‌باشد . مقسوم علیه‌های مثبت n همه اعداد ی به شکل

$$\prod_{i=1}^{\infty} p_i^{c_i}$$

هستند که درآن $0 \leq c_i \leq a_i$. حاصل ضربها ، البته ، **متناهی** می‌باشند .

قضیهٔ ۱۲۰۱ . هرگاه دو عدد صحیح و مثبت a و b دارای تجزیه‌های

$$a = \prod_{i=1}^{\infty} p_i^{a_i}, \qquad b = \prod_{i=1}^{\infty} p_i^{b_i}$$

باشند ، آنگاه بمعم آنها تجزیهٔ

$$(a, b) = \prod_{i=1}^{\infty} p_i^{c_i}$$

را دارد ، که درآن هر c_i مساوی $\min\{a_i, b_i\}$ ، یعنی کوچکترین a_i و b_i ، است .

برهان . فرض کنیم $d = \prod_{i=1}^{\infty} p_i^{c_i}$. چون $c_i \leq a_i$ و $c_i \leq b_i$ ، داریم $d|a$ و $d|b$ ؛ درنتیجه ، d یک مقسوم علیه مشترک a و b است . فرض‌کنیم e یک مقسوم علیه مشترک a و b بوده ، و می‌نویسیم $e = \prod_{i=1}^{\infty} p_i^{e_i}$. دراین صورت ، $e_i \leq a_i$ و $e_i \leq b_i$. درنتیجه ، $e_i \leq c_i$. بنابراین ، $e|d$ ؛ درنتیجه ، d بمعم a و b می‌باشد .

۶۰۱ سری متقابلهای اعداد اول

قضیهٔ ۱۳۰۱ . سری نامتناهی $\sum_{n=1}^{\infty} 1/p_n$ واگراست .

برهان . برهان‌کوتاه زیر از این قضیه از آن کلارکسون[1] [۱۱] است . فرض می‌کنیم سری

---

1. Clarkson

همگرا باشد و تناقضی بدست می‌آوریم . اگر سری همگرا باشد ، عدد صحیحی چون k هست بطوری که

$$\sum_{m=k+1}^{\infty} \frac{1}{p_m} < \frac{1}{2}.$$

فرض کنیم $Q = p_1 \cdots p_k$ ، واعداد $1 + nQ$ ، به‌ازای $n = 1, 2, \ldots$ ،رادرنظرمی‌گیریم . هیچیک از اینها بر اعداد اول $p_1, \ldots, p_k$ بخشپذیر نیست . بنابراین ، همهٔ عوامل اول $1 + nQ$ درمیان‌اعداداول $p_{k+1}, p_{k+2}, \ldots$ قرار دارند . بنابراین ،به‌ازای‌هر $r \geq 1$ ، داریم

$$\sum_{n=1}^{r} \frac{1}{1 + nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t,$$

زیرا مجموع طرف راست همهٔ جملات سمت چپ را دربین جملاتش دارد . اما طرف راست این نامساوی تحت تسلط سری هندسی همگرای

$$\sum_{t=1}^{\infty} \left(\frac{1}{2} \right)^t$$

است . بنابراین ، سری $\sum_{n=1}^{\infty} 1/(1 + nQ)$ دارای مجموعهای جزئی کراندار است ، و در نتیجه ، همگرا می‌باشد . اما این یک تناقض است ، زیرا آزمون انتگرال یا آزمون مقایسهٔ حد نشان می‌دهد که این سری واگرا می‌باشد .

تذکر. واگرایی سری $\sum 1/p_n$ ابتدا در ۱۷۳۷ به‌وسیلهٔ اویلر [۲۰] ثابت شد ، و همو بود که دریافت این واگرایی قضیهٔ اقلیدس را در باب وجود بی‌نهایت عدد اول ایجاب می‌کند .

در یکی از فصول آتی یک فرمول مجانبی بدست می‌آوریم نشانگر آنکه مجموعهای جزئی $\sum_{k=1}^{n} 1/p_k$ همانند $\log(\log n)$ به بی‌نهایت میل می‌کنند.

۷.۱ الگوریتم اقلیدس

قضیهٔ ۱۲.۱ ، وقتی تجزیه به عوامل اول a و b معلوم باشند ، یک روش عملی برای محاسبهٔ (a, b) بمعم بدست می‌دهد . اما ممکن است در تجزیه به عوامل اول محاسبات زیادی لازم باشد ، و روند دیگری لازم است تا به محاسبات کمتری نیاز داشته باشد .

فرایندِمفیدی‌وجود دارد، به‌نام الگوریتم اقلیدس، که محتاج به تجزیهٔ a و b نیست. این فرایند بر تقسیمات متوالی استوار است و در آن از قضیهٔ زیر استفاده می‌شود.

قضیهٔ ۱۴۰۱ *(الگوریتم‌تقسیم)*. ***به‌ازای اعداد صحیح a و b که $b > 0$ جفت منحصر بفردی از اعداد صحیح مانند q و r وجود دارد بطوری که***

$a = bq + r$، ***که درآن*** $0 \leq r < b$.

بعلاوه، $r = 0$ اگر و فقط اگر $b | a$.

تذکر. می‌گوییم q **خارج قسمت** و r **باقیمانده** در تقسیم a به b می‌باشند.

برهان. فرض کنیم S مجموعهٔ اعداد صحیح نامنفی به‌صورت زیر باشد:

$S = \{y : y \geq 0$ ، $y = a - bx$ ، x یک عدد صحیح‌است$\}$.

این یک مجموعهٔ ناتهی از اعداد صحیح نامنفی است؛ درنتیجه، دارای کوچکترین عضو است، مثلاً $a - bq$. قرار می‌دهیم $r = a - bq$. پس $a = bq + r$ و $r \geq 0$. حال نشان می‌دهیم $r < b$. فرض می‌کنیم $r \geq b$. پس $0 \leq r - b < r$. اما $r - b \in S$، زیرا $r - b = a - b(q + 1)$. بنابراین، $r - b$ یک عضو S کوچکتر از کوچکترین عضو، یعنی r، است. این تناقض‌نشان می‌دهد که $r < b$. جفت q, r منحصر بفرد است، زیرا هرگاه جفت دیگری از این نوع، مثلاً q', r'، وجود می‌داشت، آنگاه $bq + r = bq' + r'$؛ درنتیجه، $b(q - q') = r' - r$. بنابراین، $b|(r' - r)$. هرگاه $r' - r \neq 0$، این‌ایجاب‌می‌کند که $b \leq |r - r'|$ که یک تناقض است. بنابراین، $r' = r$ و $q' = q$. بالاخره، واضح است که $r = 0$ اگر و فقط اگر $b|a$.

تذکر. با اینکه قضیهٔ ۱۴۰۱ یک قضیهٔ **وجودی** است، اثباتش‌روشی برای محاسبهٔخارج قسمت q و باقیماندهٔ r بدست می‌دهد. ما از a به قدر کافی مضرب b کم می‌کنیم (یا به a می‌افزاییم) تامعلوم شودکه‌کوچکترین عدد نامنفی به شکل $a - bx$ بدست‌آورده‌ایم.

قضیهٔ ۱۵۰۱ (الگوریتم اقلیدس). ***فرض‌کنیم‌اعداد صحیح و مثبت a و b داده شده باشند، که $b \nmid a$. همچنین، $r_0 = a, r_1 = b$، و الگوریتم‌تقسیم را متوالیاً بکار بریم تا مجموعهٔ باقیمانده‌های $r_2, r_3, \ldots, r_n, r_{n+1}$ بدست آید که بترتیب با روابط زیر تعریف می‌شوند:***

$$\begin{aligned} r_0 &= r_1q_1 + r_2, && 0 < r_2 < r_1,\\ r_1 &= r_2q_2 + r_3, && 0 < r_3 < r_2,\\ &\vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, && 0 < r_n < r_{n-1},\\ r_{n-1} &= r_nq_n + r_{n+1}, && r_{n+1} = 0. \end{aligned}$$

دراین‌صورت ، آخرین باقیماندهٔ ناصفر دراین فرایند (a, b) است ، یعنی بمعم a و b .

برهان. مرحله‌ای وجـود دارد که درآن $r_{n+1} = 0$ ، زیرا r_i نزولی و نامنفی است. آخرین‌رابطه ، یعنی $r_{n-1} = r_nq_n$ ، نشان می‌دهد که $r_n|r_{n-1}$. رابطهٔ ماقبل آخر نشان می‌دهد کـه $r_n|r_{n-2}$. بنابر استقرا ، می‌بینیم کـه r_n هر r_i را عاد می‌کند. بخصوص، $r_n|r_1 = b$ و $r_n|r_0 = a$ ؛ درنتیجـه ، r_n یک مقسوم علیه مشترک a و b است. حال فرض‌کنیم d یک مقسوم علیه مشترک a و b باشد. تعریف r_2 نشان می‌دهد که $d|r_2$. رابطهٔ بعدی‌نشان می‌دهدکه $d|r_3$. بنابراستقرا ، d هر r_i را عاد می‌کند ؛ درنتیجه ، $d|r_n$. بنابراین ، r_n بمعم مطلوب می‌باشد.

۸۰۱ بزرگترین مقسوم علیه مشترک بیش از دو عدد

بزرگترین مقسوم علیه مشترک سه عدد صحیح a, b, c با (a, b, c) نموده و با رابطهٔ

$$(a, b, c) = (a, (b, c))$$

تعریف مـی‌شود. بنابر قضیهٔ ۴۰۱ (ب) ، داریم $(a, (b, c)) = ((a, b), c)$؛ درنتیجه ، بمعم فقط تابع a, b, c بوده و به‌ترتیب نوشتن آنـها بستگی ندارد.

بهمین ترتیب ، بمعم n عدد صحیح $a_1, \ldots, a_n$ به استقرا با رابطهٔ

$$(a_1, \ldots, a_n) = (a_1, (a_2, \ldots, a_n))$$

تعریف می‌شود. این عدد نیز از ترتیب آمدن a_i ها مستقل است.

هرگاه $d = (a_1, \ldots, a_n)$ ، به‌آسانی تحقیق می‌شود که d هر a_i را عاد می‌کند وهر مقسوم علیـه مشترک d را عاد می‌نماید. بعـلاوه ، d ترکیبی خطی از a_i هاست. یعنی ، اعداد صحیحی چون $x_1, \ldots, x_n$ وجود دارند بطوری که

$$(a_1, \ldots, a_n) = a_1x_1 + \cdots + a_nx_n.$$

هرگاه $d = 1$ ، گوییم ایـن اعداد **نسبت بهم اول** اند. مثلاً ، 2 ، 3 ، و 10 نسبت بهم اول می‌باشند.

هرگاه وقتـی $i \neq j$ ، $(a_i, a_j) = 1$ ، گوییم اعداد $a_1, \ldots, a_n$ **دو بدو نسبت بهم**

اول‌اند . هرگاه $a_1, \ldots, a_n$ دوبدو نسبت بهم اول باشند ، آنگاه $(a_1, \ldots, a_n) = 1$. بهرحال ، مثال $(2, 3, 10)$ نشان می‌دهد که عکس آن لزوما" درست نیست .

تمرین برای فصل ۱

دراین تمرینات ، حروف کوچک لاتینی $a, b, c, \ldots, x, y, z$ نمایش اعدادی صحیح‌اند . هر یک از احکام تمرینهای ۱ تا ۶ را ثابت کنید .

۱ . هرگاه $(a, b) = 1$ و $c|a$ و $d|b$ ، آنگاه $(c, d) = 1$.

۲ . هرگاه $(a, b) = (a, c) = 1$ ، آنگاه $(a, bc) = 1$.

۳ . هرگاه $(a, b) = 1$ ، آنگاه به‌ازای هر $n \geq 1, k \geq 1$ ، $(a^n, b^k) = 1$.

۴ . هرگاه $(a, b) = 1$ ، آنگاه $(a + b, a - b)$ مساوی 1 یا 2 است .

۵ . هرگاه $(a, b) = 1$ ، آنگاه $(a + b, a^2 - ab + b^2)$ مساوی 1 یا 3 است .

۶ . هرگاه $(a, b) = 1$ و $d|(a + b)$ ، آنگاه $(a, d) = (b, d) = 1$.

۷ . عدد گویای a/b با خاصیت $(a, b) = 1$ یک **کسر تحویل ناپذیر** نامیده می‌شود . اگر مجموع دوکسرتحویل ناپذیریک عدد صحیح باشد ، مثلا" $(a/b) + (c/d) = n$ ، ثابت کنید که $|b| = |d|$.

۸ . یک عدد صحیح را **فارغ از مربع** گویند اگر بر مربع هیچ‌عدد اول بخشپذیر نباشد . ثابت کنید به‌ازای هر $n \geq 1$ اعداد منحصر بفرد $a > 0$ و $b > 0$ وجود دارند بطوری که $n = a^2b$ ، که درآن b فارغ از مربع است .

۹ . برای هریک از احکام زیر یا برهان بیاورید یا مثال نقض:

(آ) هرگاه $b^2|n$ و $a^2|n$ و $a^2 \leq b^2$ ، آنگاه $a|b$ ؛

(ب) هرگاه b^2 بزرگترین مقسوم علیه مجذور n باشد ، آنگاه $a^2|n$ ایجاب می‌کند که $a|b$.

۱۰ . به‌ازای x و y معلوم ، فرض‌کنید $m = ax + by, n = cx + dy$ ، که درآن $ad - bc = \pm 1$ ، ثابت کنید که $(m, n) = (x, y)$.

۱۱ . ثابت کنید که اگر $n > 1$ ، $n^4 + 4$ مرکب است .

در تمرینهای ۱۲ ، ۱۳ ، و ۱۴ ، a, b, c, m, n نمایش اعداد صحیح مثبت‌اند .

۱۲ . برای هریک از احکام زیر یا برهان بیاورید یا مثال نقض:

(آ) هرگاه $a^n|b^n$ ، آنگاه $a|b$ ؛

(ب) هرگاه $n^n|m^m$ ، آنگاه $n|m$ ؛

(پ) هرگاه $a^n|2b^n$ و $n>1$ ، آنگاه $a|b$.

۱۳ . (آ) ثابت کنید هرگاه $(a, b)=1$ و $(a/b)^m=n$ ، آنگاه $b=1$.

(ب) ثابت کنید هرگاه n توان m م عدد صحیح مثبتی نباشد، آنگاه $n^{1/m}$ گنگ است .

۱۴ . ثابت کنید هرگاه $(a, b)=1$ و $ab=c^n$ ، آنگاه به‌ازای x و y ی $a=x^n$ و $b=y^n$.

[**راهنمایی .** $d=(a, c)$ را درنظر بگیرید .]

۱۵ . ثابت کنید هر $n\geq 12$ مجموع دو عدد مرکب است .

۱۶ . ثابت کنید که اگر 2^n-1 اول باشد ، n اول است .

۱۷ . ثابت کنید که اگر 2^n+1 اول باشد ، n توانی از 2 است .

۱۸ . هرگاه $m\neq n$ ، $(a^{2^m}+1, a^{2^n}+1)$ بمعم را برحسب a حساب کنید . [**راهنمایی .** فرض کنید $A_n=a^{2^n}+1$ و نشان دهید که اگر $m>n$ ، $A_n|(A_m-2)$.]

۱۹ . **دنبالهٔ فیبوناچی**[1] $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$ با فرمول بازگشتی $a_{n+1}=a_n+a_{n-1}$ ، با $a_1=a_2=1$ ، تعریف می‌شود . ثابت کنید به‌ازای هر n ، $(a_n, a_{n+1})=1$.

۲۰ . فرض کنید $d=(826, 1890)$. با استفاده از الگوریتم اقلیدس، d را حساب کنید ، سپس d را به‌صورت ترکیبی خطی از 826 و 1890 بیان دارید .

۲۱ . کوچکترین مضرب مشترک (کمم) دو عدد صحیح a و b با $[a, b]$ یا aMb نموده شده و به صورت زیر تعریف می‌شود :

اگر $a\neq 0$ و $b\neq 0$ ، $[a, b]=|ab|\,(a, b)$ ؛

اگر $a=0$ یا $b=0$ ، $[a, b]=0$.

ثابت کنید کمم از خواص زیر برخوردار است :

(آ) هرگاه $a=\prod_{i=1}^{x} p_i^{a_i}$ و $b=\prod_{i=1}^{x} p_i^{b_i}$ ، آنگاه $[a, b]=\prod_{i=1}^{x} p_i^{c_i}$ ، که درآن $c_i=\max\{a_i, b_i\}$ ؛

(ب) $(aDb)Mc=(aMc)D(bMc)$ ؛

(پ) $(aMb)Dc=(aDc)M(bDc)$.

(D و M نسبت بهم پخشپذیراند) .

۲۲ . ثابت کنید که $(a, b)=(a+b, [a, b])$.

۲۳ . مجموع دو عدد صحیح مثبت 5264 و کوچکترین‌مضرب مشترک آنها 200,340 است. این دو عدد را معین کنید .

---

1. *Fibonacci*.

۲۴ . خاصیت ضربی زیر را در مورد کمم ثابت کنید :

$$(ah, bk) = (a, b)(h, k)\left(\frac{a}{(a, b)}, \frac{k}{(h, k)}\right)\left(\frac{b}{(a, b)}, \frac{h}{(h, k)}\right).$$

بخصوص، این نشان می‌دهد که هر وقت $(a, b) = (h, k) = 1$ ، $(ah, bk) = (a, k)(b, h)$.

هریک از احکام تمرینهای ۲۵ تا ۲۸ را ثابت کنید . تمام اعدادِ صحیح مثبت فرض می‌شوند .

۲۵ . هرگاه $(a, b) = 1$ ، آنگاه $x > 0$ و $y > 0$ ی وجود دارند بطوری که $ax - by = 1$.

۲۶ . هرگاه $(a, b) = 1$ و $x^a = y^b$ ، آنگاه بازای n ی $x = n^b$ و $y = n^a$. [**راهنمایی** . از تمرینهای ۲۵ و ۱۳ استفاده کنید .]

۲۷ . (آ) هرگاه $(a, b) = 1$ ، آنگاه بازای هر $n > ab$ ، x و y مثبتی هستند بطوری که $n = ax + by$.

(ب) هرگاه $(a, b) = 1$ ، آنگاه x و y مثبتی وجود ندارند که $ab = ax + by$.

۲۸ . هرگاه $a > 1$ ، آنگاه $(a^m - 1, a^n - 1) = a^{(m, n)} - 1$.

۲۹ . بازای $n > 0$ معلوم ، فرض کنید S مجموعه‌ای باشد که عنصرهایش اعداد صحیح مثبت نابیشتر از $2n$ اند بطوری که اگر a و b در S بوده و $a \neq b$ ، $a \nmid b$. ماکزیمم اعداد صحیحی که S می‌تواند شامل باشد چیست؟ [**راهنمایی** . S می‌تواند حداکثر یکی از اعداد صحیح $1, 2, 2^2, 2^3, \ldots$ ، حداکثر یکی از اعداد صحیح $3, 3 \cdot 2, 3 \cdot 2^2, \ldots$ ، و غیره را شامل می‌شود .]

۳۰ . هرگاه $n > 1$ ، ثابت کنید مجموع

$$\sum_{k=1}^{n} \frac{1}{k}$$

یک عدد صحیح نیست .

توابع حسابی و ضرب دیریکله ۲

۱۰۲ مقدمه

نظریهٔ اعداد، همچون شاخه‌های بسیار دیگر ریاضیات، اغلب با دنباله‌هایی از اعداد حقیقی یا مختلط سروکار دارد. درنظریهٔ اعداد، این دنباله‌ها را **توابع حسابی** می‌نامند.

تعریف. یک تابع حقیقی یا مختلط تعریف شده بر مجموعهٔ اعداد صحیح مثبت یک ***تابع حسابی*** یا یک ***تابع نظریهٔ اعداد*** نامیده می‌شود.

دراین فصل چند تابع‌حسابی معرفی می‌شوند که در مطالعهٔ خواص بخشپذیری اعداد صحیح و توزیع اعداد اول نقش مهمی دارند. همچنین، ضرب دیریکله مطرح می‌شود که در توضیح روابط‌بین توابع حسابی مختلف یاری دهنده است.

بحث را با دو مثال مهم، یعنی ***تابع موبیوس***[1] $\mu(n)$ و ***تابع کامل اویلر*** $\varphi(n)$، آغاز می‌کنیم.

۲۰۲ تابع موبیوس $\mu(n)$

تعریف. ***تابع موبیوس*** μ به صورت زیر تعریف می‌شود:

$$\mu(1) = 1;$$

هرگاه $n > 1$، می‌نویسیم $n = p_1^{a_1} \cdots p_k^{a_k}$. دراین صورت،

اگر $a_1 = a_2 = \cdots = a_k = 1$، $\mu(n) = (-1)^k$؛

درغیر این‌صورت، $\mu(n) = 0$.

---

1. Möbius

توجه کنید که $\mu(n) = 0$ اگر و فقط اگر n عامل مربعی بزرگتر از 1 داشته باشد. ذیلاً جدول مختصری از مقادیر $\mu(n)$ آمده است.

n:	1	2	3	4	5	6	7	8	9	10
$\mu(n)$:	1	-1	-1	0	-1	1	-1	0	0	1

تابع موبیوس درجاهای مختلفی از نظریهٔ اعداد ظاهر می‌شود. یکی از خواص اساسی آن فرمول بسیار ساده‌ای است برای مجموع مقسوم علیهی $\sum_{d|n} \mu(d)$، که روی مقسوم علیه‌های مثبت n گرفته می‌شود. دراین فرمول، $[x]$ بزرگترین عدد صحیح نابیشتر از x است.

قضیهٔ ۱.۲. هرگاه $n \geq 1$، داریم

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{اگر } n = 1 \\ 0 & \text{اگر } n > 1 \end{cases}$$

برهان. واضح است که اگر $n = 1$، این فرمول برقرار است. پس فرض می‌کنیم $n > 1$ و می‌نویسیم $n = p_1^{a_1} \cdots p_k^{a_k}$. در مجموع $\sum_{d|n} \mu(d)$ جملات ناصفر فقط از $d = 1$ و آن مقسوم علیه‌های n که حاصل ضرب اعداد اول متمایزی هستند ناشی می‌شوند. بنابراین،

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \cdots + \mu(p_k) + \mu(p_1p_2) + \cdots + \mu(p_{k-1}p_k)$$
$$+ \cdots + \mu(p_1p_2\cdots p_k)$$
$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = (1-1)^k = 0.$$

۳.۲ تابع کامل اویلر $\varphi(n)$

تعریف. اگر $n \geq 1$، *کامل اویلر* $\varphi(n)$ مساوی تعداد اعداد صحیح مثبتی تعریف می‌شود که از n بیشتر نبوده و نسبت به n اول می‌باشند؛ بنابراین،

$$\varphi(n) = \sum_{k=1}^{n}{}' \, 1, \qquad (1)$$

که درآن $'$ نشان می‌دهد که مجموع روی k هایی گرفته شده که نسبت به n اول می‌باشند.

ذیلاً جدول مختصری از مقادیر $\varphi(n)$ آمده است:

n:	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$:	1	1	2	2	4	2	6	4	6	4

همانند $\mu(n)$ ، فرمول ساده‌ای برای مجموع مقسوم علیهی $\sum_{d|n}\varphi(d)$ وجود دارد.

قضیهٔ ۲.۲ . *اگر* $n \geq 1$ ، *داریم*

$$\sum_{d|n}\varphi(d) = n \cdot$$

برهان . فرض کنیم S مجموعهٔ $\{1, 2, \ldots, n\}$ باشد. S را به مجموعه‌هایی از هم جدا به‌صورت زیر افراز می‌کنیم: به‌ازای هر مقسوم علیه d از n ، قرار می‌دهیم

$$A(d) = \{k : (k, n) = d, 1 \leq k \leq n\};$$

یعنی، $A(d)$ شامل آن عنصرهایی از S است که بمعم آنها با n مساوی d است. $A(d)$ ها گردآیهٔ ازهم جدایی می‌سازند که اجتماع آن S است. بنابراین، اگر $f(d)$ عدهٔ اعداد صحیح در $A(d)$ باشد، داریم

$$\sum_{d|n} f(d) = n \cdot \qquad (۲)$$

اما $(k, n) = d$ اگر و فقط اگر $(k/d, n/d) = 1$ ، و $0 < k \leq n$ اگر و فقط اگر $0 < k/d \leq n/d$. از اینرو، اگر فرض کنیم $q = k/d$ ، یک تناظر یک به یک بین عناصر موجود در $A(d)$ و اعداد صحیح q صادق در $0 < q \leq n/d$ که $(q, n/d) = 1$ وجود خواهد داشت. تعداد این q ها $\varphi(n/d)$ است. لذا، $f(d) = \varphi(n/d)$ و (۲) به‌صورت زیر در می‌آید:

$$\sum_{d|n}\varphi(n/d) = n.$$

اما این با عبارت $\sum_{d|n}\varphi(d) = n$ معادل است، زیرا وقتی d همهٔ مقسوم علیه‌های n را بگیرد، n/d نیز چنین می‌کند. این برهان را تمام خواهد کرد.

۴.۲ یک رابطه که φ و μ را بهم مربوط می‌کند

تابع کامل اویلر با فرمول زیر به تابع موبیوس مربوط می‌شود:

قضیهٔ ۳.۲ . *اگر* $n \geq 1$ ، *داریم*

$$\varphi(n) = \sum_{d|n}\mu(d)\frac{n}{d}.$$

برهان . مجموع (۱) معرف $\varphi(n)$ را می‌توان به شکل زیر نوشت :

$$\varphi(n) = \sum_{k=1}^{n} \left[\frac{1}{(n,k)}\right],$$

که درآن k همهٔ اعداد صحیح نابیشتر از n را می‌گیرد . حال ، با استفاده از قضیهٔ ۱۰۲ با (n,k) به‌جای n ، خواهیم داشت

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d).$$

به‌ازای مقسوم علیه ثابت d از n ، باید روی تمام k هایی با $1 \le k \le n$ جمعبندی کنیم که مضربی از d اند . هرگاه بنویسیم $k = qd$ ، آنگاه $1 \le k \le n$ اگروفقط اگر $1 \le q \le n/d$. از اینرو ، مجموع اخیر برای $\varphi(n)$ را می‌توان به‌صورت زیر نوشت :

$$\varphi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d) \frac{n}{d}.$$

این قضیه را ثابت خواهد کرد .

۵۰۲ فرمول حاصلضرب برای $\varphi(n)$

مجموع مربوط به $\varphi(n)$ در قضیهٔ ۳۰۲ را می‌توان به‌صورت حاصل ضربی که روی مقسوم علیه‌های اول و متمایز n گرفته شده نیز بیان کرد .

قضیهٔ ۴۰۲ . *اگر* $n \ge 1$ *، داریم*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \qquad (۳)$$

برهان . به‌ازای $n = 1$ ، حاصلضرب تهی است ، زیرا عدد اولی که 1 را عاد کندوجود ندارد . دراین حالت ، به‌حاصل ضرب مقدار 1 داده می‌شود .

پس‌فرض‌کنیم $n > 1$ و $p_1, \ldots, p_r$ مقسوم علیه‌های اول و متمایز n باشند . حاصل‌ضرب را می‌توان به‌صورت زیر نوشت :

$$\prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \qquad (۴)$$

$$= 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \cdots + \frac{(-1)^r}{p_1 p_2 \cdots p_r}.$$

طرف راست، و در جمله‌ای مانند $\sum 1/p_ip_jp_k$ ، فرض است که تمام حاصل ضربهای ممکن $p_ip_jp_k$ از عوامل اول متمایز n سه تا سه تا درنظر گرفته شده است. توجه کنید که هرجملهٔ سمت‌راست (۴) به شکل $\pm 1/d$ است، که درآن d یک مقسوم علیه n است که مساوی 1 یا حاصل ضربی از اعداد اول متمایز می‌باشد. صورت، یعنی ± 1 ، درست مساوی $\mu(d)$ است. چون $\mu(d) = 0$ اگر d برمربع p_i ی بخشپذیرباشد، پس مجموع (۴) درست مساوی

$$\sum_{d|n} \frac{\mu(d)}{d}$$

می‌باشد. این قضیه را ثابت خواهد کرد.

بسیاری از خواص $\varphi(n)$ را می‌توان به‌آسانی از این فرمول حاصل ضرب نتیجه گرفت. بعضی از اینها در قضیهٔ بعد ذکر شده‌اند.

قضیهٔ ۵.۲ . *تابع کامل اویلر دارای خواص زیر است:*

(آ) *به‌ازای هر عدد اول* p *و* $\alpha \geq 1$ ، $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ ؛

(ب) $\varphi(mn) = \varphi(m)\varphi(n)(d/\varphi(d))$ ، *که درآن* $d = (m, n)$ ؛

(پ) *اگر* $(m, n) = 1$ ، $\varphi(mn) = \varphi(m)\varphi(n)$ ؛

(ت) $a|b$ *ایجاب می‌کند که* $\varphi(a)|\varphi(b)$ ؛

(ث) $\varphi(n)$ *به‌ازای* $n \geq 3$ *زوج‌است. بعلاوه، اگر* n *دارای* r *عامل‌اول فرد متمایزباشد،* $2^r|\varphi(n)$.

برهان. قسمت (آ) فوراً با فرض $n = p^\alpha$ در (۳) نتیجه می‌شود. برای‌اثبات قسمت (ب)، می‌نویسیم

$$\frac{\varphi(n)}{n} = \prod_{p|n}\left(1 - \frac{1}{p}\right).$$

حال توجه‌می‌کنیم که‌هر مقسوم علیه اول mn یک مقسوم علیه اول m است یا n ، و آن اعداد اولی که هردوی m و n را عاد می‌کنند (m, n) را نیز عاد می‌کنند. بنابراین،

$$\frac{\varphi(mn)}{mn} = \prod_{p|mn}\left(1 - \frac{1}{p}\right) = \frac{\prod_{p|m}\left(1 - \frac{1}{p}\right)\prod_{p|n}\left(1 - \frac{1}{p}\right)}{\prod_{p|(m,n)}\left(1 - \frac{1}{p}\right)} = \frac{\frac{\varphi(m)}{m}\frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}},$$

که از آن (ب) بدست می‌آید . قسمت (پ) حالت خاصی از (ب) می‌باشد .

حال (ت) را از (ب) بدست می‌آوریم . چون $a|b$ ، داریم $b = ac$ که درآن b $1 \le c \le b$. هرگاه $c = b$ ، آنگاه $a = 1$ و قسمت (ت) خودبخود برقرار است . بنابراین ، فرض می‌کنیم $c < b$. از (ب) داریم

$$\varphi(b) = \varphi(ac) = \varphi(a)\varphi(c)\frac{d}{\varphi(d)} = d\varphi(a)\frac{\varphi(c)}{\varphi(d)}, \qquad (۵)$$

که درآن $d = (a, c)$. حال نتیجه به استقرار روی b حاصل می‌شود . به‌ازای $b = 1$ نتیجه خودبخود حاصل است . پس فرض کنیم (ت) به‌ازای هر عدد صحیح کوچکتر از b برقرار باشد . دراین صورت ، به‌ازای c برقرار است ؛ درنتیجه ، $\varphi(d)|\varphi(c)$ زیرا $d|c$. بنابراین ، طرف راست (۵) مضربی از $\varphi(a)$ است ، به‌این معنی که $\varphi(a)|\varphi(b)$. این (ت) را ثابت خواهد کرد .

حال (ث) را ثابت می‌کنیم . اگر $\alpha \ge 2$ $n = 2^\alpha$ ، قسمت (آ) نشان می‌دهد که $\varphi(n)$ زوج است . اگر n دست کم یک عامل اول فرد داشته باشد ، می‌نویسیم

$$\varphi(n) = n\prod_{p|n}\frac{p-1}{p} = \frac{n}{\prod_{p|n} p}\prod_{p|n}(p-1) = c(n)\prod_{p|n}(p-1),$$

که درآن $c(n)$ یک عدد صحیح است . حاصل ضربی که در $c(n)$ ضرب شده زوج است ؛ درنتیجه ، $\varphi(n)$ زوج می‌باشد . بعلاوه ، هرعدد اول فرد مانند p یک عامل 2 به‌این‌حاصل ضرب می‌دهد ؛ درنتیجه ، اگر n دارای r عامل اول فرد متمایز باشد ، $2^r|\varphi(n)$.

۶.۲ ضرب دیریکله‌ٔ توابع حسابی

در قضیه‌ٔ ۳.۲ ثابت شد که

$$\varphi(n) = \sum_{d|n}\mu(d)\frac{n}{d}.$$

مجموع طرف راست ازآن‌نوع مجموعهایی است که در نظریه‌ٔ اعداد بارها ظاهر می‌شوند . این مجموعها به‌شکل

$$\sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

می‌باشند ، که درآن f و g توابعی حسابی بوده و مطالعه‌ٔ بعضی از خواص مشترک این مجموعها سودمند است . بعدا" می‌بینیم که مجموعهایی از این نوع در نظریه‌ٔ سریهای دیریکله به‌طور طبیعی ظاهر می‌شوند . مفید است که این مجموعها به‌عنوان نوع جدیدی

ازضرب توابع حسابی گرفته شود ، و این دیدگاهی است که ای . تی . بل[1] [۴] در۱۹۱۵ ارائه داده است .

تعریف . هرگاه f و g دوتابع حسابی باشند ، حاصل‌ضرب دیریکله (یا پیچش دیریکله) آنها تابعی حسابی مانند h است که با رابطهٔ

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

تعریف می‌شود .

نمادگذاری . بـرای h می‌نویسیم $f * g$ و بـرای $h(n)$ می‌نویسیم $(f * g)(n)$ ، و علامت N را بـرای تابع حسابی که به‌ازای هر n ، $N(n) = n$ بکار می‌بریم . با این نمادگذاری ، قضیهٔ ۳.۲ را می‌توان به شکل

$$\varphi = \mu * N$$

بیان کرد .

قضیهٔ زیر خواص جبری ضرب دیریکله را توصیف می‌کند .

قضیهٔ ۶.۲ . ضرب دیـریکله تعویضپذیر و شرکتپذیر است . یعنی ، به‌ازای هر سه‌تابع حسابی f, g, k ، داریم

$$f * g = g * f \quad \text{(قانون تعویضپذیری)}$$
$$(f * g) * k = f * (g * k) \quad \text{(قانون شرکتپذیری)}$$

برهان . ابتدا توجه می‌کنیم که تعریف $f * g$ را می‌توان به‌صورت زیر نیز بیان کرد :

$$(f * g)(n) = \sum_{a \cdot b = n} f(a)g(b),$$

که‌درآن a و b روی تمام اعداد صحیح مثبت که حاصل ضربشان n است تغییر می‌کنند . این خودبخود خاصیت تعویضپذیری را آشکار می‌کند .

برای‌اثبات خاصیت شرکتپذیری ، قرار می‌دهیم $A = g * k$ و $f * A = f * (g * k)$.

---

1. E. T. Bell

داریم

$$(f * A)(n) = \sum_{a\cdot d=n} f(a)A(d) = \sum_{a\cdot d=n} f(a) \sum_{b\cdot c=d} g(b)k(c)$$

$$= \sum_{a\cdot b\cdot c=n} f(a)g(b)k(c).$$

بهمین نحـو ، اگر قرار دهیم $B = f * g$ و $B * k$ را درنظر بگیریم ، به‌همان فرمول برای $(B * k)(n)$ می‌رسیم . لذا ، $f * A = B * k$ ، بـدین معنـی که ضرب دیریکله شرکتپذ یر است .

حال برای این ضرب عنصر همانی معرفی می‌کنیم .

تعریف . تابع حسابی I به‌صورت زیر :

$$I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{اگر } n = 1 \text{ ،} \\ 0 & \text{اگر } n > 1 \text{ ،} \end{cases}$$

تابع همانی نامیده می‌شود .

قضیهٔ ۷.۲ . به‌ازای هر f ، داریم $I * f = f * I = f$.

برهان . داریم

$$(f * I)(n) = \sum_{d|n} f(d)I\left(\frac{n}{d}\right) = \sum_{d|n} f(d)\left[\frac{d}{n}\right] = f(n)$$

زیرا که ، اگر $d < n$ ، $[d/n] = 0$.

۷.۲ معکوسهای دیریکله و فرمول انعکاس موبیوس

قضیهٔ ۸.۲ . هرگاه f یک‌تابع حسابی بوده و $f(1) \neq 0$ ، یک تابع حسابی منحصربفرد مانند f^{-1} هست ، به‌نام معکوس دیریکلهٔ f ، بطوری که

$$f * f^{-1} = f^{-1} * f = I.$$

بعلاوه ، f^{-1} از فرمولهای بازگشتی زیر بدست می‌آید :

$$f^{-1}(1) = \frac{1}{f(1)} \text{ ، و به‌ازای } n > 1 \text{ ، } f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) .$$

برهان. با معلوم بودن f ، نشان می‌دهیم که معادلهٔ $(f*f^{-1})(n) = I(n)$ نسبت به مقادیر تابعی $f^{-1}(n)$ جواب منحصر بفرد دارد. به‌ازای $n = 1$ ، باید معادلهٔ

$$(f * f^{-1})(1) = I(1)$$

را حل کنیم، که به معادلهٔ

$$f(1)f^{-1}(1) = 1$$

تقلیل می‌یابد. چون $f(1) \neq 0$ ، یک و فقط یک جواب، یعنی $f^{-1}(1) = 1/f(1)$ ، وجود دارد. حال فرض کنیم مقادیر تابعی $f^{-1}(k)$ به‌ازای $k < n$ به‌طور منحصر بفرد مشخص شده باشند. دراین صورت، باید معادلهٔ $(f * f^{-1})(n) = I(n)$ ، یا

$$\sum_{d|n} f\left(\frac{n}{d}\right)f^{-1}(d) = 0$$

را حل کنیم. این معادله را می‌توان به‌صورت زیر نوشت:

$$f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right)f^{-1}(d) = 0.$$

اگر مقادیر $f^{-1}(d)$ به‌ازای همهٔ مقسوم علیه‌های $d < n$ معلوم باشند، چون $f(1) \neq 0$ ، مقدار بفردی برای $f^{-1}(n)$ ، یعنی

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right)f^{-1}(d),$$

وجود دارد. این امر وجود و یکتایی f^{-1} را به‌استقرا ثابت می‌کند.

تذکر. داریم $(f * g)(1) = f(1)g(1)$. لذا، اگر $f(1) \neq 0$ و $g(1) \neq 0$ ، $(f * g)(1) \neq 0$. این مطلب، همراه با قضایای ۲.۶ ، ۲.۷ ، و ۲.۸ ، به‌ما می‌گوید که، به‌زبان نظریهٔ گروهها، مجموعهٔ تمام توابع حسابی f که $f(1) \neq 0$ نسبت به عمل $*$ یک گروه آبلی تشکیل می‌دهند، که درآن عنصر همانی تابع I می‌باشد. خواننده می‌تواند به‌آسانی تحقیق کند که

اگر $f(1) \neq 0$ و $g(1) \neq 0$ ، $(f * g)^{-1} = f^{-1} * g^{-1}$.

تعریف. *تابع یکهٔ* u یک تابع حسابی است که به‌ازای هر n با $u(n) = 1$ تعریف می‌شود.

قضیهٔ ۱.۲ می‌گوید که $\sum_{d|n} \mu(d) = I(n)$ این با نماد ضرب دیریکله به‌صورت زیر درمی‌آید :

$$\mu * u = I.$$

از اینرو، u و μ معکوسهای دیریکلهٔ یکدیگرند :

$$u = \mu^{-1} \quad \text{و} \quad \mu = u^{-1}.$$

با این خاصیت سادهٔ تابع موبیوس، همراه با خاصیت شرکتپذیری ضرب دیریکله، می‌توان برای قضیهٔ بعد برهان ساده‌ای آورد.

قضیهٔ ۹.۲ . فرمول انعکاس موبیوس. *معادلهٔ*

$$f(n) = \sum_{d|n} g(d) \tag{۶}$$

ایجاب می‌کند که

$$g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right). \tag{۷}$$

بعکس، (۷) رابطهٔ (۶) را نتیجه می‌دهد.

برهان. معادلهٔ (۶) می‌گوید که $f = g * u$. ضرب در μ نتیجه می‌دهد که $f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g$ ، که همان (۷) است. بالعکس، ضرب $f * \mu = g$ در u رابطهٔ (۶) را نتیجه خواهد داد.

فرمول انعکاس موبیوس قبلاً در قالب یک جفت فرمول در قضایای ۲.۲ و ۳.۲ بیان شده است :

$$n = \sum_{d|n} \varphi(d), \qquad \varphi(n) = \sum_{d|n} d\mu\left(\frac{n}{d}\right).$$

۸.۲ تابع منگولد[1] $\Lambda(n)$

حال تابع منگولد Λ را معرفی می‌کنیم، که در توزیع اعداد اول نقشی اساسی عهده‌دار است.

---

1. Mangoldt

تعریف . به‌ازای هر عدد صحیح $n \geq 1$ ، تعریف می‌کنیم

$$\Lambda(n) = \begin{cases} \log p \text{، } n = p^m & \text{اگر به‌ازای عدد اولی چون } p \text{ و عدد صحیحی چون } m \geq 1 \text{ ،} \\ 0 & \text{درغیر این‌صورت ،} \end{cases}$$

ذیلا" جدول مختصری از مقادیر $\Lambda(n)$ آمده است :

n:	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$:	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0

برهان قضیهٔ زیر نشان می‌دهد که‌چطور این تابع از قضیهٔ اساسی حساب به‌طور طبیعی ناشی می‌شود .

قضیهٔ ۱۰۰۲ . *اگر* $n \geq 1$ ، *داریم*

$$\log n = \sum_{d|n} \Lambda(d). \qquad (۸)$$

برهان . قضیه‌درحالت $n = 1$ درست‌است ، زیرا هر دو طرف 0 اند . لذا ، فرض می‌کنیم $n > 1$ و می‌نویسیم

$$n = \prod_{k=1}^{r} p_k^{a_k}.$$

با گرفتن لگاریتم ، داریم

$$\log n = \sum_{k=1}^{r} a_k \log p_k.$$

حال مجموع سمت‌راست (۸) را درنظر می‌گیریم . دراین مجموع ، جملات ناصفر فقط‌ازآن مقسوم‌علیه‌های d می‌آیندکه‌به شکل p_k^m ، به‌ازای $m = 1, 2, \ldots, a_k$ و $k = 1, 2, \ldots, r$ ، می‌باشند . بنابراین ،

$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^{r} a_k \log p_k = \log n,$$

که (۸) را ثابت خواهد کرد .

حال ، با استفاده از انعکاس موبیوس، $\Lambda(n)$ را برحسب لگاریتم بیان می‌کنیم .

قضیهٔ ۱۱۰۲ . *اگر* $n \geq 1$ ، *داریم*

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d.$$

برهان. با معکوس کردن (۸) به‌وسیلهٔ فرمول انعکاس موبیوس، بدست می‌آید که

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d$$

$$= I(n) \log n - \sum_{d|n} \mu(d) \log d.$$

چون به‌ازای هر n ، $I(n) \log n = 0$ ، برهان تمام می‌باشد.

۹.۲ توابع ضربی

قبلاً متذکر شدیم که مجموعهٔ تمام توابع حسابی f که $f(1) \neq 0$ تحت ضرب دیریکله یک‌گروه آبلی تشکیل می‌دهد. دراین بخش زیر گروه مهمی از این گروه، مرکب از توابعی به‌نام **توابع ضربی**، را مورد بحث قرار می‌دهیم.

تعریف. تابع حسابی f را ضربی نامیم اگر متحد صفر نبوده و،

درصورت $(m, n) = 1$ ، $f(mn) = f(m) f(n)$.

تابع ضربی f را *کاملاً* ضربی نامیم اگر

به‌ازای هر m, n نیز داشته باشیم $f(mn) = f(m) f(n)$.

مثال ۱. فرض‌کنیم $f_\alpha(n) = n^\alpha$ ، که درآن α یک عدد حقیقی یا مختلط ثابت است. این تابع کاملاً ضربی است. بخصوص، تابع یکهٔ $u = f_0$ کاملاً ضربی است. تابع f_α را با N^α نشان داده و آن را **تابع توان** می‌نامیم.

مثال ۲. تابع همانی $I(n) = [1/n]$ کاملاً ضربی است.

مثال ۳. تابع موبیوس ضربی است ولی کاملاً ضربی نیست. این مطلب به آسانی از تعریف $\mu(n)$ معلوم می‌شود. دو عدد صحیح نسبت بهم اول m و n را درنظر می‌گیریم. اگر m یا n عاملی به‌صورت مربع یک عدد اول داشته باشد، mn نیز چنین است، و $\mu(mn)$ و $\mu(m)\mu(n)$ هر دو صفرند. اگر هیچیک عامل مربع نداشته باشد، می‌نویسیم $m = p_1 \cdots p_s$

و $n = q_1 \cdots q_t$ که درآنها p_i و q_i اعداد اول متمایزی هستند . دراین صورت ، $\mu(m) = (-1)^s$ ، $\mu(n) = (-1)^t$ ، و $\mu(mn) = (-1)^{s+t} = \mu(m)\mu(n)$ ، این نشان می‌دهد که μ ضربی است . این تابع کاملاً " ضربی نیست ، زیرا $\mu(4) = 0$ ولی $\mu(2)\mu(2) = 1$.

مثال ۴. تابع کامل اویلر $\varphi(n)$ ضربی است . این مطلب قسمت (پ) قضیهٔ ۵.۲ است . این تابع کاملاً " ضربی نیست ، زیرا $\varphi(4) = 2$ حال آنکه $\varphi(2)\varphi(2) = 1$.

مثال ۵. ضرب معمولی fg دو تابع حسابی f و g با فرمول معمولی

$$(fg)(n) = f(n)g(n)$$

تعریف می‌شود . بهمین ترتیب ، خارج قسمت f/g با فرمول زیر تعریف می‌شود :

$$\left(\frac{f}{g}\right)(n) = \frac{f(n)}{g(n)} \quad \text{،} \quad g(n) \neq 0 \text{ اگر}$$

اگر f و g ضربی باشند ، fg و f/g نیز چنین‌اند . اگر f و g کاملاً " ضربی باشند ، fg و f/g نیز چنین می‌باشند .

حال چند خاصیت را که بین همهٔ توابع ضربی مشترکند نتیجه می‌گیریم .

قضیهٔ ۱۲.۲ . *هرگاه f ضربی باشد ، آنگاه $f(1) = 1$.*

برهان. داریم $f(n) = f(1)f(n)$ ، زیرا ، بازای هر n ، $(n, 1) = 1$. چون f متحد صفر نیست ، بازای n ی داریم $f(n) \neq 0$ ؛ درنتیجه ، $f(1) = 1$.

تذکر. چون $\Lambda(1) = 0$ ، تابع منگولد ضربی نیست .

قضیهٔ ۱۳.۲ . *تابع f مفروض است بطوری که $f(1) = 1$. دراین صورت ،*

(آ) f ضربی است اگر و فقط اگر بازای همهٔ p_i های اول و همهٔ اعداد صحیح $a_i \geq 1$ ،

$$f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1^{a_1}) \cdots f(p_r^{a_r});$$

(ب) هرگاه f ضربی باشد ، آنگاه f کاملاً " ضربی است اگر و فقط اگر بازای همهٔ p های اول و همهٔ اعداد صحیح $a \geq 1$ ،

$$f(p^a) = f(p)^a .$$

برهان. اثبات بـه‌آسانی از تعریفها نتیجه می‌شود و به‌عنوان تمرین به خواننده محول می‌گردد.

۱۰.۲ توابع ضربی و ضرب دیریکله

قضیهٔ ۱۴.۲ . *هرگاه f و g ضربی باشند، حاصل‌ضرب دیریکلهٔ آنها $f * g$ نیزچنین است.*

برهان. فرض‌کنیم $h = f * g$ و اعداد صحیح نسبت بهم اول m و n را اختیار می‌کنیم. دراین صورت،

$$h(mn) = \sum_{c|mn} f(c)g\left(\frac{mn}{c}\right).$$

اما هرمقسوم علیه c از mn را می‌توان به‌شکل $c = ab$ نوشت، که درآن $a|m$ و $b|n$. بعلاوه، $(a, b) = 1$ ، $(m/a, n/b) = 1$ ، و تناظر یک به یکی بین مجموعهٔ حاصل ضربهای ab و مقسوم علیه‌های c از mn وجود دارد. بنابراین،

$$h(mn) = \sum_{\substack{a|m \\ b|n}} f(ab)g\left(\frac{mn}{ab}\right) = \sum_{\substack{a|m \\ b|n}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)$$

$$= \sum_{a|m} f(a)g\left(\frac{m}{a}\right) \sum_{b|n} f(b)g\left(\frac{n}{b}\right) = h(m)h(n).$$

این برهان را تمام خواهد کرد.

تذکر. حاصل ضرب دیریکلهٔ دو تابع کاملا" ضربی لازم نیست کاملا" ضربی باشد.

با اصلاح جزئی برهان فوق می‌توان قضیهٔ زیر را ثابت کرد.

قضیهٔ ۱۵.۲ . *هرگاه g و $f * g$ هر دو ضربی باشند، f نیز ضربی می‌باشد.*

برهان. فرض‌می‌کنیم f ضربی نباشد و نتیجه می‌گیریم که $f * g$ نیز ضربی نیست. قرار می‌دهیم $h = f * g$. چون f ضربی نیست، اعداد صحیح مثبتی مانند m و n وجود دارند، که $(m, n) = 1$ ، بطوری که

$$f(mn) \neq f(m)f(n).$$

جفت m و n را طوری‌اختیار می‌کنیم که حاصل ضرب mn کوچکترین مقدار ممکن را داشته باشد.

هرگاه $mn = 1$ ، آنگاه $f(1) \neq f(1)f(1)$ ؛ درنتیجه، $f(1) \neq 1$. چون $h(1) = f(1)g(1) = f(1) \neq 1$ ، این نشان می‌دهد که h ضربی نیست.

هرگاه $mn > 1$ ، به‌ازای هردوعدد صحیح‌ومثبت a و b که $(a, b) = 1$ و $ab < mn$ داریم $f(ab) = f(a)f(b)$. حال مثل برهان قضیهٔ ۱۴۰۲ استدلال می‌کنیم، جز آنکه در مجموع معرف $h(mn)$ جملهٔ نظیر به $a = m, b = n$ را جدا می‌کنیم. دراین صورت، خواهیم داشت

$$h(mn) = \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(ab)g\left(\frac{mn}{ab}\right) + f(mn)g(1) = \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) + f(mn)$$
$$= \sum_{a|m} f(a)g\left(\frac{m}{a}\right)\sum_{b|n} f(b)g\left(\frac{n}{b}\right) - f(m)f(n) + f(mn)$$
$$= h(m)h(n) - f(m)f(n) + f(mn).$$

چون $f(mn) \neq f(m)f(n)$ ، این‌نشان‌می‌دهد که $h(mn) \neq h(m)h(n)$ ؛ درنتیجه، h ضربی نیست. این تناقض برهان را تمام خواهد کرد.

قضیهٔ ۱۶۰۲ . *هرگاه g ضربی نباشد، g^{-1} ، یعنی معکوس دیریکلهٔ آن، نیز چنین است.*

برهان. چون g و $I = g * g^{-1}$ هر دو ضربی‌اند، این مطلب فوراً از قضیهٔ ۱۵۰۲ نتیجه می‌شود. (برای برهان دیگر، ر.ک. تمرین ۳۴۰۲).

تذکر. قضایای ۱۴۰۲ و ۱۶۰۲ با هم نشان می‌دهند که مجموعهٔ توابع ضربی زیر گروهی‌است از گروه تمام توابع حسابی f که $f(1) \neq 0$.

۱۱۰۲ معکوس یک تابع کاملاً ضربی

معکوس دیریکلهٔ یک تابع کاملاً ضربی را می‌توان به‌سادگی مشخص کرد.

قضیهٔ ۱۷۰۲ . *فرض کنیم f ضربی باشد. دراین صورت، f کاملاً ضربی است اگر و*

فقط اگر

$$\text{به‌ازای هر } n \geq 1 \text{ ، } f^{-1}(n) = \mu(n)f(n) \text{ .}$$

برهان . فرض کنیم $g(n) = \mu(n)f(n)$. اگر f کاملا" ضربی باشد ، داریم

$$(g * f)(n) = \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = f(n)\sum_{d|n} \mu(d) = f(n)I(n) = I(n)$$

زیرا $f(1) = 1$ و ، به‌ازای $n > 1$ ، $I(n) = 0$. بنابراین ، $g = f^{-1}$.

بعکس، فرض کنیم $f^{-1}(n) = \mu(n)f(n)$. برای اثبات کاملا" ضربی بودن f کافی است ثابت کنیم به‌ازای توانهای اعداد اول ، $f(p^a) = f(p)^a$. معادلهٔ $f^{-1}(n) = \mu(n)f(n)$ ایجاب می‌کند که

$$\text{به‌ازای هر } n > 1 \text{ ، } \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = 0 \text{ .}$$

لذا ، با فرض $n = p^a$ ، داریم

$$\mu(1)f(1)f(p)^a + \mu(p)f(p)f(p^{a-1}) = 0,$$

که از آن معلوم می‌شود که $f(p^a) = f(p)f(p^{a-1})$. این ایجاب می‌کند که $f(p^a) = f(p)^a$ ؛ درنتیجه ، f کاملا" ضربی می‌باشد .

مثال . معکوس تابع φ اویلر . چون $\varphi = \mu * N$ ، داریم $\varphi^{-1} = \mu^{-1} * N^{-1}$. اما $N^{-1} = \mu N$ ، زیرا N کاملا" ضربی است ؛ درنتیجه ،

$$\varphi^{-1} = \mu^{-1} * \mu N = u * \mu N.$$

بنابراین ،

$$\varphi^{-1}(n) = \sum_{d|n} d\mu(d).$$

قضیهٔ زیر نشان می‌دهد که

$$\varphi^{-1}(n) = \prod_{p|n} (1 - p).$$

قضیهٔ ۲ ・ ۱۸ . ***اگر f ضربی باشد ، داریم***

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n} (1 - f(p)).$$

برهان. فرض کنیم

$$g(n) = \sum_{d|n} \mu(d)f(d).$$

دراین‌صورت، g ضربی‌است؛ درنتیجه، برای تعیین $g(n)$ کافی است $g(p^a)$ محاسبه‌شود. امـا

$$g(p^a) = \sum_{d|p^a} \mu(d)f(d) = \mu(1)f(1) + \mu(p)f(p) = 1 - f(p).$$

بنابراین،

$$g(n) = \prod_{p|n} g(p^a) = \prod_{p|n} (1 - f(p)).$$

۱۲.۲ تابع لیوویل[1] $\lambda(n)$

یک نمونهٔ مهم از توابع کاملاً ضربی تابع لیوویل λ است، که به‌صورت زیر تعریف‌می‌شود:

تعریف. تعریف می‌کنیم $\lambda(1) = 1$؛ و اگر $n = p_1^{a_1} \cdots p_k^{a_k}$، تعریف می‌کنیم

$$\lambda(n) = (-1)^{a_1 + \cdots + a_k}.$$

از این تعریف فوراً معلوم می‌شود که λ کاملاً ضربی است. قضیهٔ زیر مجموع‌مقسوم علیهی λ را توصیف خواهد کرد.

قضیهٔ ۱۹.۲. به‌ازای هر $n \geq 1$، داریم

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{اگر } n \text{ مربع باشد،} \\ 0 & \text{درغیر اینصورت،} \end{cases}$$

همچنین، به‌ازای هر n، $\lambda^{-1}(n) = |\mu(n)|$.

برهان. فرض کنیم $g(n) = \sum_{d|n} \lambda(d)$. g ضربی‌است؛ درنتیجه، برای تعیین $g(n)$ فقط کافی است $g(p^a)$ را به‌ازای توانهای اعداد اول حساب کنیم. داریم

---

1. Liouville

$$g(p^a) = \sum_{d|p^a} \lambda(d) = 1 + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^a)$$

$$= 1 - 1 + 1 - \cdots + (-1)^a = \begin{cases} 0 & \text{اگر } a \text{ فرد باشد،} \\ 1 & \text{اگر } a \text{ زوج باشد،} \end{cases}$$

از اینرو، اگـر $n = \prod_{i=1}^{k} p_i^{a_i}$ ، داریم $g(n) = \prod_{i=1}^{k} g(p_i^{a_i})$. اگر نمای a_i فرد باشد، $g(p_i^{a_i}) = 0$ ؛ درنتیجه $g(n) = 0$ ، اگر همهٔ a_i ها زوج باشند ، بهازای هر i ، $g(p_i^{a_i}) = 1$ و $g(n) = 1$. این نشان می‌دهد که اگر n مربع باشد ، $g(n) = 1$ ؛ و ، درغیر اینصورت ، $g(n) = 0$. همچنین ، $\lambda^{-1}(n) = \mu(n)\lambda(n) = \mu^2(n) = |\mu(n)|$ ،

۱۳۰۲ توابع مقسوم علیهی $\sigma_\alpha(n)$

تعریف . بهازای هر α حقیقی یا مختلط و هر عدد صحیح $n \geq 1$ ، تعریف می‌کنیم

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha;$$

یعنی، مساوی مجموع توانهای α ام مقسوم علیه‌های n .

توابع σ_α که به‌این‌طریق تعریف می‌شوند **توابع مقسوم علیهی** نامیده می‌شوند . این توابع ضربی‌اند ، زیرا $\sigma_\alpha = u * N^\alpha$ ؛ یعنی، مساوی حاصل ضرب دیریکلهٔ دو تابع ضربی .

وقتـی $\alpha = 0$ ، $\sigma_0(n)$ **تعداد** مقسوم علیه‌های n است ؛ این عدد را اغلب با $d(n)$ نشان می‌دهند .

وقتی $\alpha = 1$ ، $\sigma_1(n)$ **مجموع** مقسوم علیه‌های n است ؛ این عدد را اغلب با $\sigma(n)$ نشان می‌دهند .

چون σ_α ضربی است ، داریم

$$\sigma_\alpha(p_1^{a_1} \cdots p_k^{a_k}) = \sigma_\alpha(p_1^{a_1}) \cdots \sigma_\alpha(p_k^{a_k}).$$

برای محاسبهٔ $\sigma_\alpha(p^a)$ توجه می‌کنیم که مقسوم علیه‌های یک توان اول مانند p^a عبارتند از

$$1, p, p^2, \ldots, p^a,$$

درنتیجه ،

$$\sigma_\alpha(p^a) = 1^\alpha + p^\alpha + p^{2\alpha} + \cdots + p^{a\alpha} = \frac{p^{\alpha(a+1)} - 1}{p^\alpha - 1} \quad \text{اگر } \alpha \neq 0 \text{ ،}$$

$$= a + 1 \quad \text{اگر } \alpha = 0 \text{ ،}$$

معکوس دیریکلهٔ σ_α را نیز می‌توان به‌صورت ترکیبی خطی از توانهای α ام مقسوم علیه‌های n بیان کرد .

قضیهٔ ۲۰۰۲ . به‌ازای $n \geq 1$ ، داریم

$$\sigma_\alpha^{-1}(n) = \sum_{d|n} d^\alpha \mu(d)\mu\left(\frac{n}{d}\right).$$

برهان. چون $\sigma_\alpha = N^\alpha * u$ و N^α کاملاً" ضربی است، داریم

$$\sigma_\alpha^{-1} = (\mu N^\alpha) * u^{-1} = (\mu N^\alpha) * \mu.$$

۱۴۰۲ پیچشهای تعمیم یافته

در تمام این بخش، F یک تابع حقیقی یا مختلط است که بر محور حقیقی مثبت $(0, +\infty)$ تعریف شده و به‌ازای $0 < x < 1$ ، $F(x) = 0$. مجموعهایی از نوع

$$\sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right)$$

مکرر درنظریهٔ اعداد ظاهر می‌شوند. دراینجا α یک تابع حسابی است. با این مجموع تابع جدید G بر $(0, +\infty)$ تعریف می‌شود که به‌ازای $0 < x < 1$ نیز صفر است. این G را با $\alpha \circ F$ نشان می‌دهیم. بنابراین،

$$(\alpha \circ F)(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$

اگر به‌ازای هر عدد غیر صحیح x ، $F(x) = 0$ ، تحدید F به اعداد صحیح یک تابع حسابی است و معلوم می‌شود که به‌ازای هر عدد صحیح $m \geq 1$ ،

$$(\alpha \circ F)(m) = (\alpha * F)(m);$$

درنتیجه، عمل $\circ$ را می‌توان تعمیمی از پیچش دیریکلهٔ $*$ دانست.

عمل $\circ$ ، درحالت کلی، نه تعویضپذیر است نه شرکتپذیر. با اینحال، قضیهٔ زیر جانشین مفیدی برای قانون شرکتپذیری است.

قضیهٔ ۲۱۰۲ . خاصیت شرکتپذیری مربوط به $\circ$ و $*$. به‌ازای هر دو تابع حسابی α و β ، داریم

$$\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F. \qquad (۹)$$

برهان. به‌ازای $x > 0$ ، داریم

$$\{\alpha \circ (\beta \circ F)\}(x) = \sum_{n \leq x} \alpha(n) \sum_{m \leq x/n} \beta(m) F\left(\frac{x}{mn}\right) = \sum_{mn \leq x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right)$$

$$= \sum_{k\le x}\left(\sum_{n|k}\alpha(n)\beta\left(\frac{k}{n}\right)\right)F\left(\frac{x}{k}\right) = \sum_{k\le x}(\alpha * \beta)(k)F\left(\frac{x}{k}\right)$$
$$= \{(\alpha * \beta)\circ F\}(x).$$

این برهان را تمام خواهد کرد.

حال توجه می‌کنیم که تابع همانی $I(n)=[1/n]$ برای پیچش دیریکله یک همانی چپ برای عمل $\circ$ است. یعنی، داریم

$$(I\circ F)(x) = \sum_{n\le x}\left[\frac{1}{n}\right]F\left(\frac{x}{n}\right) = F(x).$$

حال، با استفاده از این و خاصیت شرکتپذیری، فرمول انعکاس زیر را ثابت می‌کنیم.

قضیهٔ ۲۲.۲ . فرمول انعکاس تعمیم یافته. *اگر α معکوس دیریکلهٔ α^{-1} داشته باشد، معادلهٔ*

$$G(x) = \sum_{n\le x}\alpha(n)F\left(\frac{x}{n}\right) \qquad (۱۰)$$

ایجاب می‌کند که

$$F(x) = \sum_{n\le x}\alpha^{-1}(n)G\left(\frac{x}{n}\right). \qquad (۱۱)$$

بعکس، معادلهٔ (۱۱) معادلهٔ (۱۰) را نتیجه خواهد داد.

برهان. هرگاه $G=\alpha\circ F$، آنگاه

$$\alpha^{-1}\circ G = \alpha^{-1}\circ(\alpha\circ F) = (\alpha^{-1} * \alpha)\circ F = I\circ F = F.$$

لذا، (۱۰) معادلهٔ (۱۱) را ایجاب می‌کند. عکس این مطلب به روش مشابه ثابت می‌شود.

حالت خاص زیر از اهمیتی ویژه برخوردار است.

قضیهٔ ۲۳.۲ . فرمول انعکاس موبیوس تعمیم یافته. *هرگاه α کاملاً" ضربی باشد،*

اگر و فقط اگر $G(x) = \sum_{n\le x}\alpha(n)F\left(\frac{x}{n}\right)$ ، $F(x) = \sum_{n\le x}\mu(n)\alpha(n)G\left(\frac{x}{n}\right)$.

برهان. دراین‌حالت $\alpha^{-1}(n) = \mu(n)\alpha(n)$.

۱۵.۲ سریهای توانی صوری

درحساب دیفرانسیل و انتگرال، یک سری نامتناهی به‌شکل

$$\sum_{n=0}^{\infty} a(n)x^n = a(0) + a(1)x + a(2)x^2 + \cdots + a(n)x^n + \cdots \qquad (۱۲)$$

یک‌**سری توانی** از x نامیده می‌شود. x و ضرایب $a(n)$ اعدادی حقیقی یا مختلط‌اند. به هرسری توانی یک شعاع همگرایی مانند $r \geq 0$ نظیر می‌شود بطوری که سری به‌طور مطلق همگراست اگر $|x| < r$ و واگراست اگر $|x| > r$. (شعاع r می‌تواند $+\infty$ باشد.)

دراین بخش، به سریهای توانی از دیدگاه دیگری می‌نگریم. آنها را سریهای‌توانی صوری می‌نامیم تا از سریهای توانی معمولی حساب دیفرانسیل وانتگرال متمایز باشند. در نظریهٔ سریهای توانی صوری، به x هیچگاه مقدار عددی نمی‌دهند، و مسائل همگرایی‌یا واگرایی مورد توجه نیستند.

موضوع مورد توجه دنبالهٔ

$$(a(0), a(1), \ldots, a(n), \ldots) \qquad (۱۳)$$

از ضرایب است. آنچه را که با سریهای توانی صوری می‌کنیم می‌شود با دنبالهٔ ضرایب کرد به‌این نحو که گویی یک بردار بی‌نهایت بعدی است با مولفه‌های $a(0), a(1), \ldots$. لیکن، برای اهداف ما، مناسبتر آن است که جملات را به‌صورت ضرایب یک سری توانی مانند (۱۲) نشان دهیم تا مولفه‌های یک بردار مانند (۱۳). علامت x^n برای تعیین موضع ضریب n م $a(n)$ بکار می‌رود. ضریب $a(0)$ **ضریب ثابت** سری نامیده می‌شود.

ما بر سریهای توانی صوری به‌طور جبری عمل می‌کنیم به‌این نحو که گویی سریهای توانی همگرایند. اگر $A(x)$ و $B(x)$ دو سری توانی صوری باشند، مثلاً"

$$A(x) = \sum_{n=0}^{\infty} a(n)x^n \quad \text{و} \quad B(x) = \sum_{n=0}^{\infty} b(n)x^n ،$$

تعریف می‌کنیم:

تساوی: $A(x) = B(x)$ یعنی به‌ازای هر $n \geq 0$ ، $a(n) = b(n)$ ؛

مجموع: $A(x) + B(x) = \sum_{n=0}^{\infty} (a(n) + b(n))x^n$ ؛

حاصل ضرب: $A(x)B(x) = \sum_{n=0}^{\infty} c(n)x^n$ ، که درآن

$$c(n) = \sum_{k=0}^{n} a(k)b(n-k). \tag{۱۴}$$

دنبالهٔ $\{c(n)\}$ معین شده با (۱۴) **حاصل ضرب کشی**[1] دنباله‌های $\{a(n)\}$ و $\{b(n)\}$ نام دارد.

خواننده می‌تواند به‌آسانی تحقیق کند که این دو عمل در قوانین تعویضپذیری و شرکتپذیری صدق می‌کنند، و ضرب نسبت به جمع پخشپذیر است. به زبان جبر مدرن، سریهای توانی صوری یک **حلقه** تشکیل می‌دهند. این حلقه برای جمع یک **عنصر صفر** دارد که با 0 نموده می‌شود:

$$\sum_{n=0}^{\infty} a(n)x^n = 0،\ \text{که درآن به‌ازای هر } n \geq 0 ،\ a(n) = 0\ ؛$$

و برای ضرب یک **عنصر همانی** دارد که با 1 نموده می‌شود:

$$\sum_{n=0}^{\infty} a(n)x^n = 1 ،\ \text{که درآن } a(0) = 1 \text{ و به‌ازای هر } n \geq 1 ،\ a(n) = 0 \ .$$

یک سری توانی صوری یک **چند جمله‌ای صوری** نام‌دارداگر همهٔ ضرایب آن ازمرتبه‌ای به‌بعد 0 باشند.

به‌ازای هرسری توانی صوری $A(x) = \sum_{n=0}^{\infty} a(n)x^n$ با ضریب ثابت $a(0) \neq 0$ ، یک‌سری توانی صوری منحصر بفرد مانند $B(x) = \sum_{n=0}^{\infty} b(n)x^n$ وجود دارد که $A(x)B(x) = 1$. ضرایب آن را می‌توان با حل دستگاه نامتناهی از معادلات

$$\begin{aligned}
&a(0)b(0) = 1\\
&a(0)b(1) + a(1)b(0) = 0,\\
&a(0)b(2) + a(1)b(1) + a(2)b(0) = 0,\\
&\qquad\vdots
\end{aligned}$$

بترتیب نسبت به $b(0), b(1), b(2), \ldots$ تعیین کرد. سری $B(x)$ **معکوس** $A(x)$ نام دارد و با $A(x)^{-1}$ یا $1/A(x)$ نموده می‌شود.

سری خاص

$$A(x) = 1 + \sum_{n=1}^{\infty} a^n x^n$$

یک **سری هندسی** خوانده می‌شود. دراینجا a یک عدد حقیقی یا مختلط دلخواه است.

---

1. *Cauchy*

معکوس آن چندجمله‌ای صوری

$$B(x) = 1 - ax$$

می‌باشد. به‌عبارت دیگر، داریم

$$\frac{1}{1-ax} = 1 + \sum_{n=1}^{\infty} a^n x^n.$$

۱۶.۲ سری بل یک تابع حسابی

ای. تی. بل از سریهای توانی صوری برای بررسی خواص توابع حسابی ضربی استفاده کرد.

تعریف. به‌ازای تابع حسابی f و عدد اول p، سری توانی صوری

$$f_p(x) = \sum_{n=0}^{\infty} f(p^n)x^n$$

را سری بل f به هنگ p می‌نامیم.

سریهای بل خصوصا" وقتی مفیدند که f ضربی باشد.

قضیهٔ ۲۴.۲. قضیهٔ یکتایی. *فرض‌کنیم f و g توابعی ضربی باشند. در این صورت، $f = g$ اگر و فقط اگر*

به‌ازای هر عدد اول p، $f_p(x) = g_p(x)$.

برهان. هرگاه $f = g$، آنگاه به‌ازای هر p و هر $n \geq 0$، $f(p^n) = g(p^n)$؛ درنتیجه، $f_p(x) = g_p(x)$. بعکس، هرگاه به‌ازای هر p، $f_p(x) = g_p(x)$، آنگاه به‌ازای هر $n \geq 0$، $f(p^n) = g(p^n)$. چون f و g ضربی و در تمام توانهای اعداد اول مساوی‌اند، درتمام اعداد صحیح مثبت یکی می‌باشند؛ و درنتیجه، $f = g$.

به‌آسانی می‌توان سری بل را برای بعضی از توابع ضربی که پیشتر دراین فصل ذکر شدند مشخص کرد.

مثال ۱. تابع موبیوس μ. چون $\mu(p) = -1$ و، به‌ازای $n \geq 2$، $\mu(p^n) = 0$، داریم

$$\mu_p(x) = 1 - x.$$

مثال ۲. تابع کامل اویلر φ. چون به‌ازای $n \geq 1$، $\varphi(p^n) = p^n - p^{n-1}$، داریم

$$\varphi_p(x) = 1 + \sum_{n=1}^{\infty}(p^n - p^{n-1})x^n = \sum_{n=0}^{\infty} p^n x^n - x\sum_{n=0}^{\infty} p^n x^n$$

$$= (1-x)\sum_{n=0}^{\infty} p^n x^n = \frac{1-x}{1-px}.$$

مثال ۳. توابع کاملا" ضربی. اگر f کاملا" ضربی باشد، به‌ازای هر $n \geq 0$، $f(p^n) = f(p)^n$؛ درنتیجه، سری بل $f_p(x)$ یک سری هندسی می‌باشد:

$$f_p(x) = \sum_{n=0}^{\infty} f(p)^n x^n = \frac{1}{1-f(p)x}.$$

بخصوص، سریهای بل زیر را برای تابع همانی I، تابع یکهٔ u، تابع توان N^α، و تابع لیوویل λ خواهیم داشت:

$$I_p(x) = 1.$$

$$u_p(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

$$N_p^\alpha(x) = 1 + \sum_{n=1}^{\infty} p^{\alpha n} x^n = \frac{1}{1-p^\alpha x}.$$

$$\lambda_p(x) = \sum_{n=0}^{\infty} (-1)^n x^n = \frac{1}{1+x}.$$

۱۷۰۲ سریهای بل و ضرب دیریکله

قضیهٔ زیر ضرب سریهای بل را به‌ضرب دیریکله مربوط می‌کند.

قضیهٔ ۲۵۰۲. به‌ازای هر دو تابع حسابی f و g، قرار می‌دهیم $h = f * g$. دراین صورت، به‌ازای هر عدد اول p، داریم

$$h_p(x) = f_p(x)g_p(x).$$

برهان. چون مقسوم علیه‌های p^n عبارتند از $1, p, p^2, \ldots, p^n$، داریم

$$h(p^n) = \sum_{d|p^n} f(d)g\left(\frac{p^n}{d}\right) = \sum_{k=0}^{n} f(p^k)g(p^{n-k}).$$

این برهان را تمام می‌کند، زیرا مجموع اخیر حاصل ضرب کشی دنباله‌های $\{f(p^n)\}$ و $\{g(p^n)\}$ است.

مثال ۱. چون $\mu^2(n) = \lambda^{-1}(n)$ ، سری بل μ^2 به هنگ p برابر است با

$$\mu_p^2(x) = \frac{1}{\lambda_p(x)} = 1 + x.$$

مثال ۲. چون $\sigma_\alpha = N^\alpha * u$ ، سری بل σ_α به هنگ p مساوی است با

$$(\sigma_\alpha)_p(x) = N_p^\alpha(x)u_p(x) = \frac{1}{1 - p^\alpha x}\cdot\frac{1}{1 - x} = \frac{1}{1 - \sigma_\alpha(p)x + p^\alpha x^2}.$$

مثال ۳. این مثال نشان می‌دهد که چطور می‌توان از سری بل برای کشف اتحادهای مربوط به توابع حسابی استفاده کرد. فرض کنیم

$$f(n) = 2^{\nu(n)},$$

که درآن $\nu(1) = 0$ و، اگر $n = p_1^{a_1}\cdots p_k^{a_k}$ ، $\nu(n) = k$. f ضربی است و سری بل آن به هنگ p مساوی است با

$$f_p(x) = 1 + \sum_{n=1}^{\infty} 2^{\nu(p^n)}x^n = 1 + \sum_{n=1}^{\infty} 2x^n = 1 + \frac{2x}{1 - x} = \frac{1 + x}{1 - x}.$$

بنابراین،

$$f_p(x) = \mu_p^2(x)u_p(x)$$

که $f = \mu^2 * u$ یا

$$2^{\nu(n)} = \sum_{d|n} \mu^2(d)$$

را ایجاب می‌کند.

۱۸۰۲ مشتقات توابع حسابی

تعریف. به‌ازای هر تابع حسابی f ، مشتق آن f' را تابع حسابیی می‌گیریم که با معادلهٔ زیر تعریف می‌شود:

به‌ازای $n \geq 1$ ، $f'(n) = f(n)\log n$.

چند مثال. چون به‌ازای هر n ، $I(n)\log n = 0$ ، داریم $I' = 0$. و چون به‌ازای هر n ، $u(n) = 1$ ، خواهیم داشت $u'(n) = \log n$. درنتیجه، فرمول $\sum_{d|n} \Lambda(d) = \log n$ را می‌توان به صورت زیر نوشت:

$$\Lambda * u = u'. \tag{۱۵}$$

این مشتق در بسیاری از خواص مشتق معمولی حساب دیفرانسیل و انتگرال مقدماتی سهیم است . مثلا" ، قواعد معمولی برای مشتقگیری از مجموعها و حاصل ضربها ، اگر حاصل ضربها دیریکله باشند ، نیز برقرارند .

قضیهٔ ۲۶.۲ . *اگر f و g توابعی حسابی باشند ، داریم*

(آ) $(f+g)' = f' + g'$ ؛

(ب) $(f*g)' = f'*g + f*g'$ ؛

(پ) $(f^{-1})' = -f'*(f*f)^{-1}$ ، **مشروط بر اینکه** $f(1) \neq 0$.

برهان. اثبات (آ) واضح است . البته ، بنا به فرض، $f+g$ تابعی است که بهازای هر n ، $(f+g)(n) = f(n) + g(n)$.

برای اثبات (ب) ، از اتحاد $\log n = \log d + \log(n/d)$ استفاده کرده مینویسیم

$$\begin{aligned}(f*g)'(n) &= \sum_{d|n} f(d)g\left(\frac{n}{d}\right)\log n \\ &= \sum_{d|n} f(d)\log d\, g\left(\frac{n}{d}\right) + \sum_{d|n} f(d)g\left(\frac{n}{d}\right)\log\left(\frac{n}{d}\right) \\ &= (f'*g)(n) + (f*g')(n).\end{aligned}$$

برای اثبات (پ) ، قسمت (ب) را درمورد فرمول $I' = 0$ بکار میبریم و بخاطر میآوریم که $I = f*f^{-1}$. اینکار نتیجه میدهد که

$$0 = (f*f^{-1})' = f'*f^{-1} + f*(f^{-1})';$$

درنتیجه ،

$$f*(f^{-1})' = -f'*f^{-1}.$$

حال ، با ضرب در f^{-1} ، نتیجه میشود که

$$(f^{-1})' = -(f'*f^{-1})*f^{-1} = -f'*(f^{-1}*f^{-1}).$$

اما $f^{-1}*f^{-1} = (f*f)^{-1}$ ؛ درنتیجه ، (پ) ثابت خواهد شد .

۱۹.۲ اتحاد سلبرگ

با استفاده از مفهوم مشتق میتوان سریعا" فرمولی از سلبرگ را بدست آورد که گاهی به

عنوان نقطهٔ شروع یک برهان مقدماتی قضیهٔ اعداد اول بکار می‌رود .

قضیهٔ ۲۷.۲ . اتحاد سلبرگ. به‌ازای $n \geq 1$ ، داریم

$$\Lambda(n)\log n + \sum_{d|n} \Lambda(d)\Lambda\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)\log^2 \frac{n}{d}.$$

برهان. معادلهٔ (۱۵) می‌گوید که $\Lambda * u = u'$. با مشتقگیری از این معادله نتیجه می‌شود که

$$\Lambda' * u + \Lambda * u' = u''$$

یا، چون $u' = \Lambda * u$ ،

$$\Lambda' * u + \Lambda * (\Lambda * u) = u''$$

حال، با ضرب دو طرف در $\mu = u^{-1}$ ، بدست می‌آوریم که

$$\Lambda' + \Lambda * \Lambda = u'' * \mu,$$

و این اتحاد مطلوب می‌باشد .

تمرین برای فصل ۲

۱ . جمیع اعداد صحیح n را بیابید که

(آ) $\varphi(n) = n/2$ ؛ (ب) $\varphi(n) = \varphi(2n)$ ؛ (پ) $\varphi(n) = 12$.

۲ . برای هریک از احکام زیر یا برهان بیاورید یا مثال نقض:

(آ) هرگاه $(m, n) = 1$ ، آنگاه $(\varphi(m), \varphi(n)) = 1$ ؛

(ب) هرگاه n مرکب باشد، آنگاه $(n, \varphi(n)) > 1$ ؛

(پ) هرگاه اعداد اولی که m و n را عاد می‌کنند یکی باشند ، آنگاه $n\varphi(m) = m\varphi(n)$.

۳ . ثابت کنید که

$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}.$$

۴ . ثابت کنید، به‌ازای هر n که حداکثر 8 عامل اول متمایز داشته باشد ، $\varphi(n) > n/6$.

۵ . تعریف کنید $\nu(1) = 0$ و، به‌ازای $n > 1$ ، $\nu(n)$ را تعداد عوامل اول متمایز n بینگارید . فرض کنید $f = \mu * \nu$ و ثابت کنید $f(n)$ یا 0 است یا 1 .

۶ . ثابت کنید که

$$\sum_{d^2|n} \mu(d) = \mu^2(n)$$

و ، بطور کلی ،

$$\sum_{d^k|n}\mu(d)=\begin{cases}0 & \text{اگر به‌ازای } m>1 \text{ ، } m^k|n \text{ ،}\\ 1 & \text{درغیر این‌صورت ،}\end{cases}$$

مجموع اخیر روی تمام مقسوم علیه‌های مثبت d از n که توان k ام آنها نیز n را عاد می‌کنند گرفته می شود .

۷ . فرض کنید $\mu(p,d)$ مقدارتابع موبیوس در بمعم p و d باشد . ثابت کنید به‌ازای هر عدد اول p داریم

$$\sum_{d|n}\mu(d)\mu(p,d)=\begin{cases}1 & \text{اگر } n=1 \text{ ،}\\ 2 & \text{اگر } a\geq 1 \text{ ، } n=p^a \text{ ،}\\ 0 & \text{درغیر این‌صورت ،}\end{cases}$$

۸ . ثابت کنید که اگر $m\geq 1$ و n بیش از m عامل اول متمایز داشته باشد ،

$$\sum_{d|n}\mu(d)\log^m d=0.$$

[**راهنمایی .** استقرا .]

۹ . هرگاه x حقیقی بوده و $x\geq 1$ ، $\varphi(x,n)$ را تعداد اعداد صحیح مثبت نابیشتر از x که نسبت به n اولند بگیرید . [توجه کنید که $\varphi(n,n)=\varphi(n)$.] ثابت کنید که

$$\varphi(x,n)=\sum_{d|n}\mu(d)\left[\frac{x}{d}\right] \quad \text{و} \quad \sum_{d|n}\varphi\left(\frac{x}{d},\frac{n}{d}\right)=[x].$$

در تمرینهای ۱۰ ، ۱۱ ، و ۱۲ ، $d(n)$ تعداد مقسوم علیه‌های مثبت n است .

۱۰ . ثابت کنید که $\prod_{t|n}t=n^{d(n)/2}$.

۱۱ . ثابت کنید $d(n)$ فرد است اگر و فقط اگر n مربع باشد .

۱۲ . ثابت کنید که $\sum_{t|n}d(t)^3=\left(\sum_{t|n}d(t)\right)^2$.

۱۳ . **شکل حاصل ضربی فرمول انعکاس موبیوس.** هرگاه به‌ازای هر n ، $f(n)>0$ ، $a(n)$ حقیقی باشد ، و $a(1)\neq 0$ ، ثابت کنید

$$g(n)=\prod_{d|n}f(d)^{a(n/d)} \quad \text{اگر و فقط اگر} \quad f(n)=\prod_{d|n}g(d)^{b(n/d)} \text{ ،}$$

که درآن $b=a^{-1}$ ، یعنی مساوی معکوس دیریکله‌ٔ a است .

۱۴ . فرض کنید $f(x)$ به‌ازای هر x گویا در $0\leq x\leq 1$ تعریف شده باشد ، و قرار دهید

$$F(n)=\sum_{k=1}^{n}f\left(\frac{k}{n}\right), \qquad F^*(n)=\sum_{\substack{k=1\\(k,n)=1}}^{n}f\left(\frac{k}{n}\right).$$

(آ) ثابت کنید $F^* = \mu * F$ ، یعنی مساوی حاصل ضرب دیریکلهٔ μ و F .

(ب) با استفاده از (آ) و یا بـه‌وسایل دیگـر ، ثابت کنید $\mu(n)$ مجموع ریشه‌های n م اولیهٔ واحد است :

$$\mu(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} e^{2\pi ik/n}.$$

۱۵ . فرض‌کنید $\varphi_k(n)$ مجموع توانهای k ام اعداد نابیشتر از n و نسبت به n اول باشد . توجه کنید که $\varphi_0(n) = \varphi(n)$. با استفاده از تمرین ۱۴ یا به‌وسایل دیگر ، ثابت کنید که

$$\sum_{d|n} \frac{\varphi_k(d)}{d^k} = \frac{1^k + \cdots + n^k}{n^k}.$$

۱۶ . فرمول تمرین ۱۵ را معکوس کرده ، به‌ازای $n > 1$ ، بدست آورید که

$$\varphi_1(n) = \frac{1}{2} n\varphi(n) \quad و \quad \varphi_2(n) = \frac{1}{3} n^2\varphi(n) + \frac{n}{6}\prod_{p|n}(1-p) \; .$$

فرمول نظیر را برای $\varphi_3(n)$ نتیجه بگیرید .

۱۷ . تابع کامل ژردان[1] J_k تعمیم تابع کامل اویلر است که با

$$J_k(n) = n^k \prod_{p|n}(1 - p^{-k})$$

تعریف می‌شود .

(آ) ثابت کنید که

$$J_k(n) = \sum_{d|n} \mu(d)\left(\frac{n}{d}\right)^k \quad و \quad n^k = \sum_{d|n} J_k(d) \; .$$

(ب) سری بل مربوط‌به J_k را مشخص کنید .

۱۸ . ثابت کنید هر عدد به شکل $2^{a-1}(2^a - 1)$ تام است اگر $2^a - 1$ اول باشد .

۱۹ . ثابت کنید کـه اگر n زوج و تام باشد ، به‌ازای $a \geq 2$ ای $n = 2^{a-1}(2^a - 1)$. معلوم نیست که اعداد تام فرد وجود دارند یا نه . اما می‌دانیم که عدد تام فردی باکمتر از 7 عامل اول وجود ندارد .

۲۰ . فرض‌کنید $P(n)$ حاصل ضرب اعداد صحیح مثبت نابیشتر از n بوده و نسبت به n اول باشند . ثابت کنید که

$$P(n) = n^{\varphi(n)} \prod_{d|n}\left(\frac{d!}{d^d}\right)^{\mu(n/d)}.$$

---

1. Jordan

۲۱ . فرض کنید $f(n) = [\sqrt{n}] - [\sqrt{n-1}]$. ثابت کنید f ضربی است اما کاملا" ضربی نیست .

۲۲ . ثابت کنید که

$$\sigma_1(n) = \sum_{d|n} \varphi(d)\sigma_0\left(\frac{n}{d}\right),$$

و تعمیم مربوط به $\sigma_\alpha(n)$ را بدست آورید . (بیش از یک تعمیم وجود دارد .)

۲۳ . حکم زیر را ثابت کنید یا برای آن مثال نقض بزنید . هرگاه f ضربی باشد ، آنگاه $F(n) = \prod_{d|n} f(d)$ نیز ضربی است .

۲۴ . فرض کنید $A(x)$ و $B(x)$ دو سری توانی صوری باشند . اگر حاصلضرب $A(x)B(x)$ سریها صفر باشد ، ثابت کنید که لااقل یکی از عوامل صفر است . به عبارت دیگر ، حلقهٔ سریهای توانی صوری مقسوم علیه صفر ندارد .

۲۵ . فرض کنید f ضربی باشد . ثابت کنید :

(آ) بهازای هر n فارغ از مربع ، $f^{-1}(n) = \mu(n)f(n)$ ؛

(ب) بهازای هر p اول ، $f^{-1}(p^2) = f(p)^2 - f(p^2)$.

۲۶ . فرض کنید f ضربی باشد . ثابت کنید f کاملا" ضربی است اگر و فقط اگر بهازای هر p اول و هر عدد صحیح $a \geq 2$ ، $f^{-1}(p^a) = 0$.

۲۷ . (آ) هرگاه f کاملا" ضربی باشد ، ثابت کنید بهازای هر دو تابع حسابی g و h ،

$$f \cdot (g * h) = (f \cdot g) * (f \cdot h)$$

که درآن $f \cdot g$ حاصل ضرب معمولی است : $(f \cdot g)(n) = f(n)g(n)$.

(ب) هرگاه f ضربی بوده و رابطهٔ قسمت (آ) بهازای $g = \mu$ و $h = \mu^{-1}$ برقرار باشد ، ثابت کنید f کاملا" ضربی میباشد .

۲۸ . (آ) هرگاه f کاملا" ضربی باشد ، ثابت کنید بهازای هر تابع حسابی g که $g(1) \neq 0$ ،

$$(f \cdot g)^{-1} = f \cdot g^{-1} .$$

(ب) هرگاه f ضربی بوده و رابطهٔ قسمت (آ) بهازای $g = \mu^{-1}$ برقرار باشد ، ثابت کنید f کاملا" ضربی میباشد .

۲۹ . ثابت کنید یک تابع حسابی ضربی مانند g هست که بهازای هر تابع حسابی f

$$\sum_{k=1}^{n} f((k, n)) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

دراینجا (k, n) بمعم n و k است . بااستفاده از این اتحاد ، ثابت کنید که

$$\sum_{k=1}^{n}(k,n)\mu((k,n))=\mu(n).$$

۳۰ . فرض‌کنید f ضربی بوده و g تابع حسابی دلخواهی باشد . همچنین ،
(آ) به‌ازای هر p اول و هر $n \ge 1$ ، $f(p^{n+1})=f(p)f(p^n)-g(p)f(p^{n-1})$.
ثابت کنید به‌ازای هر p اول ، سری بل مربوط به f به شکل

$$f_p(x)=\frac{1}{1-f(p)x+g(p)x^2} \qquad (ب)$$

می‌باشد . بعکس ، ثابت کنید (ب) حکم (آ) را ایجاب می‌کند .

۳۱ . (ادامهٔ تمرین ۳۰) . هرگاه g کاملاً ضربی باشد ، ثابت کنید حکم (آ) تمرین ۳۰ رابطهٔ زیر را ایجاب می‌کند :

$$f(m)f(n)=\sum_{d|(m,n)}g(d)f\left(\frac{mn}{d^2}\right),$$

که در آن مجموع روی مقسوم علیه‌های مثبت (m,n) بمعم گرفته می‌شود .
[**راهنمایی .** ابتدا حالت $m=p^a, n=p^b$ را درنظر بگیرید .]

۳۲ . ثابت کنید که

$$\sigma_\alpha(m)\sigma_\alpha(n)=\sum_{d|(m,n)}d^\alpha\sigma_\alpha\left(\frac{mn}{d^2}\right).$$

۳۳ . ثابت کنید تابع لیوویل از فرمول زیر بدست می‌آید :

$$\lambda(n)=\sum_{d^2|n}\mu\left(\frac{n}{d^2}\right).$$

۳۴ . این تمرین برهان دیگری از قضیهٔ ۲.۱۶ بدست می‌دهد ، که می‌گوید معکوس دیریکلهٔ یک تابع ضربی ضربی است . فرض‌کنید g ضربی بوده و $f=g^{-1}$.
(آ) ثابت کنید هرگاه p اول باشد ، آنگاه به‌ازای $k \ge 1$ داریم

$$f(p^k)=-\sum_{t=1}^{k}g(p^t)f(p^{k-t}).$$

(ب) فرض‌کنید h تابع ضربی منحصر بفردی باشد که با f در توانهای اعداد اول یکی است . نشان دهید که $h*g$ با تابع همانی I در توانهای اول یکی است ، و نتیجه بگیرید که $h*g=I$. این نشان می‌دهد که $f=h$ ؛ درنتیجه ، f ضربی می‌باشد .

۳۵ . هرگاه f و g ضربی بوده و a و b اعداد صحیح مثبتی باشند که $a \ge b$ ، ثابت کنید

تابع h که با

$$h(n) = \sum_{d^a|n} f\left(\frac{n}{d^a}\right) g\left(\frac{n}{d^b}\right)$$

داده می‌شود نیز ضربی می‌باشد. مجموع روی آن مقسوم علیه‌های d از n گرفته‌شده که d^a ، n را عاد می‌کند.

توابع موبیوس از مرتبهٔ k

اگر $k \geq 1$ ، μ_k ، یعنی تابع موبیوس از مرتبهٔ k ، به‌صورت زیر تعریف می‌شود:

$\mu_k(1) = 1,$

$\mu_k(n) = 0$ ، $p^{k+1}|n$ ، p اگر به‌ازای عدد اولی چون

$\mu_k(n) = (-1)^r$ ، $n = p_1^k \cdots p_r^k \prod_{i>r} p_i$ و $0 \leq a_i < k$ اگر

$\mu_k(n) = 1$ ، درغیر این‌صورت

به‌عبارت دیگر، $\mu_k(n)$ درصورتی صفراست که n برتوان $(k+1)$م عدد اولی بخشپذیر باشد؛ در غیر این صورت، $\mu_k(n)$ مساوی 1 است مگرآنکه تجزیه به اعداد اول n شامل توانهای k ام درست r عدد اول متمایز باشد، که دراین صورت $\mu_k(n) = (-1)^r$. توجه کنید که $\mu_1 = \mu$ ، یعنی مساوی تابع موبیوس معمولی است.

خواص توابع μ_k را که در تمرینهای زیر ذکر شده‌اند ثابت کنید.

۳۶. هرگاه $k \geq 1$ ، آنگاه $\mu_k(n^k) = \mu(n)$.

۳۷. هریک از توابع μ_k ضربی است.

۳۸. اگر $k \geq 2$ ، داریم

$$\mu_k(n) = \sum_{d^k|n} \mu_{k-1}\left(\frac{n}{d^k}\right) \mu_{k-1}\left(\frac{n}{d}\right).$$

۳۹. اگر $k \geq 1$ ، داریم

$$|\mu_k(n)| = \sum_{d^{k+1}|n} \mu(d).$$

۴۰. به‌ازای هر عدد اول p ، سری بل مربوط به μ_k با

$$(\mu_k)_p(x) = \frac{1 - 2x^k + x^{k+1}}{1 - x}$$

داده می‌شود.

متوسطهای توابع حسابی ۳

۱.۳ مقدمه

در فصل پیش، چند اتحاد درباب توابع حسابی $\mu(n), \varphi(n), \Lambda(n)$ ، و توابع مقسوم علیهی $\sigma_\alpha(n)$ مطرح شدند. حال به تحقیق در رفتار این توابع و توابع حسابی دیگر $f(n)$ بهازای مقادیر بزرگ n میپردازیم.

برای مثال، $d(n)$ ، یعنی تعداد مقسوم علیههای n را درنظر میگیریم. این تابع مقدار 2 را بینهایت بار (وقتی n اول است) میگیرد، ونیز، وقتی تعداد مقسوم علیههای n زیاد باشد، مقادیر بزرگ دلخواه را خواهدگرفت. بنابراین، مقادیر $d(n)$ ، وقتی n بزرگ میشود، بهطور قابل ملاحظهای بالا و پایین میرود.

بسیاری از توابع حسابی از این نظر وضع ثابتی ندارند و تعیین رفتار آنها بهازای n های بزرگ اغلب مشکل است. گاهی مفیدتر آن است که میانگین حسابی

$$\tilde{f}(n) = \frac{1}{n} \sum_{k=1}^{n} f(k)$$

را بررسی کنیم. متوسطها نوسانات را از بین میبرند طوری که ازمقادیر میانگین $\tilde{f}(n)$ رفتار منظمتری تا $f(n)$ انتظار میرود. این وضع در مورد تابع مقسوم علیهی $d(n)$ مسلم است. بعدها ثابت میکنیم که متوسط $\tilde{d}(n)$ ، بهازای n های بزرگ، مانند $\log n$ رشد میکند؛ بهطور دقیقتر،

$$\lim_{n\to\infty} \frac{\tilde{d}(n)}{\log n} = 1. \qquad (۱)$$

این را اینطور توصیف میکنند که میگویند مرتبهٔ متوسط $d(n)$ مساوی $\log n$ است.

برای بررسی متوسط تابع حسابی f بهنکاتی از مجموعهای جزئی آن $\sum_{k=1}^{n} f(k)$ نیازاست. گاهی شایسته است که اندیس بالایی n با عدد حقیقی مثبت دلخواه x عوض

شده و مجموعهایی به‌شکل

$$\sum_{k \le x} f(k)$$

درنظر گرفته شوند . دراینجا فرض است که اندیس k از 1 تا $[x]$ ، یعنی بزرگترین عدد صحیح نابیشتراز x ، تغییرمی‌کند . اگر $0 < x < 1$ ، مجموع فوق تهی است و به‌آن مقدار 0 را نسبت می‌دهیم . هدف ما تعیین رفتار این مجموع به‌عنوان تابعی از x ، بویژه x های بزرگ ، است .

برای تابع مقسوم علیهی ، نتیجه‌ای را ثابت می‌کنیم که به‌وسیلهٔ دیریکله در ۱۸۴۹ بدست آمد ، که این نتیجه از (۱) قویتر است ؛ یعنی ، ثابت می‌کنیم به‌ازای هر $x \ge 1$ ،

$$\sum_{k \le x} d(k) = x \log x + (2C - 1)x + O(\sqrt{x}) \cdot \qquad (۲)$$

در اینجا C ثابت اویلر است ، که با معادلهٔ زیر تعریف می‌شود :

$$C = \lim_{n \to \infty}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right). \qquad (۳)$$

علامت $O(\sqrt{x})$ نمایش‌تابع نامعلومی از x است ، که از ضریب ثابتی از $\sqrt{x}$ سریعتر رشد نمی‌کند . این نمونه‌ای است از نماد "اوی بزرگ" ، که به‌صورت زیر تعریف می‌شود .

۲.۳ نماد اولی بزرگ . تساوی مجانبی توابع

تعریف . هرگاه به‌ازای هر $x \ge a$ ، $g(x) > 0$ ، می‌نویسیم

$$f(x) = O(g(x)) \qquad (\text{بخوانید : " } f(x) \text{ اوی بزرگ } g(x) \text{ است"})$$

به‌این معنی که خارج قسمت $f(x)/g(x)$ به‌ازای $x \ge a$ کراندار است ؛ یعنی ، ثابتی مانند $M > 0$ هست بطوری که

به‌ازای هر $x \ge a$ ، $|f(x)| \le Mg(x)$.

یک معادله به‌شکل

$$f(x) = h(x) + O(g(x))$$

یعنی $f(x) - h(x) = O(g(x))$. می‌بینیم که به‌ازای $t \ge a$ ، $f(t) = O(g(t))$ نتیجه‌می‌دهد که به‌ازای $x \ge a$ ، $\int_a^x f(t)\,dt = O(\int_a^x g(t)\,dt)$.

تعریف . هرگاه

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$$

می‌گوییم $f(x)$ ، وقتی $x \to \infty$ ، **مجانب** $g(x)$ است ، و می‌نویسیم

$$f(x) \sim g(x) \qquad \text{وقتی } x \to \infty ،$$

مثلاً ، معادلهٔ (۲) ایجاب می‌کند که

$$\sum_{k \le x} d(k) \sim x \log x \qquad \text{وقتی } x \to \infty ،$$

در معادلهٔ (۲) ، جملهٔ $x \log x$ **مقدار مجانبی** مجموع نامیده می‌شود ، دو جملهٔ دیگر خطای ناشی از تقریب مجموع به مقدار مجانبی‌اش را نمایش می‌دهند . اگر این خطا $E(x)$ باشد ، (۲) می‌گوید که

$$E(x) = (2C - 1)x + O(\sqrt{x}). \tag{۴}$$

این رابطه را می‌توان به‌صورت $E(x) = O(x)$ نوشت ، که معادله‌ای است صحیح ولی اطلاعات دقیقتر ناشی از (۴) را بازگو نمی‌کند . معادلهٔ (۴) می‌گوید که مقدار مجانبی $E(x)$ مساوی $(2C - 1)x$ است .

۳.۳ فرمول جمعبندی اویلر

گاهی می‌توان مقدار مجانبی یک مجموع جزئی را از مقایسه‌اش با یک انتگرال بدست‌آورد . یک فرمول جمعبندی از اویلر ، برای خطای حاصل در چنین تقریب عبارت دقیقی بدست می‌دهد . دراین فرمول ، $[t]$ بزرگترین عدد صحیح نابیشتر از t است .

قضیهٔ ۳.۱ . فرمول جمعبندی اویلر. *هرگاه f بر بازهٔ $[y, x]$ ، که $0 < y < x$ ، مشتق پیوسته داشته باشد ، آنگاه*

$$\sum_{y < n \le x} f(n) = \int_y^x f(t)\, dt + \int_y^x (t - [t]) f'(t)\, dt + f(x)([x] - x) - f(y)([y] - y). \tag{۵}$$

برهان . فرض‌کنیم $k = [x]$ ، $m = [y]$. به‌ازای اعداد صحیح n و $n - 1$ در $[y, x]$ ، داریم

$$\int_{n-1}^n [t] f'(t)\, dt = \int_{n-1}^n (n-1) f'(t)\, dt = (n-1)\{f(n) - f(n-1)\}$$
$$= \{nf(n) - (n-1)f(n-1)\} - f(n).$$

با جمعبندی از $n = m + 1$ تا $n = k$ ، خواهیم داشت

$$\int_m^k [t]f'(t)\,dt = \sum_{n=m+1}^{k} \{nf(n) - (n-1)f(n-1)\} - \sum_{y<n\le x} f(n)$$
$$= kf(k) - mf(m) - \sum_{y<n\le x} f(n);$$

لذا ،

$$\sum_{y<n\le x} f(n) = -\int_m^k [t]f'(t)\,dt + kf(k) - mf(m) \tag{۶}$$
$$= -\int_y^x [t]f'(t)\,dt + kf(x) - mf(y).$$

انتگرالگیری به‌طریقهٔ‌جزء به‌جزء نتیجه می‌دهد که

$$\int_y^x f(t)\,dt = xf(x) - yf(y) - \int_y^x tf'(t)\,dt,$$

و ، از تلفیق این با (۶) ، رابطهٔ (۵) بدست می‌آید .

۴.۳ چند فرمول مجانبی مقدماتی

در قضیهٔ زیر چند فرمول مجانبی ذکر شده‌اند که نتایج سادهٔ فرمول جمعبندی اویلر می‌باشند . در قسمت (آ) ، ثابت C ثابت اویلر است که در (۳) تعریف شد . در قسمت (ب) ، $\zeta(s)$ تابع زتای ریمان است که با معادلات زیر تعریف می‌شود :

اگر $s > 1$ ، $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ ؛

اگر $0 < s < 1$ ، $\zeta(s) = \lim_{x\to\infty} \left(\sum_{n\le x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \right)$.

قضیهٔ ۲.۳ . هرگاه $x \ge 1$ ، داریم

(آ) $\sum_{n\le x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$ ؛

(ب) اگر $s > 0, s \ne 1$ ، $\sum_{n\le x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s})$ ؛

(پ) اگر $s > 1$ ، $\sum_{n>x} \frac{1}{n^s} = O(x^{1-s})$ ؛

(ت) اگر $\alpha \geq 0$ ، $\sum_{n\leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha})$.

برهان. در قسمت (آ) ، با فرض $f(t) = 1/t$ در فرمول جمعبندی اویلر داریم

$$\sum_{n\leq x}\frac{1}{n} = \int_1^x \frac{dt}{t} - \int_1^x \frac{t-[t]}{t^2}\,dt + 1 - \frac{x-[x]}{x}$$

$$= \log x - \int_1^x \frac{t-[t]}{t^2}\,dt + 1 + O\left(\frac{1}{x}\right)$$

$$= \log x + 1 - \int_1^{\infty} \frac{t-[t]}{t^2}\,dt + \int_x^{\infty}\frac{t-[t]}{t^2}\,dt + O\left(\frac{1}{x}\right).$$

انتگرال‌مجازی $\int_1^{\infty} (t-[t])t^{-2}\,dt$ وجوددارد،زیراتحت‌تسلط $\int_1^{\infty} t^{-2}\,dt$ است.همچنین ،

$$0 \leq \int_x^{\infty}\frac{t-[t]}{t^2}\,dt \leq \int_x^{\infty}\frac{1}{t^2}\,dt = \frac{1}{x};$$

درنتیجه ، معادلهٔ اخیر به‌صورت زیر درمی‌آید :

$$\sum_{n\leq x}\frac{1}{n} = \log x + 1 - \int_1^{\infty}\frac{t-[t]}{t^2}\,dt + O\left(\frac{1}{x}\right).$$

این (آ) را به‌ازای

$$C = 1 - \int_1^{\infty}\frac{t-[t]}{t^2}\,dt$$

ثابت می‌کند . با فرض $x \to \infty$ در (آ) ، معلوم می‌شود که

$$\lim_{x\to\infty}\left(\sum_{n\leq x}\frac{1}{n} - \log x\right) = 1 - \int_1^{\infty}\frac{t-[t]}{t^2}\,dt;$$

درنتیجه ، C نیز مساوی ثابت اویلر می‌باشد .

برای اثبات قسمت (ب) ، از استدلالی مشابه برای تابع $f(x) = x^{-s}$ ، که درآن $s > 0, s \neq 1$ ، استفاده می‌کنیم . فرمول جمعبندی اویلر نتیجه می‌دهد که

$$\sum_{n\leq x}\frac{1}{n^s} = \int_1^x \frac{dt}{t^s} - s\int_1^x \frac{t-[t]}{t^{s+1}}\,dt + 1 - \frac{x-[x]}{x^s}$$

$$= \frac{x^{1-s}}{1-s} - \frac{1}{1-s} + 1 - s\int_1^x \frac{t-[t]}{t^{s+1}}\,dt + O(x^{-s}).$$

بنابراین ،

$$\sum_{n\le x}\frac{1}{n^s}=\frac{x^{1-s}}{1-s}+C(s)+O(x^{-s}), \tag{۷}$$

که درآن

$$C(s)=1-\frac{1}{1-s}-s\int_1^\infty \frac{t-[t]}{t^{s+1}}\,dt.$$

اگر $s>1$ ، طرف چپ (۷) ، وقتی $x\to\infty$ ، به $\zeta(s)$ ، و جملات x^{1-s} و x^{-s} هر دو به 0 نزدیک می‌شوند. بنابراین، اگر $s>1$ ، $C(s)=\zeta(s)$. اگر $0<s<1$ ، $x^{-s}\to 0$ و (۷) نشان می‌دهد که

$$\lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n^s}-\frac{x^{1-s}}{1-s}\right)=C(s).$$

بنابراین، اگر $0<s<1$ ، $C(s)$ نیزمساوی $\zeta(s)$ است. این (ب) را ثابت خواهد کرد.

برای اثبات (پ) ، اگر از (ب) به‌ازای $s>1$ استفاده کنیم، داریم

$$\sum_{n>x}\frac{1}{n^s}=\zeta(s)-\sum_{n\le x}\frac{1}{n^s}=\frac{x^{1-s}}{s-1}+O(x^{-s})=O(x^{1-s})$$

زیرا $x^{-s}\le x^{1-s}$.

بالاخره، برای اثبات (ت) ، اگر از فرمول جمعبندی اویلر به‌ازای $f(t)=t^\alpha$ استفاده کنیم، خواهیم داشت

$$\begin{aligned}\sum_{n\le x}n^\alpha &= \int_1^x t^\alpha\,dt+\alpha\int_1^x t^{\alpha-1}(t-[t])\,dt+1-(x-[x])x^\alpha\\ &=\frac{x^{\alpha+1}}{\alpha+1}-\frac{1}{\alpha+1}+O\left(\alpha\int_1^x t^{\alpha-1}\,dt\right)+O(x^\alpha)\\ &=\frac{x^{\alpha+1}}{\alpha+1}+O(x^\alpha).\end{aligned}$$

۵.۳ مرتبهٔ متوسط $d(n)$

دراین بخش، فرمول مجانبی دیریکله را برای مجموعهای جزئی تابع مقسوم علیهی $d(n)$ بدست می‌آوریم.

قضیهٔ ۳.۳ . به‌ازای هر $x\ge 1$ ، داریم

$$\sum_{n\le x}d(n)=x\log x+(2C-1)x+O(\sqrt{x}), \tag{۸}$$

که درآن C ثابت اویلر است.

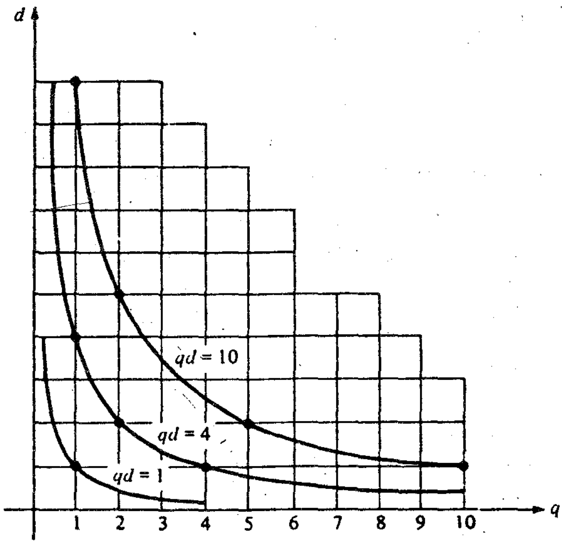
برهان. چون $d(n) = \sum_{d|n} 1$ ، داریم

$$\sum_{n\le x} d(n) = \sum_{n\le x}\sum_{d|n} 1.$$

این یک مجموع مضاعف است که روی n و d گرفته می‌شود. چون $d|n$ ، می‌توان نوشت $n = qd$ و مجموع را روی تمام جفتهای q,d از اعداد صحیح مثبت، که $qd \le x$ ، گرفت. بنابراین،

$$\sum_{n\le x} d(n) = \sum_{\substack{q,d\\ qd\le x}} 1. \qquad (۹)$$

این را می‌توان مجموعی دانست که روی نقاط مشبکهٔ معینی در صفحهٔ **qd** ، به‌صورت شکل ۱۰۳ ، گرفته می‌شود. (یک نقطهٔ مشبکه نقطه‌ای است که مختصاتش اعدادی صحیح‌اند.)



شکل ۱۰۳

نقاط مشبکه که در آنها $qd = n$ روی یک هذلولی واقعند؛ درنتیجه، مجموع (۹) تعداد نقاط مشبکهٔ واقع برهذلولیهای نظیر به $n = 1, 2, \ldots, [x]$ را می‌شمارد. به‌ازای هر $d \le x$ ثابت، می‌توان ابتدا نقاط مشبکهٔ روی پاره خط افقی $1 \le q \le x/d$ را شمرد، و سپس روی تمام $d \le x$ ها جمعبندی کرد. لذا، (۹) به‌صورت زیر درمی‌آید:

$$\sum_{n\le x} d(n) = \sum_{d\le x}\sum_{q\le x/d} 1. \tag{۱۰}$$

حال ، با استفاده از قسمت (ت) در قضیهٔ ۲.۳ به‌ازای $\alpha = 0$ ، داریم

$$\sum_{q\le x/d} 1 = \frac{x}{d} + O(1).$$

با استفاده از این و قضیهٔ ۲.۳ (آ) ، معلوم می‌شود که

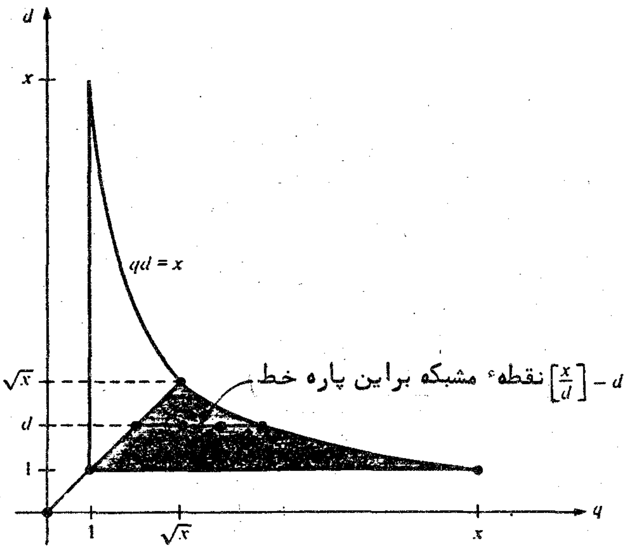
$$\sum_{n\le x} d(n) = \sum_{d\le x}\left\{\frac{x}{d} + O(1)\right\} = x\sum_{d\le x}\frac{1}{d} + O(x)$$
$$= x\left\{\log x + C + O\left(\frac{1}{x}\right)\right\} + O(x) = x\log x + O(x).$$

این صورت ضعیفی است از (۸) ایجابگر آنکه

$$\sum_{n\le x} d(n) \sim x\log x \text{ ، } x\to\infty \text{ وقتی}$$

و $\log n$ را به‌عنوان مرتبهٔ متوسط $d(n)$ بدست می‌دهد .

برای اثبات فرمول دقیقتر (۸) ، به‌مجموع (۹) بازمی‌گردیم ، که تعداد نقاط مشبکهٔ واقع در یک ناحیهٔ هذلولوی را می‌شمارد ، و از تقارن این ناحیه نسبت به خط $q = d$ استفاده می‌کنیم . تعداد کل نقاط مشبکه دراین ناحیه دوبرابر تعداد این نقاط زیر خط $q = d$ بعلاوهٔ تعداد نقاط واقع برپاره خط نیمساز است . با مراجعه به‌شکل ۲.۳ ، ملاحظه



شکل ۲.۳

می‌شود که

$$\sum_{n\le x} d(n) = 2\sum_{d\le\sqrt{x}}\left\{\left[\frac{x}{d}\right] - d\right\} + [\sqrt{x}].$$

حال، با استفاده از رابطهٔ $[y] = y + O(1)$ و قسمتهای (آ) و (ت) قضیهٔ ۲.۳، خواهیم داشت

$$\begin{aligned}\sum_{n\le x} d(n) &= 2\sum_{d\le\sqrt{x}}\left\{\frac{x}{d} - d + O(1)\right\} + O(\sqrt{x})\\ &= 2x\sum_{d\le\sqrt{x}}\frac{1}{d} - 2\sum_{d\le\sqrt{x}} d + O(\sqrt{x})\\ &= 2x\left\{\log\sqrt{x} + C + O\left(\frac{1}{\sqrt{x}}\right)\right\} - 2\left\{\frac{x}{2} + O(\sqrt{x})\right\} + O(\sqrt{x})\\ &= x\log x + (2C-1)x + O(\sqrt{x}).\end{aligned}$$

این برهان فرمول دیریکله را تمام خواهد کرد.

تذکر. جملهٔ خطای $O(\sqrt{x})$ را می‌توان اصلاح کرد. در سال ۱۹۰۳، ورونوا[1] ثابت کرد که خطا $O(x^{1/3}\log x)$ است؛ در ۱۹۲۲ وان درکورپوت[2] آن را تا $O(x^{33/100})$ بهتر کرد. بهترین تخمین تا امروز $O(x^{(12/37)+\varepsilon})$ به‌ازای هر $\varepsilon > 0$ است، که توسط کولسنیک[3] [۳۵] در ۱۹۶۹ بدست آمد. تعیین اینفیمم جمیع θ هایی که جملهٔ خطا $O(x^{\theta})$ باشد مسئلهٔ حل نشده‌ای است که به مسئلهٔ مقسوم علیه دیریکله معروف است. درسال ۱۹۱۵، هاردی[4] و لاندو[5] نشان دادند که $\inf\theta \ge 1/4$.

۶.۳ مرتبهٔ متوسط توابع مقسوم علیهی $\sigma_\alpha(n)$

حالت $\alpha = 0$ در قضیهٔ ۳.۳ درنظر گرفته شد. حال فرض می‌کنیم $\alpha > 0$ حقیقی باشد، و حالت $\alpha = 1$ را جداگانه بررسی می‌کنیم.

قضیهٔ ۴.۳ . به‌ازای هر $x \ge 1$، داریم

$$\sum_{n\le x}\sigma_1(n) = \frac{1}{2}\zeta(2)x^2 + O(x\log x). \qquad (11)$$

---

1. Voronoi 2. van der Corput 3. Kolesnik 4. Hardy 5. Landau

تذکر. می‌توان نشان داد که $\zeta(2) = \pi^2/6$. بنابراین، (۱۱) نشان می‌دهد که مرتبهٔ متوسط $\sigma_1(n)$ مساوی $\pi^2 n/12$ است.

برهان. روش اثبات شبیه روشی است که با آن صورت ضعیف قضیهٔ ۳.۳ بدست آمد. داریم

$$\sum_{n\le x}\sigma_1(n) = \sum_{n\le x}\sum_{q|n} q = \sum_{\substack{q,d\\ qd\le x}} q = \sum_{d\le x}\sum_{q\le x/d} q$$

$$= \sum_{d\le x}\left\{\frac{1}{2}\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right\} = \frac{x^2}{2}\sum_{d\le x}\frac{1}{d^2} + O\left(x\sum_{d\le x}\frac{1}{d}\right)$$

$$= \frac{x^2}{2}\left\{-\frac{1}{x} + \zeta(2) + O\left(\frac{1}{x^2}\right)\right\} + O(x\log x) = \frac{1}{2}\zeta(2)x^2 + O(x\log x),$$

که درآن از قسمتهای (آ) و (ب) قضیهٔ ۲.۳ استفاده شده است.

قضیهٔ ۵.۳ . *اگر* $x \ge 1$ *و* $\alpha > 0, \alpha \ne 1$ *، داریم*

$$\sum_{n\le x}\sigma_\alpha(n) = \frac{\zeta(\alpha+1)}{\alpha+1}x^{\alpha+1} + O(x^\beta),$$

که درآن $\beta = \max\{1, \alpha\}$.

برهان. این بار، از قسمتهای (ب) و (ت) قضیهٔ ۲.۳ استفاده می‌کنیم تا بدست آید

$$\sum_{n\le x}\sigma_\alpha(n) = \sum_{n\le x}\sum_{q|n} q^\alpha = \sum_{d\le x}\sum_{q\le x/d} q^\alpha$$

$$= \sum_{d\le x}\left\{\frac{1}{\alpha+1}\left(\frac{x}{d}\right)^{\alpha+1} + O\left(\frac{x^\alpha}{d^\alpha}\right)\right\} = \frac{x^{\alpha+1}}{\alpha+1}\sum_{d\le x}\frac{1}{d^{\alpha+1}} + O\left(x^\alpha\sum_{d\le x}\frac{1}{d^\alpha}\right)$$

$$= \frac{x^{\alpha+1}}{\alpha+1}\left\{\frac{x^{-\alpha}}{-\alpha} + \zeta(\alpha+1) + O(x^{-\alpha-1})\right\}$$

$$+ O\left(x^\alpha\left\{\frac{x^{1-\alpha}}{1-\alpha} + \zeta(\alpha) + O(x^{-\alpha})\right\}\right)$$

$$= \frac{\zeta(\alpha+1)}{\alpha+1}x^{\alpha+1} + O(x) + O(1) + O(x^\alpha) = \frac{\zeta(\alpha+1)}{\alpha+1}x^{\alpha+1} + O(x^\beta),$$

که درآن $\beta = \max\{1, \alpha\}$.

برای بدست آوردن مرتبهٔ متوسط $\sigma_\alpha(n)$ به‌ازای α منفی، می‌نویسیم $\alpha = -\beta$ که

درآن $\beta > 0$.

**قضیهٔ ۶.۳ . اگر $\beta > 0$ ، قرار می‌دهیم $\delta = \max\{0, 1 - \beta\}$.
دراین صورت ، هرگاه $x > 1$ ، آنگاه**

$$\sum_{n \le x} \sigma_{-\beta}(n) = \zeta(\beta + 1)x + O(x^{\delta}) \quad \text{اگر } \beta \neq 1 ،$$

$$= \zeta(2)x + O(\log x) \quad \text{اگر } \beta = 1 ،$$

برهان . داریم

$$\sum_{n \le x} \sigma_{-\beta}(n) = \sum_{n \le x} \sum_{d|n} \frac{1}{d^{\beta}} = \sum_{d \le x} \frac{1}{d^{\beta}} \sum_{q \le x/d} 1$$
$$= \sum_{d \le x} \frac{1}{d^{\beta}} \left\{\frac{x}{d} + O(1)\right\} = x \sum_{d \le x} \frac{1}{d^{\beta + 1}} + O\left(\sum_{d \le x} \frac{1}{d^{\beta}}\right).$$

آخرین جمله ، اگر $\beta = 1$ ، مساوی $O(\log x)$ و ، اگر $\beta \neq 1$ ، مساوی $O(x^{\delta})$ است . چون

$$x \sum_{d \le x} \frac{1}{d^{\beta + 1}} = \frac{x^{1-\beta}}{-\beta} + \zeta(\beta + 1)x + O(x^{-\beta}) = \zeta(\beta + 1)x + O(x^{1-\beta}),$$

این برهان را تمام خواهد کرد .

۷.۳ مرتبهٔ متوسط $\varphi(n)$

فرمول مجانبی برای مجموعهای جزئی کامل اویلر شامل مجموع سری

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2}$$

است . این سری به‌طور مطلق همگراست ، چرا که تحت تسلط $\sum_{n=1}^{\infty} n^{-2}$ است . در یکی‌از فصول آتی ثابت می‌کنیم که

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}. \qquad (۱۲)$$

با این فرض که این نتیجه فعلاً برقرار است ، بنابر قسمت (پ) قضیهٔ ۲.۳ ، داریم

$$\sum_{n \le x} \frac{\mu(n)}{n^2} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} - \sum_{n > x} \frac{\mu(n)}{n^2}$$
$$= \frac{6}{\pi^2} + O\left(\sum_{n > x} \frac{1}{n^2}\right) = \frac{6}{\pi^2} + O\left(\frac{1}{x}\right).$$

حال، با استفاده از این، مرتبهٔ متوسط $\varphi(n)$ را بدست می‌آوریم.

قضیهٔ ۳ . ۷ . *به‌ازای* $x > 1$ *داریم*

$$\sum_{n\le x}\varphi(n) = \frac{3}{\pi^2}x^2 + O(x\log x); \tag{۱۳}$$

درنتیجه، مرتبهٔ متوسط $\varphi(n)$ *مساوی* $3n/\pi^2$ *است.*

برهان. روش اثبات شبیه روشی است که برای توابع مقسوم علیهی بکار رفت. با رابطهٔ

$$\varphi(n) = \sum_{d|n}\mu(d)\frac{n}{d}$$

شروع کرده، بدست می‌آوریم

$$\begin{aligned}\sum_{n\le x}\varphi(n) &= \sum_{n\le x}\sum_{d|n}\mu(d)\frac{n}{d} = \sum_{\substack{q,d\\ qd\le x}}\mu(d)q = \sum_{d\le x}\mu(d)\sum_{q\le x/d}q\\ &= \sum_{d\le x}\mu(d)\left\{\frac{1}{2}\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right\}\\ &= \frac{1}{2}x^2\sum_{d\le x}\frac{\mu(d)}{d^2} + O\left(x\sum_{d\le x}\frac{1}{d}\right)\\ &= \frac{1}{2}x^2\left\{\frac{6}{\pi^2} + O\left(\frac{1}{x}\right)\right\} + O(x\log x) = \frac{3}{\pi^2}x^2 + O(x\log x).\end{aligned}$$

۳ . ۸ کاربرد در توزیع نقاط مشبکهٔ قابل رویت از مبداء

فرمول مجانبی مجموعهای جزئی $\varphi(n)$ کاربرد جالبی در قضیهٔ مربوط به توزیع نقاط مشبکه در صفحه که از مبداء قابل رویت‌اند دارد.

تعریف. دو نقطهٔ مشبکهٔ P و Q را *از دو طرف قابل رویت* گوییم اگر پاره خط واصل بین آنها نقطهٔ مشبکه‌ای غیر از نقاط انتهایی P و Q نداشته باشد.

قضیهٔ ۳ . ۸ . *دو نقطهٔ مشبکهٔ* (a, b) *و* (m, n) *از دو طرف قابل رویت‌اند اگر و فقط اگر* $a-m$ *و* $b-n$ *نسبت بهم اول باشند.*

برهان. واضح است که (a, b) و (m, n) از دو طرف قابل رویت‌اند اگر و فقط اگر

$(a-m, b-n)$ از مبداء قابل رویت باشد. بنابراین، کافی است قضیه را وقتی ثابت کنیم که $(m, n) = (0, 0)$.

فرض کنیم (a, b) از مبداء قابل رویت بوده، و $d = (a, b)$. می‌خواهیم ثابت‌کنیم $d = 1$. هرگاه $d > 1$، آنگاه $a = da'$، $b = db'$، و نقطهٔ مشبکهٔ (a', b') بر پاره خط واصل بین $(0, 0)$ و (a, b) قرار دارد. این تناقض ثابت می‌کند که $d = 1$.

بعکس، فرض کنیم $(a, b) = 1$. اگر نقطهٔ مشبکهٔ (a', b') بر پاره خط‌واصل بین $(0, 0)$ و (a, b) واقع باشد، داریم

$$a' = ta, \qquad b' = tb \text{، که } 0 < t < 1.$$

بنابراین، t گویاست؛ درنتیجه، $t = r/s$ که درآن r, s اعداد صحیح مثبتی با خاصیت $(r, s) = 1$ می‌باشند. لذا،

$$sb' = br \quad \text{و} \quad sa' = ar;$$

درنتیجه، $s|ar, s|br$. اما $(s, r) = 1$؛ درنتیجه، $s|a, s|b$. ازاینرو، چون $(a, b) = 1$، پس $s = 1$. این نامساوی $0 < t < 1$ را نقض می‌کند. بنابراین، نقطهٔ‌مشبکهٔ (a, b) از مبداء قابل رویت می‌باشد.

تعداد نقاط مشبکهٔ قابل رویت از مبداء بی‌نهایت است، و طبیعی است که از طرز توزیع آنها در صفحه استفسار شود.

یک ناحیهٔ مربعی بزرگ در صفحهٔ xy را درنظر می‌گیریم که با نامساویهای

$$|x| \le r, \qquad |y| \le r$$

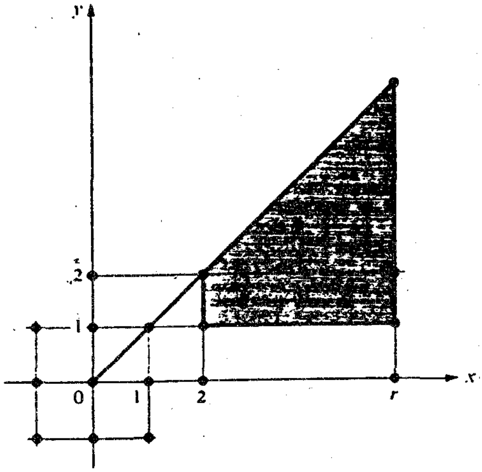
تعریف می‌شود. فرض‌کنیم $N(r)$ تعداد نقاط مشبکه دراین مربع، و $N'(r)$ تعداد نقاط قابل‌رویت درآن از مبداء باشد. خارج قسمت $N'(r)/N(r)$ نسبت نقاط مشبکهٔ واقع درمربع را که از مبداء قابل رویت‌اند می‌سنجد. قضیهٔ بعدی نشان می‌دهد که این کسر، وقتی $r \to \infty$، به‌حدی میل خواهد کرد. این حد را **چگالی** نقاط مشبکهٔ قابل رویت از مبداء می‌نامیم.

قضیهٔ ۹.۳ . *مجموعهٔ نقاط مشبکهٔ قابل رویت از مبداء دارای چگالی $6/\pi^2$ است.*

برهان. ثابت می‌کنیم که

$$\lim_{r \to \infty} \frac{N'(r)}{N(r)} = \frac{6}{\pi^2}.$$

نزدیکترین هشت نقطهٔ مشبکه به مبداء همه از مبداء قابل رویت‌اند . (ر.ک . شکل ۳.۳ .)
بنا به‌تقارن ، ملاحظه می‌شود که $N'(r)$ مساوی 8 است بعلاوهٔ 8 برابر تعداد نقاط قابل



شکل ۳.۳

رویت در ناحیهٔ

$$\{(x, y): 2 \le x \le r, \qquad 1 \le y \le x\}$$

(ناحیهٔ سایه‌دار شکل ۳.۳) . این عدد برابر است با

$$N'(r) = 8 + 8 \sum_{2 \le n \le r} \sum_{\substack{1 \le m < n \\ (m,n)=1}} 1 = 8 \sum_{1 \le n \le r} \varphi(n).$$

با استفاده از قضیهٔ ۷.۳ ، داریم

$$N'(r) = \frac{24}{\pi^2} r^2 + O(r \log r).$$

اما تعداد کل نقاط مشبکه در مربع فوق برابر است با

$$N(r) = (2[r] + 1)^2 = (2r + O(1))^2 = 4r^2 + O(r) ;$$

درنتیجه ،

$$\frac{N'(r)}{N(r)} = \frac{\frac{24}{\pi^2} r^2 + O(r \log r)}{4r^2 + O(r)} = \frac{\frac{6}{\pi^2} + O\left(\frac{\log r}{r}\right)}{1 + O\left(\frac{1}{r}\right)}.$$

بنابراین، وقتی $r \to \infty$ ، معلوم می‌شود که $N'(r)/N(r) \to 6/\pi^2$.

تذکر. قضیهٔ ۹.۳ گاهی این‌طور توصیف می‌شود که می‌گویند یک نقطهٔ مشبکه که به تصادف انتخاب شده دارای احتمال $6/\pi^2$ است که از مبداء قابل رویت باشد. یا، اگردو عدد صحیح a و b به تصادف انتخاب شوند، احتمال اینکه نسبت بهم اول باشند $6/\pi^2$ است.

۹.۳ مرتبهٔ متوسط $\mu(n)$ و $\Lambda(n)$

تعیین مرتبهٔ متوسط $\mu(n)$ و $\Lambda(n)$ بمراتب مشکلتر از مرتبهٔ متوسط $\varphi(n)$ وتوابع مقسوم علیهی است. معلوم شده که مرتبهٔ متوسط $\mu(n)$ مساوی 0 و مرتبهٔ متوسط $\Lambda(n)$ مساوی 1 است. یعنی،

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} \mu(n) = 0$$

و

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} \Lambda(n) = 1,$$

لیکن اثبات این امر ساده نیست. در فصل بعد ثابت می‌کنیم که هریک از این نتایج معادل قضیهٔ اعداد اول، یعنی

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1,$$

است، که درآن $\pi(x)$ تعداد اعداد اول نابیشتر از x است.

دراین فصل، چند اتحاد مقدماتی مربوط به $\mu(n)$ و $\Lambda(n)$ بدست می‌آیند که بعداً در مطالعهٔ توزیع اعداداول بکار خواهند رفت. این اتحادها از یک فرمول کلی ناشی می‌شوند که مجموعهای جزئی توابع حسابی دلخواه f و g را با مجموعهای جزئی حاصل ضرب دیریکلهٔ آنها $f * g$ ربط می‌دهد.

۱۰.۳ مجموعهای جزئی یک حاصلضرب دیریکله

قضیهٔ ۱۰.۳ . اگر $h = f * g$ ، قرار می‌دهیم

$$H(x) = \sum_{n\le x} h(n), \quad F(x) = \sum_{n\le x} f(n), \quad G(x) = \sum_{n\le x} g(n).$$

دراین صورت ، داریم

$$H(x) = \sum_{n\le x} f(n)G\left(\frac{x}{n}\right) = \sum_{n\le x} g(n)F\left(\frac{x}{n}\right). \qquad (۱۴)$$

برهان . ازقانون شرکتپذیری (قضیهٔ ۲۱۰۲) که اعمال $\circ$ و $*$ را بهم مربوط میسازداستفاد میکنیم . فرض کنیم

$$U(x) = \begin{cases} 0 & \text{اگر } 0 < x < 1 ، \\ 1 & \text{اگر } x \ge 1 ، \end{cases}$$

دراین صورت ، $F = f \circ U, G = g \circ U$ ، و خواهیم داشت

$$f \circ G = f \circ (g \circ U) = (f * g) \circ U = H,$$
$$g \circ F = g \circ (f \circ U) = (g * f) \circ U = H.$$

این برهان را تمام خواهد کرد .

هرگاه‌به‌ازای‌هر n ، $g(n) = 1$ ، آنگاه $G(x) = [x]$ ، و از (۱۴) نتیجهٔ زیربدست می‌آید :

قضیهٔ ۱۱۰۳ . *اگر* $F(x) = \sum_{n\le x} f(n)$ ، *داریم*

$$\sum_{n\le x}\sum_{d|n} f(d) = \sum_{n\le x} f(n)\left[\frac{x}{n}\right] = \sum_{n\le x} F\left(\frac{x}{n}\right). \qquad (۱۵)$$

۱۱۰۳ کاربرد در مورد $\mu(n)$ و $\Lambda(n)$

حال ، اگر در قضیهٔ ۱۱۰۳ $f(n)$ را مساوی $\mu(n)$ یا $\Lambda(n)$ بگیریم ، اتحادهای زیر بدست می‌آیند که بعدها در مطالعهٔ توزیع اعداد اول بکار خواهند آمد .

قضیهٔ ۱۲۰۳ . *به‌ازای* $x \ge 1$ ، *داریم*

$$\sum_{n\le x} \mu(n)\left[\frac{x}{n}\right] = 1 \qquad (۱۶)$$

و

$$\sum_{n\le x} \Lambda(n)\left[\frac{x}{n}\right] = \log [x]!. \qquad (۱۷)$$

برهان. از (۱۵) داریم

$$\sum_{n\le x}\mu(n)\left[\frac{x}{n}\right]=\sum_{n\le x}\sum_{d|n}\mu(d)=\sum_{n\le x}\left[\frac{1}{n}\right]=1$$

و

$$\sum_{n\le x}\Lambda(n)\left[\frac{x}{n}\right]=\sum_{n\le x}\sum_{d|n}\Lambda(d)=\sum_{n\le x}\log n=\log[x]!.$$

تذکر. مجموعهای مذکور در قضیهٔ ۱۲.۳ را می‌توان متوسطهای وزندار توابع $\mu(n)$ و $\Lambda(n)$ گرفت.

در قضیهٔ ۱۶.۴ ثابت خواهد شد که قضیهٔ اعداد اول از این مطلب که سری

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n}$$

همگراست و مجموعش 0 است نتیجه می‌شود. با استفاده از (۱۶)، می‌توان ثابت کرد که این سری دارای مجموعهای جزئی کراندار است.

قضیهٔ ۱۳.۳ . به‌ازای هر $x\ge 1$ ، داریم

$$\left|\sum_{n\le x}\frac{\mu(n)}{n}\right|\le 1, \tag{۱۸}$$

که درآن تساوی فقط وقتی برقرار است که $x<2$.

برهان. اگر $x<2$ ، فقط یک جمله در مجموع وجود دارد، $\mu(1)=1$. حال فرض می‌کنیم $x\ge 2$. به‌ازای هر y حقیقی، قرار می‌دهیم $\{y\}=y-[y]$. دراین صورت،

$$1=\sum_{n\le x}\mu(n)\left[\frac{x}{n}\right]=\sum_{n\le x}\mu(n)\left(\frac{x}{n}-\left\{\frac{x}{n}\right\}\right)=x\sum_{n\le x}\frac{\mu(n)}{n}-\sum_{n\le x}\mu(n)\left\{\frac{x}{n}\right\}.$$

چون $0\le\{y\}<1$ ، این ایجاب می‌کند که

$$x\left|\sum_{n\le x}\frac{\mu(n)}{n}\right|=\left|1+\sum_{n\le x}\mu(n)\left\{\frac{x}{n}\right\}\right|\le 1+\sum_{n\le x}\left\{\frac{x}{n}\right\}$$
$$=1+\{x\}+\sum_{2\le n\le x}\left\{\frac{x}{n}\right\}<1+\{x\}+[x]-1=x.$$

اگر رابطهٔ فوق بر x تقسیم شود، (۱۸) با نامساوی اکید بدست خواهد آمد.

حال به اتحاد (۱۷) در قضیهٔ ۱۲.۳، یعنی

$$\sum_{n\le x}\Lambda(n)\left[\frac{x}{n}\right]=\log[x]!, \tag{۱۷}$$

رو می‌آوریم و، با استفاده از آن، توان یک عدد اول که یک فاکتوریل را عاد می‌کند را معین می‌کنیم.

قضیهٔ ۱۴.۳ . اتحاد لژاندر. *به‌ازای هر* $x\ge 1$ *، داریم*

$$[x]!=\prod_{p\le x}p^{\alpha(p)} \tag{۱۹}$$

که درآن حاصل ضرب روی تمام اعداد اول نابیشتر از x *گرفته شده، و*

$$\alpha(p)=\sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]. \tag{۲۰}$$

تذکر. چون به‌ازای $p>x$ ، $[x/p^m]=0$ ، مجموع مربوط به $\alpha(p)$ متناهی است.

برهان. چون $\Lambda(n)=0$ مگر آنکه n توانی از یک عدد اول باشد، و $\Lambda(p^m)=\log p$ ، داریم

$$\log[x]!=\sum_{n\le x}\Lambda(n)\left[\frac{x}{n}\right]=\sum_{p\le x}\sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]\log p=\sum_{p\le x}\alpha(p)\log p,$$

که درآن $\alpha(p)$ از (۲۰) بدست می‌آید. آخرین مجموع نیز لگاریتم حاصل‌ضرب مذکور در (۱۹) است؛ درنتیجه، این برهان را تمام خواهد کرد.

حال، با استفاده از فرمول جمعبندی اویلر، یک فرمول مجانبی برای $\log[x]!$ بدست می‌آوریم.

قضیهٔ ۱۵.۳ . *اگر* $x\ge 2$ *، داریم*

$$\log[x]!=x\log x-x+O(\log x); \tag{۲۱}$$

و درنتیجه،

$$\sum_{n\le x}\Lambda(n)\left[\frac{x}{n}\right]=x\log x-x+O(\log x). \tag{۲۲}$$

برهان. با فرض $f(t)=\log t$ در فرمول جمعبندی‌اویلر (قضیهٔ ۳.۱۰)، بدست می‌آوریم

$$\sum_{n\le x}\log n=\int_1^x\log t\,dt+\int_1^x\frac{t-[t]}{t}\,dt-(x-[x])\log x$$
$$=x\log x-x+1+\int_1^x\frac{t-[t]}{t}\,dt+O(\log x).$$

این (۲۱) را ثابت می‌کند، زیرا

$$\int_1^x\frac{t-[t]}{t}\,dt=O\left(\int_1^x\frac{1}{t}\,dt\right)=O(\log x),$$

و (۲۲) از (۱۷) نتیجه خواهد شد.

قضیهٔ زیر نتیجه‌ای از (۲۲) است.

قضیهٔ ۱۶.۳. به‌ازای $x\ge 2$، داریم

$$\sum_{p\le x}\left[\frac{x}{p}\right]\log p=x\log x+O(x), \tag{۲۳}$$

که درآن مجموع روی همهٔ اعداد اول نابیشتر از x گرفته شده است.

برهان. چون $\Lambda(n)=0$ مگر آنکه n توانی از یک عدد اول باشد، داریم

$$\sum_{n\le x}\left[\frac{x}{n}\right]\Lambda(n)=\sum_{\substack{p\\ p^m\le x}}\sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]\Lambda(p^m).$$

اما $p^m\le x$ ایجاب می‌کندکه $p\le x$. همچنین، اگر $p>x$، $[x/p^m]=0$؛ درنتیجه، آخرین مجموع را می‌توان به‌صورت زیر نوشت:

$$\sum_{p\le x}\sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]\log p=\sum_{p\le x}\left[\frac{x}{p}\right]\log p+\sum_{p\le x}\sum_{m=2}^{\infty}\left[\frac{x}{p^m}\right]\log p.$$

حال ثابت می‌کنیم‌که مجموع آخری $O(x)$ است. داریم

$$\sum_{p\le x}\log p\sum_{m=2}^{\infty}\left[\frac{x}{p^m}\right]\le\sum_{p\le x}\log p\sum_{m=2}^{\infty}\frac{x}{p^m}=x\sum_{p\le x}\log p\sum_{m=2}^{\infty}\left(\frac{1}{p}\right)^m$$

$$= x\sum_{p\le x}\log p\cdot\frac{1}{p^2}\cdot\frac{1}{1-\frac{1}{p}} = x\sum_{p\le x}\frac{\log p}{p(p-1)}$$

$$\le x\sum_{n=2}^{\infty}\frac{\log n}{n(n-1)} = O(x).$$

لذا ، نشان داده‌ایم که

$$\sum_{n\le x}\left[\frac{x}{n}\right]\Lambda(n) = \sum_{p\le x}\left[\frac{x}{p}\right]\log p + O(x),$$

که ، وقتی با (۲۲) بکار رود ، (۲۳) را ثابت خواهد کرد .

در فصل بعد ، معادلهٔ (۲۳) برای‌بدست‌آوردن یک فرمول مجانبی جهت‌مجموعهای جزئی سری واگرای $\sum(1/p)$ بکار خواهد رفت .

۱۲.۳ اتحادی دیگر برای مجموعهای جزئی یک حاصل ضرب دیریکله

این فصل‌را با صورت کلیتری از قضیهٔ ۱۰.۳ که در فصل ۴ برای مطالعهٔ مجموعهای‌جزئی بعضی از حاصل ضربهای دیریکله بکار می‌رود پایان می‌دهیم .

مثل قضیهٔ ۱۰.۳ ، می‌نویسیم

$$F(x) = \sum_{n\le x} f(n),\qquad G(x) = \sum_{n\le x} g(n),\qquad H(x) = \sum_{n\le x}(f*g)(n)\,;$$

درنتیجه ،

$$H(x) = \sum_{n\le x}\sum_{d\mid n} f(d)g\left(\frac{n}{d}\right) = \sum_{\substack{q,d\\ qd\le x}} f(d)g(q).$$

قضیهٔ ۱۷.۳ . هرگاه a و b اعداد حقیقی مثبتی باشند بطوری که $ab = x$ ، آنگاه

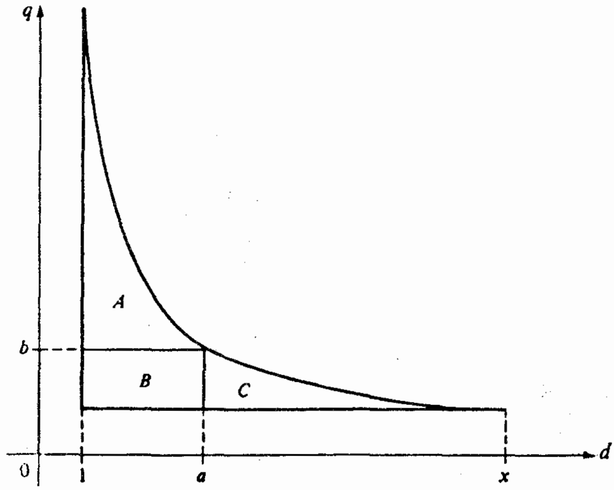
$$\sum_{\substack{q,d\\ qd\le x}} f(d)g(q) = \sum_{n\le a} f(n)G\left(\frac{x}{n}\right) + \sum_{n\le b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b). \tag{۲۴}$$

برهان . مجموع $H(x)$ سمت چپ (۲۴) روی نقاط مشبکه در ناحیهٔ هذلولوی شکل ۴.۳ گرفته می‌شود . مجموع را به دو بخش تقسیم می‌کنیم ، یکی روی نقاط مشبکه در $A \cup B$ و دیگری‌روی‌نقاط مشبکه‌در $B \cup C$. نقاط مشبکه در B دوبار به‌حساب می‌آیند ؛ درنتیجه ،

داریم

$$H(x) = \sum_{d \le a} \sum_{q \le x/d} f(d)g(q) + \sum_{q \le b} \sum_{d \le x/q} f(d)g(q) - \sum_{d \le a} \sum_{q \le b} f(d)g(q),$$

که همان (۲۴) می‌باشد.



شکل ۴.۳

تذکر. با فرض $a = 1$ و $b = 1$ ، بترتیب ، چون $f(1) = F(1)$ و $g(1) = G(1)$ ، دو معادلهٔ قضیهٔ ۱۰.۳ بدست می‌آیند.

تمرین برای فصل ۳

۱. با استفاده از فرمول جمعبندی اویلر، روابط زیر را به‌ازای $x \ge 2$ نتیجه بگیرید:

(آ) $\displaystyle\sum_{n \le x} \frac{\log n}{n} = \frac{1}{2}\log^2 x + A + O\left(\frac{\log x}{x}\right)$ ، که درآن A ثابت است؛

(ب) $\displaystyle\sum_{2 \le n \le x} \frac{1}{n \log n} = \log(\log x) + B + O\left(\frac{1}{x \log x}\right)$ ، که درآن B ثابت است.

۲. اگر $x \ge 2$ ، ثابت کنید

$\displaystyle\sum_{n \le x} \frac{d(n)}{n} = \frac{1}{2}\log^2 x + 2C \log x + O(1)$ ، که درآن C ثابت اویلر است.

۳ . اگر $x \geq 2$ و $\alpha > 0, \alpha \neq 1$ ، ثابت کنید

$$\sum_{n \leq x} \frac{d(n)}{n^\alpha} = \frac{x^{1-\alpha}\log x}{1-\alpha} + \zeta(\alpha)^2 + O(x^{1-\alpha}).$$

۴ . اگر $x \geq 2$ ، ثابت کنید

(آ) $\sum_{n \leq x} \mu(n)\left[\frac{x}{n}\right]^2 = \frac{x^2}{\zeta(2)} + O(x \log x)$ ؛

(ب) $\sum_{n \leq x} \frac{\mu(n)}{n}\left[\frac{x}{n}\right] = \frac{x}{\zeta(2)} + O(\log x)$.

۵ . اگر $x \geq 1$ ، ثابت کنید

(آ) $\sum_{n \leq x} \varphi(n) = \frac{1}{2}\sum_{n \leq x} \mu(n)\left[\frac{x}{n}\right]^2 + \frac{1}{2}$ ؛

(ب) $\sum_{n \leq x} \frac{\varphi(n)}{n} = \sum_{n \leq x} \frac{\mu(n)}{n}\left[\frac{x}{n}\right]$.

این فرمولها ، همراه با فرمولهای تمرین ۴ ، نشان می‌دهند که به‌ازای $x \geq 2$ ،

$$\sum_{n \leq x} \varphi(n) = \frac{1}{2}\frac{x^2}{\zeta(2)} + O(x \log x) \quad \text{و} \quad \sum_{n \leq x} \frac{\varphi(n)}{n} = \frac{x}{\zeta(2)} + O(\log x).$$

۶ . اگر $x \geq 2$ ، ثابت کنید

$$\sum_{n \leq x} \frac{\varphi(n)}{n^2} = \frac{1}{\zeta(2)}\log x + \frac{C}{\zeta(2)} - A + O\left(\frac{\log x}{x}\right),$$

که درآن C ثابت اویلر است و

$$A = \sum_{n=1}^{\infty} \frac{\mu(n)\log n}{n^2}.$$

۷ . دریکی‌از فصول آتی ثابت می‌شود که ، اگر $\alpha > 1$ ، $\sum_{n=1}^{\infty} \mu(n)n^{-\alpha} = 1/\zeta(\alpha)$. بافرض این نتیجه ، ثابت کنید به‌ازای $x \geq 2$ و $\alpha > 1, \alpha \neq 2$ ، داریم

$$\sum_{n \leq x} \frac{\varphi(n)}{n^\alpha} = \frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)} + \frac{\zeta(\alpha-1)}{\zeta(\alpha)} + O(x^{1-\alpha}\log x).$$

۸ . اگر $\alpha \leq 1$ و $x \geq 2$ ، ثابت کنید

$$\sum_{n \leq x} \frac{\varphi(n)}{n^\alpha} = \frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)} + O(x^{1-\alpha}\log x).$$

۹ . دریکی‌از فصول آتی ثابت می‌شود که حاصل ضرب نامتناهی $\prod_p (1-p^{-2})$ ، که‌روی

همهٔ اعداد اول گرفته شده، همگرا به مقدار $1/\zeta(2) = 6/\pi^2$ است. با فرض این نتیجه، ثابت کنید که

(آ) اگر $n \geq 2$، $\dfrac{\sigma(n)}{n} < \dfrac{n}{\varphi(n)} < \dfrac{\pi^2}{6}\dfrac{\sigma(n)}{n}$.

[راهنمایی. از فرمول $\varphi(n) = n\prod_{p|n}(1 - p^{-1})$ و رابطهٔ

$$1 + x + x^2 + \cdots = \frac{1}{1-x} = \frac{1+x}{1-x^2} \quad \text{به‌ازای} \quad x = \frac{1}{p}$$

استفاده کنید]؛

(ب) اگر $x \geq 2$،

$$\sum_{n \leq x} \frac{n}{\varphi(n)} = O(x).$$

۱۰. اگر $x \geq 2$، ثابت کنید که

$$\sum_{n \leq x} \frac{1}{\varphi(n)} = O(\log x).$$

۱۱. فرض کنید $\varphi_1(n) = n\sum_{d|n} |\mu(d)|/d$.

(آ) ثابت کنید φ_1 ضربی است و $\varphi_1(n) = n\prod_{p|n}(1 + p^{-1})$.

(ب) ثابت کنید

$$\varphi_1(n) = \sum_{d^2|n} \mu(d)\sigma\left(\frac{n}{d^2}\right)$$

که در آن مجموع روی آن مقسوم علیه‌های n گرفته شده که $d^2|n$.

(پ) ثابت کنید

$$\sum_{n \leq x} \varphi_1(n) = \sum_{d \leq \sqrt{x}} \mu(d) S\left(\frac{x}{d^2}\right)، \quad \text{که درآن} \quad S(x) = \sum_{k \leq x} \sigma(k)؛$$

سپس، با استفاده از قضیهٔ ۴.۳، نتیجه بگیرید که، به‌ازای $x \geq 2$،

$$\sum_{n \leq x} \varphi_1(n) = \frac{\zeta(2)}{2\zeta(4)} x^2 + O(x \log x).$$

مثل تمرین ۷، می‌توانید نتیجهٔ "به‌ازای $\alpha > 1$، $\sum_{n=1}^{\infty} \mu(n)n^{-\alpha} = 1/\zeta(\alpha)$" را دانسته بگیرید.

۱۲. به‌ازای $s > 0$ حقیقی و $k \geq 1$ صحیح، برای مجموعهای جزئی

$$\sum_{\substack{n \leq x \\ (n,k)=1}} \frac{1}{n^s},$$

یک فرمول مجانبی بیابید با جملهٔ خطایی که، وقتی $x \to \infty$ ، به 0 میل نماید. مطمئن شوید که حالت $s = 1$ درنظر گرفته شده است.

خواص تابع بزرگترین عدد صحیح

به‌ازای هر x حقیقی، علامت $[x]$ یعنی بزرگترین عدد صحیح نابیشتر از x . تمرینهای ۱۳ تا ۲۶ چند خاصیت تابع بزرگترین عدد صحیح را توصیف می‌کنند. دراین تمرینها، x و y اعدادی حقیقی‌اند، و n یک عدد صحیح می‌باشد.

۱۳ . احکام زیر را ثابت کنید:

(آ) هرگاه $x = k + y$ که‌درآن k عددی‌صحیح‌است‌و $0 \le y < 1$ ، آنگاه $k = [x]$ ؛

(ب) $[x + n] = [x] + n$ ؛

(پ) $$[-x] = \begin{cases} -[x] & \text{اگر } x = [x] \text{ ،} \\ -[x] - 1 & \text{اگر } x \neq [x] \text{ ؛} \end{cases}$$

(ت) اگر $n \ge 1$ ، $[x/n] = [[x]/n]$.

۱۴ . اگر $0 < y < 1$ ، مقادیر ممکن $[x] - [x - y]$ چیست؟

۱۵ . عدد $\{x\} = x - [x]$ **جزء کسری** x نامیده می‌شود. این عدد در نامساویهای $0 \le \{x\} < 1$ صدق می‌کند، با $\{x\} = 0$ اگر و فقط اگر x یک عدد صحیح باشد. مقادیر ممکن $\{x\} + \{-x\}$ چیست؟

۱۶ . (آ) ثابت کنید که $[2x] - 2[x]$ یا 0 است یا 1 .

(ب) ثابت کنید که $[2x] + [2y] \ge [x] + [y] + [x + y]$.

۱۷ . ثابت کنید که $[x] + [x + \frac{1}{2}] = [2x]$ و، بطور کلی،

$$\sum_{k=0}^{n-1}\left[x + \frac{k}{n}\right] = [nx].$$

۱۸ . فرض کنید $f(x) = x - [x] - \frac{1}{2}$. ثابت کنید که

$$\sum_{k=0}^{n-1} f\left(x + \frac{k}{n}\right) = f(nx)$$

و نتیجه بگیرید که

به‌ازای هر $m \ge 1$ و هر x حقیقی، $\left|\sum_{n=1}^{m} f\left(2^n x + \frac{1}{2}\right)\right| \le 1$.

۱۹ . به فرض آنکه h و k اعداد صحیح فرد مثبتی بوده و $(h, k) = 1$ ، قرار دهید

$$a = (k - 1)/2, b = (h - 1)/2 .$$

(آ) ثابت کنید که $ab = \sum_{r=1}^{b} [kr/h] + \sum_{r=1}^{a} [hr/k]$.

راهنمایی . نقاط مشبکه .

(ب) نتیجهٔ متناظر با $(h, k) = d$ را بدست آورید .

۲۰ . اگر n عدد صحیح مثبتی باشد ، ثابت کنیدکه $[\sqrt{n} + \sqrt{n+1}] = [\sqrt{4n+2}]$.

۲۱ . جمیع اعداد صحیح و مثبت n که $[\sqrt{n}]$ ، n را عاد می‌کند را معین کنید .

۲۲ . ثابت کنید که اگر n عدد صحیح مثبتی باشد ،

$$\left[\frac{8n+13}{25}\right] - \left[\frac{n - 12 - \left[\frac{n-17}{25}\right]}{3}\right]$$

از n مستقل است .

۲۳ . ثابت کنید که

$$\sum_{n \le x} \lambda(n)\left[\frac{x}{n}\right] = [\sqrt{x}].$$

۲۴ . ثابت کنید که

$$\sum_{n \le x} \left[\sqrt{\frac{x}{n}}\right] = \sum_{n \le \sqrt{x}} \left[\frac{x}{n^2}\right]$$

۲۵ . ثابت کنید که

$$\sum_{k=1}^{n} \left[\frac{k}{2}\right] = \left[\frac{n^2}{4}\right]$$

و

$$\sum_{k=1}^{n} \left[\frac{k}{3}\right] = \left[\frac{n(n-1)}{6}\right]$$

۲۶ . هرگاه $a = 1, 2, \ldots, 7$ ، ثابت‌کنید عدد صحیحی مانند b (وابسته به a) هست‌که

$$\sum_{k=1}^{n} \left[\frac{k}{a}\right] = \left[\frac{(2n+b)^2}{8a}\right]$$

۴
چند قضیه مقدماتی در باب توزیع اعداد اول

۱.۴ مقدمه

فرض کنیم $\pi(x)$ ، به‌ازای $x > 0$ ، تعداد اعداد اول نابیشتر از x باشد. دراین صورت، وقتی $x \to \infty$ ، $\pi(x) \to \infty$ ، زیرا بی‌نهایت عدد اول وجود دارد. رفتار $\pi(x)$ به‌عنوان تابعی از x موضوع مطالعهٔ بسیاری ازریاضیدانان مشهور از قرن هجده تاکنون قرار گرفته است. بررسی جداول اعداد اول گاوس (۱۷۹۲) و لژاندر (۱۷۹۸) را به‌این حدس که $\pi(x)$ مجانب $x/\log x$ است، یعنی

$$\lim_{x \to \infty} \frac{\pi(x)\log x}{x} = 1,$$

رسانید. این حدس ابتدا در ۱۸۹۶ توسط هادامار [۲۸] ودولاواله پوسن [۷۱] ثابت‌شد و امروزه به ***قضیهٔ اعداد اول*** شهرت دارد.

برهانهای قضیهٔ اعداد اول، بسته به روشهای بکار رفته‌در آنها، **تحلیلی** یا **مقدماتی** نامیده می‌شوند. برهان هادامار و دولاواله پوسن تحلیلی است، و در آن از نظریهٔ توابع مختلط و خواص تابع زتای ریمان استفاده می‌شود. در ۱۹۴۹، یک برهان مقدماتی به‌وسیلهٔ ا. سلبرگ و پی. اردوش کشف شد. دراین برهان نه از تابع زتا استفاده شده و نه از نظریهٔ توابع مختلط، لیکن برهان کاملا" پیچیده‌ای است. در آخر این فصل مختصر توضیحی از نکات اصلی این برهان مقدماتی خواهیم داد. در فصل ۱۳ برهان تحلیلی کوتاهی می‌آوریم که از این برهان مقدماتی روشنتر است.

دراین فصل عمدتا" به توابع مقدماتی درباب اعداد اول توجه داریم. بالاخص، نشان می‌دهیم که قضیهٔ اعداد اول را می‌توان به چند شکل معادل بیان کرد.

مثلا"، نشان می‌دهیم که قضیهٔ اعداد اول معادل فرمول مجانبی زیر است:

$$\sum_{n \le x} \Lambda(n) \sim x \text{ ، } x \to \infty \text{ وقتی } . \qquad (1)$$

مجموعهای جزئی تابع منگولد $\Lambda(n)$ تابعی را تعریف می‌کنند که توسط چبیشف در ۱۸۴۸ معرفی شد.

۲.۴ توابع چبیشف $\psi(x)$ و $\vartheta(x)$

تعریف. به‌ازای $x > 0$، تابع ψ چبیشف با فرمول

$$\psi(x) = \sum_{n \le x} \Lambda(n)$$

تعریف می‌شود. بنابراین، فرمول مجانبی (۱) می‌گوید که

$$\lim_{x \to \infty} \frac{\psi(x)}{x} = 1. \tag{۲}$$

چون $\Lambda(n) = 0$ مگر آنکه n توانی از یک عدد اول باشد، می‌توان تعریف $\psi(x)$ را به‌صورت زیر نیز بیان کرد:

$$\psi(x) = \sum_{n \le x} \Lambda(n) = \sum_{m=1}^{\infty} \sum_{\substack{p \\ p^m \le x}} \Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p \le x^{1/m}} \log p.$$

مجموع روی m یک‌مجموع متناهی‌است. درواقع، مجموع روی p تهی است اگر $x^{1/m} < 2$؛ یعنی، اگر $(1/m)\log x < \log 2$، یا اگر

$$m > \frac{\log x}{\log 2} = \log_2 x.$$

بنابراین، داریم

$$\psi(x) = \sum_{m \le \log_2 x} \sum_{p \le x^{1/m}} \log p.$$

این را می‌توان با معرفی تابع دیگری از چبیشف به شکلی که کمی فرق دارد نوشت.

تعریف. اگر $x > 0$، تابع ϑ چبیشف با معادلهٔ زیر تعریف می‌شود:

$$\vartheta(x) = \sum_{p \le x} \log p,$$

که درآن p همهٔ اعداد اول نابیشتر از x را می‌گیرد.

حال آخرین فرمول برای $\psi(x)$ را می‌توان به‌صورت زیر بیان کرد:

$$\psi(x) = \sum_{m \le \log_2 x} \vartheta(x^{1/m}). \tag{۳}$$

قضیهٔ زیر دو کسر $\psi(x)/x$ و $\vartheta(x)/x$ را بهم مربوط خواهد ساخت.

قضیهٔ ۴.۱۰ به‌ازای $x > 0$، داریم

$$0 \le \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \le \frac{(\log x)^2}{2\sqrt{x}\log 2}.$$

تذکر. این نامساوی ایجاب می‌کند که

$$\lim_{x \to \infty}\left(\frac{\psi(x)}{x} - \frac{\vartheta(x)}{x}\right) = 0.$$

به عبارت دیگر، اگر یکی از $\psi(x)/x$ و $\vartheta(x)/x$ به‌حدی میل کند، دیگری نیز چنین می‌کند و دو حد مساوی می‌باشند.

برهان. از (۳) درمی‌یابیم که

$$0 \le \psi(x) - \vartheta(x) = \sum_{2 \le m \le \log_2 x} \vartheta(x^{1/m}).$$

اما از تعریف $\vartheta(x)$ نامساوی بدیهی زیر را داریم

$$\vartheta(x) \le \sum_{p \le x} \log x \le x \log x\,;$$

درنتیجه،

$$0 \le \psi(x) - \vartheta(x) \le \sum_{2 \le m \le \log_2 x} x^{1/m} \log(x^{1/m}) \le (\log_2 x)\sqrt{x}\log\sqrt{x}$$
$$= \frac{\log x}{\log 2}\cdot\frac{\sqrt{x}}{2}\log x = \frac{\sqrt{x}(\log x)^2}{2\log 2}.$$

حال با تقسیم بر x قضیه بدست می‌آید.

۴.۳ روابطی که $\vartheta(x)$ و $\pi(x)$ را بهم مربوط می‌کنند

دراین بخش دو فرمول بدست می‌آوریم که $\vartheta(x)$ و $\pi(x)$ را بهم ربط می‌دهند. از اینها برای اثبات اینکه قضیهٔ اعداد اول معادل رابطهٔ حدی

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1$$

است استفاده خواهد شد.

هر دو تابع $\pi(x)$ و $\vartheta(x)$ توابعی پله‌ای‌اند که در اعداد اول جهش دارند؛ $\pi(x)$ در هر عدد اول p جهش 1 دارد، درحالی که $\vartheta(x)$ در p جهش $\log p$ خواهد داشت. مجموعهای مربوط به توابع پله‌ای از این نوع را می‌توان به‌وسیلهٔ قضیهٔ زیر به‌صورت انتگرال بیان کرد.

قضیهٔ ۲.۴ . اتحاد آبل[1]. به‌ازای هر تابع حسابی $a(n)$، قرار می‌دهیم

$$A(x) = \sum_{n\le x} a(n),$$

که در آن اگر $x < 1$ ، $A(x) = 0$. فرض کنیم f بر بازهٔ $[y, x]$ ، که $0 < y < x$ ، مشتق پیوسته داشته باشد. دراین صورت، داریم

$$\sum_{y<n\le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)\,dt. \qquad (۴)$$

برهان. فرض‌کنیم $k = [x]$ و $m = [y]$؛ درنتیجه، $A(x) = A(k)$ و $A(y) = A(m)$. دراین صورت،

$$\begin{aligned}
\sum_{y<n\le x} a(n)f(n) &= \sum_{n=m+1}^{k} a(n)f(n) = \sum_{n=m+1}^{k} \{A(n) - A(n-1)\}f(n)\\
&= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1)\\
&= \sum_{n=m+1}^{k-1} A(n)\{f(n) - f(n+1)\} + A(k)f(k) - A(m)f(m+1)\\
&= -\sum_{n=m+1}^{k-1} A(n)\int_n^{n+1} f'(t)\,dt + A(k)f(k) - A(m)f(m+1)\\
&= -\sum_{n=m+1}^{k-1} \int_n^{n+1} A(t)f'(t)\,dt + A(k)f(k) - A(m)f(m+1)\\
&= -\int_{m+1}^{k} A(t)f'(t)\,dt + A(x)f(x) - \int_k^x A(t)f'(t)\,dt
\end{aligned}$$

---

1. Abel

$$-A(y)f(y)-\int_y^{m+1}A(t)f'(t)\,dt$$
$$=A(x)f(x)-A(y)f(y)-\int_y^x A(t)f'(t)\,dt.$$

برهان دیگر. برای‌خوانندگان‌آشنا با انتگرالگیری ریمان ــ اشتیل یس[1] برهان کوتاهتری از (۴) وجود دارد. (ر.ک. [۲] ، فصل ۷.) چون $A(x)$ یک تابع پله‌ای با جهش $f(n)$ در هر عددصحیح n است ،مجموع در (۴) را می‌توان به‌صورت یک انتگرال‌ریمان ــ اشتیل‌یس بیان کرد :

$$\sum_{y<n\le x}a(n)f(n)=\int_y^x f(t)\,dA(t).$$

انتگرالگیری به‌طریقهٔ جزء به‌جزء نتیجه می‌دهد که

$$\sum_{y<n\le x}a(n)f(n)=f(x)A(x)-f(y)A(y)-\int_y^x A(t)\,df(t)$$
$$=f(x)A(x)-f(y)A(y)-\int_y^x A(t)f'(t)\,dt.$$

تذکر. چون‌به‌ازای $t<1$ ، $A(t)=0$ ، معادلهٔ (۴) به‌ازای $y<1$ شکل زیر را به‌خود می‌گیرد :

$$\sum_{n\le x}a(n)f(n)=A(x)f(x)-\int_1^x A(t)f'(t)\,dt. \tag{۵}$$

همچنین ، باید توجه داشت که فرمول جمعبندی اویلر را می‌توان به‌آسانی از (۴) بدست‌آورد. درواقع ، اگر به‌ازای هر $n\ge 1$ ، $a(n)=1$ ، معلوم می‌شود که $A(x)=[x]$ و (۴) ایجاب می‌کند که

$$\sum_{y<n\le x}f(n)=f(x)[x]-f(y)[y]-\int_y^x [t]f'(t)\,dt.$$

اگر این فرمول را با فرمول‌انتگرالگیری به طریقهٔ جزء به‌جزء

$$\int_y^x tf'(t)\,dt=xf(x)-yf(y)-\int_y^x f(t)\,dt$$

---

1. Stieltjes

تلفیق کنیم ، فوراً فرمول جمعبندی اویلر (قضیهٔ ۱۰۳) بدست خواهد آمد .

حال ، با استفاده از (۴) ، $\vartheta(x)$ و $\pi(x)$ را برحسب انتگرالها بیان می‌کنیم :

قضیهٔ ۳۰۴ . به‌ازای $x \geq 2$ ، داریم

$$\vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}\,dt \tag{۶}$$

و

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t\log^2 t}\,dt. \tag{۷}$$

برهان . فرض کنیم $a(n)$ تابع مشخص اعداد اول باشد ؛ یعنی ،

$$a(n) = \begin{cases} 1 & \text{اگر } n \text{ اول باشد ،} \\ 0 & \text{درغیر این‌صورت ،} \end{cases}$$

دراین‌صورت ، داریم

$$\pi(x) = \sum_{p \leq x} 1 = \sum_{1 < n \leq x} a(n) \quad \text{و} \quad \vartheta(x) = \sum_{p \leq x} \log p = \sum_{1 < n \leq x} a(n)\log n \ .$$

با اختیار $f(x) = \log x$ در (۴) و $y = 1$ ، داریم

$$\vartheta(x) = \sum_{1 < n \leq x} a(n)\log n = \pi(x)\log x - \pi(1)\log 1 - \int_1^x \frac{\pi(t)}{t}\,dt,$$

که (۶) را ثابت می‌کند زیرا ، به‌ازای $t < 2$ ، $\pi(t) = 0$.

حال فرض می‌کنیم $b(n) = a(n)\log n$ و می‌نویسیم

$$\pi(x) = \sum_{3/2 < n \leq x} b(n)\frac{1}{\log n}, \qquad \vartheta(x) = \sum_{n \leq x} b(n).$$

با اختیار $f(x) = 1/\log x$ در (۴) و $y = 3/2$ ، خواهیم داشت

$$\pi(x) = \frac{\vartheta(x)}{\log x} - \frac{\vartheta(3/2)}{\log 3/2} + \int_{3/2}^x \frac{\vartheta(t)}{t\log^2 t}\,dt,$$

که (۷) را ثابت می‌کند زیرا ، اگر $t < 2$ ، $\vartheta(t) = 0$.

۴۰۴ شکلهای معادل قضیهٔ اعداد اول

قضیهٔ ۴.۴ . روابط زیر از حیث منطقی معادل‌اند :

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1; \tag{۸}$$

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1; \tag{۹}$$

$$\lim_{x\to\infty} \frac{\psi(x)}{x} = 1; \tag{۱۰}$$

برهان . از (۶) و (۷) بترتیب داریم

$$\frac{\vartheta(x)}{x} = \frac{\pi(x)\log x}{x} - \frac{1}{x}\int_2^x \frac{\pi(t)}{t}\,dt$$

و

$$\frac{\pi(x)\log x}{x} = \frac{\vartheta(x)}{x} + \frac{\log x}{x}\int_2^x \frac{\vartheta(t)\,dt}{t\log^2 t}.$$

برای اثبات اینکه (۸) رابطهٔ (۹) را ایجاب می‌کند ، فقط کافی است نشان دهیم که از (۸)

$$\lim_{x\to\infty} \frac{1}{x}\int_2^x \frac{\pi(t)}{t}\,dt = 0$$

نتیجه می‌شود . اما (۸) ایجاب می‌کندکه ، به‌ازای $t \geq 2$ ، $\frac{\pi(t)}{t} = O\left(\frac{1}{\log t}\right)$ ؛ درنتیجه ،

$$\frac{1}{x}\int_2^x \frac{\pi(t)}{t}\,dt = O\left(\frac{1}{x}\int_2^x \frac{dt}{\log t}\right).$$

اما

$$\int_2^x \frac{dt}{\log t} = \int_2^{\sqrt{x}} \frac{dt}{\log t} + \int_{\sqrt{x}}^x \frac{dt}{\log t} \leq \frac{\sqrt{x}}{\log 2} + \frac{x-\sqrt{x}}{\log\sqrt{x}}\ ;$$

درنتیجه ،

وقتی $x \to \infty$ ، $\frac{1}{x}\int_2^x \frac{dt}{\log t} \to 0$.

این نشان می‌دهد که (۸) رابطهٔ (۹) را ایجاب می‌کند .

برای اثبات اینکه (۹) رابطهٔ (۸) را ایجاب می‌کند ، فقط کافی است نشان دهیم

که از (۹)

$$\lim_{x\to\infty} \frac{\log x}{x} \int_2^x \frac{\vartheta(t)\, dt}{t \log^2 t} = 0$$

نتیجه می‌شود. اما (۹) ایجاب می‌کند که $\vartheta(t) = O(t)$؛ درنتیجه،

$$\frac{\log x}{x} \int_2^x \frac{\vartheta(t)\, dt}{t \log^2 t} = O\left(\frac{\log x}{x} \int_2^x \frac{dt}{\log^2 t}\right).$$

اما

$$\int_2^x \frac{dt}{\log^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} \leq \frac{\sqrt{x}}{\log^2 2} + \frac{x - \sqrt{x}}{\log^2 \sqrt{x}}.$$

بنابراین،

وقتی $x \to \infty$، $\frac{\log x}{x} \int_2^x \frac{dt}{\log^2 t} \to 0$.

این ثابت می‌کند که (۹) رابطهٔ (۸) را ایجاب می‌کند؛ درنتیجه، (۸) و (۹) معادل می‌باشند. ما از قبل (از قضیهٔ ۴.۱) می‌دانیم که (۹) و (۱۰) معادل می‌باشند.

قضیهٔ زیر قضیهٔ اعداد اول را به‌مقدار مجانبی n مین عدد اول مربوط می‌کند.

قضیهٔ ۴.۵. فرض‌کنیم p_n، n مین عدد اول باشد. دراین صورت، روابط مجانبی زیر منطقاً" معادل‌اند:

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1; \tag{۱۱}$$

$$\lim_{x\to\infty} \frac{\pi(x)\log \pi(x)}{x} = 1; \tag{۱۲}$$

$$\lim_{n\to\infty} \frac{p_n}{n \log n} = 1. \tag{۱۳}$$

برهان. نشان می‌دهیم که (۱۱) رابطهٔ (۱۲)، (۱۲) رابطهٔ (۱۳)، (۱۳) رابطهٔ (۱۲)، و (۱۲) رابطهٔ (۱۱) را ایجاب می‌کند.

فرض‌کنیم (۱۱) برقرار باشد. با گرفتن لگاریتم، داریم

$$\lim_{x\to\infty} [\log \pi(x) + \log\log x - \log x] = 0$$

یا

$$\lim_{x\to\infty}\left[\log x\left(\frac{\log \pi(x)}{\log x}+\frac{\log\log x}{\log x}-1\right)\right]=0.$$

چون، وقتی $x \to \infty$، $\log x \to \infty$، نتیجه می‌شود که

$$\lim_{x\to\infty}\left(\frac{\log \pi(x)}{\log x}+\frac{\log\log x}{\log x}-1\right)=0\ ,$$

که از آن خواهیم داشت

$$\lim_{x\to\infty}\frac{\log \pi(x)}{\log x}=1.$$

این، همراه با (۱۱)، (۱۲) را نتیجه می‌دهد.

حال فرض کنیم (۱۲) برقرار باشد. هرگاه $x = p_n$، آنگاه $\pi(x) = n$ و

$$\pi(x)\log \pi(x) = n \log n;$$

درنتیجه، (۱۲) ایجاب می‌کند که

$$\lim_{n\to\infty}\frac{n\log n}{p_n}=1.$$

بنابراین، (۱۲) رابطهٔ (۱۳) را ایجاب می‌کند.

حال فرض کنیم (۱۳) برقرار باشد. با معلوم بودن x، n را با نامساویهای

$$p_n \leq x < p_{n+1}$$

تعریف می‌کنیم؛ درنتیجه، $n = \pi(x)$. با تقسیم بر $n \log n$، داریم

$$\frac{p_n}{n\log n}\leq\frac{x}{n\log n}<\frac{p_{n+1}}{n\log n}=\frac{p_{n+1}}{(n+1)\log(n+1)}\frac{(n+1)\log(n+1)}{n\log n}.$$

حال، با فرض $n\to\infty$ و استفاده از (۱۳)، خواهیم داشت

$$\lim_{n\to\infty}\frac{x}{n\log n}=1 \quad \text{یا} \quad \lim_{x\to\infty}\frac{x}{\pi(x)\log \pi(x)}=1\ .$$

بنابراین، (۱۳) رابطهٔ (۱۲) را ایجاب خواهد کرد.

بالاخره، نشان می‌دهیم که (۱۲) رابطهٔ (۱۱) را ایجاب می‌کند. اگر در (۱۲) لگاریتم بگیریم، داریم

$$\lim_{x\to\infty}(\log \pi(x) + \log\log \pi(x) - \log x) = 0$$

یا

$$\lim_{x\to\infty}\left[\log \pi(x)\left(1+\frac{\log\log \pi(x)}{\log \pi(x)}-\frac{\log x}{\log \pi(x)}\right)\right]=0.$$

چون $\log \pi(x) \to \infty$ ، نتیجه می‌شود که

$$\lim_{x\to\infty}\left(1+\frac{\log\log \pi(x)}{\log \pi(x)}-\frac{\log x}{\log \pi(x)}\right)=0$$

یا

$$\lim_{x\to\infty}\frac{\log x}{\log \pi(x)}=1.$$

این ، همراه با (۱۲) ، رابطهٔ (۱۱) را نتیجه خواهد داد .

۵.۴ نامساویهای مربوط به $\pi(n)$ و p_n

قضیهٔ اعداداول می‌گوید که ، وقتی $n \to \infty$ ، $\pi(n) \sim n/\log n$. نامساویهای قضیهٔ بعدی نشان‌می‌دهندکه $n/\log n$ مرتبهٔ دقیق‌اندازهٔ $\pi(n)$ است .اگرچه با سعی بیشترنامساویهای بهتری‌بدست می‌آیند (ر.ک. [۶۰]) ، قضیهٔ زیر بخاطر سرشت مقدماتی برهانش مورد توجه است .

قضیهٔ ۶.۴ . به‌ازای هر عدد صحیح $n \geq 2$ ، داریم

$$\frac{1}{6}\frac{n}{\log n} < \pi(n) < 6\frac{n}{\log n}. \tag{۱۴}$$

برهان. با نامساویهای

$$2^n \leq \binom{2n}{n} < 4^n \tag{۱۵}$$

شروع می‌کنیم ، که درآنها $\binom{2n}{n}=\frac{(2n)!}{n!n!}$ یک ضریب دوجمله‌ای است . نامساوی طرف راست از رابطهٔ

$$4^n=(1+1)^{2n}=\sum_{k=0}^{2n}\binom{2n}{k}>\binom{2n}{n},$$

و نامساوی‌دیگربه‌آسانی‌به‌استقرا ثابت می‌شود . با گرفتن لگاریتم در (۱۵) ، درمی‌یابیم که

$$n \log 2 \le \log(2n)! - 2\log n! < n \log 4. \tag{۱۶}$$

اما قضیهٔ ۱۴.۳ ایجاب می‌کند که

$$\log n! = \sum_{p \le n} \alpha(p) \log p$$

که درآن مجموع روی اعداد اول گرفته شده است و $\alpha(p)$ از رابطهٔ زیر بدست می‌آید :

$$\alpha(p) = \sum_{m=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^m}\right].$$

بنابراین،

$$\log(2n)! - 2\log n! = \sum_{p \le 2n} \sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} \left\{\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right]\right\} \log p. \tag{۱۷}$$

چون $[2x] - 2[x]$ مساوی 0 یا 1 است ،نامساوی سمت چپ در (۱۶) ایجاب می‌کندکه

$$n \log 2 \le \sum_{p \le 2n} \left(\sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} 1\right) \log p \le \sum_{p \le 2n} \log 2n = \pi(2n) \log 2n.$$

این نتیجه می‌دهد که

$$\pi(2n) \ge \frac{n \log 2}{\log 2n} = \frac{2n}{\log 2n} \frac{\log 2}{2} > \frac{1}{4} \frac{2n}{\log 2n} \tag{۱۸}$$

زیرا $\log 2 > 1/2$. برای اعداد صحیح فرد داریم

$$\pi(2n+1) \ge \pi(2n) > \frac{1}{4}\frac{2n}{\log 2n} > \frac{1}{4}\frac{2n}{2n+1}\frac{2n+1}{\log(2n+1)} \ge \frac{1}{6}\frac{2n+1}{\log(2n+1)}$$

زیرا $2n/(2n+1) \ge 2/3$. این ،همراه‌با (۱۸) ، نتیجه می‌دهد که ، به‌ازای هر $n \ge 2$ ،

$$\pi(n) > \frac{1}{6}\frac{n}{\log n}$$

که نامساوی سمت چپ در (۱۴) را ثابت می‌کند .

برای اثبات نامساوی دیگر ، به (۱۷) باز می‌گردیم و جملهٔ نظیر به $m = 1$ را جدا می‌کنیم . بقیهٔ جملات نامنفی‌اند؛ درنتیجه ، داریم

$$\log(2n)! - 2\log n! \ge \sum_{p \le 2n} \left\{\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right\} \log p.$$

به‌ازای p های اول در بازهٔ $n < p \le 2n$ ، داریم $[2n/p] - 2[n/p] = 1$ ؛ درنتیجه ،

$$\log(2n)! - 2\log n! \ge \sum_{n<p\le 2n} \log p = \vartheta(2n) - \vartheta(n).$$

بنابراین ، (۱۶) ایجاب می‌کند که

$$\vartheta(2n) - \vartheta(n) < n \log 4.$$

بخصوص، اگر n توانی از 2 باشد ، این نتیجه می‌دهد که

$$\vartheta(2^{r+1}) - \vartheta(2^r) < 2^r \log 4 = 2^{r+1} \log 2.$$

با جمعبندی روی $r = 0, 1, 2, \ldots, k$ ، مجموع سمت چپ توی هم می‌رود و خواهیم داشت

$$\vartheta(2^{k+1}) < 2^{k+2} \log 2.$$

حال k را طوری اختیار می‌کنیم که $2^k \le n < 2^{k+1}$ و بدست می‌آوریم

$$\vartheta(n) \le \vartheta(2^{k+1}) < 2^{k+2} \log 2 \le 4n \log 2.$$

اما ، اگر $1 > \alpha > 0$ ، داریم

$$(\pi(n) - \pi(n^\alpha))\log n^\alpha < \sum_{n^\alpha < p \le n} \log p \le \vartheta(n) < 4n \log 2;$$

درنتیجه ،

$$\pi(n) < \frac{4n \log 2}{\alpha \log n} + \pi(n^\alpha) < \frac{4n \log 2}{\alpha \log n} + n^\alpha$$
$$= \frac{n}{\log n}\left(\frac{4 \log 2}{\alpha} + \frac{\log n}{n^{1-\alpha}}\right).$$

حال ،اگر $c > 0$ و $x \ge 1$ ، تابع $f(x) = x^{-c} \log x$ در $x = e^{1/c}$ به‌ماکزیمم خودمی‌رسد ؛ درنتیجه ، به‌ازای $n \ge 1$ ، $n^{-c} \log n \le 1/(ce)$. با فرض $\alpha = 2/3$ در آخرین نامساوی برای $\pi(n)$ ، درمی‌یابیم که

$$\pi(n) < \frac{n}{\log n}\left(6 \log 2 + \frac{3}{e}\right) < 6 \frac{n}{\log n}.$$

این برهان را تمام خواهد کرد .

با استفاده از قضیهٔ ۶.۴ ، می‌توان برای اندازهٔ n مین عدد اول کرانهای بالایی و پایینی بدست آورد :

قضیهٔ ۷.۴ . به‌ازای $n \ge 1$ ، n مین عدد اول p_n در نامساویهای زیر صدق می‌کند :

$$\frac{1}{6} n \log n < p_n < 12\left(n \log n + n \log \frac{12}{e}\right). \tag{۱۹}$$

برهان. هرگاه $k = p_n$، آنگاه $k \geq 2$ و $n = \pi(k)$. از (۱۴) داریم

$$n = \pi(k) < 6 \frac{k}{\log k} = 6 \frac{p_n}{\log p_n};$$

درنتیجه،

$$p_n > \frac{1}{6} n \log p_n > \frac{1}{6} n \log n.$$

این کران پایینی در (۱۹) را بدست می‌دهد.

برای یافتن کران بالایی، مجددا" از (۱۴) استفاده کرده می‌نویسیم

$$n = \pi(k) > \frac{1}{6} \frac{k}{\log k} = \frac{1}{6} \frac{p_n}{\log p_n},$$

که از آن درمی‌یابیم که

$$p_n < 6n \log p_n. \tag{۲۰}$$

چون‌به‌ازای $x \geq 1$، $\log x \leq (2/e)\sqrt{x}$، داریم $\log p_n \leq (2/e)\sqrt{p_n}$؛ درنتیجه، (۲۰) ایجاب می‌کند که

$$\sqrt{p_n} < \frac{12}{e} n.$$

بنابراین،

$$\frac{1}{2} \log p_n < \log n + \log \frac{12}{e}$$

که از آن، با استفاده از (۲۰)، نتیجه می‌شود که

$$p_n < 6n\left(2 \log n + 2 \log \frac{12}{e}\right).$$

این کران بالایی در (۱۹) را ثابت می‌کند.

تذکر. کران بالایی در (۱۹) بی‌درنگ نشان می‌دهد که سری

$$\sum_{n=1}^{\infty} \frac{1}{p_n},$$

به‌وسیلهٔ مقایسه با $\sum_{n=2}^{\infty} 1/(n \log n)$، واگراست.

۶.۴ قضیهٔ تاوبری شاپیرو[1]

نشان دادیم که قضیهٔ اعداد اول با فرمول مجانبی زیر معادل است:

$$\text{وقتی}\ x \to \infty \text{ ،} \quad \frac{1}{x}\sum_{n \le x} \Lambda(n) \sim 1 \text{ .} \tag{۲۱}$$

در قضیهٔ ۱۵.۳ فرمول مجانبی مربوطهٔ زیر را بدست آوردیم:

$$\sum_{n \le x} \Lambda(n)\left[\frac{x}{n}\right] = x \log x - x + O(\log x). \tag{۲۲}$$

هر دو مجموع در (۲۱) و (۲۲) متوسطهای وزندار تابع $\Lambda(n)$ اند. هر جملهٔ $\Lambda(n)$ در (۲۱) در عامل وزندار $1/x$ و در (۲۲) در $[x/n]$ ضرب شده است.

قضایایی که متوسطهای وزندار مختلف یک تابع را بهم مربوط می‌کنند *قضایای تاوبری* نامیده می‌شوند. حال به یک قضیهٔ تاوبری می‌پردازیم که در ۱۹۵۰ به‌وسیلهٔ اچ. ان. شاپیرو [۶۴] ثابت شد. این قضیه مجموعهای به شکل $\sum_{n \le x} a(n)$ را به مجموعهای به‌شکل $\sum_{n \le x} a(n)[x/n]$ به‌ازای $a(n)$های نامنفی مربوط می‌کند.

قضیهٔ ۸.۴ . فرض کنیم $\{a(n)\}$ یک دنبالهٔ نامنفی باشد بطوری که

$$\text{به‌ازای هر}\ x \ge 1 \text{ ،} \quad \sum_{n \le x} a(n)\left[\frac{x}{n}\right] = x \log x + O(x) \text{ .} \tag{۲۳}$$

در این صورت،

(آ) به‌ازای $x \ge 1$ ، داریم

$$\sum_{n \le x} \frac{a(n)}{n} = \log x + O(1);$$

(به‌عبارت دیگر، حذف کروشه‌ها در (۲۳) نتیجهٔ صحیحی بدست می‌دهد)؛

(ب) ثابتی مانند $B > 0$ وجود دارد بطوری که

$$\text{به‌ازای هر}\ x \ge 1 \text{ ،} \quad \sum_{n \le x} a(n) \le Bx \text{ ؛}$$

(پ) ثابتی مانند $A > 0$ و $x_0 > 0$ وجود دارند بطوری که

$$\text{به‌ازای}\ x \ge x_0 \text{ ،} \quad \sum_{n \le x} a(n) \ge Ax \text{ .}$$

برهان. فرض می‌کنیم

---

1. Shapiro

$$S(x) = \sum_{n \le x} a(n), \qquad T(x) = \sum_{n \le x} a(n)\left[\frac{x}{n}\right].$$

ابتدا (ب) را ثابت می‌کنیم. برای این‌کار، نامساوی

$$S(x) - S\left(\frac{x}{2}\right) \le T(x) - 2T\left(\frac{x}{2}\right) \tag{۲۴}$$

را ثابت می‌کنیم. می‌نویسیم

$$\begin{aligned} T(x) - 2T\left(\frac{x}{2}\right) &= \sum_{n \le x}\left[\frac{x}{n}\right]a(n) - 2\sum_{n \le x/2}\left[\frac{x}{2n}\right]a(n) \\ &= \sum_{n \le x/2}\left(\left[\frac{x}{n}\right] - 2\left[\frac{x}{2n}\right]\right)a(n) + \sum_{x/2 < n \le x}\left[\frac{x}{n}\right]a(n). \end{aligned}$$

چون $[2y] - 2[y]$ مساوی 0 یا 1 است، اولین مجموع نامنفی است؛ درنتیجه،

$$T(x) - 2T\left(\frac{x}{2}\right) \ge \sum_{x/2 < n \le x}\left[\frac{x}{n}\right]a(n) = \sum_{x/2 < n \le x} a(n) = S(x) - S\left(\frac{x}{2}\right).$$

این (۲۴) را ثابت می‌کند. اما (۲۳) ایجاب می‌کند که

$$T(x) - 2T\left(\frac{x}{2}\right) = x\log x + O(x) - 2\left(\frac{x}{2}\log\frac{x}{2} + O(x)\right) = O(x).$$

بنابراین، (۲۴) نتیجه می‌دهد که $S(x) - S(x/2) = O(x)$. این یعنی ثابتی مانند $K > 0$ هست بطوری که

$$\text{به‌ازای هر } x \ge 1 \text{ ،} \quad S(x) - S\left(\frac{x}{2}\right) \le Kx.$$

اگر x را بترتیب با $x/2, x/4, \ldots$ عوض کنیم، بدست می‌آید

$$S\left(\frac{x}{2}\right) - S\left(\frac{x}{4}\right) \le K\frac{x}{2},$$
$$S\left(\frac{x}{4}\right) - S\left(\frac{x}{8}\right) \le K\frac{x}{4},$$

و غیره. توجه کنید که وقتی $2^n > x$، $S(x/2^n) = 0$. با افزودن این نامساویها بهم، داریم

$$S(x) \le Kx\left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right) = 2Kx.$$

این (ب) را به‌ازای $B = 2K$ ثابت می‌کند.

حال (آ) را ثابت‌می‌کنیم. می‌نویسیم $[x/n] = (x/n) + O(1)$ و، بنابر قسمت (ب)، بدست می‌آوریم

$$T(x) = \sum_{n \le x} \left[\frac{x}{n}\right] a(n) = \sum_{n \le x} \left(\frac{x}{n} + O(1)\right) a(n) = x \sum_{n \le x} \frac{a(n)}{n} + O\left(\sum_{n \le x} a(n)\right)$$
$$= x \sum_{n \le x} \frac{a(n)}{n} + O(x).$$

درنتیجه،

$$\sum_{n \le x} \frac{a(n)}{n} = \frac{1}{x} T(x) + O(1) = \log x + O(1).$$

این (آ) را ثابت می‌کند.

بالاخره، (پ) را ثابت می‌کنیم. فرض کنیم

$$A(x) = \sum_{n \le x} \frac{a(n)}{n}.$$

دراین صورت، (آ) را می‌توان به‌صورت زیر نوشت:

$$A(x) = \log x + R(x),$$

که درآن $R(x)$ جملهٔ خطا می‌باشد. چون $R(x) = O(1)$، به‌ازای یک $M > 0$ داریم $|R(x)| \le M$.

α را با خاصیت $0 < \alpha < 1$ اختیار می‌کنیم (α لحظه‌ای دیگر دقیقتر مشخص می‌شود) و تفاضل

$$A(x) - A(\alpha x) = \sum_{\alpha x < n \le x} \frac{a(n)}{n} = \sum_{n \le x} \frac{a(n)}{n} - \sum_{n \le \alpha x} \frac{a(n)}{n}$$

را درنظرمی‌گیریم. اگر $x \ge 1$ و $\alpha x \ge 1$، می‌توان فرمول مجانبی مربوط به $A(x)$ را بکار برد و نوشت

$$\begin{aligned} A(x) - A(\alpha x) &= \log x + R(x) - (\log \alpha x + R(\alpha x)) \\ &= -\log \alpha + R(x) - R(\alpha x) \\ &\ge -\log \alpha - |R(x)| - |R(\alpha x)| \ge -\log \alpha - 2M. \end{aligned}$$

حال α را طوری اختیار می‌کنیم که $-\log \alpha - 2M = 1$. برای این‌کار باید $\log \alpha = -2M - 1$، یا $\alpha = e^{-2M-1}$. توجه کنید که $0 < \alpha < 1$. برای این α نامساوی زیر را داریم:

اگر $x \ge 1/\alpha$، $A(x) - A(\alpha x) \ge 1$.

اما

$$A(x) - A(\alpha x) = \sum_{\alpha x < n \le x} \frac{a(n)}{n} \le \frac{1}{\alpha x} \sum_{n \le x} a(n) = \frac{S(x)}{\alpha x}.$$

درنتیجه،

اگر $x \ge 1/\alpha$ ، $\frac{S(x)}{\alpha x} \ge 1$.

بنابراین، اگر $x \ge 1/\alpha$ ، $S(x) \ge \alpha x$ ، که (پ) را به‌ازای $A = \alpha$ و $x_0 = 1/\alpha$ ثابت می‌کند .

۷.۴ کاربردهای قضیهٔ شاپیرو

معادلهٔ (۲۲) ایجاب می‌کند که

$$\sum_{n \le x} \Lambda(n) \left[\frac{x}{n}\right] = x \log x + O(x).$$

چون $\Lambda(n) \ge 0$ ، می‌توان با اعمال قضیهٔ شاپیرو به‌ازای $a(n) = \Lambda(n)$ قضیهٔ زیر را بدست‌آورد :

قضیهٔ ۹.۴ . *به‌ازای هر $x \ge 1$ ، داریم*

$$\sum_{n \le x} \frac{\Lambda(n)}{n} = \log x + O(1). \qquad (۲۵)$$

همچنین، ثابتهای مثبتی چون c_1 و c_2 وجود دارند بطوری که

به‌ازای هر $x \ge 1$ ، $\psi(x) \le c_1 x$

و

به‌ازای x های به‌قدر کافی بزرگ، $\psi(x) \ge c_2 x$.

کاربرد دیگر را می‌توان از فرمول مجانبی

$$\sum_{p \le x} \left[\frac{x}{p}\right] \log p = x \log x + O(x) ,$$

که در قضیهٔ ۱۶.۳ ثابت شد، بدست آورد . این فرمول را می‌توان به‌شکل زیر نوشت :

$$\sum_{n \le x} \Lambda_1(n) \left[\frac{x}{n}\right] = x \log x + O(x), \qquad (۲۶)$$

که درآن Λ_1 تابعی است که به‌صورت زیر تعریف می‌شود :

$$\Lambda_1(n) = \begin{cases} \log p & \text{اگر } n \text{ عدد اول } p \text{ باشد،} \\ 0 & \text{درغیر اینصورت،} \end{cases}$$

چون $\Lambda_1(n) \geq 0$ ، معادلهٔ (۲۶) نشان‌می‌دهدکه‌فرض‌قضیهٔ شاپیروبه‌ازای $a(n) = \Lambda_1(n)$ برقرار است. چون $\vartheta(x) = \sum_{n \leq x} \Lambda_1(n)$ ، قسمت (آ) قضیهٔ شاپیرو فرمول مجانبی زیر را به‌ما می‌دهد.

قضیهٔ ۱۰.۴ . به‌ازای هر $x \geq 1$ ، داریم

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1). \qquad (۲۷)$$

همچنین، ثابتهایی مانند c_1 و c_2 وجود دارند بطوری که

به‌ازای هر $x \geq 1$ ، $\vartheta(x) \leq c_1 x$

و

به‌ازای x های به‌قدر کافی بزرگ، $\vartheta(x) \geq c_2 x$.

در قضیهٔ ۱۱.۳ ثابت شد که به‌ازای هر تابع حسابی $f(n)$ با مجموعهای جزئی $F(x) = \sum_{n \leq x} f(n)$ ،

$$\sum_{n \leq x} f(n)\left[\frac{x}{n}\right] = \sum_{n \leq x} F\left(\frac{x}{n}\right):$$

چون $\psi(x) = \sum_{n \leq x} \Lambda(n)$ و $\vartheta(x) = \sum_{n \leq x} \Lambda_1(n)$ ، فرمولهای مجانبی در (۲۲) و (۲۶) را می‌توان مستقیما" برحسب $\psi(x)$ و $\vartheta(x)$ بیان کرد. این امر را در یک قضیهٔ صوری بیان می‌کنیم:

قضیهٔ ۱۱.۴ . به‌ازای هر $x \geq 1$ ، داریم

$$\sum_{n \leq x} \psi\left(\frac{x}{n}\right) = x \log x - x + O(\log x) \qquad (۲۸)$$

و

$$\sum_{n \leq x} \vartheta\left(\frac{x}{n}\right) = x \log x + O(x).$$

۸.۴ یک فرمول مجانبی برای مجموعهای جزئی $\sum_{p \leq x} (1/p)$

در فصل ۱ ثابت شد که سری $\sum(1/p)$ واگراست. حال برای مجموعهای جزئی آن یک‌فرمول مجانبی بدست می‌آوریم. این نتیجه کاربردی است از قضیهٔ ۱۰.۴، معادلهٔ (۲۷).

قضیهٔ ۱۲.۴ . ثابتی مانند A هست بطوری که

به‌ازای هر $x \geq 2$، $\sum_{p \leq x} \frac{1}{p} = \log\log x + A + O\left(\frac{1}{\log x}\right)$. (۲۹)

برهان. فرض کنیم

$$A(x) = \sum_{p \leq x} \frac{\log p}{p}$$

و

$$a(n) = \begin{cases} 1 & \text{اگر } n \text{ اول باشد،} \\ 0 & \text{درغیر این‌صورت،} \end{cases}$$

دراین صورت،

$$\sum_{p \leq x} \frac{1}{p} = \sum_{n \leq x} \frac{a(n)}{n} \quad \text{و} \quad A(x) = \sum_{n \leq x} \frac{a(n)}{n} \log n\ .$$

بنابراین، با فرض $f(t) = 1/\log t$ در قضیهٔ ۲.۴ معلوم می‌شود که، چون به‌ازای $t < 2$، $A(t) = 0$،

$$\sum_{p \leq x} \frac{1}{p} = \frac{A(x)}{\log x} + \int_2^x \frac{A(t)}{t \log^2 t}\, dt. \tag{۳۰}$$

از (۲۷) داریم $A(x) = \log x + R(x)$، که درآن $R(x) = O(1)$. با استفاده از این در طرف راست (۳۰)، درمی‌یابیم که

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} &= \frac{\log x + O(1)}{\log x} + \int_2^x \frac{\log t + R(t)}{t \log^2 t}\, dt \\ &= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{dt}{t \log t} + \int_2^x \frac{R(t)}{t \log^2 t}\, dt. \end{aligned} \tag{۳۱}$$

اما

$$\int_2^x \frac{dt}{t \log t} = \log\log x - \log\log 2$$

و

$$\int_2^x \frac{R(t)}{t\log^2 t}\,dt = \int_2^\infty \frac{R(t)}{t\log^2 t}\,dt - \int_x^\infty \frac{R(t)}{t\log^2 t}\,dt,$$

وجود انتگرال مجازی را شرط $R(t) = O(1)$ تضمین می‌کند. اما

$$\int_x^\infty \frac{R(t)}{t\log^2 t}\,dt = O\left(\int_x^\infty \frac{dt}{t\log^2 t}\right) = O\left(\frac{1}{\log x}\right).$$

درنتیجه، معادلهٔ (۳۱) را می‌توان به‌صورت زیر نوشت:

$$\sum_{p\le x} \frac{1}{p} = \log\log x + 1 - \log\log 2 + \int_2^\infty \frac{R(t)}{t\log^2 t}\,dt + O\left(\frac{1}{\log x}\right).$$

این قضیه را به‌ازای

$$A = 1 - \log\log 2 + \int_2^\infty \frac{R(t)}{t\log^2 t}\,dt$$

ثابت خواهد کرد.

۹.۴ مجموعه‌های جزئی تابع موبیوس

تعریف. اگر $x \ge 1$، تعریف می‌کنیم

$$M(x) = \sum_{n\le x} \mu(n).$$

مرتبهٔ دقیق اندازهٔ $M(x)$ معلوم نیست. شواهد عددی القا می‌کنند که اگر $x > 1$، $|M(x)| < \sqrt{x}$؛
اما این نامساوی، مشهور به حدس مرتنس[1]، نه اثبات‌شده است نه انکار. بهترین نتیجهٔ O ای که تا امروز بدست آمده عبارت است از

$$M(x) = O(x\delta(x))$$

که درآن به‌ازای ثابت مثبتی چون A، $\delta(x) = \exp\{-A\log^{3/5} x(\log\log x)^{-1/5}\}$. (برهانی در والفیس[2] [۷۵] داده شده است.)

دراین بخش حکم ضعیفتر

$$\lim_{x\to\infty} \frac{M(x)}{x} = 0$$

را ثابت می‌کنیم، که معادل قضیهٔ اعداد اول است. ابتدا $M(x)$ را به متوسط وزندار

1. Mertens 2. Walfisz

$\mu(n)$ مربوط می‌کنیم .

تعریف . اگر $x \geq 1$ ، تعریف می‌کنیم

$$H(x) = \sum_{n \leq x} \mu(n) \log n.$$

قضیهٔ زیر نشان می‌دهد که رفتار $M(x)/x$ به وسیلهٔ رفتار $H(x)/(x \log x)$ مشخص می‌شود .

قضیهٔ ۱۳.۴ . داریم

$$\lim_{x \to \infty} \left(\frac{M(x)}{x} - \frac{H(x)}{x \log x} \right) = 0. \qquad (۳۲)$$

برهان . با فرض $f(t) = \log t$ در قضیهٔ ۲.۴ ، بدست می‌آوریم

$$H(x) = \sum_{n \leq x} \mu(n) \log n = M(x) \log x - \int_1^x \frac{M(t)}{t}\, dt.$$

درنتیجه ، اگر $x > 1$ ، داریم

$$\frac{M(x)}{x} - \frac{H(x)}{x \log x} = \frac{1}{x \log x} \int_1^x \frac{M(t)}{t}\, dt.$$

بنابراین ، برای اثبات قضیه باید نشان دهیم که

$$\lim_{x \to \infty} \frac{1}{x \log x} \int_1^x \frac{M(t)}{t}\, dt = 0. \qquad (۳۳)$$

اما تخمین بدیهی $M(x) = O(x)$ را داریم ؛ درنتیجه ،

$$\int_1^x \frac{M(t)}{t}\, dt = O\left(\int_1^x dt \right) = O(x),$$

که از آن (۳۳) ، و درنتیجه (۳۲) ، را خواهیم داشت .

قضیهٔ ۱۴.۴ . *قضیهٔ اعداد اول ایجاب می‌کند که*

$$\lim_{x \to \infty} \frac{M(x)}{x} = 0.$$

برهان. از قضیهٔ اعداد اول به شکل $\psi(x) \sim x$ استفاده کرده، ثابت می‌کنیم وقتی $x \to \infty$ ، $H(x)/(x \log x) \to 0$. برای این‌کار به اتحاد زیر نیاز داریم :

$$-H(x) = -\sum_{n \le x} \mu(n) \log n = \sum_{n \le x} \mu(n) \psi\left(\frac{x}{n}\right). \tag{۳۴}$$

برای اثبات (۳۴) با قضیهٔ ۱۱.۰۲ شروع می‌کنیم ، که می‌گوید

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d$$

و با اعمال انعکاس موبیوس بدست می‌آوریم

$$-\mu(n) \log n = \sum_{d|n} \mu(d) \Lambda\left(\frac{n}{d}\right).$$

با جمعبندی روی تمام $n \le x$ های و استفاده از قضیهٔ ۱۰.۳ به‌ازای $f = \mu, g = \Lambda$ ، (۳۴) را خواهیم داشت.

چون $\psi(x) \sim x$ ، اگر $\varepsilon > 0$ مفروض باشد ، ثابتی چون $A > 0$ وجود دارد بطوری کــه

$$\text{به‌ازای } x \ge A \text{ ،} \quad \left|\frac{\psi(x)}{x} - 1\right| < \varepsilon \text{ .}$$

به عبارت دیگر،

$$\text{به‌ازای } x \ge A \text{ ،} \quad |\psi(x) - x| < \varepsilon x \text{ .} \tag{۳۵}$$

$x > A$ را اختیار کرده و مجموع سمت راست (۳۴) را به‌دو قسمت تجزیه می‌کنیم :

$$\sum_{n \le y} + \sum_{y < n \le x},$$

که در آن $y = [x/A]$. در مجموع اول داریم $n \le y$ ؛ درنتیجه، $n \le x/A$ ؛ و لذا، $x/n \ge A$. از اینرو، می‌توان با استفاده از (۳۵) نوشت :

$$\text{اگر } n \le y \text{ ،} \quad \left|\psi\left(\frac{x}{n}\right) - \frac{x}{n}\right| < \varepsilon \frac{x}{n} \text{ .}$$

بنابراین،

$$\sum_{n \le y} \mu(n) \psi\left(\frac{x}{n}\right) = \sum_{n \le y} \mu(n)\left(\frac{x}{n} + \psi\left(\frac{x}{n}\right) - \frac{x}{n}\right)$$
$$= x \sum_{n \le y} \frac{\mu(n)}{n} + \sum_{n \le y} \mu(n)\left(\psi\left(\frac{x}{n}\right) - \frac{x}{n}\right);$$

درنتیجه،

$$\left|\sum_{n\le y}\mu(n)\psi\left(\frac{x}{n}\right)\right| \le x\left|\sum_{n\le y}\frac{\mu(n)}{n}\right| + \sum_{n\le y}\left|\psi\left(\frac{x}{n}\right)-\frac{x}{n}\right|$$
$$< x+\varepsilon\sum_{n\le y}\frac{x}{n} < x+\varepsilon x(1+\log y)$$
$$< x+\varepsilon x+\varepsilon x\log x.$$

درمجموع دوم داریم $y < n \le x$ ؛ درنتیجه، $n \ge y+1$. بنابراین،

$$\frac{x}{n} \le \frac{x}{y+1} < A$$

زیرا

$$y \le \frac{x}{A} < y+1.$$

نامساوی $A > (x/n)$ ایجاب می‌کند که $\psi(x/n) \le \psi(A)$. ازاینرو، مجموع دوم تحت‌تسلط $x\psi(A)$ می‌باشد. درنتیجه، اگر $\varepsilon < 1$ ، کل مجموع در (۳۴) تحت تسلط

$$(1+\varepsilon)x+\varepsilon x\log x+x\psi(A) < (2+\psi(A))x+\varepsilon x\log x$$

می‌باشد. به‌عبارت دیگر، به‌ازای هر ε که $0<\varepsilon<1$ ،

اگر $x > A$ ، $|H(x)| < (2+\psi(A))x+\varepsilon x\log x$ ،

یا

$$\frac{|H(x)|}{x\log x} < \frac{2+\psi(A)}{\log x}+\varepsilon.$$

حال $B > A$ را طوری می‌گیریم که $x > B$ نامساوی $(2+\psi(A))/\log x < \varepsilon$ را ایجاب کند. دراین صورت، به‌ازای $x > B$ ، خواهیم داشت

$$\frac{|H(x)|}{x\log x} < 2\varepsilon,$$

نشانگر آنکه، وقتی $x\to\infty$ ، $H(x)/(x\log x)\to 0$.

حال می‌پردازیم به عکس قضیهٔ ۱۴۰۴ ، و ثابت می‌کنیم رابطهٔ

$$\lim_{x\to\infty}\frac{M(x)}{x}=0 \qquad (۳۶)$$

قضیهٔ اعداد اول را ایجاب می‌کند. ابتدا نماد "اوی کوچک" را معرفی می‌کنیم.

تعریف . نماد

وقتی $x \to \infty$ ، $f(x) = o(g(x))$ (بخوانید : $f(x)$ اوی کوچک $g(x)$ است) یعنی

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0.$$

هر معادله به شکل

وقتی $x \to \infty$ ، $f(x) = h(x) + o(g(x))$

یعنی ، وقتی $x \to \infty$ ، $f(x) - h(x) = o(g(x))$.

بنابراین ، (۳۶) می‌گوید که

وقتی $x \to \infty$ ، $M(x) = o(x)$

و قضیهٔ اعداد اول ، بیان شده به شکل $\psi(x) \sim x$ ، را نیز می‌توان به‌صورت زیر نوشت :

وقتی $x \to \infty$ ، $\psi(x) = x + o(x)$.

بطور کلی ، یک رابطهٔ مجانبی به‌صورت

وقتی $x \to \infty$ ، $f(x) \sim g(x)$

معادل است با

وقتی $x \to \infty$ ، $f(x) = g(x) + o(g(x))$:

همچنین ، توجه‌می‌کنیم که وقتی $x \to \infty$ ، $f(x) = O(1)$ ایجاب می‌کند که $f(x) = o(x)$.

قضیهٔ ۱۵.۴ . *رابطهٔ*

وقتی $x \to \infty$ ، $M(x) = o(x)$ (۳۷)

ایجاب می‌کند که وقتی $x \to \infty$ ، $\psi(x) \sim x$.

برهان. ابتدا $\psi(x)$ را با فرمولی به‌نوع

$$\psi(x) = x - \sum_{\substack{q,\,d \\ qd \le x}} \mu(d) f(q) + O(1) \qquad (۳۸)$$

بیان می‌کنیم و ، سپس، با استفاده از (۳۷) ، نشان می‌دهیم که مجموع ، وقتی $x \to \infty$ ، $o(x)$ است . تابع f در (۳۸) به‌صورت زیر داده شده است :

$$f(n) = \sigma_0(n) - \log n - 2C,$$

که درآن C ثابت اویلر بوده و $\sigma_0(n) = d(n)$ تعداد مقسوم علیه‌های n است . برای بدست آوردن (۳۸) ، با اتحادهای زیر شروع می‌کنیم :

$$[x] = \sum_{n \le x} 1, \qquad \psi(x) = \sum_{n \le x} \Lambda(n), \qquad 1 = \sum_{n \le x} \left[\frac{1}{n}\right]$$

و هر جمعوند را به‌صورت زیر با حاصل ضرب دیریکلهٔ شامل تابع موبیوس بیان می‌کنیم :

$$1 = \sum_{d|n} \mu(d)\sigma_0\left(\frac{n}{d}\right), \qquad \Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d}, \qquad \left[\frac{1}{n}\right] = \sum_{d|n} \mu(d).$$

دراین صورت ،

$$\begin{aligned}
[x] - \psi(x) - 2C &= \sum_{n \le x} \left\{1 - \Lambda(n) - 2C\left[\frac{1}{n}\right]\right\} \\
&= \sum_{n \le x} \sum_{d|n} \mu(d)\left\{\sigma_0\left(\frac{n}{d}\right) - \log \frac{n}{d} - 2C\right\} \\
&= \sum_{\substack{q,d \\ qd \le x}} \mu(d)\{\sigma_0(q) - \log q - 2C\} \\
&= \sum_{\substack{q,d \\ qd \le x}} \mu(d) f(q).
\end{aligned}$$

این (۳۸) را ایجاب می‌کند . بنابراین ، برهان قضیه درصورتی کامل است که نشان دهیم

$$\text{وقتی } x \to \infty \text{ ،} \quad \sum_{\substack{q,d \\ qd \le x}} \mu(d) f(q) = o(x) . \tag{۳۹}$$

برای این منظور ، از قضیهٔ ۱۷۰۳ استفاده کرده می‌نویسیم

$$\sum_{\substack{q,d \\ qd \le x}} \mu(d) f(q) = \sum_{n \le b} \mu(n) F\left(\frac{x}{n}\right) + \sum_{n \le a} f(n) M\left(\frac{x}{n}\right) - F(a)M(b) \tag{۴۰}$$

که درآن a و b اعداد مثبت دلخواهی‌اند بطوری که $ab = x$ و

$$F(x) = \sum_{n \le x} f(n).$$

حال ، با استفاده از فرمول دیریکله (قضیهٔ ۳۰۳)،

$$\sum_{n \le x} \sigma_0(n) = x \log x + (2C - 1)x + O(\sqrt{x})$$

همراه با رابطهٔ

$$\sum_{n \le x} \log n = \log[x]! = x \log x - x + O(\log x)$$

نشان می‌دهیم که $F(x) = O(\sqrt{x})$. از اینها نتیجه می‌شود که

$$F(x) = \sum_{n \le x} \sigma_0(n) - \sum_{n \le x} \log n - 2C \sum_{n \le x}$$

$$= x\log x + (2C-1)x + O(\sqrt{x}) - (x\log x - x + O(\log x))$$
$$-2Cx + O(1)$$
$$= O(\sqrt{x}) + O(\log x) + O(1) = O(\sqrt{x}).$$

بنابراین، ثابتی مانند $B > 0$ وجود دارد بطوری که

بهازای هر $x \geq 1$ ، $|F(x)| \leq B\sqrt{x}$.

با استفاده از این در اولین مجموع سمت راست (۴۰) ، بهازای ثابتی چون $A > B > 0$ خواهیم داشت

$$\left|\sum_{n\leq b}\mu(n)F\left(\frac{x}{n}\right)\right| \leq B\sum_{n\leq b}\sqrt{\frac{x}{n}} \leq A\sqrt{xb} = \frac{Ax}{\sqrt{a}}\,. \qquad (۴۱)$$

حال فرض کنیم $\varepsilon > 0$ دلخواه باشد، و $a > 1$ را طوری اختیار میکنیم که

$$\frac{A}{\sqrt{a}} < \varepsilon.$$

دراین صورت، (۴۱) چنین خواهد شد:

$$\text{بهازای هر } x \geq 1 \text{ ،} \quad \left|\sum_{n\leq b}\mu(n)F\left(\frac{x}{n}\right)\right| < \varepsilon x. \qquad (۴۲)$$

توجه کنید که a تابع ε است ولی تابع x نیست.

چون وقتی $x \to \infty$ ، $M(x) = O(x)$ ، بهازای همان ε ، $c > 0$ ای (فقطوابسته به ε) وجود دارد بطوری که

$x > c$ ایجاب میکند که $\frac{|M(x)|}{x} < \frac{\varepsilon}{K}$ ،

که درآن K عدد مثبتی است. (بزودی K را مشخص خواهیم کرد.) دومین مجموع سمت راست (۴۰) در روابطزیر صدق میکند:

$$\left|\sum_{n\leq a}f(n)M\left(\frac{x}{n}\right)\right| \leq \sum_{n\leq a}|f(n)|\frac{\varepsilon}{K}\frac{x}{n} = \frac{\varepsilon x}{K}\sum_{n\leq a}\frac{|f(n)|}{n} \qquad (۴۳)$$

مشروط براینکهبهازایهر $n \leq a$ ، $x/n > c$. بنابراین، (۴۳) بهازای $x > ac$ برقراراست.
حال فرض میکنیم

$$K = \sum_{n\leq a}\frac{|f(n)|}{n}.$$

دراین صورت، (۴۳) ایجاب میکند که

$$\text{اگر } x > ac \text{ ،} \quad \left|\sum_{n\leq a}f(n)M\left(\frac{x}{n}\right)\right| < \varepsilon x \qquad (۴۴)$$

آخرین مجموع سمت راست (۴۰) تحت تسلط

$$|F(a)M(b)| \leq A\sqrt{a}\,|M(b)| < A\sqrt{a}b < \varepsilon\sqrt{b}\sqrt{a}b = \varepsilon\sqrt{x}b < \varepsilon x$$

است، مشروط براینکه $\sqrt{x} > a$ یا $x > a^2$. ازتلفیق این‌با (۴۴) و (۴۲)، معلوم می‌شود که (۴۰) ایجاب می‌کند که

$$\Big| \sum_{\substack{q,d \\ qd \leq x}} \mu(d) f(q) \Big| < 3\varepsilon x$$

مشروط براینکه $x > a^2$ و $x > ac$، که درآنها a و c فقط تابع ε می‌باشند. این (۳۹) را ثابت خواهد کرد.

قضیهٔ ۱۶.۴. *اگر*

$$A(x) = \sum_{n \leq x} \frac{\mu(n)}{n},$$

رابطهٔ

$$A(x) = o(1) \text{ ، وقتی } x \to \infty \qquad (۴۵)$$

قضیهٔ اعداد اول را ایجاب می‌کند. به عبارت دیگر، قضیهٔ اعداد اول نتیجه‌ای است‌از اینکه سری

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n}$$

همگرا و دارای مجموع 0 است.

تذکر. همچنین، می‌توان نشان داد (ر.ک. [۳]) که قضیهٔ اعداد اول همگرایی این سری را به 0 ایجاب می‌کند؛ درنتیجه، (۴۵) معادل قضیهٔ اعداد اول می‌باشد.

برهان. نشان می‌دهیم که (۴۵) رابطهٔ $M(x) = o(x)$ را ایجاب می‌کند. بنابر اتحاد آبل، داریم

$$M(x) = \sum_{n \leq x} \mu(n) = \sum_{n \leq x} \frac{\mu(n)}{n} n = xA(x) - \int_1^x A(t)\, dt;$$

درنتیجه،

$$\frac{M(x)}{x} = A(x) - \frac{1}{x}\int_1^x A(t)\, dt.$$

بنابراین، برای اتمام برهان، کافی است نشان دهیم که

$$\lim_{x\to\infty} \frac{1}{x}\int_1^x A(t)\,dt = 0. \tag{۴۶}$$

حال اگر $\varepsilon > 0$ مفروض باشد، c ای (فقط تابع ε) هست بطوری که اگر $x \geq c$، $|A(x)| < \varepsilon$. چون به‌ازای هر $x \geq 1$، $|A(x)| \leq 1$، داریم

$$\left|\frac{1}{x}\int_1^x A(t)\,dt\right| \leq \left|\frac{1}{x}\int_1^c A(t)\,dt\right| + \left|\frac{1}{x}\int_c^x A(t)\,dt\right| \leq \frac{c-1}{x} + \frac{\varepsilon(x-c)}{x}.$$

با فرض $x \to \infty$، معلوم می‌شود که

$$\limsup_{x\to\infty}\left|\frac{1}{x}\int_1^x A(t)\,dt\right| \leq \varepsilon,$$

و چون ε دلخواه است، این (۴۶) را ثابت خواهد کرد.

۱۰.۴ طرح اختصاری یک برهان مقدماتی قضیهٔ اعداد اول

دراین بخش، طرح اختصاری یک برهان مقدماتی قضیهٔ اعداد اول را بیان می‌کنیم. جزئیات کامل آن‌را می‌توان در [۳۱] یا [۴۶] یافت. کلید این برهان یک فرمول مجانبی ازسلبرگ است که می‌گوید

$$\psi(x)\log x + \sum_{n\leq x}\Lambda(n)\psi\left(\frac{x}{n}\right) = 2x\log x + O(x).$$

اثبات فرمول سلبرگ نسبتاً ساده است و در بخش بعد داده می‌شود. دراین بخش، مراحل اصلی استنتاج قضیهٔ اعداد اول از فرمول سلبرگ به‌اختصار ذکر می‌شوند.

اولاً، فرمول سلبرگ را می‌توان به‌شکل مناسبتری درآورد که مستلزم تابع

$$\sigma(x) = e^{-x}\psi(e^x) - 1$$

باشد. فرمول سلبرگ یک نامساوی انتگرال به‌شکل

$$|\sigma(x)|x^2 \leq 2\int_0^x\int_0^y |\sigma(u)|\,du\,dy + O(x) \tag{۴۷}$$

را ایجاب می‌کند، و قضیهٔ اعداد اول معادل آن است که نشان دهیم، وقتی $x \to \infty$، $\sigma(x) \to 0$. بنابراین، اگر فرض کنیم

$$C = \limsup_{x\to\infty}|\sigma(x)|,$$

قضیهٔ اعداد اول معادل آن است که نشان دهیم $C = 0$. این با فرض $C > 0$ و رسیدن

به تناقض به صورت زیر ثابت شده است . از تعریف C داریم

$$|\sigma(x)| \leq C + g(x), \tag{۴۸}$$

که درآن ، وقتی $x \to \infty$ ، $g(x) \to 0$. اگر $C > 0$ ، این نامساوی، همراه با (۴۷) ، نامساوی دیگر زیر از همان نوع را نتیجه می‌دهد :

$$|\sigma(x)| \leq C' + h(x), \tag{۴۹}$$

که درآن $0 < C' < C$ و، وقتی $x \to \infty$ ، $h(x) \to 0$. استنتاج (۴۹) از (۴۷) و (۴۸) طولانی‌ترین قسمت برهان است . با فرض $x \to \infty$ در (۴۹) ، معلوم می‌شود که $C \leq C'$ ، تناقضی که برهان را تمام خواهد کرد .

۱۱.۴ فرمول مجانبی سلبرگ

مافرمول‌سلبرگ‌را به‌روشی که تاتوزاوا[1] و ایسکی[2] [۶۸] در ۱۹۵۱ دادند نتیجه‌می‌گیریم . این روش مبتنی بر قضیهٔ زیر است که سرشت یک فرمول انعکاس را دارد .

قضیهٔ ۱۷.۴ . *فرض‌کنیم F یک تابع حقیقی یا مختلط باشد که بر $(0, \infty)$ تعریف شده است ، و نیز*

$$G(x) = \log x \sum_{n \leq x} F\left(\frac{x}{n}\right).$$

دراین صورت ،

$$F(x)\log x + \sum_{n \leq x} F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{d \leq x} \mu(d) G\left(\frac{x}{d}\right).$$

برهان . ابتدا $F(x)\log x$ را به‌صورت مجموع می‌نویسیم :

$$F(x)\log x = \sum_{n \leq x} \left[\frac{1}{n}\right] F\left(\frac{x}{n}\right)\log \frac{x}{n} = \sum_{n \leq x} F\left(\frac{x}{n}\right)\log \frac{x}{n} \sum_{d|n} \mu(d).$$

دراین صورت ، با استفاده از اتحاد قضیهٔ ۱۱.۲ ، یعنی

$$\Lambda(n) = \sum_{d|n} \mu(d)\log \frac{n}{d} \ ,$$

می‌نویسیم

1. Tatuzawa 2. Iseki

$$\sum_{n\le x} F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{n\le x} F\left(\frac{x}{n}\right)\sum_{d|n}\mu(d)\log\frac{n}{d}.$$

با افزودن این معادلات بهم ، درمی‌یابیم که

$$F(x)\log x + \sum_{n\le x} F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{n\le x} F\left(\frac{x}{n}\right)\sum_{d|n}\mu(d)\left\{\log\frac{x}{n} + \log\frac{n}{d}\right\}$$
$$= \sum_{n\le x}\sum_{d|n} F\left(\frac{x}{n}\right)\mu(d)\log\frac{x}{d}.$$

در مجموع آخر ، اگر بنویسیم $n = qd$ ، داریم

$$\sum_{n\le x}\sum_{d|n} F\left(\frac{x}{n}\right)\mu(d)\log\frac{x}{d} = \sum_{d\le x}\mu(d)\log\frac{x}{d}\sum_{q\le x/d} F\left(\frac{x}{qd}\right) = \sum_{d\le x}\mu(d)G\left(\frac{x}{d}\right),$$

که قضیه را ثابت خواهد کرد .

قضیهٔ ۱۸.۴ . فرمول مجانبی سلبرگ. به‌ازای $x > 0$ ، داریم

$$\psi(x)\log x + \sum_{n\le x}\Lambda(n)\psi\left(\frac{x}{n}\right) = 2x\log x + O(x).$$

برهان. قضیهٔ ۱۷.۴ را درمورد تابع $F_1(x) = \psi(x)$ و نیز $F_2(x) = x - C - 1$ ، که‌در آن C ثابت اویلر است ، بکار می‌بریم . درمورد F_1 ، داریم

$$G_1(x) = \log x\sum_{n\le x}\psi\left(\frac{x}{n}\right) = x\log^2 x - x\log x + O(\log^2 x),$$

که درآن از قضیهٔ ۱۱.۴ استفاده کرده‌ایم . درمورد F_2 ، داریم

$$G_2(x) = \log x\sum_{n\le x} F_2\left(\frac{x}{n}\right) = \log x\sum_{n\le x}\left(\frac{x}{n} - C - 1\right)$$
$$= x\log x\sum_{n\le x}\frac{1}{n} - (C+1)\log x\sum_{n\le x} 1$$
$$= x\log x\left(\log x + C + O\left(\frac{1}{x}\right)\right) - (C+1)\log x(x + O(1))$$
$$= x\log^2 x - x\log x + O(\log x).$$

از مقایسهٔ فرمولهای $G_1(x)$ و $G_2(x)$ با هم ، می‌بینیم که $G_1(x) - G_2(x) = O(\log^2 x)$. در واقع ، ما فقط از تخمین ضعیفتر

$$G_1(x) - G_2(x) = O(\sqrt{x})$$

استفاده می‌کنیم .

حال قضیهٔ ۱۷.۴ را درمورد هریک از F_1 و F_2 بکار می‌بریم و دو رابطهٔ حاصل رااز هم کم می‌کنیم . بنابر قضیهٔ ۲.۳ (ب) ، تفاضل دو طرف راست مساوی است با

$$\sum_{d \le x} \mu(d)\left\{G_1\left(\frac{x}{d}\right) - G_2\left(\frac{x}{d}\right)\right\} = O\left(\sum_{d \le x} \sqrt{\frac{x}{d}}\right) = O\left(\sqrt{x}\sum_{d \le x} \frac{1}{\sqrt{d}}\right) = O(x) .$$

بنابراین، تفاضل دو طرف چپ نیز $O(x)$ است . به عبارت دیگر ، داریم

$$\{\psi(x) - (x - C - 1)\}\log x + \sum_{n \le x} \left\{\psi\left(\frac{x}{n}\right) - \left(\frac{x}{n} - C - 1\right)\right\}\Lambda(n) = O(x).$$

با آرایش مجدد جملات و استفاده از قضیهٔ ۹.۴ ، معلوم می‌شود که

$$\begin{aligned}\psi(x)\log x + \sum_{n \le x} \psi\left(\frac{x}{n}\right)\Lambda(n) &= (x - C - 1)\log x \\ &\quad + \sum_{n \le x} \left(\frac{x}{n} - C - 1\right)\Lambda(n) + O(x) \\ &= 2x \log x + O(x).\end{aligned}$$

تمرین برای فصل ۴

۱ . فرض‌کنید $S = \{1, 5, 9, 13, 17, \ldots\}$ مجموعهٔ تمام اعداد صحیح مثبت به شکل $4n + 1$ باشد . عنصر p از S یک S *اول* نامیده می‌شود اگر $p > 1$ و تنها مقسوم علیه‌های p در بین‌عناصر S عبارت از 1 و p باشند . (مثلاً ، 49 یک S اول است .)
عنصر $n > 1$ در S که یک S اول نباشد یک S **مرکب** نامیده می‌شود .
(آ) ثابت کنید هر S مرکب حاصل ضربی از S اولهاست .
(ب) کوچکترین S مرکبی را بیابید که بتوان آن را به بیش از یک طریق به‌صورت حاصل ضربی از S اولها بیان کرد .
این مثال نشان می‌دهد که یکتایی تجزیه در S برقرار نیست .

۲ . مجموعهٔ متناهی زیر از اعداد صحیح را درنظر بگیرید :

$$T = \{1, 7, 11, 13, 17, 19, 23, 29\}.$$

(آ) به‌ازای هر p اول در بازهٔ $30 < p < 100$ ، جفت m, n از اعداد صحیح ،که $m \ge 0$ و $n \in T$ ،را طوری معین کنید که $p = 30m + n$.
(ب) حکم زیررا یا اثبات کنید یا برایش مثال نقض بزنید : هر عدد اول $p > 5$ را

می‌توان به‌شکل $30m + n$ نوشت، که درآن $m \geq 0$ و $n \in T$.

۳ . فرض کنید $f(x) = x^2 + x + 41$. کوچکترین عدد صحیح $x \geq 0$ را بیابید که به‌ازای آن $f(x)$ مرکب باشد.

۴ . فرض کنید $f(x) = a_0 + a_1x + \cdots + a_nx^n$ یک چندجمله‌ای با ضرایب صحیح باشد، که درآن $a_n > 0$ و $n \geq 1$. ثابت کنید $f(x)$ به‌ازای بی‌نهایت عدد صحیح x مرکب است.

۵ . ثابت کنید به‌ازای هر $n > 1$ ، n عدد مرکب متوالی وجود دارد.

۶ . ثابت کنید چند جمله‌ایهایی چون P و Q وجود ندارند که

$$\pi(x) = \frac{P(x)}{Q(x)} \text{ ، } x = 1, 2, 3, \ldots \text{ به‌ازای}$$

۷ . فرض کنید $a_1 < a_2 < \cdots < a_n \leq x$ مجموعه‌ای از اعداد صحیح مثبت باشد بطوری‌که هیچ a_i حاصل ضرب a_i های دیگر را عاد نکند. ثابت کنید که $n \leq \pi(x)$.

۸ . مطلوب است محاسبهٔ بالاترین توان 10 که $1000!$ را عاد کند.

۹ . تصاعدحسابی

$$h, h + k, h + 2k, \ldots, h + nk, \ldots$$

از اعداد صحیح که درآن $0 < k < 2000$ مفروض است. اگر $h + nk$ به‌ازای $n = t, t + 1, \ldots, t + r$ اول باشد، ثابت کنید که $r \leq 9$. به عبارت دیگر، حداکثر 10 جملهٔ متوالی این تصاعد می‌توانند اول باشند.

۱۰ . فرض کنید s_n مجموع جزئی n م سری

$$\sum_{r=1}^{\infty} \frac{1}{r(r + 1)}$$

باشد. ثابت کنید به‌ازای هر عدد صحیح $k > 1$ ، اعداد صحیحی مانند m و n وجود دارند بطوری که $s_m - s_n = 1/k$.

۱۱ . فرض کنید s_n مجموع اولین n عدد اول باشد. ثابت کنید به‌ازای هر n ، عدد صحیحی هست که مربعش بین s_n و s_{n+1} قرار دارد.

هریک از تمرینهای ۱۲ تا ۱۶ را حل کنید. دراین دسته از تمرینات می‌توانید از قضیهٔ اعداد اول استفاده کنید.

۱۲ . هرگاه $a > 0$ و $b > 0$ ، آنگاه وقتی $x \to \infty$ ، $\pi(ax)/\pi(bx) \sim a/b$.

۱۳ . هرگاه $0 < a < b$ ، x_0 ی هست بطوری که اگر $x \geq x_0$ ، $\pi(ax) < \pi(bx)$.

۱۴ . هرگاه $0 < a < b$ ، x_0 ی هست بطوری که به‌ازای $x \geq x_0$ اقلا" یک عدد اول بین

ax و bx وجود دارد.

۱۵ . هر بازه مانند $[a, b]$ که $0 < a < b$ شامل عددی گویا به‌شکل p/q است، که در آن p و q اول می‌باشند.

۱۶ . (آ) به‌ازای عدد صحیح و مثبت n ، عدد صحیح مثبتی مانند k و عدد اولی چون p وجود دارند بطوری که $10^k n < p < 10^k(n+1)$.

(ب) به‌ازای m عدد صحیح $a_1, \ldots, a_m$ بطوری که به‌ازای $i = 1, 2, \ldots, m$ ، $0 \le a_i \le 9$ ، عدد اولی چون p وجود دارد که m رقم اول بسط اعشاری آن $a_1, \ldots, a_m$ می‌باشند.

۱۷ . عدد صحیح $n > 1$ با دو تجزیهٔ $n = \prod_{i=1}^{r} p_i$ و $n = \prod_{i=1}^{t} q_i$ که در آنها p_i ها اول (نه لزوماً متمایز) و q_i ها اعداد صحیح دلخواهی بزرگتر از یک‌اند مفروض است. فرض کنید α یک عدد اول نامنفی باشد.

(آ) هرگاه $\alpha \ge 1$ ، ثابت کنید که

$$\sum_{i=1}^{r} p_i^{\alpha} \le \sum_{i=1}^{t} q_i^{\alpha}.$$

(ب) نامساوی نظیر را که درحالت $0 \le \alpha < 1$ این مجموعها را بهم مربوط می‌کند بدست آورید.

۱۸ . ثابت کنید که دو رابطهٔ زیر معادلند:

(آ) $$\pi(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right);$$

(ب) $$\vartheta(x) = x + O\left(\frac{x}{\log x}\right).$$

۱۹ . اگر $x \ge 2$ ، قرار دهید

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$$ (انتگرال لگاریتمی x)

(آ) ثابت کنید که

$$\mathrm{Li}(x) = \frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t} - \frac{2}{\log 2},$$

و، بطور کلی،

$$\mathrm{Li}(x) = \frac{x}{\log x}\left(1 + \sum_{k=1}^{n-1} \frac{k!}{\log^k x}\right) + n! \int_2^x \frac{dt}{\log^{n+1} t} + C_n,$$

که درآن C_n مستقل از x است.

(ب) اگر $x \geq 2$، ثابت کنید که

$$\int_2^x \frac{dt}{\log^n t} = O\left(\frac{x}{\log^n x}\right).$$

۲۰. فرض کنید f یک تابع حسابی باشد بطوری که

به‌ازای $x \geq 2$، $\sum_{p \leq x} f(p)\log p = (ax + b)\log x + cx + O(1)$.

ثابت کنید ثابتی چون A (وابسته به f) هست بطوری که اگر $x \geq 2$،

$$\sum_{p \leq x} f(p) = ax + (a + c)\left(\frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t}\right) + b\log(\log x) + A + O\left(\frac{1}{\log x}\right).$$

۲۱. دو تابع حقیقی $S(x)$ و $T(x)$ مفروضند بطوری که

به‌ازای هر $x \geq 1$، $T(x) = \sum_{n \leq x} S\left(\frac{x}{n}\right)$.

اگر $S(x) = O(x)$ و c ثابت مثبتی باشد، ثابت کنید رابطهٔ

وقتی $x \to \infty$، $S(x) \sim cx$

رابطهٔ

وقتی $x \to \infty$، $T(x) \sim cx\log x$

را ایجاب خواهد کرد.

۲۲. ثابت کنید فرمول سلبرگ، بصورتی که در قضیهٔ ۱۸۰۴ بیان شده، معادل هریک از روابط زیر است:

(آ) $\psi(x)\log x + \sum_{p \leq x} \psi\left(\frac{x}{p}\right)\log p = 2x\log x + O(x)$؛

(ب) $\vartheta(x)\log x + \sum_{p \leq x} \vartheta\left(\frac{x}{p}\right)\log p = 2x\log x + O(x)$.

۲۳. فرض کنید $M(x) = \sum_{n \leq x} \mu(n)$. ثابت کنید که

$$M(x)\log x + \sum_{n \leq x} M\left(\frac{x}{n}\right)\Lambda(n) = O(x)$$

و

$$M(x)\log x + \sum_{p \leq x} M\left(\frac{x}{p}\right)\log p = O(x).$$

[راهنمایی . قضیهٔ ۴ . ۱۷ .]

۲۴ . فرض کنید $A(x)$ به‌ازای هر $x > 0$ تعریف شده باشد

و وقتی $x \to \infty$ ، $T(x) = \sum_{n \le x} A\left(\frac{x}{n}\right) = ax \log x + bx + o\left(\frac{x}{\log x}\right)$ ،

که درآن a و b ثابت‌اند . ثابت کنید

وقتی $x \to \infty$ ، $A(x)\log x + \sum_{n \le x} A\left(\frac{x}{n}\right)\Lambda(n) = 2ax \log x + o(x \log x)$.

تحقیق کنید که فرمول سلبرگ قضیهٔ ۴ . ۱۸ یک حالت خاص است .

۲۵ . ثابت کنید قضیهٔ اعداد اول به‌شکل $\psi(x) \sim x$ فرمول مجانبی سلبرگ در قضیهٔ ۴ . ۱۸ با جملهٔ خطای $o(x \log x)$ ، وقتی $x \to \infty$ ، را ایجاب می‌کند .

۲۶ . در سال ۱۸۵۱ ، چبیشف ثابت کرد که اگر $\psi(x)/x$ ، وقتی $x \to \infty$ ، به‌حدی میل کند ، این حدمساوی 1 است . دراین تمرین برهان ساده‌ای از این نتیجه به‌اختصار ذکر می‌شود که مبتنی بر فرمول

$$\sum_{n \le x} \psi\left(\frac{x}{n}\right) = x \log x + O(x) \qquad (۵۰)$$

است که از قضیهٔ ۴ . ۱۱ نتیجه می‌گردد .

(آ) فرض کنید $\delta = \limsup_{x \to \infty}(\psi(x)/x)$. به‌ازای $\varepsilon > 0$ مفروض، $N = N(\varepsilon)$ را طوری اختیارکنید که $x \ge N$ نامساوی $\psi(x) \le (\delta + \varepsilon)x$ را ایجاب کند . مجموع (۵۰) رابه دوقسمت‌تقسیم کنید ، یکی به‌ازای $n \le x/N$ و دیگری به‌ازای $n > x/N$ ، و باتخمین هر قسمت نامساوی

$$\sum_{n \le x} \psi\left(\frac{x}{n}\right) \le (\delta + \varepsilon)x \log x + x\psi(N)$$

را بدست آورید . از مقایسهٔ این با (۵۰) ، نتیجه بگیرید که $\delta \ge 1$.

(ب) فرض کنید $\gamma = \liminf_{x \to \infty}(\psi(x)/x)$ و ، با استدلالی شبیه استدلال (آ) ، نتیجه بگیرید که $\gamma \le 1$. بنابراین ، هرگاه وقتی $x \to \infty$ ، $\psi(x)/x$ حد داشته باشد ،آنگاه $\gamma = \delta = 1$.

در تمرینهای۲۷تا ۳۰ فرض کنید $A(x) = \sum_{n \le x} a(n)$ ، که درآن $a(n)$ در نامساوی زیرصدق می‌کند :

$$\text{به‌ازای هر } n \ge 1 \text{ ،} \quad a(n) \ge 0 \qquad (۵۱)$$

و نیز

$$\sum_{n\le x} A\left(\frac{x}{n}\right) = \sum_{n\le x} a(n)\left[\frac{x}{n}\right] = ax\log x + bx + o\left(\frac{x}{\log x}\right)$$ وقتی $x \to \infty$ ، (۵۲)

وقتی $a(n) = \Lambda(n)$ ، این روابط به‌ازای $a = 1$ و $b = -1$ برقرارند. تمرینهای زیر نشان می‌دهند که (۵۱) و (۵۲) ، همراه با قضیهٔ اعداد اول، یعنی $\psi(x) \sim x$ ، ایجاب می‌کنند که $A(x) \sim ax$. این را با قضیهٔ ۴.۸ (قضیهٔ تاوبری شاپیرو) مقایسه کنید که در آن فقط (۵۱) و شرط ضعیفتر $\sum_{n\le x} A(x/n) = ax\log x + O(x)$ مفروضند و نتیجه بگیرید که به‌ازای ثوابت مثبتی چون C و B ، $Cx \le A(x) \le Bx$.

۲۷ . ثابت کنید که

(آ) $$\sum_{n\le x} A\left(\frac{x}{n}\right)\Lambda(n) = \sum_{n\le\sqrt{x}} A\left(\frac{x}{n}\right)\Lambda(n) + \sum_{n\le\sqrt{x}} \psi\left(\frac{x}{n}\right)a(n) + O(x)$$ ،

و با استفاده از آن نتیجه بگیرید که

(ب) $$\frac{A(x)}{x} + \frac{1}{x\log x}\sum_{n\le\sqrt{x}} A\left(\frac{x}{n}\right)\Lambda(n) + \frac{1}{x\log x}\sum_{n\le\sqrt{x}} \psi\left(\frac{x}{n}\right)a(n) = 2a + o(1)$$.

۲۸ . فرض کنید $\alpha = \liminf_{x\to\infty}(A(x)/x)$ و $\beta = \limsup_{x\to\infty}(A(x)/x)$.

(آ) $\varepsilon > 0$ دلخواه‌را اختیار و با استفاده از اینکه به‌ازای هر x/t به‌قدر کافی بزرگ

$$\psi\left(\frac{x}{t}\right) < (1+\varepsilon)\frac{x}{t} \quad \text{و} \quad A\left(\frac{x}{t}\right) < (\beta+\varepsilon)\frac{x}{t}$$

از تمرین ۲۷ (ب) نتیجه بگیرید که

$$\alpha + \frac{\beta}{2} + \frac{a}{2} + \frac{\varepsilon}{2} + \frac{a\varepsilon}{2} > 2a.$$

چون ε دلخواه است، این ایجاب می‌کند که

$$\alpha + \frac{\beta}{2} + \frac{a}{2} \ge 2a.$$

[**راهنمایی.** فرض کنید $x \to \infty$ بطوری که $A(x)/x \to \alpha$].

(ب) با استدلالی مشابه، ثابت کنید که

$$\beta + \frac{\alpha}{2} + \frac{a}{2} \le 2a$$

و نتیجه بگیرید که $\alpha = \beta = a$. به‌عبارت دیگر، وقتی $x \to \infty$ ، $A(x) \sim ax$.

۲۹ . فرض کنید $a(n) = 1 + \mu(n)$ و تحقیق کنید که (۵۲) به‌ازای $a = 1$ و $b = 2C - 1$ ، که C ثابت اویلر است، برقرار است. نشان دهید که تمرین ۲۸ ایجاب می‌کند که

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\le x}\mu(n) = 0.$$

این برهان دیگری از قضیهٔ ۱۴.۴ بدست می‌دهد.

۳۰. در تمرین ۲۸، فرض کنید قضیهٔ اعداد اول دانسته نباشد. به‌جای آن، فرض کنید

$$\gamma = \liminf_{x\to\infty} \frac{\psi(x)}{x}, \qquad \delta = \limsup_{x\to\infty} \frac{\psi(x)}{x}.$$

(آ) نشان دهید که استدلال تمرین ۲۸ به‌نامساویهای

$$\alpha + \frac{\beta}{2} + \frac{a\delta}{2} \geq 2a, \qquad \beta + \frac{\alpha}{2} + \frac{a\gamma}{2} \leq 2a$$

منجر می‌شود.

(ب) با استفاده از نامساویهای قسمت (آ)، ثابت کنید که

$$a\gamma \leq \alpha \leq \beta \leq a\delta.$$

این نشان می‌دهد که بین همهٔ $a(n)$ های صادق در (۵۱) و (۵۲) با a ثابت، حدود

$$\limsup_{x\to\infty} \frac{A(x)}{x} \quad \text{و} \quad \liminf_{x\to\infty} \frac{A(x)}{x}$$

بیشترین اختلاف را وقتی دارند که $a(n) = a\Lambda(n)$. از اینرو، برای آنکه $A(x) \sim ax$ را از (۵۱) و (۵۲) نتیجه بگیریم، کافی است فقط حالت خاص $a(n) = a\Lambda(n)$ را مورد بحث قرار دهیم.

۵ همنهشتیها

۱.۵ تعریف و خواص اساسی همنهشتیها

گاوس نماد قابل توجهی را معرفی کرد که بسیاری از مسائل بخشپذیری اعداد صحیح با آن ساده می‌شوند. وی با این‌کار شاخهٔ جدیدی از نظریهٔ اعداد را ابداع نمود به‌نام *نظریهٔ همنهشتیها*، که مبانی آن دراین فصل مورد بحث قرار خواهند گرفت.

حروف کوچک لاتینی و یونانی نمایش‌اعداد صحیح (مثبت، منفی، یا صفر)اند مگر آنکه خلاف آن تصریح شود.

تعریف. فرض کنیم a, b, m اعدادی صحیح باشند و $m > 0$. گوییم a *همنهشت* b به هنگ m است، و می‌نویسیم

$$a \equiv b \pmod{m}, \tag{۱}$$

اگر m تفاضل $a-b$ را عاد نماید. عدد m هنگ همنهشتی نامیده می‌شود. به عبارت دیگر، همنهشتی (۱) معادل رابطهٔ بخشپذیری

$$m|(a-b)$$

است. درحالت خاص، $a \equiv 0 \pmod{m}$ اگر و فقط‌اگر $m|a$. بنابراین، $a \equiv b \pmod{m}$ اگر و فقط اگر $a-b \equiv 0 \pmod{m}$. اگر $m \nmid (a-b)$، می‌نویسیم $a \not\equiv b \pmod{m}$ و می‌گوییم a و b *ناهمنهشت‌اند* به هنگ m.

چند مثال

۱. $19 \equiv 7 \pmod{12}$, $1 \equiv -1 \pmod{2}$, $3^2 \equiv -1 \pmod{5}$.

۲. n زوج است اگر و فقط‌اگر $n \equiv 0 \pmod{2}$.

۳. n فرد است اگر و فقط‌اگر $n \equiv 1 \pmod{2}$.

۴ . به‌ازای هر a و b ، $a \equiv b \pmod 1$.

۵ . هرگاه $a \equiv b \pmod m$ ، آنگاه وقتی $d|m, d > 0$ داریم $a \equiv b \pmod d$.

گاوس علامت همنهشتی $\equiv$ را بخاطر تشابهش با علامت تساوی $=$ انتخاب کرد . دو قضیهٔ بعد نشان می‌دهند که همنهشتیها درواقع بسیاری از خواص صوری تساویها را دارند .

قضیهٔ ۱۰۵ . *همنهشتی یک رابطهٔ هم‌ارزی است . یعنی ، داریم*

(آ) $a \equiv a \pmod m$ *(انعکاس)*؛

(ب) $a \equiv b \pmod m$ *ایجاب می‌کند که* $b \equiv a \pmod m$ *(تقارن)*؛

(پ) $a \equiv b \pmod m$ و $b \equiv c \pmod m$ *ایجاب می‌کنند که* $a \equiv c \pmod m$ *(تعدی)* .

برهان . برهان فوراً از خواص بخشپذیری زیر نتیجه می‌شود :

(آ) $m|0$ ؛

(ب) هرگاه $m|(a-b)$ ، آنگاه $m|(b-a)$ ؛

(پ) هرگاه $m|(a-b)$ و $m|(b-c)$ ، آنگاه $m|(a-b)+(b-c) = a-c$.

قضیهٔ ۲۰۵ . *هرگاه* $a \equiv b \pmod m$ و $\alpha \equiv \beta \pmod m$ ، *آنگاه*

(آ) *به ازای هر دو عدد صحیح* x و y ، $ax + \alpha y \equiv bx + \beta y \pmod m$ ؛

(ب) $a\alpha \equiv b\beta \pmod m$ ؛

(پ) *به‌ازای هر عدد صحیح مثبت* n ، $a^n \equiv b^n \pmod m$ ؛

(ت) *به‌ازای هر چند جمله‌ای* f *با ضرایب صحیح* ، $f(a) \equiv f(b) \pmod m$.

برهان . (آ) چون $m|(a-b)$ و $m|(\alpha-\beta)$ ، داریم

$$m|x(a-b) + y(\alpha-\beta) = (ax+\alpha y) - (bx+\beta y).$$

(ب) توجه‌کنید‌که ،بنابرقسمت (آ) ، $a\alpha - b\beta = \alpha(a-b) + b(\alpha-\beta) \equiv 0 \pmod m$.

(پ) در قسمت (ب) $\alpha = a$ و $\beta = b$ را اختیار و از استقرا روی n استفاده می‌کنیم .

(ت) از قسمت (پ) و استقرا روی درجهٔ f استفاده می‌کنیم .

قضیهٔ ۲۰۵ می‌گوید که دو همنهشتی با یک هنگ را می‌توان جمله به جمله بهم افزود ، از یکدیگر کم کرد ، یا درهم ضرب نمود ، بنحوی که گویی تساوی‌اند . این مطلب برای

تعدادی متناهی همنهشتی با یک هنگ نیز برقرار است.

قبل از بیان خواص دیگر همنهشتیها، دو مثال می‌آوریم که سودمندی آنها را نشان می‌دهند.

مثال ۱. آزمون بخشپذیری بر 9 . عدد صحیح $n > 0$ بر 9 بخشپذیر است اگر و فقط اگر مجموع ارقامش در بسط اعشاری بر 9 بخشپذیر باشد. این خاصیت به‌آسانی با استفاده از همنهشتیها اثبات می‌شود. هرگاه رقمهای n در بسط اعشاری $a_0, a_1, \dots, a_k$ باشند، آنگاه

$$n = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^ka_k.$$

با استفاده از قضیهٔ ۲.۵، به هنگ 9 داریم

$$10 \equiv 1, \qquad 10^2 \equiv 1, \dots, \qquad 10^k \equiv 1 \pmod 9);$$

درنتیجه،

$$n \equiv a_0 + a_1 + \cdots + a_k \pmod 9.$$

توجه کنید که تمام این همنهشتیها به هنگ 3 نیز برقرارند؛ درنتیجه، یک عدد بر 3 بخشپذیر است اگر و فقط اگر مجموع ارقامش بر 3 بخشپذیر باشد.

مثال ۲. به اعداد فرما، یعنی $F_n = 2^{2^n} + 1$، در مقدمهٔ تاریخی اشاره شد. اولین پنج عدد فرما اولند:

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65,537.$$

حال، بی‌آنکه F_5 را حساب کنیم، نشان می‌دهیم که F_5 بر 641 بخشپذیر است. برای این‌کار توانهای متوالی 2^{2^n} به هنگ 641 را درنظر می‌گیریم. داریم

$$2^2 = 4, \qquad 2^4 = 16, \qquad 2^8 = 256, \qquad 2^{16} = 65,536 \equiv 154 \pmod{641};$$

لذا،

$$2^{32} \equiv (154)^2 = 23,716 \equiv 640 \equiv -1 \pmod{641}.$$

بنابراین، $F_5 = 2^{32} + 1 \equiv 0 \pmod{641}$؛ درنتیجه، F_5 مرکب می‌باشد.

حال به خواص عمومی همنهشتیها باز می‌گردیم. عاملهای ناصفر مشترک را همیشه نمی‌توان از طرفین یک همنهشتی مثل معادلات حذف کرد. مثلاً، دوطرف همنهشتی

$$48 \equiv 18 \pmod{10}$$

بر 6 بخشپذیراند، اما اگر عامل مشترک 6 را حذف کنیم، به‌نتیجهٔ نادرست

$3 \equiv 8 \pmod{10}$ خواهیم رسید. قضیهٔ زیر نشان می‌دهد که، اگر هنگ نیز بر عامل مشترک بخشپذیر باشد، عامل مشترک قابل حذف خواهد بود.

قضیهٔ ۳.۵ . هرگاه $c > 0$،
$a \equiv b \pmod{m}$ *اگر و فقط اگر* $ac \equiv bc \pmod{mc}$.

برهان. داریم $m|(b-a)$ اگر و فقط اگر $cm|c(b-a)$.

قضیهٔ بعدی قانون حذف را توصیف می‌کند، که می‌توان از آن وقتی هنگ بر عامل مشترک بخشپذیر نیست استفاده کرد.

قضیهٔ ۴.۵ . قانون حذف. هرگاه $ac \equiv bc \pmod{m}$ و $d = (m, c)$، آنگاه

$$a \equiv b \left(\bmod \frac{m}{d}\right).$$

به‌عبارت دیگر، عامل مشترک c را درصورتی می‌توان حذف کرد که هنگ بر $d = (m, c)$ بخشپذیر باشد. بخصوص، عامل مشترکی که نسبت به هنگ اول باشد همیشه قابل حذف است.

برهان. چون $ac \equiv bc \pmod{m}$، داریم
$m|c(a-b)$؛ درنتیجه، $\frac{m}{d}\Big|\frac{c}{d}(a-b)$.
اما $(m/d, c/d) = 1$؛ بنابراین، $m/d|(a-b)$.

قضیهٔ ۵.۵ . فرض کنیم $a \equiv b \pmod{m}$. هرگاه $d|m$ و $d|a$، آنگاه $d|b$.

برهان. کافی است فرض کنیم $d > 0$. هرگاه $d|m$، آنگاه $a \equiv b \pmod{m}$ ایجاب می‌کند که $a \equiv b \pmod{d}$. اما، هرگاه $d|a$، آنگاه $a \equiv 0 \pmod{d}$؛ درنتیجه، $b \equiv 0 \pmod{d}$.

قضیهٔ ۶.۵ . هرگاه $a \equiv b \pmod{m}$، آنگاه $(a, m) = (b, m)$. به‌عبارت دیگر، اعداد

همنهشت به هنگ m، دارای یک بمعم با m می‌باشند.

برهان. فرض کنیم $d = (a, m)$ و $e = (b, m)$. دراین‌صورت، $d|m$ و $d|a$؛ درنتیجه، $d|b$. بنابراین، $d|e$. بهمین ترتیب، $e|m, e|b$؛ درنتیجه، $e|a$. لذا، $e|d$. بنابراین، $d = e$.

قضیهٔ ۷.۵. هرگاه $a \equiv b \pmod m$ و $0 \leq |b - a| < m$، آنگاه $a = b$.

برهان. چون $m|(a - b)$، داریم $m \leq |a - b|$ مگر آنکه $a - b = 0$.

قضیهٔ ۸.۵. $a \equiv b \pmod m$ اگروفقط‌اگر a و b درتقسیم بر m یک باقیمانده‌داشته باشند.

برهان. می‌نویسیم $b = mQ + R$, $a = mq + r$، که درآنها $0 \leq r < m$ و $0 \leq R < m$. پس $a - b \equiv r - R \pmod m$ و $0 \leq |r - R| < m$. حال قضیهٔ ۷.۵ را بکار می‌بریم.

قضیهٔ ۹.۵. هرگاه $a \equiv b \pmod m$ و $a \equiv b \pmod n$ که درآنها $(m, n) = 1$، آنگاه $a \equiv b \pmod{mn}$.

برهان. چون m و n هردو $a - b$ را عاد می‌کنند، حاصل ضرب آنها نیز چنین است زیرا $(m, n) = 1$.

۲.۵ رده‌های مانده‌ای و دستگاههای مانده‌ای تام

تعریف. هنگ ثابت $m > 0$ را درنظر می‌گیریم. مجموعهٔ تمام اعداد صحیح x که $x \equiv a \pmod m$ را با $\hat{a}$ نشان می‌دهیم و $\hat{a}$ را ردهٔ مانده‌ای a به هنگ m می‌نامیم.

بنابراین، $\hat{a}$ عبارت است از تمام اعداد صحیح به‌شکل $a + mq$، که درآن $q = 0, \pm 1, \pm 2, \ldots$.

خواص رده‌های مانده‌ای مذکور درزیر نتایج سادهٔ این تعریف‌اند.

قضیهٔ ۱۰.۵ . به‌ازای هنگ مفروض m ،

(آ) $\hat{a} = \hat{b}$ *اگر و فقط اگر* $a \equiv b \pmod m$ ؛

(ب) دو عدد صحیح x و y *دریک‌ردهٔ مانده‌ای اند اگر و فقط اگر* $x \equiv y \pmod m$ ؛

(پ) m ردهٔ *مانده‌ای* $\hat{1}, \hat{2}, \ldots, \hat{m}$ *از هم جدا هستند و اجتماعشان مجموعهٔ تمام اعداد صحیح است.*

برهان. قسمتهای (آ) و (ب) فوراً از تعریف نتیجه می‌شوند. برای اثبات (پ)، توجه می‌کنیم که (بنابرقضیهٔ ۷.۵) اعداد $0, 1, 2, \ldots, m-1$ ناهمنهشت به هنگ m اند. لذا، بنابر قسمت (ب)، رده‌های مانده‌ای

$$\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{m-1}$$

از هم جدا هستند. اما هر عدد صحیح x باید درست در یکی از این رده‌ها باشد، زیرا $x = qm + r$ که درآن $0 \le r < m$ ؛ درنتیجه، $x \equiv r \pmod m$ ؛ و لذا، $x \in \hat{r}$. چون $\hat{0} = \hat{m}$ ، این (پ) را ثابت خواهد کرد.

تعریف. یک مجموعه از m نماینده، یکی از هر ردهٔ مانده‌ای $\hat{1}, \hat{2}, \ldots, \hat{m}$ ، یک *دستگاه مانده‌ای تام به هنگ* m نامیده می‌شود.

چند مثال. هر مجموعه مرکب از m عدد صحیح و ناهمنهشت به‌هنگ m یک دستگاه مانده‌ای تام به هنگ m است. مثلاً،

$$\{1, 2, \ldots, m\}; \qquad \{0, 1, 2, \ldots, m-1\};$$
$$\{1, m+2, 2m+3, 3m+4, \ldots, m^2\}.$$

قضیهٔ ۱۱.۵ . فرض‌کنیم $(k, m) = 1$. هرگاه $\{a_1, \ldots, a_m\}$ *یک دستگاه مانده‌ای تام به هنگ* m *باشد،* $\{ka_1, \ldots, ka_m\}$ *نیز چنین است.*

برهان. هرگاه $ka_i \equiv ka_j \pmod m$ ، آنگاه $a_i \equiv a_j \pmod m$ زیرا $(k, m) = 1$. لذا، هیچ دو عنصر مجموعهٔ $\{ka_1, \ldots, ka_m\}$ همنهشت به هنگ m نیستند. چون دراین مجموعه m عنصر وجود دارند، یک دستگاه مانده‌ای تام تشکیل خواهند داد.

۳.۵ همنهشتیهای خطی

همنهشتیهای چندجمله‌ای را می‌توان تا حدود زیادی مثل معادلات چندجمله‌ای در جبر

مطالعه کرد. بااینحال، دراینجا به‌چند جمله‌ایهای $f(x)$ با ضرایب صحیح می‌پردازیم؛ درنتیجهٔ، مقادیر این چندجمله‌ایها درصورت صحیح بودن x صحیح می‌باشند. عدد صحیح x صادق در همنهشتی چندجمله‌ای

$$f(x) \equiv 0 \pmod{m} \qquad (۲)$$

یک **جواب** همنهشتی نام دارد. البته، اگر $x \equiv y \pmod{m}$، $f(x) \equiv f(y) \pmod{m}$؛ درنتیجه، هر همنهشتی جوابدار بی‌نهایت جواب دارد. بنابراین، قرار می‌گذاریم جوابهای متعلق به یک ردهٔ مانده‌ای متمایز محسوب نشوند. و وقتی از **تعداد** جوابهای یک همنهشتی نظیر (۲) صحبت می‌شود منظور تعداد جوابهای **ناهمنهشت** است؛ یعنی، تعدادجوابهای موجود در مجموعهٔ $\{1, 2, \ldots, m\}$ یا هر دستگاه مانده‌ای تام به هنگ m دیگر. بنابراین، هرهمنهشتی چندجمله‌ای به هنگ m حداکثر m جواب خواهدداشت.

مثال ۱. همنهشتی خطی $2x \equiv 3 \pmod{4}$ جواب ندارد، زیرا $2x - 3$ به‌ازای هر x فرد است؛ و درنتیجه، نمی‌تواند بر 4 بخشپذیر باشد.

مثال ۲. همنهشتی درجهٔ دو $x^2 \equiv 1 \pmod{8}$ دقیقاً" چهار جواب دارد که عبارتند از $x \equiv 1, 3, 5, 7 \pmod{8}$.

نظریهٔ همنهشتیهای خطی با سه قضیهٔ زیر کاملا" توصیف می‌شود.

قضیهٔ ۱۲۰۵. فرض کنیم $(a, m) = 1$. **دراین صورت، همنهشتی خطی**

$$ax \equiv b \pmod{m} \qquad (۳)$$

دقیقا" یک جواب خواهد داشت.

برهان. فقط کافی است اعداد $1, 2, \ldots, m$ را امتحان کنیم، زیرا این اعداد یک دستگاه مانده‌ای تام تشکیل می‌دهند. لذا، حاصل ضرب $a, 2a, \ldots, ma$ را تشکیل می‌دهیم. چون $(a, m) = 1$، این اعداد نیز یک دستگاه مانده‌ای تام تشکیل می‌دهند. از اینرو، درست یکی از این حاصل ضربها همنهشت b به هنگ m است. یعنی، درست یک x در (۳) صدق می‌کند.

با آنکه قضیهٔ ۱۲۰۵ می‌گوید که همنهشتی خطی (۳) درصورتی که $(a, m) = 1$

جواب منحصر بفرد دارد، طرز تعیین این جواب را نمی‌گوید جز اینکه همهٔ اعداد دریک دستگاه ماندهای تام را امتحان کنیم. روشهای تحقیقی دیگری برای تعیین جواب وجود دارند، که برخی از آنها بعداً" دراین فصل مطرح می‌شوند.

تذکر. اگر $(a, m) = 1$ ، جواب منحصر بفرد همنهشتی $ax \equiv 1 \pmod{m}$ **متقابل** a به هنگ m نامیده می‌شود. اگر a' متقابل a باشد، ba' جواب (۳) خواهد بود.

قضیهٔ ۱۴۰۵ . فرض کنیم $(a, m) = d$. دراین صورت، همنهشتی خطی

$$ax \equiv b \pmod{m} \tag{۴}$$

دارای جواب است اگر و فقط اگر $d|b$.

برهان. اگر یک جواب موجود باشد، $d|b$ زیرا $d|m$ و $d|a$. بعکس، اگر $d|b$ ، همنهشتی

$$\frac{a}{d}x \equiv \frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right)$$

یک‌جواب دارد زیرا $(a/d, m/d) = 1$ ، و این جواب یک جواب (۴) نیز می‌باشد.

قضیهٔ ۱۴۰۵ . فرض کنیم $(a, m) = d$ و $d|b$. دراین صورت، همنهشتی خطی

$$ax \equiv b \pmod{m} \tag{۵}$$

دقیقاً" d جواب به هنگ m دارند. این جوابها عبارتند از

$$t, t + \frac{m}{d}, t + 2\frac{m}{d}, \ldots, t + (d-1)\frac{m}{d}, \tag{۶}$$

که درآنها t جواب (منحصر بفرد به هنگ m/d) همنهشتی خطی

$$\frac{a}{d}x \equiv \frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right) \tag{۷}$$

می‌باشد.

برهان. هر جواب (۷) یک جواب (۵) نیز هست. بعکس، هر جواب (۵) در (۷) صدق می‌کند. اما d عدد مذکور در (۶) جوابهای (۷)، و درنتیجه (۵)، می‌باشند. هیچ دوتا از اینها همنهشت به هنگ m نیستند، زیراروابط

$0 \le r < d, 0 \le s < d$ که درآنها ، $t + r\frac{m}{d} \equiv t + s\frac{m}{d} \pmod{m}$

ایجاب می‌کنند که

$r \equiv s \pmod{d}$ ، درنتیجه ؛ $r\frac{m}{d} \equiv s\frac{m}{d} \pmod{m}$

اما $0 \le |r - s| < d$ ؛ درنتیجه ، $r = s$.

باقی می‌ماند اثبات اینکه (۵) جوابی جز جوابهای (۶) ندارد. هرگاه y یک‌جواب (۵) باشد ،آنگاه $ay \equiv at \pmod{m}$ ؛ درنتیجه ، $y \equiv t \pmod{m/d}$. از اینرو ، به‌ازای k ای ، $y = t + km/d$. اما ، بـه‌ازای r ی صادق در $0 \le r < d$ ، $k \equiv r \pmod{d}$. از اینرو ،

$k\frac{m}{d} \equiv r\frac{m}{d} \pmod{m}$ ؛ درنتیجه ، $y \equiv t + r\frac{m}{d} \pmod{m}$.

بنابراین ، y همنهشت یکی‌ازاعداد (۶) به هنگ m می‌باشد . این برهان را تمام خواهد کـرد .

در فصل ۱ ثابت کردیم که بمعم دو عدد a و b ترکیبی خطی از a و b است . این مطلب را می‌توان از قضیهٔ ۱۴۰۵ نیز نتیجه گرفت .

قضیهٔ ۱۵۰۵ . هرگاه $(a, b) = d$ ، اعداد صحیحی چون x و y وجود دارند بطوری‌که

$$ax + by = d. \tag{۸}$$

برهان . همنهشتی خطـی $ax \equiv d \pmod{b}$ دارای جـواب است .از اینـرو ، عـــدد صحیحی مانند y هست بطوری‌که $d - ax = by$. این نتیجه می‌دهدکه $ax + by = d$، که همان مطلوب است .

تذکر . از نظر هنـدسی ، جفتهـای (x, y) صادق در (۸) نقاط مشبکهٔ واقع بر یک خط مستقیم‌اند . مختص x هریک از این نقاط جواب همنهشتی $ax \equiv d \pmod{b}$ می‌باشد .

۴۰۵ دستگاههای مانده‌ای تحویل یافته و قضیهٔ اویلر ــ فرما

تعریف . منظور از یک *دستگاه مانده‌ای تحویل یافته* به هنگ m یعنی مجموعه‌ای مرکب از $\varphi(m)$ عدد صحیح ناهمنهشت به هنگ m بطوری‌که هریک از آنها نسبت به m اول باشد .

تذکر. $\varphi(m)$ کامل اویلر است، که در فصل ۲ معرفی شد.

قضیهٔ ۱۶.۵ . هرگاه $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ یک دستگاه ماندهای تحویل یافته به هنگ m بوده و $(k, m) = 1$، آنگاه $\{ka_1, ka_2, \ldots, ka_{\varphi(m)}\}$ نیز یک دستگاه ماندهای تحویل یافته به هنگ m میباشد.

برهان. هیچ دو عدد ka_i همنهشت به هنگ m نیستند. همچنین، از اینکه $(a_i, m) = (k, m) = 1$ داریم $(ka_i, m) = 1$؛ درنتیجه، هر ka_i نسبت به m اول میباشد.

قضیهٔ ۱۷.۵ . قضیهٔ اویلر ــ فرما. فرض کنیم $(a, m) = 1$. در این صورت، داریم

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

برهان. فرض کنیم $\{b_1, b_2, \ldots, b_{\varphi(m)}\}$ یک دستگاه ماندهای تحویل یافته به هنگ m باشد. در این صورت، $\{ab_1, ab_2, \ldots, ab_{\varphi(m)}\}$ نیز یک دستگاه ماندهای تحویل یافته است. از اینرو، حاصل ضرب تمام اعداد صحیح در مجموعهٔ اول همنهشت حاصل ضرب اعداد در مجموعهٔ دوم است. بنابراین،

$$b_1 \cdots b_{\varphi(m)} \equiv a^{\varphi(m)} b_1 \cdots b_{\varphi(m)} \pmod m.$$

هر b_i نسبت به m اول است؛ درنتیجه، میتوان با حذف هر b_i قضیه را بدست آورد.

قضیهٔ ۱۸.۵ . هرگاه عدد اول p، a را عاد نکند، آنگاه

$$a^{p-1} \equiv 1 \pmod p.$$

برهان. این نتیجهای است از قضیهٔ پیش، زیرا $\varphi(p) = p - 1$.

قضیهٔ ۱۹.۵ . قضیهٔ کوچک فرما. بهازای هر عدد صحیح a و هر عدد اول p، داریم

$$a^p \equiv a \pmod p.$$

برهان. اگر $p \nmid a$، این قضیهٔ ۱۸.۵ است. اگر $p | a$، a^p و a هر دو همنهشت

0 به هنگ p می‌باشند.

قضیهٔ اویلر ــ فرما را می‌توان برای محاسبهٔ جوابهای یک همنهشتی خطی بکاربرد.

قضیهٔ ۲۰۰۵ . هرگاه $(a, m) = 1$ ، جواب (منحصر بفرد به هنگ m) همنهشتی خطی

$$ax \equiv b \pmod{m} \tag{۹}$$

عبارت است از

$$x \equiv ba^{\varphi(m)-1} \pmod{m}. \tag{۱۰}$$

برهان. عدد x که با (۱۰) داده‌شده، بخاطر قضیهٔ اویلر ــ فرما، در (۹) صدق می‌کند. جواب به هنگ m منحصر بفرد است، زیرا $(a, m) = 1$.

مثال ۱. همنهشتی $5x \equiv 3 \pmod{24}$ را حل کنید.

حل. چون $(5, 24) = 1$ ، یک جواب منحصر بفرد وجود دارد. با استفاده از (۱۰)، معلوم می‌شود که

$$x \equiv 3 \cdot 5^{\varphi(24)-1} \equiv 3 \cdot 5^7 \pmod{24}$$

زیرا $\varphi(24) = \varphi(3)\varphi(8) = 2 \cdot 4$. به هنگ 24 داریم $5^2 \equiv 1$ ، و $5^4 \equiv 5^6 \equiv 1$ ، $5^7 \equiv 5$ ؛ درنتیجه، $x \equiv 15 \pmod{24}$.

مثال ۲. همنهشتی $25x \equiv 15 \pmod{120}$ را حل کنید.

حل. چون $d = (25, 120) = 5$ و $d|15$ ، همنهشتی دقیقا " پنج جواب به هنگ 120 دارد. برای یافتن آنها بر 5 تقسیم کرده و همنهشتی $5x \equiv 3 \pmod{24}$ را حل می‌کنیم. بااستفاده از مثال ۱ و قضیهٔ ۱۴۰۵، معلوم می‌شود که پنج جواب عبارتند از $x = 15 + 24k, k = 0, 1, 2, 3, 4$ ، یا

$$x \equiv 15, 39, 63, 87, 111 \pmod{120}.$$

۵۰۵ همنهشتیهای چند جمله‌ای به هنگ p . قضیهٔ لاگرانژ

قضیهٔ اساسی جبر می‌گوید که، به‌ازای هر چند جمله‌ای f از درجهٔ $n \geq 1$ ، معادلهٔ

$f(x) = 0$ دارای n جواب در اعداد مختلط است. مشابه مستقیم این قضیه برای همنهشتیهای چندجمله‌ای وجود ندارد. مثلاً، دیدیم که بعضی از همنهشتیهای خطی جواب ندارند، بعضی درست یک جواب دارند، و بعضی بیش از یک جواب دارند. لذا، حتی در این حالت خاص، ظاهراً رابطهٔ ساده‌ای بین تعداد جوابها و درجهٔ چندجمله‌ای وجود ندارد. لیکن، برای همنهشتیها به هنگ یک **عدد اول**، قضیهٔ زیر را از لاگرانژ داریم.

قضیهٔ ۲۱.۵ (لاگرانژ). *به‌ازای عدد اول p، فرض کنیم*

$$f(x) = c_0 + c_1 x + \cdots + c_n x^n$$

یک چندجمله‌ای از درجهٔ n با ضرایب صحیح باشد بطوری که $c_n \not\equiv 0 \pmod p$. در این صورت، همنهشتی چندجمله‌ای

$$f(x) \equiv 0 \pmod p \qquad (۱۱)$$

حداکثر n جواب خواهد داشت.

تذکر. این نتیجه برای هنگهای مرکب درست نیست. مثلاً، همنهشتی درجهٔ دو $x^2 \equiv 1 \pmod 8$ چهار جواب دارد.

برهان. از استقرا روی n، یعنی درجهٔ f، استفاده می‌کنیم. وقتی $n = 1$، همنهشتی خطی است:

$$c_1 x + c_0 \equiv \pmod p.$$

چون $c_1 \not\equiv 0 \pmod p$، داریم $(c_1, p) = 1$ و دقیقاً یک جواب وجود دارد. پس فرض کنیم قضیه برای چندجمله‌ایهای درجهٔ $n-1$ درست باشد. همچنین، فرض کنیم همنهشتی (۱۱) دارای $n+1$ جواب ناهمنهشت به هنگ p باشد، مثلاً،

$$x_0, x_1, \ldots, x_n,$$

که در آنها به‌ازای هر $k = 0, 1, \ldots, n$، $f(x_k) \equiv 0 \pmod p$. حال تناقض بدست می‌آوریم. اتحاد جبری

$$f(x) - f(x_0) = \sum_{r=1}^{n} c_r(x^r - x_0^r) = (x - x_0)g(x)$$

را داریم، که در آن $g(x)$ یک چندجمله‌ای درجهٔ $n-1$ با ضرایب صحیح و ضریب پیشرو c_n است. لذا، چون $f(x_k) \equiv f(x_0) \equiv 0 \pmod p$، داریم

$$f(x_k) - f(x_0) = (x_k - x_0)g(x_k) \equiv 0 \pmod p.$$

اما، اگر $k \neq 0$ ، $x_k - x_0 \not\equiv 0 \pmod p$ ؛ درنتیجه، باید به‌ازای هر $k \neq 0$ داشته باشیم $g(x_k) \equiv 0 \pmod p$. این یعنی همنهشتی $g(x) \equiv 0 \pmod p$ دارای n جواب ناهمنهشت به هنگ p است، که با فرض استقرا متناقض می‌باشد. این برهان را تمام خواهد کرد.

۶.۵ کاربردهای قضیهٔ لاگرانژ

قضیهٔ ۲۲.۵ . *هرگاه $f(x) = c_0 + c_1x + \cdots + c_nx^n$ یک چندجمله‌ای از درجهٔ n با ضرایب صحیح بوده، و همنهشتی*

$$f(x) \equiv 0 \pmod p$$

بیش از n جواب داشته باشد، که درآن p اول است، آنگاه هر ضریب f بر p بخشپذیر خواهد بود.

برهان. اگرضریبی بر p بخشپذیرنباشد، c_k راآن ضریب با بیشترین اندیس می‌گیریم. دراین صورت، $k \leq n$ و همنهشتی

$$c_0 + c_1x + \cdots + c_kx^k \equiv 0 \pmod p$$

بیش‌از k جواب دارد؛ درنتیجه، بنابر قضیهٔ لاگرانژ، $p|c_k$ ، که یک تناقض می‌باشد.

حال قضیهٔ ۲۲.۵ را بر یک چندجمله‌ای خاص اعمال می‌کنیم.

قضیهٔ ۲۳.۵ . *به‌ازای هر عدد اول p ، همهٔ ضریبهای چندجمله‌ای*

$$f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$$

بر p بخشپذیر است.

برهان. فرض‌کنیم $g(x) = (x-1)(x-2)\cdots(x-p+1)$. ریشه‌های g عبارتند از $1, 2, \ldots, p-1$ ؛ درنتیجه، در همنهشتی

$$g(x) \equiv 0 \pmod p$$

صدق می‌کنند. بنابر قضیهٔ اویلر ــ فرما، این اعداد در همنهشتی $h(x) \equiv 0 \pmod p$ نیز صدق می‌کنند، که درآن

$$h(x) = x^{p-1} - 1.$$

تفاضل $f(x) = g(x) - h(x)$ از درجهٔ $p-2$ است ولی همنهشتی $f(x) \equiv 0 \pmod p$

دارای $p-1$ جواب $1,\ 2,\dots,p-1$ می‌باشد. بنابراین، طبق قضیهٔ ۲۲.۵، هرضریب $f(x)$ بر p بخشپذیر است.

دو قضیهٔ بعدی با توجه به دو ضریب خاص چندجمله‌ای $f(x)$ در قضیهٔ ۲۳.۵ بدست می‌آیند.

قضیهٔ ۲۴.۵ . قضیهٔ ویلسون[1] . *به‌ازای هر عدد اول p، داریم*

$$(p-1)! \equiv -1 \pmod p.$$

برهان. جملهٔ ثابت چندجمله‌ای $f(x)$ در قضیهٔ ۲۳.۵ عبارت است از $(p-1)!+1$.

تذکر. عکس قضیهٔ ویلسون نیز برقرار است. یعنی، اگر $n>1$ و $(n-1)! \equiv -1 \pmod n$، n اول می‌باشد. (ر.ک. تمرین ۷.۵)

قضیهٔ ۲۵.۵ . قضیهٔ ولستن هولم[2] . *به‌ازای هر عدد اول $p \geq 5$، داریم*

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}.$$

برهان. مجموع مورد نظر مجموع حاصل ضربهای اعداد $1, 2, \dots, p-1$ است هربار $p-2$ تا. این مجموع نیز مساوی ضریب $x-$ در چندجمله‌ای

$$g(x) = (x-1)(x-2)\cdots(x-p+1)$$

است. درواقع، $g(x)$ را می‌توان به‌شکل زیر نوشت:

$$g(x) = x^{p-1} - S_1x^{p-2} + S_2x^{p-3} - \cdots + S_{p-3}x^2 - S_{p-2}x + (p-1)!,$$

که درآن ضریب S_k تابع متقارن مقدماتی k ام از ریشه‌هاست؛ یعنی، مجموع حاصل‌ضربهای اعداد $1, 2, \dots, p-1$ هربار k تا. قضیهٔ ۲۳.۵ نشان می‌دهد که هریک از اعداد $S_1, S_2, \dots, S_{p-2}$ بر p بخشپذیر است. می‌خواهیم نشان دهیم که S_{p-2} بر p^2 بخشپذیر است.

حاصل ضرب مربوط به $g(x)$ نشان می‌دهد که $g(p) = (p-1)!$؛ درنتیجه،

---

1. Wilson 2. Wolstenholme

$$(p-1)! = p^{p-1} - S_1 p^{p-2} + \cdots + S_{p-3} p^2 - S_{p-2} p + (p-1)!.$$

با حذف $(p-1)!$ و تحویل معادله با $\mod p^3$ ، معلوم می‌شود که، چون $p > 5$ ،

$$pS_{p-2} \equiv 0 \pmod{p^3};$$

و درنتیجه، همانطور که مطلوب است، $S_{p-2} \equiv 0 \pmod{p^2}$.

۷.۵ همنهشتیهای خطی همزمان. قضیهٔ باقیماندهٔ چینی

یک دستگاه از دو یا چند همنهشتی خطی لزوماً جواب ندارد، حتی اگر هر همنهشتی جواب داشته باشد. مثلاً x ی نیست که در $x \equiv 1 \pmod 2$ و $x \equiv 0 \pmod 4$ صدق کند، اگرچه هریک از این همنهشتیها جداگانه جواب دارند. دراین مثال، هنگهای 2 و 4 نسبت بهم اول نیستند. ذیلاً ثابت می‌کنیم که هر دستگاه از دو یا چند همنهشتی خطی که هریک جواب منحصر بفرد دارند را می‌توان درصورتی حل کرد که هنگها دوبدو نسبت بهم اول باشند. با یک حالت خاص شروع می‌کنیم.

قضیهٔ ۲۶.۵ . قضیهٔ باقیماندهٔ چینی. *فرض‌کنیم $m_1, \ldots, m_r$ اعداد صحیح‌مثبتی باشند دوبدو نسبت بهم اول:*

اگر $i \neq k$ ، $(m_i, m_k) = 1$.

همچنین، $b_1, \ldots, b_r$ اعداد صحیح‌دلخواهی باشند. دراین صورت، دستگاه همنهشتیهای

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ x &\equiv b_r \pmod{m_r} \end{aligned}$$

دقیقاً یک جواب به هنگ حاصل ضرب $m_1 \cdots m_r$ خواهد داشت.

برهان. فرض کنیم $M = m_1 \cdots m_r$ و $M_k = M/m_k$. دراین صورت $(M_k, m_k) = 1$ ؛ درنتیجه، هر M_k متقابل منحصر بفرد M'_k به هنگ m_k را دارد. حال فرض می‌کنیم

$$x = b_1 M_1 M'_1 + b_2 M_2 M'_2 + \cdots + b_r M_r M'_r.$$

هر جمله دراین مجموع را به هنگ m_k درنظر می‌گیریم. چون به‌ازای $i \neq k$ ، $M_i \equiv 0 \pmod{m_k}$ ، خواهیم داشت

$$x \equiv b_k M_k M'_k \equiv b_k \pmod{m_k}.$$

لذا، x در هر همنهشتی دستگاه صدق می‌کند. اما به‌آسانی معلوم می‌شود که دستگاه فقط یک جواب به هنگ M دارد. درواقع، اگر x و y دو جواب دستگاه باشند، به‌ازای هر

k داریم $x \equiv y \pmod{m_k}$ و، چون m_k ها دوبدو نسبت بهم اولند، نیز خواهیم داشت $x \equiv y \pmod{M}$. این برهان را تمام خواهد کرد.

حال تعمیم زیر به‌آسانی قابل حصول است.

قضیهٔ ۲۷۰۵ . *فرض‌کنیم $m_1, \ldots, m_r$ دوبدو نسبت بهم اول باشند. همچنین، $b_1, \ldots, b_r$ اعداد صحیح دلخواهی بوده و $a_1, \ldots, a_r$ در روابط زیر صدق کنند:*

به‌ازای $k = 1, 2, \ldots, r$، $(a_k, m_k) = 1$.

دراین صورت، دستگاه همنهشتیهای خطی

$$a_1 x \equiv b_1 \pmod{m_1}$$
$$\vdots$$
$$a_r x \equiv b_r \pmod{m_r}$$

دقیقاً " یک جواب به هنگ $m_1 m_2 \cdots m_r$ خواهد داشت.

برهان. فرض‌کنیم a'_k متقابل a_k به هنگ m_k باشد. این متقابل وجود دارد زیرا $(a_k, m_k) = 1$. پس‌همنهشتی $a_k x \equiv b_k \pmod{m_k}$ معادل‌همنهشتی $x \equiv b_k a'_k \pmod{m_k}$ است. حال قضیهٔ ۲۶۰۵ را بکار می‌بریم.

۸۰۵ کاربردهای قضیه باقیماندهٔ چینی

اولین کاربرد مربوط است به همنهشتیهای چندجمله‌ای با هنگهای مرکب.

قضیهٔ ۲۸۰۵ . *فرض‌کنیم f یک چندجمله‌ای با ضرایب صحیح بوده، $m_1, m_2, \ldots, m_r$ اعداد صحیح مثبتی باشند که دوبدو نسبت بهم اولند، و $m = m_1 m_2 \cdots m_r$. دراین صورت، همنهشتی*

$$f(x) \equiv 0 \pmod{m} \qquad (۱۲)$$

دارای جواب است اگر و فقط اگر هر همنهشتی

$$f(x) \equiv 0 \pmod{m_i} \qquad (i = 1, 2, \ldots, r) \qquad (۱۳)$$

جواب داشته باشد. بعلاوه، هرگاه $\nu(m)$ و $\nu(m_i)$ بترتیب تعداد جوابهای (۱۲) و (۱۳) باشند، آنگاه

$$\nu(m) = \nu(m_1)\nu(m_2) \cdots \nu(m_r). \qquad (۱۴)$$

برهان. هرگاه $f(a) \equiv 0 \pmod m$، آنگاه، بهازای هر i، $f(a) \equiv 0 \pmod{m_i}$. بنابراین، هر جواب (۱۲) یک جواب (۱۳) نیز هست.

بعکس، فرض‌کنیم a_i یک‌جواب (۱۳) باشد. دراین صورت، طبق قضیهٔ باقیماندهٔ چینی، عدد صحیحی مانند a هست بطوری که

بهازای $i = 1, 2, \ldots, r$، $a \equiv a_i \pmod{m_i}$؛ (۱۵)

درنتیجه،

$$f(a) \equiv f(a_i) \equiv 0 \pmod{m_i}.$$

چون هنگها دوبدو نسبت بهم اولند، نیز داریم $f(a) \equiv 0 \pmod m$. از اینرو، اگر هر همنهشتی در (۱۳) جواب داشته باشد، (۱۲) نیز جواب خواهد داشت.

همچنین، بنابر قضیهٔ ۲۶.۵، می‌دانیم که هر r تایی $(a_1, \ldots, a_r)$ از جوابهای همنهشتیهای (۱۳) عدد صحیح و منحصر بفرد a به هنگ m می‌دهد که در (۱۵) صادق است. وقتی هر a_i، $v(m_i)$ جواب (۱۳) را بگیرد، تعداد اعداد صحیح a صادق در (۱۵)، و درنتیجه (۱۳)، مساوی $v(m_1) \cdots v(m_r)$ است. این (۱۴) را ثابت خواهد کرد.

تذکر. اگر m تجزیه به‌عوامل اول

$$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

را داشته باشد، می‌توان در قضیهٔ ۲۸.۵ فرض کرد $m_i = p_i^{\alpha_i}$ و دید که مسئلهٔ حل یک همنهشتی چندجمله‌ای‌برای‌یک هنگ مرکب به مسئله درمورد هنگها به‌صورت توان اعداد اول تحویل می‌شود. بعدها نشان می‌دهیم که مسئله را می‌توان بیشتر به همنهشتیهای چندجمله‌ای یا هنگهای اول بعلاوهٔ مجموعه‌ای از همنهشتیهای خطی تحویل کرد. (ر.ک. بخش ۹.۵.)

کاربرد بعدی قضیهٔ باقیماندهٔ چینی مربوط‌است به مجموعهٔ نقاط مشبکهٔ قابل رویت از مبداء. (ر.ک. بخش ۸.۳.)

قضیهٔ ۲۹.۵. مجموعهٔ نقاط مشبکه در صفحه و قابل رویت از مبداء شامل رخنه‌های مربعی‌بدلخواه بزرگ‌است. یعنی، بهازای هر عدد صحیح $k > 0$، یک نقطهٔ مشبکه‌مانند (a, b) هست بطوری که هیچیک از نقاط مشبکهٔ

$$(a + r, b + s), \quad 0 < r \le k, 0 < s \le k$$

از مبداء قابل رویت نیست.

برهان. فرض کنیم $p_1, p_2, \ldots$ دنباله‌ای از اعداد اول باشد. به‌ازای $k > 0$، ماتریس $k \times k$ ای را درنظر می‌گیریم که درایه‌های اولین سطرش از اولین k عدد اول، درایه‌های دومین سطرش از k عدد اول بعدی تشکیل شده است، و غیره. فرض کنیم m_i حاصل ضرب اعداد اول در سطر i م بوده و M_i حاصل ضرب اعداد اول در ستون i م باشد. دراین صورت، اعداد m_i دوبدو نسبت بهم اولند، مثل M_i ها.

حال مجموعهٔ همنهشتیهای زیر را درنظر می‌گیریم:

$$\begin{aligned} x &\equiv -1 \pmod{m_1} \\ x &\equiv -2 \pmod{m_2} \\ &\vdots \\ x &\equiv -k \pmod{m_k}. \end{aligned}$$

این دستگاه جوابی مانند a دارد که به هنگ $m_1 \cdots m_k$ منحصر بفرد است. بهمین نحو، دستگاه

$$\begin{aligned} y &\equiv -1 \pmod{M_1} \\ &\vdots \\ y &\equiv -k \pmod{M_k} \end{aligned}$$

جوابی مانند b دارد که با $\operatorname{mod} M_1 \cdots M_k = m_1 \cdots m_k$ منحصر بفرد است.

حال مربعی با رئوس متقابل (a, b) و $(a + k, b + k)$ را درنظر می‌گیریم. هر نقطهٔ مشبکهٔ داخل این مربع به‌شکل

$(a + r, b + s)$ است، که درآن $0 < r < k, 0 < s < k$،

و نقاطی که درآنها $r = k$ یا $s = k$ برکرانهٔ مربع قرار دارند. حال نشان می‌دهیم که هیچیک از این نقاط از مبداء قابل رویت نیست. درواقع،

$a \equiv -r \pmod{m_r}$ و $b \equiv -s \pmod{M_s}$؛

درنتیجه، عدد اول واقع در سطر r و ستون s هر دوی $a + r$ و $b + s$ را عاد می‌کند. بنابراین، $a + r$ و $b + s$ نسبت بهم اول نیستند؛ و لذا، نقطهٔ مشبکهٔ $(a + r, b + s)$ از مبداء قابل رویت نمی‌باشد.

۹.۵ همنهشتیهای چند جمله‌ای به هنگهای توان اعداد اول

قضیهٔ ۲۸.۵ نشان می‌دهد که مسئلهٔ حل یک همنهشتی چندجمله‌ای

$$f(x) \equiv 0 \pmod{m}$$

را می‌توان به‌حل یک دستگاه از همنهشتیها مانند

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \qquad (i = 1, 2, \ldots, r)$$

تحویل کرد، که درآن $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. دراین بخش، نشان می‌دهیم که مسئله را می‌توان بیشتر به همنهشتیها با هنگهای اول بعلاوهٔ مجموعه‌ای از همنهشتیهای خطی تحویل کرد.

فرض کنیم f یک چندجمله‌ای با ضرایب صحیح بوده، و به‌ازای عدد اولی چون p و $\alpha \geq 2$ ای، همنهشتی

$$f(x) \equiv 0 \pmod{p^\alpha} \tag{۱۶}$$

جوابی مانند $x = a$ داشته باشد، که درآن a طوری انتخاب شده است که در بازهٔ

$$0 \leq a < p^\alpha$$

قرار دارد. این جواب در هر همنهشتی $f(x) \equiv 0 \pmod{p^\beta}$ به‌ازای هر $\alpha > \beta$ صدق می‌کند. بالاخص، a در همنهشتی

$$f(x) \equiv 0 \pmod{p^{\alpha-1}} \tag{۱۷}$$

صدق می‌کند. حال a را بر $p^{\alpha-1}$ تقسیم کرده و می‌نویسیم

$$a = qp^{\alpha-1} + r \text{ ، که درآن } 0 \leq r < p^{\alpha-1} . \tag{۱۸}$$

گوییم باقیماندهٔ r که با (۱۸) مشخص می‌شود به‌وسیلهٔ a **تولید** می‌گردد. چون $r \equiv a \pmod{p^{\alpha-1}}$ ، عدد r یک جواب (۱۷) نیز هست. به‌عبارت دیگر، هر جواب a ازهمنهشتی (۱۶) در بازهٔ $0 \leq a < p^\alpha$ جوابی از همنهشتی (۱۷) مانند r دربازهٔ $0 \leq r < p^{\alpha-1}$ تولید می‌کند.

حال فرض کنیم باجواب r از (۱۷) دربازهٔ $0 \leq r < p^{\alpha-1}$ شروع کرده ومی‌پرسیم آیا جوابی مانند a از (۱۶) دربازهٔ $0 \leq a < p^\alpha$ وجود دارد که r را تولید کند. اگر چنین‌باشد، می‌گوییم r را می‌توان از $p^{\alpha-1}$ تا p^α *بالا برد*. قضیهٔ بعدی نشان می‌دهد که امکان بالا بردن r به $f(r)$ به هنگ p^α و مشتق $f'(r)$ به هنگ p بستگی‌دارد.

قضیهٔ ۵ . ۳۰ . *فرض‌کنیم $\alpha \geq 2$ و r جوابی از همنهشتی*

$$f(x) \equiv 0 \pmod{p^{\alpha-1}} \tag{۱۹}$$

واقع در بازهٔ $0 \leq r < p^{\alpha-1}$ باشد.

(آ) فرض کنیم $f'(r) \not\equiv 0 \pmod{p}$. دراین صورت، r را می‌توان به‌طور منحصر بفرد از $p^{\alpha-1}$ تا p^α بالا برد. یعنی، a ی منحصر بفردی در بازهٔ $0 \leq a < p^\alpha$ هست که r را

تولید و در همنهشتی

$$f(x) \equiv 0 \pmod{p^\alpha} \tag{۲۰}$$

صدق می‌کند.

(ب) فرض کنیم $f'(r) \equiv 0 \pmod p$. دراین صورت، دوحالت وجود دارند:

(ب-۱) اگر $f(r) \equiv 0 \pmod{p^\alpha}$ ، r را می‌توان به p طریق مختلف از $p^{\alpha-1}$ تا p^α بالا برد؛

(ب-۲) اگر $f(r) \not\equiv 0 \pmod{p^\alpha}$ ، r را نمی‌توان از $p^{\alpha-1}$ تا p^α بالا برد.

برهان. اگر n درجهٔ f باشد، به‌ازای هر x و h اتحاد (فرمول تیلور) زیر را داریم:

$$f(x+h) = f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + \cdots + \frac{f^{(n)}(x)}{n!}h^n. \tag{۲۱}$$

توجه کنید که هرچند جمله‌ای $f^{(k)}(x)/k!$ دارای ضرایب صحیح است. (خواننده باید این راتحقیق کند.) حال در (۲۱) $x = r$ را اختیار می‌کنیم، که درآن r یک جواب (۱۹) دربازهٔ $0 \le r < p^{\alpha-1}$ است، و فرض می‌کنیم $h = qp^{\alpha-1}$ ، که درآن q یک عدد صحیح است که بزودی مشخص می‌شود. چون $\alpha \ge 2$ ، جملات (۲۱) که شامل h^2 و توانهای بالاتراز h اند مضارب‌صحیحی‌از p^α می‌باشند. بنابراین، (۲۱) همنهشتی زیر را بدست می‌دهد:

$$f(r + qp^{\alpha-1}) \equiv f(r) + f'(r)qp^{\alpha-1} \pmod{p^\alpha}.$$

چون r در (۱۹) صدق می‌کند، به‌ازای‌عددصحیحی چون k می‌توان نوشت $f(r) = kp^{\alpha-1}$ و آخرین همنهشتی به‌صورت زیر درمی‌آید:

$$f(r + qp^{\alpha-1}) \equiv \{qf'(r) + k\}p^{\alpha-1} \pmod{p^\alpha}.$$

حال فرض کنیم

$$a = r + qp^{\alpha-1}. \tag{۲۲}$$

دراین صورت، a در همنهشتی (۲۰) صدق می‌کند اگر و فقط‌اگر q در همنهشتی خطی

$$qf'(r) + k \equiv 0 \pmod p \tag{۲۳}$$

صدق کند. اگر $f'(r) \not\equiv 0 \pmod p$ ، این همنهشتی جواب منحصر بفرد q به هنگ p دارد، و اگر q دربازهٔ $0 \le q < p$ اختیار شود، عدد a که با (۲۲) داده می‌شود در (۲۰) صدق خواهد کرد و در بازهٔ $0 \le a < p^\alpha$ قرار خواهد داشت.

از آن‌سو، اگر $f'(r) \equiv 0 \pmod p$ ، (۲۳) جوابی مانند q دارد اگر و فقط‌اگر $p|k$؛ یعنی، اگر و فقط‌اگر $f(r) \equiv 0 \pmod{p^\alpha}$. اگر $p \nmid k$ ، q ای نمی‌توان اختیارکرد

که a در (۲۰) صدق کند. اما، اگر $p|k$ ، p مقدار $q = 0, 1, \ldots, p-1$ ، p جواب a از (۲۰) بدست می‌دهند که r را تولید کرده و در بازهٔ $0 \leq a < p^\alpha$ قرار دارند. این برهان را تمام خواهد کرد.

برهان قضیهٔ پیش روشی برای بدست آوردن جوابهای همنهشتی (۲۰) درصورت معلوم بودن جوابهای (۱۹) نیز توصیف می‌کند. با اعمال مکرر این روش، مسئله مآلاً به‌مسئلهٔ حل همنهشتی

$$f(x) \equiv 0 \pmod{p} \tag{۲۴}$$

تحویل می‌شود.

اگر (۲۴) جواب نداشته باشد، (۲۰) نیز جواب ندارد. اگر (۲۴) جواب داشته باشد، یکی از آنها، مثلاً r ، را که در بازهٔ $0 \leq r < p$ قرار دارد انتخاب می‌کنیم. متناظر r ، 0 ، 1 ، یا p جواب همنهشتی

$$f(x) \equiv 0 \pmod{p^2}, \tag{۲۵}$$

بسته‌به‌تعداد $f'(r)$ و $k = f(r)/p$ ، وجوددارند. اگر $p \nmid k$ و $p|f'(r)$ ، r را نمی‌توان تا یک جواب (۲۵) بالا برد. دراین‌حالت، از نو با جواب متفاوت r شروع می‌کنیم. اگر هیچ r را نشود بالا برد، (۲۵) جواب نخواهد داشت.

اگر به‌ازای r ی $p|k$ ، همنهشتی خطی

$$qf'(r) + k \equiv 0 \pmod{p}$$

را امتحان می‌کنیم. این همنهشتی، بنابرآنکه $p \nmid f'(r)$ یا $p|f'(r)$ ، دارای 1 یا p جواب q است. به‌ازای‌هرجواب q ، عدد $a = r + qp$ یک جواب (۲۵) است. به‌ازای هر جواب (۲۵)، می‌توان، با استفاده از روندی مشابه، همهٔ جوابهای

$$f(x) \equiv 0 \pmod{p^3}$$

را پیدا کرد، و بهمین ترتیب ادامه داد تا همهٔ جوابهای (۲۰) بدست آیند.

۵.۱۰ اصل رده‌بندی چلیپایی

بعضی ازمسائل نظریهٔ اعداد رامی‌توان با اعمال یک قضیهٔ ترکیباتی کلی درباب مجموعه‌ها به‌نام ***اصل رده‌بندی چلیپایی*** مطالعه کرد. این اصل فرمولی است که تعداد عنصرهای مجموعهٔ متناهی S را که به‌زیرمجموعه‌های ازپیش معلوم $S_1, \ldots, S_n$ تعلق ندارند می‌شمارد.

نمادگذاری. هرگاه T یک زیرمجموعهٔ S باشد، برای‌تعداد عناصر T می‌نویسیم $N(T)$.

همچنین، $S - T$ مجموعهٔ تمام عناصری از S است که در T نیستند. بنابراین،

$$S - \bigcup_{i=1}^{n} S_i$$

از عناصری از S تشکیل شده که در هیچ زیرمجموعهٔ $S_1, \ldots, S_n$ نیست. برای اختصار، به‌جای اشتراکهای... $S_i \cap S_j,\ S_i \cap S_j \cap S_k,$ بترتیب می‌نویسیم ... $S_iS_j,\ S_iS_jS_k, \ldots$.

قضیهٔ ۵.۱۰۳. اصل رده‌بندی چلیپایی. *هرگاه $S_1, \ldots, S_n$ زیرمجموعه‌هایی از مجموعهٔ متناهی S باشند، آنگاه*

$$N\left(S - \bigcup_{i=1}^{n} S_i\right) = N(S) - \sum_{1 \le i \le n} N(S_i) + \sum_{1 \le i < j \le n} N(S_iS_j)$$
$$- \sum_{1 \le i < j < k \le n} N(S_iS_jS_k) + \cdots + (-1)^n N(S_1S_2 \cdots S_n).$$

برهان. هرگاه $T \subseteq S$، $N_r(T)$ را تعداد عناصر T می‌گیریم که درهیچیک از r زیر مجموعهٔ اول $S_1, \ldots, S_r$ نیستند، و $N_0(T)$ را خود $N(T)$ می‌گیریم. عناصری که با $N_{r-1}(T)$ شماره می‌شوند به دو مجموعهٔ از هم جدا تجزیه می‌شوند، آنهایی که در S_r نیستند و آنهایی که در S_r هستند. بنابراین، داریم

$$N_{r-1}(T) = N_r(T) + N_{r-1}(TS_r).$$

از اینرو،

$$N_r(T) = N_{r-1}(T) - N_{r-1}(TS_r). \tag{۲۶}$$

حال $T = S$ را اختیار و، با استفاده از (۲۶)، هر جملهٔ سمت راست را برحسب N_{r-2} بیان می‌کنیم. داریم

$$N_r(S) = \{N_{r-2}(S) - N_{r-2}(SS_{r-1})\} - \{N_{r-2}(S_r) - N_{r-2}(S_rS_{r-1})\}$$
$$= N_{r-2}(S) - N_{r-2}(S_{r-1}) - N_{r-2}(S_r) + N_{r-2}(S_rS_{r-1}).$$

با اعمال مکرر (۲۶)، مآلاً" خواهیم داشت

$$N_r(S) = N_0(S) - \sum_{i=1}^{r} N_0(S_i) + \sum_{1 \le i < j \le r} N_0(S_iS_j) - \cdots + (-1)^r N_0(S_1 \cdots S_r).$$

این، وقتی $r = n$، فرمول مطلوب را خواهد داد.

مثال. فرمول حاصل ضرب برای کامل اویلر را می‌توان از اصل رده‌بندی چلیپایی بدست

آورد. فرض کنیم $p_1, \ldots, p_r$ مقسوم‌علیه‌های اول متمایز n باشند. همچنین، $S = \{1, 2, \ldots, n\}$ و S_k زیرمجموعهٔ S مرکب از اعداد صحیحی باشد که بر p_k بخشپذیراند. اعداد در S و نسبت به n اول آنهایی هستند که در هیچیک از مجموعه‌های $S_1, \ldots, S_r$ قرار ندارند؛ درنتیجه،

$$\varphi(n) = N\left(S - \bigcup_{k=1}^{r} S_k\right).$$

اگر $d|n$، n/d مضرب از d در S وجود دارند. بنابراین،

$$N(S_i) = \frac{n}{p_i}, N(S_i S_j) = \frac{n}{p_i p_j}, \ldots, N(S_1 \cdots S_r) = \frac{n}{p_1 \cdots p_r};$$

درنتیجه، از اصل رده‌بندی چلیپایی حاصل می‌شود

$$\begin{aligned}\varphi(n) &= n - \sum_{i=1}^{n} \frac{n}{p_i} + \sum_{1 \le i < j \le r} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 \cdots p_r} \\ &= n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right).\end{aligned}$$

درکاربرد بعدی اصل رده‌بندی چلیپایی، تعداد عناصر یک دستگاه مانده‌ای تحویل یافته به هنگ k که به یک ردهٔ مانده‌ای r به هنگ d، که $d|k$ و $(r, d) = 1$، تعلق دارد شمرده خواهد شد.

قضیهٔ ۳۲.۵. *اعداد صحیح* r، d، و k **مفروضند بطوری‌که** $d|k$، $0 < d$، $k \ge 1$، و $(r, d) = 1$. **دراین صورت، تعداد عناصر مجموعهٔ**

$$S = \{r + td : t = 1, 2, \ldots, k/d\}$$

که نسبت به k *اولند مساوی* $\varphi(k)/\varphi(d)$ *می‌باشد*.

برهان. هرگاه عدد اول p، k و $r + td$ را عاد کند، آنگاه $p \nmid d$؛ درغیر این صورت، $p|r$، که با فرض $(r, d) = 1$ متناقض است. از اینرو، اعداد اولی که k را عاد می‌کنند و عنصری از S اند آنهایی هستند که k را عاد می‌کنند ولی d را عاد نمی‌کنند. آنها را $p_1, \ldots, p_m$ نامیده و فرض می‌کنیم

$$k' = p_1 p_2 \cdots p_m.$$

دراین صورت، عناصری از S که نسبت به k اولند آنهایی هستند که برهیچیک از این

اعداد اول بخشپذیر نیستند . فرض کنیم

$$S_i = \{x : x \in S \quad , \quad p_i | x\} \qquad (i = 1, 2, \ldots, m).$$

هرگاه $x \in S_i$ و $x = r + td$ ، آنگاه $r + td \equiv 0 \pmod{p_i}$. چون $p_i \nmid d$ ، یک t منحصر بفرد به هنگ p_i دارای این خاصیت وجود دارد ، بنابراین ، دقیقا" یک t در هربازهٔ $[1, p_i], [p_i + 1, 2p_i], \ldots, [(q-1)p_i + 1, qp_i]$ ، که $qp_i = k/d$ ، وجوددارد . بنابراین ،

$$N(S_i) = \frac{k/d}{p_i}.$$

بهمین ترتیب ،

$$N(S_i S_j) = \frac{k/d}{p_i p_j}, \ldots, N(S_1 \cdots S_m) = \frac{k/d}{p_1 \cdots p_m}.$$

بنابراین ، طبق اصل رده‌بندی چلیپایی ، تعداد اعداد صحیح در S و نسبت به k اول مساوی است با

$$N\left(S - \bigcup_{i=1}^{m} S_i\right) = \frac{k}{d} \sum_{\delta | k'} \frac{\mu(\delta)}{\delta} = \frac{k}{d} \prod_{p | k'} \left(1 - \frac{1}{p}\right) = \frac{k \prod_{p|k} \left(1 - \frac{1}{p}\right)}{d \prod_{p|d} \left(1 - \frac{1}{p}\right)} = \frac{\varphi(k)}{\varphi(d)}.$$

۱۱.۵ خاصیت تجزیهٔ دستگاههای مانده‌ای تحویل یافته

به‌عنوان کاربردی از قضیهٔ پیش، خاصیتی از دستگاههای مانده‌ای تحویل یافته را مطرح می‌کنیم که در یکی از فصول آتی بکار می‌رود . با یک مثال عددی شروع می‌کنیم .

فرض کنیم S یک دستگاه مانده‌ای تحویل یافته به هنگ 15 باشد ؛ مثلا" ،

$$S = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

8 عنصر S را با یک ماتریس 2×4 به‌صورت زیر نشان می‌دهیم:

$$\begin{bmatrix} 1 & 2 \\ 4 & 8 \\ 7 & 11 \\ 13 & 14 \end{bmatrix}.$$

توجه‌کنید که هرسطر شامل یک دستگاه مانده‌ای تحویل یافته‌به هنگ 3 است ، و اعداد هر ستون همنهشت یکدیگربه هنگ 3 هستند . این‌مثال یک خاصیت عمومی دستگاههای مانده‌ای تحویل یافته را نشان می‌دهد که در قضیهٔ زیر توصیف شده است .

قضیهٔ ۳۳.۵ . *فرض‌کنیم S یک دستگاه مانده‌ای تحویل یافته به هنگ k بوده، و $d > 0$ یک مقسوم‌علیه k باشد. دراین صورت، تجزیه‌های زیر از S را خواهیم داشت:*
(آ) S اجتماع $\varphi(k)/\varphi(d)$ مجموعهٔ از هم‌جداست ، هرکدام یک دستگاه مانده‌ای تحویل یافته به هنگ d ؛
(ب) S اجتماع $\varphi(d)$ مجموعهٔ ازهم‌جداست ، هریک مرکب از $\varphi(k)/\varphi(d)$ عدد همنهشت یکدیگر به هنگ d .

تذکر. در مثال پیش، $k = 15$ و $d = 3$. سطرهای ماتریس مجموعه‌های از هم‌جدای قسمت (آ) ، و ستونهای آن مجموعه‌های از هم‌جدای قسمت (ب) را نشان می‌دهند. اگر قضیه را برای مقسوم علیه $d = 5$ بکار بریم ،تجزیه‌ای بدست می‌آید که با ماتریس زیر داده می‌شود:

$$\begin{bmatrix} 1 & 2 & 4 & 8 \\ 11 & 7 & 14 & 13 \end{bmatrix}.$$

هر سطر یک دستگاه مانده‌ای تحویل یافته به‌هنگ 5 است ، و هرستون از اعدادی تشکیل شده که همنهشت یکدیگر به هنگ 5 می‌باشند.

برهان. ابتدا ثابت می‌کنیم‌که خواص (آ) و (ب) معادل‌اند. اگر (ب) برقرار باشد، می‌توان $\varphi(k)$ عنصر S را ،بااستفاده‌از $\varphi(d)$ مجموعهٔ از هم‌جدای (ب) به‌صورت ستون، به‌شکل یک ماتریس نشان داد. این ماتریس دارای $\varphi(k)/\varphi(d)$ سطر است. هر سطر شامل یک‌دستگاه تحویل یافته به هنگ d است ، و اینها مجموعه‌های از هم‌جدای مطلوب برای قسمت (آ) است. بهمین نحو، بـه‌آسانی معلوم می‌شود که (آ) قسمت (ب) را ایجاب خواهد کرد.

حال (ب) را ثابت می‌کنیم. فرض کنیم S_d یک دستگاه مانده‌ای تحویل یافته به هنگ d بوده، و $r \in S_d$. ثابت می‌کنیم دست کم $\varphi(k)/\varphi(d)$ عدد صحیح n در S ، متمایز به هنگ k ، وجود دارند بطوری که $n \equiv r \pmod d$ ·چون $\varphi(d)$ مقدار از r در S_d و $\varphi(k)$ عدد صحیح در S وجود دارند، بیش از $\varphi(k)/\varphi(d)$ تا از این n ها وجود ندارند ؛ درنتیجه، این قسمت (ب) را ثابت خواهدکرد.

اعدادمطلوب n از رده‌های مانده‌ای به هنگ k که با k/d عدد صحیح زیر نموده می‌شود انتخاب می‌گردد:

$$r, r + d, r + 2d, \ldots, r + \frac{k}{d} d.$$

این اعداد همنهشت یکدیگر به هنگ d اند و ناهمنهشت به هنگ k می‌باشند. چون $(r, d) = 1$ ، قضیهٔ ۳۲۰۵ نشان می‌دهد که $\varphi(k)/\varphi(d)$ تا از آنها نسبت به k اولند؛ درنتیجه، این برهان را تمام خواهد کرد. (برای برهان متفاوتی مبتنی بر نظریهٔ گروهها، ر.ک. [۱].)

تمرین برای فصل ۵

۱. فرض کنید S مجموعه‌ای از n عدد صحیح باشد (که لزوماً متمایز نیستند). ثابت کنید یک زیرمجموعهٔ ناتهی از S مجموعی بخشپذیر بر n دارد.

۲. ثابت کنید به‌ازای هر عدد صحیح n ، $5n^3 + 7n^5 \equiv 0 \pmod{12}$.

۳. (آ) همهٔ اعداد صحیح مثبت n را بیابید که $n^{13} \equiv n \pmod{1365}$.

(ب) همهٔ اعداد صحیح مثبت n را بیابید که $n^{17} \equiv n \pmod{4080}$.

۴. (آ) ثابت کنید وقتی $n = 4$ و وقتی $n = p^a$ ، که در آن p اول است و $p \equiv 3 \pmod 4$ ، داریم $\varphi(n) \equiv 2 \pmod 4$.

(ب) همهٔ nهایی را بیابید که $\varphi(n) \equiv 2 \pmod 4$.

۵. یک یارد چوبی که با اینچ مدرج شده مجدداً به 70 قسمت مساوی تقسیم می‌شود. ثابت کنید در بین چهار کوتاهترین تقسیم دوتا دارای نقاط انتهایی چپ نظیر به 1 و 19 اینچ هستند. نقاط انتهایی راست دوتای دیگر چه هستند؟

۶. همهٔ x هایی را بیابید که در دستگاه همنهشتیهای

$$x \equiv 1 \pmod 3, \qquad x \equiv 2 \pmod 4, \qquad x \equiv 3 \pmod 5$$

صدق کنند.

۷. عکس قضیهٔ ویلسون را ثابت کنید: هرگاه $(n-1)! + 1 \equiv 0 \pmod n$ ، آنگاه n اول است اگر $n > 1$.

۸. همهٔ اعداد صحیح مثبت n را بیابید که $(n-1)! + 1$ توانی از n باشد.

۹. به‌ازای عدد اول فرد p ، فرض کنید $q = (p-1)/2$. ثابت کنید

$$(q!)^2 + (-1)^q \equiv 0 \pmod p.$$

این $q!$ را، وقتی $p \equiv 1 \pmod 4$ ، به‌عنوان جواب صریحی از همنهشتی $x^2 + 1 \equiv 0 \pmod p$ بدست داده، و نشان می‌دهد که اگر $p \equiv 3 \pmod 4$ ، $q! \equiv \pm 1 \pmod p$. هیچ قاعدهٔ کلی ساده‌ای برای تعیین علامت شناخته نشده‌است.

۱۰. هرگاه p فرد بوده و $p > 1$ ، ثابت کنید که

$$1^2 3^2 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod p$$

و

$$2^2 4^2 6^2 \cdots (p-1)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

۱۱ . فرض کنید p یک عدد اول باشد، $p \geq 5$ ، و بنویسید

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p} = \frac{r}{ps}.$$

ثابت کنید که $p^3 | (r-s)$.

۱۲ . اگر p اول باشد، ثابت کنید که

$$\binom{n}{p} \equiv \left[\frac{n}{p}\right] \pmod{p}.$$

همچنین، اگر $p^\alpha | [n/p]$ ، ثابت کنید که

$$p^\alpha \Big| \binom{n}{p}.$$

۱۳ . فرض کنید a, b, n اعداد صحیح مثبتی باشند بطوری که n ، $a^n - b^n$ را عاد نماید . ثابت کنید که n ، $(a^n - b^n)/(a-b)$ را نیز عاد می‌کند .

۱۴ . فرض کنید a ، b ، و x_0 اعداد صحیح مثبتی باشند و تعریف می‌کنیم :

به‌ازای $n = 1, 2, \ldots$ ، $x_n = ax_{n-1} + b$.

ثابت کنید که همهٔ x_n ها اول نیستند .

۱۵ . فرض‌کنید n, r, a اعداد صحیح مثبتی باشند . همنهشتی $n^2 \equiv n \pmod{10^a}$ ایجاب می‌کند که به‌ازای هر r ، $n^r \equiv n \pmod{10^a}$. جمیع مقادیر r که $n^r \equiv n \pmod{10^a}$ همنهشتی $n^2 \equiv n \pmod{10^a}$ را ایجاب می‌کند پیدا نمایید .

۱۶ . فرض کنید n, a, d اعدادصحیح معلومی‌بوده‌و $(a, d) = 1$. ثابت کنید عددصحیحی مانند m هست بطوری که $m \equiv a \pmod{d}$ و $(m, n) = 1$.

۱۷ . فرض کنید f یک‌تابع حسابی‌بامقادیر صحیح‌باشد بطوری که به‌ازای‌هر $m \geq 1, n \geq 1$ ،

$$f(m+n) \equiv f(n) \pmod{m}.$$

فرض کنید $g(n)$ تعداد مقادیر (به انضمام تکرارهای) $f(1), f(2), \ldots, f(n)$ بخشپذیر بر n بوده، و $h(n)$ تعداد ایـن‌مقادیر باشد که نسبت به n اولند . ثابت کنید که

$$h(n) = n \sum_{d|n} \mu(d) \frac{g(d)}{d}.$$

۱۸ . به‌ازای‌عدد صحیح و فرد $n > 3$ ، فرض کنید k و t کوچکترین عدد صحیح مثبتی باشند که $kn + 1$ و tn هر دو مربع هستند . ثابت کنید n اول است اگر و فقط اگر

هردوی k و t بزرگتر از $n/4$ باشند.

۱۹. ثابت کنید هر عضو مجموعهٔ متشکل از $n-1$ عدد صحیح متوالی

$$n!+2, n!+3, \ldots, n!+n$$

بر عدد اولی که هیچ عضو دیگر مجموعه را عاد نکند بخشپذیر است.

۲۰. ثابت کنید به‌ازای هر دو عدد صحیح و مثبت n و k، مجموعه‌ای از n عدد صحیح متوالی هست بطوری که هر عضو آن بر k عامل اول متمایزی که هیچیک از اعضای دیگر مجموعه را عاد نمی‌کنند بخشپذیر است.

۲۱. فرض کنید عدد صحیح و مثبت n مربع نباشد. ثابت کنید به‌ازای هر عدد صحیح a که نسبت به n اول است، اعداد صحیحی مانند x و y صادق در $ax \equiv y \pmod{n}$ وجود دارند، که درآن $0 < x < \sqrt{n}$ و $0 < |y| < \sqrt{n}$.

۲۲. فرض کنید p اول باشد، $p \equiv 1 \pmod 4$، $q = (p-1)/2$، و $a = q!$.

(آ) ثابت کنید اعداد صحیح مثبتی چون x و y صادق در $0 < x < \sqrt{p}$ و $0 < y < \sqrt{p}$ وجود دارند بطوری که

$$a^2x^2 - y^2 \equiv 0 \pmod{p}.$$

(ب) به‌ازای x و y قسمت (آ)، ثابت کنید $p = x^2 + y^2$. این نشان می‌دهد که هر عدد اول $p \equiv 1 \pmod 4$ مجموع دو مربع است.

(پ) ثابت کنید هیچ عدد اولی مانند $p \equiv 3 \pmod 4$ مجموع دو مربع نیست.

۶
گروههای آبلی متناهی و مشخصهای آنها

۱.۶ چند تعریف

در فصل ۲ فرصتی بود تا به‌گروهها اشاره‌ای کنیم ، اما از خواص آنها استفادهٔ اساسی نکردیم .حال می‌خواهیم در چند جنبهٔ مقدماتی نظریهٔ گروهها مفصلتر بحث کنیم . در فصل ۷، بحث ما از قضیهٔ دیریکله درباب اعداد اول درتصاعدهای حسابی به معرفتی از توابعی حسابی به‌نام **مشخصهای دیریکله** نیاز دارد . با آنکه مشخصهای دیریکله را می‌توان بی‌اطلاع از گروهها بررسی کرد ، آشنایی مختصری از نظریهٔ گروهها ، به نظریهٔ مشخصهای دیریکله زمینهٔ طبیعی‌تری می‌بخشد و بحث را ساده‌تر خواهدکرد .

تعریف . اصول موضوع گروه. یک گروه مانند G مجموعه‌ای است ناتهی از عناصر همراه بایک عمل دوتایی ، که با $\cdot$ نموده می‌شود ، بطوری که در اصول موضوع زیر صدق می‌کنند :

(آ) **بسته بودن.** به‌ازای هر a و هر b در G ، $a \cdot b$ نیز در G است ؛

(ب) **شرکتپذیری.** به‌ازای هر a, b, c در G ، داریم $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ؛

(پ) **وجود همانی.** عنصر منحصر بفردی مانند e در G هست ، به‌نام همانی ، بطوری که به‌ازای هر a در G ، $a \cdot e = e \cdot a = a$ ؛

(ت) **وجود معکوسها.** به‌ازای هر a در G ، عنصر منحصر بفردی مانند b در G هست بطوری که $a \cdot b = b \cdot a = e$. این b با a^{-1} نموده و **معکوس** a نامیده می‌شود .

تذکر. ما معمولا" نقطه را حذف کرده به‌جای $a \cdot b$ می‌نویسیم ab .

تعریف. گروه آبلی . گروه G را **آبلی** گوییم اگر هرجفت از عناصر آن تعویض شوند ؛ یعنی ،

به‌ازای هر a و هر b در G ، $ab = ba$.

تعریف . گروه متناهی . گروه G را *متناهی* خوانیم اگر G یک مجموعهٔ متناهی باشد . در این حالت ، تعداد عناصر G **مرتبهٔ** G نامیده و با $|G|$ نموده می‌شود .

تعریف . زیرگروه . زیر مجموعهٔ ناتهی G' از گروه G که خود ، تحت‌همان عمل ، گروه باشد یک **زیرگروه** G نامیده می‌شود .

۲.۶ چند مثال از گروهها و زیرگروهها

مثال ۱ . زیرگروههای بدیهی . هر گروه مانند G دست کم دو زیر گروه دارد ، G خودش و مجموعهٔ $\{e\}$ مرکب از فقط عنصر همانی .

مثال ۲ . اعداد صحیح تحت جمع . مجموعهٔ تمام اعداد صحیح ، با $+$ به عنوان عمل و 0 به‌عنوان همانی ، یک گروه آبلی است . معکوس n ، $-n$ می‌باشد .

مثال ۳ . اعداد مختلط تحت ضرب . مجموعهٔ تمام اعداد مختلط ناصفر ، با ضرب معمولی اعداد مختلط به‌عنوان عمل و 1 به‌عنوان همانی یک گروه آبلی است . معکوس z متقابل $1/z$ است . مجموعهٔ تمام اعداد مختلط با قدرمطلق 1 یک زیرگروه است .

مثال ۴ . ریشهٔ n م واحد . گروههای امثلهٔ ۲ و ۳ گروههایی نامتناهی‌اند . مثالی از یک گروه متناهی مجموعهٔ $\{1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}\}$ است ، که درآن $\varepsilon = e^{2\pi i/n}$ و عمل . ضرب معمولی اعداد مختلط می‌باشد . این گروه ، که از مرتبهٔ n است ، ***گروه ریشه‌های n م واحد*** نامیده می‌شود . این گروه زیر گروه هر دو گروه مثال ۳ می‌باشد .

۳.۶ خواص مقدماتی گروهها

قضایای مقدماتی زیر مربوطند به‌گروه دلخواه G . G آبلی یا متناهی نیست ، مگر آنکه خلافش تصریح شود .

قضیهٔ ۱.۶ . قوانین حذف . *هرگاه عناصر a, b, c از G در*

$$ac = bc \qquad \text{یا} \qquad ca = cb$$

صدق کنند، آنگاه $a = b$.

برهان. درحالت اول، طرفین را از راست در c^{-1} ضرب و از شرکتپذیری استفاده می‌کنیم. درحالت دوم، طرفین را از چپ در c^{-1} ضرب خواهیم کرد.

قضیهٔ ۲.۶ . خواص معکوسها. *در هر گروه مانند G،*

(آ) $e^{-1} = e$ ؛

(ب) *به‌ازای هر a در G، $(a^{-1})^{-1} = a$ ؛*

(پ) *به‌ازای هر a و b در G، $(ab)^{-1} = b^{-1}a^{-1}$ (به‌ترتیب عکس توجه کنید)؛*

(ت) *به‌ازای هر a و b در G، معادلهٔ $ax = b$ دارای جواب منحصر بفرد $x = a^{-1}b$ است، معادلهٔ $ya = b$ جواب منحصر بفرد $y = ba^{-1}$ را خواهد داشت.*

برهان

(آ) چون $ee = ee^{-1}$، با حذف e بدست می‌آید که $e = e^{-1}$.

(ب) چون $aa^{-1} = e$ و معکوسها منحصر بفرد هستند، a معکوس a^{-1} می‌باشد.

(پ) بنابر شرکتپذیری، داریم

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e;$$

درنتیجه، $b^{-1}a^{-1}$ معکوس ab می‌باشد.

(ت) مجدداً، بنابر شرکتپذیری، داریم

$$a(a^{-1}b) = (aa^{-1})b = b \quad \text{و} \quad (ba^{-1})a = b(a^{-1}a) = b.$$

جوابها، بخاطر قوانین حذف، منحصر بفرد می‌باشند.

تعریف. توانهای یک عنصر. هرگاه $a \in G$، a^n را به‌ازای هرعدد صحیح n با روابط زیر تعریف می‌کنیم:

$$a^0 = e \text{؛ به‌ازای } n > 0 \text{،} \quad a^{-n} = (a^{-1})^n \quad \text{و} \quad a^n = aa^{n-1}.$$

قوانین نماییهای مذکور درزیر را می‌توان به استقرا ثابت کرد. برهانها را حذف می‌کنیم.

قضیهٔ ۳.۶ . *هرگاه $a \in G$، هر دوتوان از a تعویض می‌شوند و، به‌ازای هر دو عدد*

صحیح m و n ، داریم

$$a^m a^n = a^{m+n} = a^n a^m \quad \text{و} \quad (a^m)^n = a^{mn} = (a^n)^m$$

بعلاوه ، هرگاه a و b تعویض بشوند ، خواهیم داشت

$$a^n b^n = (ab)^n.$$

قضیهٔ ۴.۶ . محک زیرگروه. هرگاه G' یک زیر مجموعهٔ ناتهی گروه G باشد ، آنگاه G' زیرگروه است اگر و فقط اگر G' در اصول موضوع (آ) و (ت) گروه صدق نماید :

(آ) **بسته بودن.** هرگاه $a, b \in G'$ ، آنگاه $ab \in G'$ ؛

(ت) **وجود معکوس.** هرگاه $a \in G'$ ، آنگاه $a^{-1} \in G'$.

برهان. مسلما" هرزیرگروه G' این خواص را داراست . بعکس، اگر G' در (آ) و (ت) صدق کند ، به‌آسانی می‌توان نشان داد که G' دراصول موضوع (ب) و (پ) نیز صدق می‌کند . اصل موضوع (ب) ، یعنی شرکتپذیری ، در G' برقرار است ، زیرا برای جمیع عناصر G برقرار است . برای اثبات برقراری (پ) ، توجه می‌کنیم که عنصری مانند a در G' وجوددارد (چون G' ناتهی‌است) که معکوسش $a^{-1} \in G'$ (بنابر (ت)) ؛ از اینرو، بنابر (آ) ، $aa^{-1} \in G'$. اما $aa^{-1} = e$ ؛ درنتیجه ، $e \in G'$.

۴.۶ ساختن زیرگروهها

می‌توان با انتخاب عنصر a در گروه مفروض G و تشکیل مجموعهٔ تمام توانهایش : a^n ، $n = 0, \pm 1, \pm 2, \ldots$ ، همواره زیرگروهی از G را ساخت . واضح است که این مجموعه در اصول موضوع (آ) و (ت) صدق می‌کند ؛ درنتیجه ، یک زیرگروه G است . آن را **زیرگروه دوری تولید شده به‌وسیلهٔ** a نامیده و با $\langle a \rangle$ نشان می‌دهیم .

توجه‌کنیدکه $\langle a \rangle$ آبلی‌است ، حتی اگر G آبلی نباشد . هرگاه به‌ازای عدد صحیح مثبتی چون n ، $a^n = e$ ، کوچکترین $n > 0$ با این‌خاصیت وجود دارد و زیرگروه $\langle a \rangle$ یک گروه متناهی از مرتبهٔ n می‌باشد :

$$\langle a \rangle = \{a, a^2, \ldots, a^{n-1}, a^n = e\}.$$

عدد صحیح n **مرتبهٔ عنصر** a نیز نام دارد . مثالی از یک زیرگروه دوری از مرتبهٔ n گروه ریشه‌های n م واحد است که در بخش ۲.۶ متذکر شدیم .

قضیهٔ بعدی نشان‌می‌دهدکه هر عنصر یک گروه متناهی دارای مرتبهٔ متناهی است .

قضیهٔ ۵.۶ . هرگاه G متناهی‌بوده‌و $a \in G$ ، آنگاه‌عدد صحیح مثبتی مانند $n \leq |G|$ وجود دارد بطوری که $a^n = e$.

برهان. فرض کنیم $g = |G|$. دراین صورت ، دست کم دو عنصر از $g+1$ عنصر

$$e, a, a^2, \ldots, a^g$$

از G باید مساوی باشند. فرض‌کنیم $a^r = a^s$ ، که درآن $0 \leq s < r \leq g$. دراین‌صورت ، داریم

$$e = a^r(a^s)^{-1} = a^{r-s}.$$

این قضیه را به‌ازای $n = r - s$ ثابت می‌کند.

همانطور که در بخش ۲.۶ ذکر شد ، هر گروه مانند G دو زیرگروه بدیهی دارد ، $\{e\}$ و خود G . وقتی G یک گروه آبلی متناهی باشد ، فرایند ساده‌ای برای ساختن یک گردآیهٔ صعودی از زیر گروههای بین $\{e\}$ و G وجو د دارد. این فرایند ، که در قضیهٔ ۸.۶ توصیف می‌شود ، بر نکات زیر استوار است :

هرگاه G' زیر گروه گروه متناهی G باشد ، آنگاه به‌ازای هر عنصر a در G ، عدد صحیحی‌مانند n هست بطوری که $a^n \in G'$. هرگاه a از قبل در G' باشد ، n را مساوی 1 می‌گیریم. هرگاه $a \notin G'$ ، می‌توان n رامرتبهٔ a گرفت ، زیرا $a^n = e \in G'$. بهرحال ، ممکن است توان مثبت کوچکتری از a باشد که در G' قرار داشته باشد. بنابراصل خوش ترتیبی ، کوچکترین عدد صحیح مثبت n هست که $a^n \in G'$. این عدد را **شاخص** a در G' می‌نامیم.

قضیهٔ ۶.۶ . فرض کنیم G' زیر گروه گروه آبلی متناهی G باشد ، که $G' \neq G$. عنصر a در G راطوری‌اختیار می‌کنیم که $a \notin G'$ ، و فرض می‌کنیم h شاخص a در G' باشد. دراین صورت ، مجموعهٔ حاصل ضربهای

$$G'' = \{xa^k : k = 0, 1, 2, \ldots, h-1 \text{ و } x \in G'\}$$

یک زیر گروه G است شامل G' . بعلاوه ، مرتبهٔ G'' ، h برابر مرتبهٔ G' می‌باشد :

$$|G''| = h|G'|$$

برهان. برای اثبات اینکه G'' زیر گروه است از محک زیر گروه استفاده می‌کنیم. ابتدا بسته بودن را امتحان می‌کنیم. دو عنصر در G'' ، مثلاً xa^k و ya^j که $x, y \in G'$ و

h ، $0 \le k < h, 0 \le j < h$ را اختیار می‌کنیم . چون G آبلی است ، حاصل ضرب عناصر مساوی است با

$$(xy)a^{k+j}. \qquad (۱)$$

اما $k + j = qh + r$ ، که در آن $0 \le r < h$. از اینرو ،

$$a^{k+j} = a^{qh+r} = a^{qh}a^r = za^r,$$

که درآن ، چون $a^h \in G'$ ، $z = a^{qh} = (a^h)^q \in G'$. بنابراین ، عنصر (۱) مساوی است با $(xyz)a^r = wa^r$ ، که در آن $w \in G'$ و $0 \le r < h$. این ثابت می‌کند که G'' در اصل موضوع بسته بودن صدق می‌کند .

حال نشان می‌دهیم که معکوس هر عنصر در G'' نیز در G'' است . عنصر دلخواهی در G'' ، مثلا" xa^k ، را اختیارمی‌کنیم . اگر $k = 0$ ، معکوس x^{-1} است که در G'' قرار دارد . اگر $0 < k < h$ ، معکوس عبارت است از عنصر

$$ya^{h-k} \text{ ، که در آن } y = x^{-1}(a^h)^{-1} \text{ ،}$$

که مجددا" در G'' است . این نشان می‌دهد که G'' واقعا" زیر گروه G است . **واضح است** که G'' شامل G' می‌باشد .

حال مرتبهٔ G'' راتعیین می‌کنیم . فرض کنیم $m = |G'|$. وقتی x ، m عنصر G' و k ، h عددصحیح $0, 1, 2, \ldots, h-1$ رابگیرد ، mh حاصل ضرب xa^k خواهیم داشت . اگر نشان دهیم که همهٔ اینها **متمایز** اند ، G'' مرتبهٔ mh را خواهد داشت . از این حاصل ضربها دوتا ، مثلا" xa^k و ya^j ، را درنظر می‌گیریم و فرض می‌کنیم

$$xa^k = ya^j \text{ ، که درآن } 0 \le j \le k < h.$$

دراین صورت ، $a^{k-j} = x^{-1}y$ و $0 \le k - j < h$. چون $x^{-1}y \in G'$ ، باید a^{k-j} در G' باشد ؛ درنتیجه ، $x = y$ ؛ و لذا ، $k = j$. این برهان را تمام خواهد کرد .

۵.۶ مشخصهای گروههای آبلی متناهی

تعریف . فرض کنیم G یک گروه دلخواه باشد . تابع مختلط f تعریف شده بر G یک مشخص G نامیده می‌شود اگر f دارای خاصیت ضربی

$$f(ab) = f(a)f(b)$$

به‌ازای هر a, b در G بوده و ، به‌ازای c ای در G ، $f(c) \ne 0$.

قضیهٔ ۷.۶ . *هرگاه f یک‌مشخص‌گروه‌متناهی G با عنصرهمانی e باشد، آنگاه $f(e) = 1$ و هر مقدار تابعی $f(a)$ یک ریشهٔ واحداست. درواقع، هرگاه $a^n = e$ ، آنگاه $f(a)^n = 1$.*

برهان. c را در G طوری اختیار می‌کنیم که $f(c) \neq 0$. چون $ce = c$ ، داریم
$$f(c)f(e) = f(c);$$
درنتیجه، $f(e) = 1$. هرگاه $a^n = e$ ، آنگاه $f(a)^n = f(a^n) = f(e) = 1$.

مثال. هر گروه G دست کم یک مشخص دارد؛ یعنی، تابعی که بر G متحد 1 است. این را **مشخص *اصلی*** می‌نامیم. قضیهٔ بعدی می‌گوید که، اگر G آبلی بوده و مرتبهٔ متناهی بزرگتر از 1 داشته باشد، مشخصهای دیگری نیز وجود خواهند داشت.

قضیهٔ ۸.۶ . *گروه آبلی متناهی G از مرتبهٔ n درست n مشخص متمایز دارد.*

برهان. در قضیهٔ ۶.۶ آموختیم که چطور از زیر گروه $G' \neq G$ زیر گروه جدید G'' شامل G' و دست کم یک عنصر دیگر a غیر متعلق به G' را بسازیم. ما برای نمایش زیر گروه G'' که در قضیهٔ ۶.۶ ساخته شد از علامت $\langle G'; a\rangle$ استفاده می‌کنیم. بنابراین،
$$\langle G'; a\rangle = \{xa^k : 0 \le k < h \quad \text{و} \quad x \in G'\}$$
که در آن h شاخص a در G' است.

حال این ساختن را، با شروع از زیر گروه $\{e\}$ که با G_1 نموده می‌شود، تکرار می‌کنیم. اگر $G_1 \neq G$ ، a_1 را عنصری از G غیر از e گرفته و تعریف می‌کنیم $G_2 = \langle G_1; a_1\rangle$. اگر $G_2 \neq G$ ، a_2 را عنصری از G که در G_2 نیست گرفته و تعریف می‌کنیم $G_3 = \langle G_2; a_2\rangle$. با ادامهٔ این کار، یک مجموعهٔ متناهی از عناصر $a_1, a_2, \ldots, a_t$ و یک مجموعهٔ نظیر از زیر گروههای $G_1, G_2, \ldots, G_{t+1}$ بدست می‌آید بطوری که
$$G_{r+1} = \langle G_r; a_r\rangle$$

و

$$G_1 \subset G_2 \subset \cdots \subset G_{t+1} = G.$$
این عمل باید بعد از چند مرحله ختم شود، زیرا گروه مفروض G متناهی است و هر G_{r+1} از سابق خود G_r عنصر بیشتری دارد. این زنجیر از زیر گروهها را درنظر گرفته و قضیه را به استقرا ثابت می‌کنیم، به این نحو که اگر برای G_r درست باشد، باید برای G_{r+1} نیز درست باشد.

واضح است که فقط یک مشخص برای G_1 وجود دارد؛ یعنی، تابعی‌که متحد ۱ است. بنابر این، فرض کنیم G_r دارای مرتبهٔ m بوده و درست m مشخص متمایز برای G_r وجود داشته‌باشند. $G_{r+1} = \langle G_r; a_r \rangle$ رادرنظرگرفته‌و فرض می‌کنیم h شاخص a_r در G_r باشد؛ یعنی، کوچکترین عدد صحیح مثبتی که $a_r^h \in G_r$. نشان می‌دهیم که درست h طریقهٔ مختلف برای‌تعمیم هر مشخص G_r به مشخصی از G_{r+1} وجود دارند، و هر مشخص G_{r+1} تعمیمی از یک مشخص G_r است. این ثابت می‌کند که G_{r+1} دقیقاً mh مشخص دارد و، چون mh مرتبهٔ G_{r+1} نیز هست، قضیه به استقرا ثابت خواهد شد.

یک عنصر نوعی در G_{r+1} به شکل

xa_r^k است، که در آن $x \in G_r$ و $0 \leq k < h$.

یک لحظه فرض کنیم بتوان مشخص f از G_r را به G_{r+1} تعمیم داد. این تعمیم را $\tilde{f}$ نامیده و ببینیم در باب $\tilde{f}(xa_r^k)$ چه می‌شود گفت. از خاصیت ضربی لازم می‌آید که

$$\tilde{f}(xa_r^k) = \tilde{f}(x)\tilde{f}(a_r)^k.$$

اما $x \in G_r$؛ درنتیجه، $\tilde{f}(x) = f(x)$ و معادلهٔ فوق ایجاب می‌کند که

$$\tilde{f}(xa_r^k) = f(x)\tilde{f}(a_r)^k.$$

این رابطه می‌گوید که $\tilde{f}(xa_r^k)$ با معلوم شدن $\tilde{f}(a_r)$ مشخص خواهد شد.

می‌پرسیم مقادیرممکن برای $\tilde{f}(a_r)$ چه هستند؟ فرض کنیم $c = a_r^h$. چون $c \in G_r$، داریم $\tilde{f}(c) = f(c)$، و چون $\tilde{f}$ ضربی است، نیز داریم $\tilde{f}(c) = \tilde{f}(a_r)^h$. از اینرو،

$$\tilde{f}(a_r)^h = f(c);$$

درنتیجه، $\tilde{f}(a_r)$ یکی از ریشه‌های h ام $f(c)$ است. از اینرو، حداکثر h انتخاب برای $\tilde{f}(a_r)$ موجود است.

این‌نکات‌نحوهٔ تعریف $\tilde{f}$ را بازگو می‌کنند. اگر f مشخص معلومی از G_r باشد، یکی ازریشه‌های h ام $f(c)$ رااختیارمی‌کنیم، که $c = a_r^h$، و $\tilde{f}(a_r)$ را مساوی این ریشه‌می‌گیریم. سپس، $\tilde{f}$ را بر بقیهٔ G_{r+1} با معادلهٔ

$$\tilde{f}(xa_r^k) = f(x)\tilde{f}(a_r)^k \tag{۲}$$

تعریف‌می‌کنیم. h انتخاب برای $\tilde{f}(a_r)$ همه متمایزند؛ درنتیجه، h طریقهٔ مختلف برای تعریف $\tilde{f}(xa_r^k)$ وجود دارند. حال‌تحقیق‌می‌کنیم تابع $\tilde{f}$ که این‌طور تعریف می‌شود دارای خاصیت ضربی مطلوب است. از (۲) معلوم می‌شود که

$$\begin{aligned}\tilde{f}(xa_r^k \cdot ya_r^j) &= \tilde{f}(xy \cdot a_r^{k+j}) = f(xy)\tilde{f}(a_r)^{k+j}\\ &= f(x)f(y)\tilde{f}(a_r)^k\tilde{f}(a_r)^j\\ &= \tilde{f}(xa_r^k)\tilde{f}(ya_r^j),\end{aligned}$$

درنتیجه، $\tilde{f}$ یک مشخص G_{r+1} است. هیچ دو تعمیم $\tilde{f}$ و $\tilde{g}$ نمی‌توانند بر G_{r+1} یکسان باشند، زیرا که دراین صورت توابع f و g که تعمیم یافته‌اند بر G_r یکسان خواهند بود. لذا، هریک از m مشخص G_r را می‌توان به h طریق مختلف برای تولید یک مشخص G_{r+1} تعمیم داد. بعلاوه، اگر φ یک مشخص G_{r+1} باشد، تحدیدش به G_r نیز یک مشخص G_r است؛ درنتیجه، عمل تعمیم همهٔ مشخصهای G_{r+1} را تولید می‌کند. این برهان را تمام خواهد کرد.

۶.۶ گروه مشخص

دراین‌بخش، G یک گروه آبلی متناهی از مرتبهٔ n است. مشخص اصلی G با f_1 نموده می‌شود. مشخصهای‌دیگر، که با $f_2, f_3, \ldots, f_n$ نموده می‌شوند، **مشخصهای غیر اصلی** نام دارند. اینها دارای این خاصیت‌اند که به‌ازای aای در G، $f(a) \neq 1$.

قضیهٔ ۶.۹. *هرگاه ضرب مشخصها با رابطهٔ*

$$(f_i f_j)(a) = f_i(a) f_j(a)$$

به‌ازای هر a در G تعریف شود، آنگاه مجموعهٔ مشخصهای G یک گروه آبلی از مرتبهٔ n تشکیل‌خواهدداد. این گروه را با $\hat{G}$ نشان می‌دهیم. عنصر همانی $\hat{G}$ مشخص اصلی f_1 است. معکوس f_i متقابل $1/f_i$ می‌باشد.

برهان. تحقیق اصول موضوع گروه تمرین سر راستی است؛ و لذا، جزئیات آن حذف می‌شود.

تذکر. به‌ازای هر مشخص f، داریم $|f(a)| = 1$. بنابراین، متقابل $1/f(a)$ مساوی مزدوج مختلط $\overline{f(a)}$ است. در نتیجه، تابع $\bar{f}$ تعریف شده با $\bar{f}(a) = \overline{f(a)}$ نیز یک مشخص G است. بعلاوه، به‌ازای هر a در G، داریم

$$\bar{f}(a) = \frac{1}{f(a)} = f(a^{-1}).$$

۷.۶ روابط تعامدی برای مشخصها

فرض کنیم G یک گروه آبلی متناهی از مرتبهٔ n با عنصرهای $a_1, a_2, \ldots, a_n$ بوده، و $f_1, f_2, \ldots, f_n$ مشخصهای G، با مشخص اصلی f_1، باشند.

نمادگذاری. ماتریس $n \times n$، $[a_{ij}]$ که عنصر a_{ij} آن در سطر i م و ستون j م

$$a_{ij} = f_i(a_j)$$

است را با $A = A(G)$ نشان می‌دهیم .

ثابت می‌کنیم که ماتریس A دارای معکوس است و سپس، با استفاده از این امر، روابط تعامدی برای مشخصها را نتیجه می‌گیریم . ابتدا مجموع درایه‌های هر سطر A را مشخص می‌کنیم .

قضیهٔ ۱۰.۶ . *مجموع درایه‌های سطر i م A مساوی است با*

$$\sum_{r=1}^{n} f_i(a_r) = \begin{cases} n\text{ ، } & (i = 1) \text{ اگر } f_i \text{ مشخص اصلی باشد} \\ 0 & \text{درغیر این‌صورت ،} \end{cases}$$

برهان. فرض کنیم S مجموع مورد نظر باشد . اگر $f_i = f_1$ ، هر جملهٔ مجموع مساوی 1 است و $S = n$. اگر $f_i \neq f_1$ ، عنصری مانند b در G هست که به‌ازای آن $f_i(b) \neq 1$. وقتی a_r عنصرهای G را می‌گیرد ، حاصل ضرب ba_r نیز چنین می‌کند . لذا ،

$$S = \sum_{r=1}^{n} f_i(ba_r) = f_i(b) \sum_{r=1}^{n} f_i(a_r) = f_i(b)S.$$

بنابراین ، $S(1 - f_i(b)) = 0$. چون $f_i(b) \neq 1$ ، نتیجه می‌شود که $S = 0$.

حال ، با استفاده از این قضیه ، نشان می‌دهیم که A دارای معکوس است .

قضیهٔ ۱۱.۶ . *فرض‌کنیم A^* مزدوج‌ترانهادهٔ ماتریس A باشد . دراین صورت ،داریم*

$$AA^* = nI,$$

که درآن I ماتریس همانی $n \times n$ است . بنابراین ، $n^{-1}A^*$ معکوس A می‌باشد .

برهان. فرض کنیم $B = AA^*$. درایهٔ b_{ij} در سطر i م و ستون j م B از رابطهٔ زیر بدست می‌آید :

$$b_{ij} = \sum_{r=1}^{n} f_i(a_r)\bar{f}_j(a_r) = \sum_{r=1}^{n} (f_i\bar{f}_j)(a_r) = \sum_{r=1}^{n} f_k(a_r),$$

که درآن $f_k = f_i\bar{f}_j = f_i/f_j$. اما $f_i/f_j = f_1$ اگر و فقط اگر $i = j$. لذا ، طبق قضیهٔ ۱۰.۶ ، داریم

$$b_{ij} = \begin{cases} n \text{ ، } & i = j \text{ اگر} \\ 0 \text{ ، } & i \neq j \text{ اگر} \end{cases}$$

به عبارت دیگر، $B = nI$.

حال ،بااستفاده از این‌امر که یک ماتریس با معکوسش تعویض می‌شود ، روابط تعامدی برای مشخصها را نتیجه می‌گیریم .

قضیهٔ ۱۲۰۶ . روابط تعامدی برای مشخصها . همواره

$$\sum_{r=1}^{n} \bar{f}_r(a_i) f_r(a_j) = \begin{cases} n \text{ ، } & a_i = a_j \text{ اگر} \\ 0 \text{ ، } & a_i \neq a_j \text{ اگر} \end{cases} \tag{۳}$$

برهان. رابطهٔ $AA^* = nI$ ایجاب می‌کند که $A^*A = nI$. اما عنصر سطر i م و ستون j م A^*A مجموع سمت چپ (۳) است . این برهان را تمام می‌کند .

تذکر. چون $\bar{f}_r(a_i) = f_r(a_i)^{-1} = f_r(a_i^{-1})$ ، جملهٔ عمومی مجموع در (۳) مساوی $f_r(a_i^{-1}) f_r(a_j) = f_r(a_i^{-1} a_j)$ است . لذا ،روابط تعامدی‌را می‌توان‌به‌صورت زیر نیز بیان‌کرد :

$$\sum_{r=1}^{n} f_r(a_i^{-1} a_j) = \begin{cases} n \text{ ، } & a_i = a_j \text{ اگر} \\ 0 \text{ ، } & a_i \neq a_j \text{ اگر} \end{cases}$$

وقتی a_i عنصر همانی e باشد ، خواهیم داشت :

قضیهٔ ۱۳۰۶ . مجموع درایه‌های ستون j م A از روابط زیر بدست می‌آید :

$$\sum_{r=1}^{n} f_r(a_j) = \begin{cases} n \text{ ، } & a_j = e \text{ اگر} \\ 0 \text{ ، } & \text{درغیر این‌صورت} \end{cases} \tag{۴}$$

۸.۶ مشخصهای دیریکله

بحث پیش مربوط به مشخصهای یک گروه آبلی متناهی و دلخواه G بود . حال G را گروه رده‌های مانده‌ای تحویل یافته به هنگ عدد صحیح مثبت و ثابت k می‌گیریم . ابتدا ثابت می‌کنیم که اگر ضرب مناسبی تعریف شود ، این رده‌های مانده‌ای گروه تشکیل خواهند داد .

به‌یاد می‌آوریم‌که یک دستگاه مانده‌ای تحویل یافته به هنگ k مجموعه‌ای است

از $\varphi(k)$ عدد صحیح ناهمنهشت به هنگ k مانند $\{a_1, a_2, \ldots, a_{\varphi(k)}\}$ که هر یک نسبت به k اول‌است. به‌ازای‌هر‌عدد صحیح a ، ردهٔ مانده‌ای نظیر، یعنی $\hat{a}$ ، مجموعهٔ تمام اعداد صحیح همنهشت a به هنگ k است :

$$\hat{a} = \{x : x \equiv a \pmod{k}\}.$$

ضرب رده‌های مانده‌ای با رابطهٔ

$$\hat{a} \cdot \hat{b} = \widehat{ab} \qquad (۵)$$

تعریف‌می‌شود. یعنی، حاصل ضرب دو ردهٔ مانده‌ای $\hat{a}$ و $\hat{b}$ ردهٔ باقیمانده‌ای‌حاصل ضرب ab می‌باشد.

قضیهٔ ۱۴.۶ . *با ضرب تعریف شده به وسیلهٔ (۵)، مجموعهٔ رده‌های مانده‌ای تحویل‌یافته به هنگ k یک‌گروه آبلی‌متناهی‌ازمرتبهٔ $\varphi(k)$ است. همانی ردهٔ مانده‌ای $\hat{1}$ است. معکوس $\hat{a}$ ردهٔ مانده‌ای $\hat{b}$ است، که $ab \equiv 1 \pmod{k}$.*

برهان. خاصیت بسته‌بودن، بخاطر طرز تعریف ضرب رده‌های مانده‌ای ، خودبخود برقرار‌است. واضح‌است که ردهٔ $\hat{1}$ عنصر همانی است. اگر $(a, k) = 1$ ، b منحصربفردی هست بطوری که $ab \equiv 1 \pmod{k}$. لذا، معکوس $\hat{a}$ مساوی $\hat{b}$ می‌باشد. بالاخره، واضح است که گروه آبلی است و مرتبه‌اش $\varphi(k)$ است.

تعریف. مشخصهای دیریکله. فرض کنیم G گروه رده‌های مانده‌ای تحویل یافته به هنگ k باشد. نظیر هر مشخص f از G ، تابع حسابی $\chi = \chi_f$ را به‌صورت زیر تعریف می‌کنیم :

$$\chi(n) = f(\hat{n}) \quad \text{،} \quad (n, k) = 1 \;\text{اگر}$$

$$\chi(n) = 0 \quad \text{،} \quad (n, k) > 1 \;\text{اگر}$$

تابع χ یک **مشخص دیریکله به هنگ** k نامیده می‌شود. مشخص اصلی χ_1 مشخصی‌است که خواص زیر را دارد :

$$\chi_1(n) = \begin{cases} 1 \quad \text{،} \quad (n, k) = 1 \;\text{اگر} \\ 0 \quad \text{،} \quad (n, k) > 1 \;\text{اگر} \end{cases}$$

قضیهٔ ۱۵.۶ . *$\varphi(k)$ مشخص دیریکلهٔ متمایز به هنگ k وجود دارند، بطوری‌که‌هریک کاملا" ضربی بوده و متناوب با دورهٔ تناوب k است. یعنی،*

$$\chi(mn) = \chi(m)\chi(n) \quad \text{، } m, n \text{ به‌ازای هر} \tag{۶}$$

و،

$$\text{به‌ازای هر } n \text{ ،} \qquad \chi(n+k) = \chi(n) \,.$$

بعکس، هرگاه χ کاملاً "ضربی‌ومتناوب‌با دورهٔ تناوب k باشد، و، درصورت $(n, k) > 1$ ، داشته باشیم $\chi(n) = 0$ ، آنگاه χ یک مشخص دیریکله به هنگ k می‌باشد.

برهان. $\varphi(k)$ مشخص مانند f برای گروه G رده‌های مانده‌ای تحویل یافته به هنگ k وجود دارند؛ در نتیجه، $\varphi(k)$ مشخص χ_f به هنگ k وجودخواهند داشت. خاصیت ضربی (۶) χ_f از خاصیت‌ضربی f ، وقتی هر دوی m و n نسبت‌به k اول‌باشند،بدست می‌آید. اگر یکی از m و n نسبت به k اول نباشد، mn نیز نیست؛ درنتیجه، هر دو طرف (۶) صفر می‌باشند. خاصیت تناوبی ازاین‌امر که $\chi_f(n) = f(\hat{n})$ و $a \equiv b \pmod{k}$ ایجاب می‌کند که $(a, k) = (b, k)$ نتیجه خواهد شد.

برای اثبات عکس، توجه می‌کنیم که تابع f تعریف شده بر G به صورت زیر:

$$\text{اگر } (n, k) = 1 \text{ ،} \quad f(\hat{n}) = \chi(n)$$

یک مشخص G است؛ درنتیجه، χ یک مشخص دیریکله به هنگ k است.

مثال. وقتی $k = 1$ یا $k = 2$ ، $\varphi(k) = 1$ و تنها مشخص دیریکله مشخص اصلی χ_1 است. به‌ازای $k \geq 3$ ، دست کم دو مشخص دیریکله وجود دارند، زیرا $\varphi(k) \geq 2$. جداول زیر کلیهٔ مشخصهای دیریکله را به‌ازای $k = 3, 4, 5$ نشان می‌دهند.

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	i	$-i$	-1	0
$\chi_4(n)$	1	$-i$	i	-1	0

$k = 5, \varphi(k) = 4$

n	1	2	3	4
$\chi_1(n)$	1	0	1	0
$\chi_2(n)$	1	0	-1	0

$k = 4, \varphi(k) = 2$

n	1	2	3
$\chi_1(n)$	1	1	0
$\chi_2(n)$	1	-1	0

$k = 3, \varphi(k) = 2$

برای پر کردن این جدولها از این امر که وقتی $(n, k) = 1$ ، $\chi(n)^{\varphi(k)} = 1$ استفاده می‌کنیم؛ درنتیجه، $\chi(n)$ یک ریشهٔ $\varphi(k)$ ام واحداست. همچنین، توجه می‌کنیم که اگر χ یک مشخص به هنگ k باشد، مزدوج مختلط‌آن $\bar{\chi}$ نیز چنین است. این اطلاع برای تکمیل جدولها به‌ازای $k = 3$ و $k = 4$ کافی می‌باشد.

وقتی $k = 5$ ، داریم $\varphi(5) = 4$ ؛ درنتیجه، وقتی $(n, 5) = 1$ ، مقادیر ممکن $\chi(n)$

عبارتند از ± 1 و $\pm i$. همچنین، $\chi(2)\chi(3) = \chi(6) = \chi(1) = 1$ ؛ درنتیجه، $\chi(2)$ و $\chi(3)$ معکوس می‌باشند. چون $\chi(4) = \chi(2)^2$ ، این اطلاع برای پر کردن جدول به‌ازای $k = 5$ کافی خواهد بود. به‌عنوان امتحان، می‌توان از قضایای ۶.۱۰ و ۶.۱۳ ، که می‌گویند مجموع درایه‌ها در هر سطر و هر ستون جز اولی صفر است، استفاده کرد. جداول زیر کلیهٔ مشخصهای دیریکله به هنگ 6 و 7 را نشان می‌دهند.

n	1	2	3	4	5	6
$\chi_1(n)$	1	0	0	0	1	0
$\chi_2(n)$	1	0	0	0	-1	0

$k = 6, \varphi(k) = 2$

n	1	2	3	4	5	6	7
$\chi_1(n)$	1	1	1	1	1	1	0
$\chi_2(n)$	1	1	-1	1	-1	-1	0
$\chi_3(n)$	1	ω^2	ω	$-\omega$	$-\omega^2$	-1	0
$\chi_4(n)$	1	ω^2	$-\omega$	$-\omega$	ω^2	1	0
$\chi_5(n)$	1	$-\omega$	ω^2	ω^2	$-\omega$	1	0
$\chi_6(n)$	1	$-\omega$	$-\omega^2$	ω^2	ω	-1	0

$\omega = e^{\pi i/3}$

$k = 7, \varphi(k) = 6$

در بحث ما از قضیهٔ دیریکله در باب اعداد اول در یک تصاعد حسابی، از رابطهٔ تعامدی زیر برای مشخصها به هنگ k استفاده خواهد شد.

قضیهٔ ۶.۱۶ . فرض کنیم $\chi_1, \dots, \chi_{\varphi(k)}$ ، $\varphi(k)$ مشخص دیریکله به هنگ k باشند. همچنین، m و n دو عدد صحیح با $(n, k) = 1$ باشند. دراین‌صورت،

$$\sum_{r=1}^{\varphi(k)} \chi_r(m)\bar{\chi}_r(n) = \begin{cases} \varphi(k) & \text{اگر } m \equiv n \pmod k \\ 0 & \text{اگر } m \not\equiv n \pmod k \end{cases}$$

برهان. اگر $(m, k) = 1$ ، درروابط تعامدی قضیهٔ ۶.۱۲ فرض می‌کنیم $a_i = \hat{n}$ و $a_j = \hat{m}$ و توجه می‌کنیم که $\hat{m} = \hat{n}$ اگر و فقط اگر $m \equiv n \pmod k$. اگر $(m, k) > 1$ ، هر جمله در مجموع صفر می‌شود و $m \not\equiv n \pmod k$.

۶.۹ مجموعهای شامل مشخصهای دیریکله

دراین بخش چند مجموع را که در برهان قضیهٔ دیریکله در باب اعداد اول درتصاعدهای حسابی ظاهر می‌شوند مطرح می‌کنیم.

اولین قضیه مربوط به یک مشخص غیر اصلی χ به هنگ k است، اما برهانش در صورتی که χ یک تابع حسابی متناوب با دورهٔ تناوب k بوده و دارای مجموعهای جزئی

کراندار است نیز معتبر است .

قضیهٔ ۱۷۰۶ . *فرض کنیم χ یک مشخص غیر اصلی به هنگ k بوده ، و f یک تابع نامنفی باشد که مشتقش $f'(x)$ به‌ازای هر $x \geq x_0$ منفی و پیوسته می‌باشد . دراین‌صورت اگر $y \geq x \geq x_0$ ، داریم*

$$\sum_{x<n\leq y} \chi(n) f(n) = O(f(x)). \tag{۷}$$

اگر ، علاوه براین ، وقتی $x \to \infty$ ، $f(x) \to 0$ ، سری نامتناهی

$$\sum_{n=1}^{\infty} \chi(n) f(n)$$

همگراست وبه‌ازای $x \geq x_0$ داریم

$$\sum_{n\leq x} \chi(n) f(n) = \sum_{n=1}^{\infty} \chi(n) f(n) + O(f(x)). \tag{۸}$$

برهان . فرض کنیم $A(x) = \sum_{n\leq x} \chi(n)$. چون χ غیر اصلی‌است ، داریم

$$A(k) = \sum_{n=1}^{k} \chi(n) = 0.$$

از خاصیت تناوب نتیجه می‌شودکه به‌ازای $n = 2, 3, \ldots$ ، $A(nk) = 0$ ؛ در نتیجه ، به‌ازای هر x ، $|A(x)| < \varphi(k)$. به عبارت دیگر ، $A(x) = O(1)$.

حال ، با استفاده از اتحاد آبل (قضیهٔ ۲۰۴) ، مجموع (۷) را به‌صورت انتگرال بیان می‌کنیم . این نتیجه می‌دهد که

$$\sum_{x<n\leq y} \chi(n) f(n) = f(y)A(y) - f(x)A(x) - \int_x^y A(t) f'(t)\, dt$$

$$= O(f(y)) + O(f(x)) + O\left(\int_x^y (-f'(t))\, dt\right) = O(f(x)).$$

و این (۷) را ثابت می‌کند . هرگاه وقتی $x \to \infty$ ، $f(x) \to 0$ ، آنگاه (۷) نشان می‌دهد که سری

$$\sum_{n=1}^{\infty} \chi(n) f(n)$$

بنابر محک همگرایی کشی ، همگراست . برای اثبات (۸) کافی است توجه کنیم که

$$\sum_{n=1}^{\infty} \chi(n)f(n) = \sum_{n \le x} \chi(n)f(n) + \lim_{y\to\infty} \sum_{x<n\le y} \chi(n)f(n).$$

بخاطر (۷) ، حد سمت راست $O(f(x))$ است . این برهان را کامل خواهد کرد .

حال ، با اعمال قضیهٔ ۱۷۰۶ بترتیب در مورد $f(x) = 1/x$ ، $f(x) = (\log x)/x$ ، و $f(x) = 1/\sqrt{x}$ بهازای $x \ge 1$ ، داریم

قضیهٔ ۱۸۰۶ . هرگاه χ یک مشخص غیر اصلی به هنگ k بوده و $x \ge 1$ ، خواهیم داشت

$$\sum_{n\le x} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + O\left(\frac{1}{x}\right), \tag{۹}$$

$$\sum_{n\le x} \frac{\chi(n)\log n}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n} + O\left(\frac{\log x}{x}\right), \tag{۱۰}$$

$$\sum_{n\le x} \frac{\chi(n)}{\sqrt{n}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}}\right). \tag{۱۱}$$

۱۰۰۶ صفر نشدن $L(1, \chi)$ بهازای غیر اصلی حقیقی χ

مجموع سری (۹) را با $L(1, \chi)$ نشان میدهیم . لذا ،

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}.$$

در اثبات قضیهٔ دیریکله لازم است بدانیم که وقتی χ یک مشخص غیر اصلی باشد ، $L(1, \chi) \neq 0$. این مطلب رادراینجا بهازای مشخصهای غیر اصلی حقیقی ثابت میکنیم . ابتدا مجموع مقسوم علیهی $\chi(n)$ را درنظر میگیریم .

قضیهٔ ۱۹۰۶ . فرضکنیم χ یک مشخص حقیقی به هنگ k بوده و

$$A(n) = \sum_{d|n} \chi(d).$$

دراین صورت ، بهازای هر n ، $A(n) \ge 0$ و ، اگر n مربع باشد ، $A(n) \ge 1$.

برهان . بهازای توانهای اول ، داریم

$$A(p^a) = \sum_{t=0}^{a} \chi(p^t) = 1 + \sum_{t=1}^{a} \chi(p)^t.$$

چون χ حقیقی است، تنهامقادیر ممکن برای $\chi(p)$ عبارتند از 0 ، 1 ، و-1. هرگاه $\chi(p) = 0$ ، آنگاه $A(p^a) = 1$ ؛ هرگاه $\chi(p) = 1$ ، آنگاه $A(p^a) = a + 1$ ؛ و هرگاه $\chi(p) = -1$ ، آنگاه

$$A(p^a) = \begin{cases} 0 & \text{اگر } a \text{ فرد باشد،} \\ 1 & \text{اگر } a \text{ زوج باشد،} \end{cases}$$

درهرحالت، هرگاه a زوج باشد، آنگاه $A(p^a) \geq 1$.

حال، اگر $n = p_1^{a_1} \cdots p_r^{a_r}$ ، $A(n) = A(p_1^{a_1}) \cdots A(p_r^{a_r})$ ، زیرا A ضربی است. هرعامل $A(p_i^{a_i}) \geq 0$ ؛ درنتیجه، $A(n) \geq 0$. همچنین، اگر n مربع باشد، هر نمای a_i زوج است؛ درنتیجه، هر عامل $A(p_i^{a_i}) \geq 1$. بنابراین، $A(n) \geq 1$. این قضیه را ثابت می‌کند.

قضیهٔ ۲۰.۶ . به‌ازای هر مشخص غیر اصلی حقیقی χ به هنگ k ، قرار می‌دهیم

$$A(n) = \sum_{d|n} \chi(d) \quad \text{و} \quad B(x) = \sum_{n \leq x} \frac{A(n)}{\sqrt{n}}.$$

دراین صورت،

(آ) وقتی $x \to \infty$ ، $B(x) \to \infty$ ؛

(ب) به‌ازای هر $x \geq 1$ ، $B(x) = 2\sqrt{x}\,L(1, \chi) + O(1)$.

بنابراین، $L(1, \chi) \neq 0$.

برهان. برای اثبات قسمت (آ)، از قضیهٔ ۱۹.۶ استفاده کرده می‌نویسیم

$$B(x) \geq \sum_{\substack{n \leq x \\ n = m^2}} \frac{1}{\sqrt{n}} = \sum_{m \leq \sqrt{x}} \frac{1}{m}.$$

مجموع آخر، وقتی $x \to \infty$ ، به ∞ میل می‌کند، زیرا سری توافقی $\sum 1/m$ واگراست.

برای اثبات قسمت (ب)، می‌نویسیم

$$B(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} \sum_{d|n} \chi(d) = \sum_{\substack{q, d \\ qd \leq x}} \frac{\chi(d)}{\sqrt{qd}}.$$

حال از قضیهٔ ۱۷.۳ کمک می‌گیریم، که می‌گوید

$$\sum_{\substack{q,d\\qd\le x}} f(d)g(q) = \sum_{n\le a} f(n)G\left(\frac{x}{n}\right) + \sum_{n\le b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b)$$

که درآن $ab = x$ ، $F(x) = \sum_{n\le x} f(n)$ ، و $G(x) = \sum_{n\le x} g(n)$. با اختیار $a = b = \sqrt{x}$ و این فرض که $f(n) = \chi(n)/\sqrt{n}, g(n) = 1/\sqrt{n}$ ، بدست می‌آید که

$$(۱۲)\quad B(x) = \sum_{\substack{q,d\\qd\le x}} \frac{\chi(d)}{\sqrt{qd}} = \sum_{n\le\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} G\left(\frac{x}{n}\right) + \sum_{n\le\sqrt{x}} \frac{1}{\sqrt{n}} F\left(\frac{x}{n}\right) - F(\sqrt{x})G(\sqrt{x}).$$

بنابر قضیهٔ ۲۰۳ ، داریم

$$G(x) = \sum_{n\le x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + A + O\left(\frac{1}{\sqrt{x}}\right),$$

که درآن A ثابت است و، بنابر قضیهٔ ۱۸۰۶ ، معادلهٔ (۱۱) ، داریم

$$F(x) = \sum_{n\le x} \frac{\chi(n)}{\sqrt{n}} = B + O\left(\frac{1}{\sqrt{x}}\right),$$

که‌درآن $B = \sum_{n=1}^{\infty} \chi(n)/\sqrt{n}$. چون $F(\sqrt{x})G(\sqrt{x}) = 2Bx^{1/4} + O(1)$ ، معادلهٔ (۱۲) نتیجه می‌دهد که

$$\begin{aligned} B(x) &= \sum_{n\le\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} \left\{2\sqrt{\frac{x}{n}} + A + O\left(\sqrt{\frac{n}{x}}\right)\right\} \\ &\quad + \sum_{n\le\sqrt{x}} \frac{1}{\sqrt{n}} \left\{B + O\left(\sqrt{\frac{n}{x}}\right)\right\} - 2Bx^{1/4} + O(1) \\ &= 2\sqrt{x} \sum_{n\le\sqrt{x}} \frac{\chi(n)}{n} + A \sum_{n\le\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}} \sum_{n\le\sqrt{x}} |\chi(n)|\right) \\ &\quad + B \sum_{n\le\sqrt{x}} \frac{1}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}} \sum_{n\le\sqrt{x}} 1\right) - 2Bx^{1/4} + O(1) \\ &= 2\sqrt{x}\, L(1,\chi) + O(1). \end{aligned}$$

این قسمت (ب) را ثابت می‌کند. حال واضح است که قسمتهای (آ) و (ب) با هم $L(1,\chi) \neq 0$ را ایجاب می‌کنند.

تمرین برای فصل ۶

۱ . فرض‌کنید G مجموعه‌ای‌از ریشه‌های n م یک‌عدد مختلط‌ناصفر باشد. هرگاه G یک

گروه تحت ضرب باشد، ثابت کنید G گروه ریشه‌های nم واحد است.

۲. فرض‌کنید G یک‌گروه‌متناهی‌ازمرتبهٔ n با عنصرهمانی e باشد. هرگاه $a_1, \ldots, a_n$، n عنصر از G، نه لزوماً متمایز، باشند، ثابت کنید اعداد صحیحی چون p و q وجود دارند بطوری که $1 \leq p \leq q \leq n$ و $a_p a_{p+1} \cdots a_q = e$.

۳. فرض کنید G مجموعهٔ تمام ماتریسهای 2×2 مانند $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ باشد، که در آن a, b, c, d اعدادی صحیح‌اند و $ad - bc = 1$. ثابت کنید G تحت ضرب ماتریسی یک گروه است. این گروه گاهی **گروه هنگی** نامیده می‌شود.

۴. فرض‌کنید $G = \langle a \rangle$ یک‌گروه دوری تولید شده به‌وسیلهٔ a باشد. ثابت کنید هرزیر گروه G دوری است. (G متناهی فرض نشده است.)

۵. فرض‌کنید G یک‌گروه‌متناهی‌ازمرتبهٔ n بوده و G' یک زیر گروه ازمرتبهٔ m باشد. ثابت کنید که $m|n$ (قضیهٔ لاگرانژ) و نتیجه بگیرید که مرتبهٔ هر عنصر G، n را عاد می‌کند.

۶. فرض کنید G یک گروه از مرتبهٔ 6 با عنصرهمانی e باشد. ثابت کنید یا G دوری است، یا دو عنصر مانند a و b در G وجود دارند بطوری که

$$G = \{a, a^2, a^3, b, ab, a^2b\},$$

و $a^3 = b^2 = e$. از این عناصر کدام ba است؟

۷. یک‌جدول‌گروهی برای‌گروه متناهی $G = \{a_1, \ldots, a_n\}$ از مرتبهٔ n یک ماتریس $n \times n$ است‌که‌درایهٔ ij آن $a_i a_j$ است. اگر $a_i a_j = e$، ثابت‌کنیدکه $a_j a_i = e$. به‌عبارت دیگر، عنصرهمانی به‌طور متقارن در جدول گروهی قرار دارد. نتیجه بگیرید که‌اگر n زوج باشد، تعداد جوابهای معادلهٔ $x^2 = e$ زوج است.

۸. تمرین ۷ را تعمیم داده، فرض‌کنید $f(p)$ تعداد جوابهای معادلهٔ $x^p = e$ باشد، که در آن p یک مقسوم علیه اول n (مرتبهٔ G) است. ثابت کنید که $p|f(p)$ (قضیهٔ کشی). [**راهنمایی.** مجموعهٔ S از p تاییهای مرتب $(a_1, \ldots, a_p)$ را که $a_i \in G$ و $a_1 \cdots a_p = e$ در نظر بگیرید. n^{p-1} تا p تایی‌در S وجود دارند. دو p تایی از این نوع‌را معادل گویند اگر یکی یک جایگشت دوری دیگری باشد. نشان دهید که $f(p)$ ردهٔ هم‌ارزی شامل فقط یک عضواند و بقیه هریک شامل فقط p عضو می‌باشد. تعداد اعضای S را به‌دو طریق بشمارید و نتیجه بگیرید که $p|f(p)$.]

۹. فرض کنید G یک گروه متناهی از مرتبهٔ n باشد. ثابت کنید n فرد است اگرو فقط‌اگر هرعنصر G مربع باشد. یعنی، به‌ازای هر a در G، عنصری مانند b در

G هست بطوری که $a = b^2$.

۱۰ . تعمیم تمرین ۹ را که در آن شرط " n فرد است" با " n نسبت به k ، به‌ازای $k \geq 2$ ای ، اول است" عوض شده است ، را بیان و اثبات کنید .

۱۱ . فرض کنید G یک‌گروه متناهی از مرتبهٔ n بوده ، و S زیر مجموعه‌ای شامل بیش از $n/2$ عنصر G باشد . ثابت کنید به‌ازای هر g در G ، عنصرهایی چون a و b در S هستند بطوری که $ab = g$.

۱۲ . فرض کنید G یک‌گروه بوده و S زیر مجموعه‌ای از n عنصر متمایز G با این‌خاصیت باشد که $a \in S$ ، $a^{-1} \notin S$ را ایجاب کند . حاصل ضرب n^2 (نه لزوما " متمایز) به شکل ab رادرنظربگیرید ،که‌درآن $a \in S$ و $b \in S$. ثابت‌کنید حداکثر $n(n-1)/2$ از این حاصل ضربها متعلق به S اند .

۱۳ . فرض کنید $f_1, \ldots, f_m$ مشخصهای گروه متناهی G از مرتبهٔ m بوده ، و a عنصری از G از مرتبهٔ n باشد . قضیهٔ ۶ . ۷ نشان می‌دهد که هر عدد $f_r(a)$ یک ریشهٔ n م واحد است . ثابت کنید هر ریشهٔ n م واحد به تعداد مساوی در اعداد $f_1(a), f_2(a), \ldots, f_m(a)$ یافت می‌شود . [**راهنمایی** . با محاسبهٔ مجموع

$$\sum_{r=1}^{m} \sum_{k=1}^{n} f_r(a^k) e^{-2\pi i k/n}$$

به دو طریق ، تعداد تکرار $e^{2\pi i/n}$ را مشخص کنید .]

۱۴ . جداولی‌بسازید که مقادیرتمام مشخصهای‌دیریکله‌به هنگ k ، به‌ازای $k = 8, 9, 10$ ، را نشان دهند .

۱۵ . فرض‌کنید χ یک مشخص غیراصلی به هنگ k باشد . ثابت کنید به‌ازای هر عدد صحیح $a < b$ ، داریم

$$\left| \sum_{n=a}^{b} \chi(n) \right| \leq \frac{1}{2} \varphi(k).$$

۱۶ . هرگاه χ یک مشخص حقیقی به هنگ k باشد ، آنگاه به‌ازای هر n ، $\chi(n)$ مساوی ± 1 یا 0 است ؛ درنتیجه ، مجموع

$$S = \sum_{n=1}^{k} n\chi(n)$$

یک عدد صحیح است . این تمرین نشان می‌دهد که $12S \equiv 0 \pmod{k}$.

(آ) هرگاه $(a, k) = 1$ ، ثابت کنید که $a\chi(a)S \equiv S \pmod{k}$.

(ب) بنویسید $k = 2^\alpha q$ ، که درآن q فرداست . نشان دهید عدد صحیحی چون

a هست بطوری‌که $(a, k) = 1$ ، $a \equiv 3 \pmod{2^\alpha}$ و $a \equiv 2 \pmod{q}$. سپس، با استفاده از (آ) ، نتیجه بگیرید که $12S \equiv 0 \pmod{k}$.

۱۷ . تابع حسابی f را **متناوب به هنگ** k گویند اگر $k > 0$ و، وقتی $m \equiv n \pmod{k}$ ، $f(m) = f(n)$. عدد صحیح k **دورهٔ تناوب** f نام دارد.

(آ) هرگاه f متناوب به هنگ k باشد، ثابت کنید f دارای کوچکترین دورهٔ تناوب مثبت k_0 است و $k_0|k$.

(ب) فرض‌کنید f متناوب و کاملاً ضربی بوده، و k کوچکترین دورهٔ تناوب مثبت f باشد. ثابت کنید که اگر $(n, k) > 1$ ، $f(n) = 0$. این نشان می‌دهد که f یک مشخص دیریکله به هنگ k است.

۱۸ . (آ) فرض‌کنید f یک مشخص دیریکله به هنگ k باشد. هرگاه k فارغ ازمربع باشد، ثابت کنید k کوچکترین دورهٔ تناوب مثبت f است.

(ب) یک مشخص‌دیریکله به هنگ k مثال بزنید که به‌ازای آن k کوچکترین‌دورهٔ تناوب مثبت f نباشد.

۷
قضیهٔ دیریکله در باب اعداد اول در تصاعدهای حسابی

۱۰۷ مقدمه

تصاعدحسابی‌اعداد فرد $1, 3, 5, \ldots, 2n+1, \ldots$ شامل بی‌نهایت عدد اول است. طبیعی است بپرسیم آیا تصاعدهای حسابی دیگر نیز این خاصیت را دارند. یک تصاعد حسابی با جملهٔ اول h و تفاضل مشترک k متشکل است از همهٔ اعداد به شکل

$$kn + h, n = 0, 1, 2, \ldots \quad (۱)$$

اگر h و k عامل مشترکی چون d داشته باشند، هر جملهٔ تصاعد بر d بخشپذیراست و، اگر $d > 1$، بیش‌ازیک‌عدد اول‌در تصاعد وجودنخواهدداشت. به عبارت‌دیگر، شرط لازم برای وجود بی‌نهایت عدد اول در تصاعد حسابی (۱) آن است که $(h, k) = 1$. دیریکله اولین کسی بود که ثابت کرد این شرط‌کافی نیز هست. یعنی، اگر $(h, k) = 1$، تصاعد حسابی (۱) شامل بی‌نهایت عدد اول است. این نتیجه، که امروزه به **قضیهٔ دیریکله** معروف است، دراین‌فصل ثابت خواهد شد.

به‌یاد می‌آوریم که اویلر وجود بی‌نهایت عدد اول را، با اثبات اینکه سری $\sum p^{-1}$، که‌روی‌همهٔ اعداد اول گرفته شده، واگراست، ثابت کرد. ایدهٔ دیریکله این بود که‌حکم متناظررا،وقتی اعداد اول در تصاعد (۱) قرار دارند، ثابت کند. وی در مقالهٔ معروف [۱۵] که در ۱۸۳۷منتشرشد، این امر را با روشهای تحلیلی استادانه‌ای سرانجام‌داد. این برهان بعدها به‌وسیلهٔ چند مولف ساده شد. برهان مذکور دراین فصل بر برهانی استوار است که در ۱۹۵۰ به‌وسیلهٔ هارولد ان. شاپیرو [۶۵] منتشر شده است و با سری $\sum p^{-1} \log p$ به‌جای $\sum p^{-1}$ سر و کار دارد.

ابتدا نشان می‌دهیم که، به‌ازای تصاعدهای خاصی، می‌توان **قضیهٔ دیریکله** را با پیرایش برهان اقلیدس درمورد بی‌نهایتی اعداد اول به‌آسانی ثابت کرد.

۲.۷ قضیهٔ دیریکله در باب اعداد اول به شکل $4n-1$ و $4n+1$

قضیهٔ ۱.۷ . بی‌نهایت عدد اول به شکل $4n-1$ وجود دارند .

برهان . به برهان خلف می‌رویم . فرض کنیم تعدادی متناهی از این اعداد اول وجود داشته باشند ، p بزرگترین آنها باشد ، و عدد صحیح

$$N = 2^2 \cdot 3 \cdot 5 \cdots p - 1$$

رادرنظر می‌گیریم . حاصل ضرب $3 \cdot 5 \cdots p$ شامل همهٔ اعداد اول نابیشتر از p به‌عنوان عامل‌است . چون N به شکل $4n-1$ است ، نمی‌تواند اول باشد زیرا $N > p$. هیچ‌عدد اول‌نابیشتر از p ، N را عاد نمی‌کند ؛ درنتیجه ، همهٔ عوامل اول N باید متجاوز از p باشند . اما همهٔ عوامل اول N نمی‌توانند به شکل $4n+1$ باشند ، زیرا حاصل ضرب دو عدد به این شکل باز عددی به این شکل است . بنابراین ، عامل اولی از N باید به شکل $4n-1$ باشد ، و این یک تناقض می‌باشد .

برای اعداد اول به شکل $4n+1$ می‌توان استدلال متفاوتی بکار برد .

قضیهٔ ۲.۷ . بی‌نهایت عدد اول به شکل $4n+1$ وجود دارند .

برهان . فرض‌کنیم N عدد صحیحی بزرگتر از 1 باشد . نشان می‌دهیم عدد اولی چون $p > N$ هست بطوری که $p \equiv 1 \pmod 4$. فرض کنیم

$$m = (N!)^2 + 1.$$

توجه‌کنیدکه m فرداست و $m > 1$. فرض کنیم p کوچکترین عامل اول m باشد . هیچیک از اعداد $2, 3, \ldots, N$ ، m را عاد نمی‌کند ؛ درنتیجه ، $p > N$. همچنین ، داریم

$$(N!)^2 \equiv -1 \pmod p.$$

اگر طرفین را به توان $(p-1)/2$ برسانیم ، معلوم می‌شود که

$$(N!)^{p-1} \equiv (-1)^{(p-1)/2} \pmod p.$$

اما ، طبق قضیهٔ اویلر ــ فرما ، $(N!)^{p-1} \equiv 1 \pmod p$ ؛ درنتیجه ،

$$(-1)^{(p-1)/2} \equiv 1 \pmod p.$$

اما تفاضل $(-1)^{(p-1)/2} - 1$ یا 0 است یا -2 ، و نمی‌تواند مساوی -2 باشد ، زیرا بر

p بخشپذیر است؛ درنتیجه، باید 0 باشد. یعنی،

$$(-1)^{(p-1)/2} = 1.$$

اما این یعنی $(p-1)/2$ زوج است؛ درنتیجه، $p \equiv 1 \pmod 4$. به‌عبارت دیگر، نشان داده‌ایم که به‌ازای هر عدد صحیح $N > 1$، عدد اولی مانند $p > N$ هست بطوری که $p \equiv 1 \pmod 4$. بنابراین، بی‌نهایت عدد اول به شکل $4n + 1$ وجود دارند.

استدلالهای ساده‌شبیه‌آنهایی‌که‌هم اکنون‌برای اعداداول به شکل $4n - 1$ و $4n + 1$ داده شدرا می‌توان برای‌تصاعدهای‌حسابی‌خاص‌دیگرنظیر $5n - 1$، $8n - 1$، $8n - 3$، و $8n + 3$ نیز بکار گرفت (ر.ک. سیرپینسکی [۶۷])، ولی تاکنون استدلال ساده‌ای از این نوع که برای تصاعد کلی $kn + h$ بکار رود یافت نشده است.

۳.۷ طرح برهان قضیهٔ دیریکله

در قضیهٔ ۴.۱۰ فرمول مجانبی

$$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1) \tag{۲}$$

بدست آمد، که در آن مجموع روی تمام اعداداول $p \le x$ گرفته شده است. ما قضیهٔ دیریکله‌را به‌عنوان نتیجه‌ای از فرمول مجانبی مربوطهٔ زیر ثابت می‌کنیم.

قضیهٔ ۳.۷. *اگر $k > 0$ و $(h, k) = 1$، به‌ازای هر $x > 1$ داریم*

$$\sum_{\substack{p \le x \\ p \equiv h \pmod k}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + O(1), \tag{۳}$$

که‌درآن‌مجموع‌روی‌آن‌اعداد اول $p \le x$ گرفته شده که همنهشت h به هنگ k می‌باشند.

چون وقتی $x \to \infty$، $\log x \to \infty$، این رابطه ایجاب می‌کند که بی‌نهایت عدد اول $p \equiv h \pmod k$ وجود دارند؛ درنتیجه، بی‌نهایت عدد اول در تصاعـــد $nk + h, n = 0, 1, 2, \ldots$ وجود خواهند داشت.

توجه‌کنید که جملهٔ اصلی سمت راست (۳) مستقل از h است. لذا، (۳) نه فقط قضیهٔ دیریکله‌را ایجاب می‌کند، بلکه نشان می‌دهد که اعداد اول در هریک از $\varphi(k)$ ردهٔ مانده‌ای تحویل‌یافته به هنگ k به یک نسبت در جملهٔ عمده در (۲) شرکت دارند.

برهان‌قضیهٔ ۳۰۷ با یک رشته لم عرضه می‌شود، که در این بخش برای توضیح طرح برهان گرد آورده شده‌اند. در سراسر فصل، نمادگذاری زیر را می‌پذیریم.

عدد صحیح و مثبت k نمایش یک هنگ ثابت است، و h یک عدد صحیح ثابت است که نسبت به k اول می‌باشد. $\varphi(k)$ مشخص دیریکله به هنگ k با

$$\chi_1, \chi_2, \ldots, \chi_{\varphi(k)}$$

نموده‌می‌شوند، که χ_1 مشخص اصلی می‌باشد. به‌ازای $\chi \neq \chi_1$، مجموع سریهای زیر را با $L(1, \chi)$ و $L'(1, \chi)$ نشان می‌دهیم:

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n},$$

$$L'(1, \chi) = -\sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n}.$$

همگرایی هریک از این سریها در قضیهٔ ۱۸۰۶ نشان داده شد. بعلاوه، در قضیهٔ ۲۰۰۶ ثابت شد که اگر χ حقیقی باشد، $L(1, \chi) \neq 0$. علامت p نمایش عددی اول است، و $\sum_{p \le x}$ مجموع روی تمام اعداد اول $p \le x$ را نشان می‌دهد.

لم ۴۰۷ . به‌ازای $x > 1$، داریم

$$\sum_{\substack{p \le x \\ p \equiv h \pmod{k}}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + \frac{1}{\varphi(k)} \sum_{r=2}^{\varphi(k)} \bar{\chi}_r(h) \sum_{p \le x} \frac{\chi_r(p)\log p}{p} + O(1).$$

واضح است که اگر نشان دهیم که به ازای هر $\chi \neq \chi_1$،

$$\sum_{p \le x} \frac{\chi(p)\log p}{p} = O(1), \tag{۴}$$

لم ۴۰۷ قضیهٔ ۳۰۷را ایجاب خواهد کرد. لم زیر این مجموع را به شکلی بیان می‌کندکه روی همهٔ اعداد اول گرفته نشده است.

لم ۵۰۷ . به‌ازای $x > 1$ و $\chi \neq \chi_1$، داریم

$$\sum_{p \le x} \frac{\chi(p)\log p}{p} = -L'(1, \chi) \sum_{n \le x} \frac{\mu(n)\chi(n)}{n} + O(1).$$

بنابراین ، اگر نشان دهیم که

$$\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}=O(1), \qquad (۵)$$

لم ۵.۷ رابطهٔ (۴) راایجاب خواهد کرد . این ، به‌نوبهٔ خود ، از لم زیر نتیجه خواهد شد .

لم ۶.۷ . به‌ازای $x>1$ و $\chi\neq\chi_1$ ، داریم

$$L(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}=O(1). \qquad (۶)$$

هرگاه $L(1,\chi)\neq 0$ ، می‌توان‌با حذف $L(1,\chi)$ در (۶)رابطهٔ (۵) را بدست آورد . بنابراین ، برهان قضیهٔ دیریکله مآلا" به صفر نشدن $L(1,\chi)$ به‌ازای هر $\chi\neq\chi_1$ بستگی دارد . همانطور که قبلا" گفتیم ، این در قضیهٔ ۲۰.۶ به‌ازای χ های حقیقی مخالف χ_1 ثابت شده است ؛ درنتیجه ، کافی است ثابت شود که به‌ازای هر $\chi\neq\chi_1$ که مقادیرمختلط را نیز مثل حقیقی می‌گیرد ، $L(1,\chi)\neq 0$.

برای این کار ، فرض کنیم $N(k)$ تعداد مشخصهای غیر اصلی χ به هنگ k باشد بطوری که $L(1,\chi)=0$. هرگاه $L(1,\chi)=0$ ، آنگاه $L(1,\bar{\chi})=0$ و $\chi\neq\bar{\chi}$ ، زیرا χ حقیقی نیست . بنابراین ، مشخصهای χ که به‌ازای آنها $L(1,\chi)=0$ به‌صورت جفتهای‌مزدوج‌اند ؛درنتیجه ، $N(k)$ زوج‌می‌باشد . هدف اثبات این است که $N(k)=0$ ، و این از فرمول مجانبی زیر نتیجه خواهد شد .

لم ۷.۷ . به‌ازای $x>1$ ، داریم

$$\sum_{\substack{p\le x\\ p\equiv 1 \pmod k}}\frac{\log p}{p}=\frac{1-N(k)}{\varphi(k)}\log x+O(1). \qquad (۷)$$

هرگاه $N(k)\neq 0$ ، آنگاه $N(k)\ge 2$ ، زیرا $N(k)$ زوج است ؛ درنتیجه ، ضریب $\log x$ در (۷)منفی است و طرف راست ، وقتی $x\to\infty$ ، به $-\infty$ میل می‌نماید . این یک تناقض‌است ، زیرا تمام جملات سمت چپ مثبت هستند . لذا ، لم ۷.۷ ایجاب می‌کند که $N(k)=0$. برهان لم ۷.۷ ، به‌نوبهٔ خود ، بر فرمول مجانبی زیر استوار است .

لم ۸۰۷ . *اگر* $\chi \neq \chi_1$ و $L(1,\chi)=0$ ، *داریم*

$$L'(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}=\log x+O(1).$$

۴۰۷ برهان لم ۴۰۷

برای اثبات لم ۴۰۷ ، با فرمول مجانبی

$$\sum_{p\le x}\frac{\log p}{p}=\log x+O(1), \tag{۲}$$

که پیشتر ذکر شد ، شروع کرده و جملات ناشی از اعداداول $p\equiv h \pmod k$ را استخراج می‌کنیم .استخراج را به‌کمک رابطهٔ تعامدی برای مشخصهای دیریکله ، به‌صورت بیان شده در قضیهٔ ۱۶۰۶ ، یعنی

$$\sum_{r=}^{\varphi(k)}\chi_r(m)\bar{\chi}_r(n)=\begin{cases}\varphi(k) & \text{اگر } m\equiv n \pmod k ، \\ 0 & \text{اگر } m\not\equiv n \pmod k ،\end{cases}$$

انجام می‌دهیم . این رابطه به ازای $(n,k)=1$ معتبر است . $m=p$ و $n=h$ ،که $(h,k)=1$ ، را اختیارکرده، سپس دو طرف را در $p^{-1}\log p$ ضرب کرده و مجموع راروی تمام $p\le x$ هایی‌می‌گیریم تا بدست آید که

$$\sum_{p\le x}\sum_{r=1}^{\varphi(k)}\chi_r(p)\bar{\chi}_r(h)\frac{\log p}{p}=\varphi(k)\sum_{\substack{p\le x\\ p\equiv h \pmod k}}\frac{\log p}{p}. \tag{۸}$$

در مجموع سمت چپ ، جملاتی که فقط شامل مشخص اصلی χ_1 اند را جدا کرده و (۸) را به‌شکل زیر می‌نویسیم :

$$\varphi(k)\sum_{\substack{p\le x\\ p\equiv h \pmod k}}\frac{\log p}{p}=\bar{\chi}_1(h)\sum_{p\le x}\frac{\chi_1(p)\log p}{p}+\sum_{r=2}^{\varphi(k)}\bar{\chi}_r(h)\sum_{p\le x}\frac{\chi_r(p)\log p}{p}. \tag{۹}$$

اما $\bar{\chi}_1(h)=1$ و $\chi_1(p)=0$ مگر آنکه $(p,k)=1$ ،که‌دراین‌حالت $\chi_1(p)=1$. بنابراین ، اولین جملهٔ سمت راست (۹) عبارت است از

$$\sum_{\substack{p\le x\\ (p,k)=1}}\frac{\log p}{p}=\sum_{p\le x}\frac{\log p}{p}-\sum_{\substack{p\le x\\ p\mid k}}\frac{\log p}{p}=\sum_{p\le x}\frac{\log p}{p}+O(1), \tag{۱۰}$$

زیرا تعدادی متناهی عدد اول k را عاد می‌کنند. از تلفیق (۱۰) با (۹) داریم

$$\varphi(k) \sum_{\substack{p \le x \\ p \equiv h \pmod{k}}} \frac{\log p}{p} = \sum_{p \le x} \frac{\log p}{p} + \sum_{r=2}^{\varphi(k)} \bar{\chi}_r(h) \sum_{p \le x} \frac{\chi_r(p)\log p}{p} + O(1).$$

با استفاده از (۲) و تقسیم بر $\varphi(k)$، لم ۴.۷ بدست خواهد آمد.

۵.۷ برهان لم ۵.۷

با مجموع

$$\sum_{n \le x} \frac{\chi(n)\Lambda(n)}{n}$$

شروع می‌کنیم، که در آن $\Lambda(n)$ تابع منگولد است، و این مجموع را به دو صورت بیان می‌کنیم. ابتدا توجه می‌کنیم که، بنابر تعریف $\Lambda(n)$،

$$\sum_{n \le x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{\substack{p \le x \\ p^a \le x}} \sum_{a=1}^{\infty} \frac{\chi(p^a)\log p}{p^a}.$$

جملات به‌ازای $a = 1$ را جدا می‌کنیم و می‌نویسیم

$$\sum_{n \le x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{p \le x} \frac{\chi(p)\log p}{p} + \sum_{\substack{p \le x \\ p^a \le x}} \sum_{a=2}^{\infty} \frac{\chi(p^a)\log p}{p^a}. \qquad (۱۱)$$

مجموع دوم تحت تسلط

$$\sum_{p} \log p \sum_{a=2}^{\infty} \frac{1}{p^a} = \sum_{p} \frac{\log p}{p(p-1)} < \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} = O(1)$$

است؛ درنتیجه، از (۱۱) داریم

$$\sum_{p \le x} \frac{\chi(p)\log p}{p} = \sum_{n \le x} \frac{\chi(n)\Lambda(n)}{n} + O(1). \qquad (۱۲)$$

حال به‌یاد می‌آوریم که $\Lambda(n) = \sum_{d|n} \mu(d)\log(n/d)$؛ درنتیجه،

$$\sum_{n \le x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{n \le x} \frac{\chi(n)}{n} \sum_{d|n} \mu(d)\log\frac{n}{d}.$$

در مجموع اخیر، بانوشتن $n = cd$ و استفاده از خاصیت ضربی χ، خواهیم داشت

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}=\sum_{d\le x}\frac{\mu(d)\chi(d)}{d}\sum_{c\le x/d}\frac{\chi(c)\log c}{c}. \tag{۱۳}$$

چون $x/d\ge 1$ ، در مجموع روی c ، می‌توان با استفاده از فرمول (۱۰) قضیهٔ ۱۸۰۶ ، بدست آورد که

$$\sum_{c\le x/d}\frac{\chi(c)\log c}{c}=-L'(1,\chi)+O\left(\frac{\log x/d}{x/d}\right).$$

حال معادلهٔ (۱۳) به‌صورت زیر درمی‌آید :

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}=-L'(1,\chi)\sum_{d\le x}\frac{\mu(d)\chi(d)}{d}+O\left(\sum_{d\le x}\frac{1}{d}\frac{\log x/d}{x/d}\right). \tag{۱۴}$$

مجموع در جملهٔ O عبارت است از

$$\frac{1}{x}\sum_{d\le x}(\log x-\log d)=\frac{1}{x}\left([x]\log x-\sum_{d\le x}\log d\right)=O(1),$$

زیرا

$$\sum_{d\le x}\log d=\log[x]!=x\log x+O(x).$$

بنابراین ، رابطهٔ (۱۴) خواهد شد

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}=-L'(1,\chi)\sum_{d\le x}\frac{\mu(d)\chi(d)}{d}+O(1),$$

که ، همراه با (۱۲) ، لم ۵۰۷ را ثابت می‌کند .

۶۰۷ برهان لم ۶۰۷

از فرمول انعکاس‌تعمیم یافتهٔ موبیوس که در قضیهٔ ۲۳۰۲ ثابت شد استفاده می‌کنیم ، که می‌گوید هرگاه α کاملاً ضربی باشد ،

$$G(x)=\sum_{n\le x}\alpha(n)F\left(\frac{x}{n}\right) \quad \text{اگر و فقط اگر} \quad F(x)=\sum_{n\le x}\mu(n)\alpha(n)G\left(\frac{x}{n}\right). \tag{۱۵}$$

با فرض $\alpha(n)=\chi(n)$ و $F(x)=x$ ، داریم

$$x=\sum_{n\le x}\mu(n)\chi(n)G\left(\frac{x}{n}\right). \tag{۱۶}$$

که در آن

$$G(x) = \sum_{n \le x} \chi(n) \frac{x}{n} = x \sum_{n \le x} \frac{\chi(n)}{n}.$$

بنابرمعادلهٔ (۹)ازقضیهٔ ۶۰۸۱ ، می‌توان نوشت $G(x) = xL(1, \chi) + O(1)$. بااستفاده از این در (۱۶) ، معلوم می‌شود که

$$x = \sum_{n \le x} \mu(n)\chi(n)\left\{\frac{x}{n} L(1, \chi) + O(1)\right\} = xL(1, \chi) \sum_{n \le x} \frac{\mu(n)\chi(n)}{n} + O(x).$$

حال ، با تقسیم بر x ، لم ۶۰۷ بدست خواهد آمد .

۷۰۷ برهان لم ۸۰۷

لم ۸۰۷ را اثبات‌و سپس ، با استفاده از آن ، لم ۷۰۷ را ثابت می‌کنیم . باردیگرازفرمول انعکاس تعمیم یافتهٔ موبیوس (۱۵) استفاده می‌کنیم . این‌بار ، بااختیار $F(x) = x \log x$، خواهیم داشت

$$x \log x = \sum_{n \le x} \mu(n)\chi(n) G\left(\frac{x}{n}\right), \tag{۱۷}$$

که در آن

$$G(x) = \sum_{n \le x} \chi(n) \frac{x}{n} \log \frac{x}{n} = x \log x \sum_{n \le x} \frac{\chi(n)}{n} - x \sum_{n \le x} \frac{\chi(n) \log n}{n}.$$

حال ، با استفاده از فرمولهای (۹) و (۱۰) قضیهٔ ۶۰۸۱ ، بدست می‌آید

$$\begin{aligned} G(x) &= x \log x\left\{L(1, \chi) + O\left(\frac{1}{x}\right)\right\} + x\left\{L'(1, \chi) + O\left(\frac{\log x}{x}\right)\right\} \\ &= xL'(1, \chi) + O(\log x), \end{aligned}$$

زیرا فرض کرده‌ایم $L(1, \chi) = 0$. بنابراین ، (۱۷) نتیجه می‌دهد که

$$\begin{aligned} x \log x &= \sum_{n \le x} \mu(n)\chi(n)\left\{\frac{x}{n} L'(1, \chi) + O\left(\log \frac{x}{n}\right)\right\} \\ &= xL'(1, \chi) \sum_{n \le x} \frac{\mu(n)\chi(n)}{n} + O\left(\sum_{n \le x} (\log x - \log n)\right). \end{aligned}$$

قبلا" متذکر شدیم که جملهٔ O سمت راست $O(x)$ است (ر.ک. برهان لم ۵۰۷) . بنابر این ، داریم

$$x \log x = xL'(1, \chi) \sum_{n \le x} \frac{\mu(n)\chi(n)}{n} + O(x),$$

و وقتی بر x تقسیم کنیم، لم ۸.۷ بدست خواهد آمد.

۸.۷ برهان لم ۷.۷

با استفاده از لم ۴.۷ به‌ازای $h = 1$، بدست می‌آید

$$\sum_{\substack{p \le x \\ p \equiv 1 \pmod k}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + \frac{1}{\varphi(k)} \sum_{r=2}^{\varphi(k)} \sum_{p \le x} \frac{\chi_r(p) \log p}{p} + O(1). \tag{۱۸}$$

در مجموع روی p سمت راست از لم ۵.۷ استفاده می‌کنیم، که می‌گوید

$$\sum_{p \le x} \frac{\chi_r(p) \log p}{p} = -L'(1, \chi_r) \sum_{n \le x} \frac{\mu(n)\chi_r(n)}{n} + O(1).$$

هرگاه $L(1, \chi_r) \neq 0$، لم ۶.۷ نشان می‌دهد که طرف راست (۱۸) $O(1)$ است. ولی، هرگاه $L(1, \chi_r) = 0$، لم ۸.۷ ایجاب می‌کند که

$$-L'(1, \chi_r) \sum_{n \le x} \frac{\mu(n)\chi_r(n)}{n} = -\log x + O(1).$$

بنابراین، مجموع سمت راست (۱۸) عبارت است از

$$\frac{1}{\varphi(k)} \{-N(k) \log x + O(1)\};$$

درنتیجه، (۱۸) خواهد شد

$$\sum_{\substack{p \le x \\ p \equiv 1 \pmod k}} \frac{\log p}{p} = \frac{1 - N(k)}{\varphi(k)} \log x + O(1).$$

این لم ۷.۷، و لذا قضیهٔ ۳.۷، را ثابت می‌نماید.

همانطور که قبلا" گفته شد، قضیهٔ ۳.۷ قضیهٔ دیریکله را ایجاب می‌کند:

قضیهٔ ۹.۷. *اگر* $k > 0$ *و* $(h, k) = 1$*، در تصاعد حسابی* $nk + h, n = 0, 1, 2, \ldots$ *بی‌نهایت عدد اول وجود دارند.*

۹.۷ توزیع اعداد اول در تصاعدهای حسابی

اگر $k > 0$ و $(a, k) = 1$، قرار می‌دهیم

$$\pi_a(x) = \sum_{\substack{p \le x \\ p \equiv a \pmod k}} 1.$$

تابع $\pi_a(x)$ تعداداعداداول نابیشتر از x در تصاعد $nk + a, n = 0, 1, 2, \ldots$ رامی‌شمارد . قضیهٔ دیریکله نشان می‌دهد که ، وقتی $x \to \infty$ ، $\pi_a(x) \to \infty$. همچنین ، قضیهٔ اعداد اول برای تصاعدهای حسابی وجود دارد ، که می‌گوید اگر $(a, k) = 1$ ،

$$\text{وقتی } x \to \infty \text{ ، } \pi_a(x) \sim \frac{\pi(x)}{\varphi(k)} \sim \frac{1}{\varphi(k)} \frac{x}{\log x} \cdot \qquad (۱۹)$$

برهان (۱۹) در [۴۴] مختصراً " شرح داده شده است .

قضیهٔ اعداد اول برای تصاعدها از فرمول قضیهٔ ۳۰۷ ، یعنی

$$\sum_{\substack{p \le x \\ p \equiv h \pmod k}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + O(1),$$

ناشی می‌شود . چون جملهٔ اصلی مستقل از h است ، ظاهراً " اعداد اول در $\varphi(k)$ ردهٔ مانده‌ای تحویل یافته به هنگ k به تساوی توزیع شده‌اند ، و (۱۹) توضیح دقیق این امر می‌باشد .

این فصل را با تنظیم دیگری از قضیهٔ اعداد اول برای تصاعدهای حسابی پایان می‌دهیم .

قضیهٔ ۱۰۰۷ . هرگاه رابطهٔ

$$\text{وقتی } x \to \infty \text{ ، } \pi_a(x) \sim \frac{\pi(x)}{\varphi(k)} \qquad (۲۰)$$

به‌ازای هر عدد صحیح a نسبت به k اول برقرار باشد ، آنگاه رابطهٔ

$$\text{وقتی } x \to \infty \text{ ، } \pi_a(x) \sim \pi_b(x) \qquad (۲۱)$$

درصورتی که $(a, k) = (b, k) = 1$ برقرار می‌باشد . بعکس ، (۲۱) رابطهٔ (۲۰) را ایجاب خواهد کرد .

برهان . واضح‌است‌که (۲۰) رابطهٔ (۲۱) را ایجاب می‌کند . برای اثبات عکس ، (۲۱) را فرض کرده و $A(k)$ را تعداد اعداد اولی که k را عاد می‌کنند می‌گیریم . اگر $x > k$ ، داریم

$$\pi(x) = \sum_{p \le x} 1 = A(k) + \sum_{\substack{p \le x \\ p \nmid k}} 1$$
$$= A(k) + \sum_{\substack{a=1 \\ (a,k)=1}}^{k} \sum_{p \le x,\ p \equiv a \pmod k} 1 = A(k) + \sum_{\substack{a=1 \\ (a,k)=1}}^{k} \pi_a(x).$$

بنابراین،

$$\frac{\pi(x) - A(k)}{\pi_b(x)} = \sum_{\substack{a=1 \\ (a,k)=1}}^{k} \frac{\pi_a(x)}{\pi_b(x)}.$$

بنابر (۲۱) ، هر جملهٔ مجموع، وقتی $x \to \infty$ ، به 1 میل می‌کند ؛درنتیجه، مجموع به $\varphi(k)$ میل خواهد کرد . بنابراین،

وقتی $x \to \infty$ ، $\dfrac{\pi(x)}{\pi_b(x)} - \dfrac{A(k)}{\pi_b(x)} \to \varphi(k)$.

اما $A(k)/\pi_b(x) \to 0$ ؛ درنتیجه، $\pi(x)/\pi_b(x) \to \varphi(k)$ ، که (۲۰) را ثابت خواهد کرد .

تمرین برای فصل ۷

در تمرینهای ۱ تا ۴ ، h و k اعداد صحیح مثبتی هستند، $(h, k) = 1$ ، و $A(h, k)$ تصاعد حسابی $A(h, k) = \{h + kx : x = 0, 1, 2, \ldots\}$ می‌باشد . تمرینهای ۱ تا ۴ باید بی‌استفاده از قضیهٔ دیریکله حل شوند .

۱ . ثابت‌کنید به‌ازای‌هر عدد صحیح $n \ge 1$ ، $A(h, k)$ بی‌نهایت عدد نسبت به n اول دارد .

۲ . ثابت کنید $A(h, k)$ شامل زیرمجموعه‌ای‌نامتناهی‌است مانند $\{a_1, a_2, \ldots\}$ بطوری که اگر $i \ne j$ ، $(a_i, a_j) = 1$.

۳ . ثابت کنید $A(h, k)$ شامل‌زیرمجموعه‌ای‌نامتناهی‌است که یک تصاعد هندسی تشکیل می‌دهد (مجموعه‌ای از اعداد به شکل $ar^n, n = 0, 1, 2, \ldots$) . این ایجاب می‌کنـد که $A(h, k)$ شامل بی‌نهایت عدد با عوامل اول یکسان است .

۴ . فرض‌کنید S یک زیر مجموعهٔ‌نامتناهی $A(h, k)$ باشد . ثابت کنید به‌ازای هر عدد صحیح‌ومثبت n ، عددی در $A(h, k)$ هست که می‌توان آن را به‌صورت حاصل ضربی با بیش از n عنصر متفاوت‌از S نوشت .

۵ . قضیهٔ دیریکله حکم زیر را ایجاب می‌کند: هرگاه h و $k > 0$ دو عدد صحیح با

خاصیت $(h,k)=1$ باشند، آنگاه دست کم یک عدد اول به شکل $kn+h$ وجود خواهد داشت. ثابت کنید این حکم نیز قضیهٔ دیریکله را ایجاب می‌کند.

۶. هرگاه $k>0$ ، $(h,k)=1$)، ثابت‌کنید عدد ثابتی چون A (وابسته به h و k) هست بطوری که اگر $x\geq 2$ ،

$$\sum_{\substack{p\leq x\\ p\equiv h\ (\mathrm{mod}\ k)}} \frac{1}{p}=\frac{1}{\varphi(k)}\log\log x+A+O\left(\frac{1}{\log x}\right).$$

۷. مجموعهٔ نامتناهی S از اعداد اول را با خاصیت زیر بسازید: هرگاه $p\in S$ و $q\in S$ ، آنگاه $(\frac{1}{2}(p-1),\frac{1}{2}(q-1))=(p,q-1)=(p-1,q)=1$.

۸. فرض کنید f یک چندجمله‌ای درجهٔ $n\geq 1$ با ضرایب صحیح و خاصیت زیر باشد: به‌ازای هر p اول، عدد اولی چون q و عدد صحیحی مثل m هست بطوری که $f(p)=q^m$. ثابت‌کنید $q=p$ ، $m=n$ و، به‌ازای هر x ، $f(x)=x^n$. [**راهنمایی.** هرگاه $q\neq p$ ، آنگاه q^{m+1} ، $f(p+tq^{m+1})-f(p)$ را به‌ازای هر $t=1,2,\ldots$ عاد می‌کند.]

۸ توابع حسابی متناوب و مجموعهای گاوس

۱.۸ توابع متناوب به هنگ k

فرض‌کنیم k یک عدد صحیح مثبت باشد. تابع حسابی f را **متناوب با دورهٔ تناوب** k (یا **متناوب به هنگ** k) گویند اگر، به‌ازای هر عدد صحیح n،

$$f(n+k) = f(n) \cdot$$

اگر k دورهٔ تناوب باشد، mk به‌ازای هر عدد صحیح $m > 0$ نیز چنین است. کوچکترین دورهٔ تناوب مثبت f **دورهٔ تناوب اساسی** نامیده می‌شود.

توابع متنـاوب را در فصـول پیشتر دیده‌ایم. مثلاً، مشخصهای دیریکله به هنگ k متناوب به هنگ k هستند. مثال ساده‌تر بزرگترین مقسوم علیه مشترک (n, k) است به عنوان تابعی از n. تناوب با رابطهٔ

$$(n+k, k) = (n, k)$$

بیان می‌شود. مثال دیگر تابع نمایی

$$f(n) = e^{2\pi imn/k}$$

است، که‌در آن m و k اعداد صحیح ثابتی هستند. عدد $e^{2\pi im/k}$ ریشهٔ k ام واحدبوده و $f(n)$ توان n م آن است. هر ترکیب خطی متناهی از این توابع، مثلاً،

$$\sum_m c(m) e^{2\pi imn/k}$$

نیز به‌ازای هـر انتخابی از ضرایب $c(m)$ متناوب به هنگ k است. اولین کار اثبات این است که هر تابع حسابی متناوب به هنگ k را می‌توان به‌صورت ترکیبی خطی از این‌نوع نوشت. ایـن مجموعها را **سریهای فوریهٔ**[1] **متناهی** می‌نامند. بحث را با یک مثال ساده

---

1. *Fourier*

ولی مهم ، معروف به مجموع هندسی ، آغاز می‌کنیم .

قضیهٔ ۱۰۸ . به‌ازای $k \geq 1$ ثابت ، فرض‌کنیم

$$g(n) = \sum_{m=0}^{k-1} e^{2\pi imn/k}.$$

دراین صورت ،

$$g(n) = \begin{cases} 0 & \text{اگر } k \nmid n ، \\ k & \text{اگر } k|n ، \end{cases}$$

برهان . چون $g(n)$ مجموع جملات در یک تصاعد هندسی است ، یعنی

$$g(n) = \sum_{m=0}^{k-1} x^m$$

که درآن $x = e^{2\pi in/k}$ ، داریم

$$g(n) = \begin{cases} \dfrac{x^k - 1}{x - 1} & \text{اگر } x \neq 1 ، \\ k & \text{اگر } x = 1 ، \end{cases}$$

اما $x^k = 1$ ، و $x = 1$ اگر و فقط اگر $k|n$ ؛ درنتیجه ، قضیه اثبات شده است .

۲۰۸ وجود سریهای فوریهٔ متناهی برای توابع حسابی متناوب

با استفاده از فرمول درونیابی چند جمله‌ای لاگرانژ ، نشان می‌دهیم که هر تابع حسابی متناوب یک بسط فوریهٔ متناهی دارد .

قضیهٔ ۲۰۸ . قضیهٔ درونیابی لاگرانژ. فرض‌کنیم $z_0, z_1, \ldots, z_{k-1}$ ، k عدد مختلط متمایز بوده ، و $w_0, w_1, \ldots, w_{k-1}$ ، k عدد مختلط باشند که لزوماً" متمایز نیستند . دراین صورت ، چندجمله‌ای منحصر بفردی مانند $P(z)$ از درجهٔ نابیشتر از $k - 1$ وجود دارد بطوری‌که

$$\text{به‌ازای } m = 0, 1, 2, \ldots, k - 1 ، \quad P(z_m) = w_m \cdot$$

برهان . چندجمله‌ای مطلوب $P(z)$ ، که چندجمله‌ای درونیاب لاگرانژ نام دارد ، را می‌توان صریحاً" به‌صورت زیر ساخت : فرض کنیم

$$A(z) = (z - z_0)(z - z_1) \cdots (z - z_{k-1})$$

و

$$A_m(z) = \frac{A(z)}{z - z_m}.$$

دراین صورت ، $A_m(z)$ یک چندجمله‌ای از درجهٔ $k - 1$ با خاصیت زیر است :

$A_m(z_m) \neq 0$ ؛ اگر $j \neq m$ ، $A_m(z_j) = 0$.

لذا ، $A_m(z)/A_m(z_m)$ یک‌چندجمله‌ای‌ازدرجهٔ $k - 1$ است‌که‌درهر z_j ، به‌ازای $j \neq m$ ، صفر می‌شود ، و در z_m دارای مقدار 1 است . بنابراین ، ترکیب خطی

$$P(z) = \sum_{m=0}^{k-1} w_m \frac{A_m(z)}{A_m(z_m)}$$

یک چندجمله‌ای از درجـهٔ نابیشتر از $k - 1$ است با این خاصیت که ، به‌ازای هر j ، $P(z_j) = w_j$. اگرچندجمله‌ای دیگری از این نوع ، مثلاً " $Q(z)$ ، وجود می‌داشت ، تفاضل $P(z) - Q(z)$ در k نقطهٔ متمایز صفر می‌شد ؛ درنتیجه ، $P(z) = Q(z)$ ، زیرا هر دو چند جمله‌ای از درجهٔ نابیشتر از $k - 1$ می‌باشند .

حال اعداد $z_0, z_1, \ldots, z_{k-1}$ را ریشه‌های k ام واحد گرفته و بدست می‌آوریم :

قضیهٔ ۳.۸ . به‌ازای k عدد مختلط $w_0, w_1, \ldots, w_{k-1}$ ، k عدد مختلط منحصربفرد مانند $a_0, a_1, \ldots, a_{k-1}$ وجود دارند بطوری که ، به‌ازای $m = 0, 1, 2, \ldots, k - 1$ ،

$$w_m = \sum_{n=0}^{k-1} a_n e^{2\pi imn/k}. \tag{1}$$

بعلاوه ، ضرایب a_n از فرمولهای زیر بدست می‌آیند :

به‌ازای $n = 0, 1, 2, \ldots, k - 1$ ،

$$a_n = \frac{1}{k} \sum_{m=0}^{k-1} w_m e^{-2\pi imn/k}. \tag{2}$$

برهان . فرض کنیم $z_m = e^{2\pi im/k}$. اعداد $z_0, z_1, \ldots, z_{k-1}$ متمایزند ؛ درنتیجه ، یک چندجمله‌ای لاگرانژ منحصربفرد مانند

$$P(z) = \sum_{n=0}^{k-1} a_n z^n$$

هست بطوری که ، به‌ازای هر $m = 0, 1, 2, \ldots, k - 1$ ، $P(z_m) = w_m$. این نشان می‌دهد

که اعــداد منحصر بفردی مانند a_n وجود دارند که در (۱) صدق می‌کنند. برای بدست آوردن فرمــول (۲) برای a_n، طرفین (۱) را در $e^{-2\pi imr/k}$، که در آن m و r اعداد صحیح نامنفی کمتر از k اند، ضرب کرده و روی m جمع می‌بندیم تا بدست آید که

$$\sum_{m=0}^{k-1} w_m e^{-2\pi imr/k} = \sum_{n=0}^{k-1} a_n \sum_{m=0}^{k-1} e^{2\pi i(n-r)m/k}.$$

طبق قضیهٔ ۱۰۸، مجموع روی m مساوی 0 است مگر آنکه $k|(n-r)$. اما $|n-r| \leq k-1$؛ درنتیجه، $k|(n-r)$ اگر و فقـط اگر $n=r$. بنابراین، تنها جملهٔ ناصفر سمت راست به‌ازای $n=r$ است و درمی‌یابیم که

$$\sum_{m=0}^{k-1} w_m e^{-2\pi imr/k} = ka_r.$$

این معادله (۲) را به‌ما خواهد داد.

قضیهٔ ۴۰۸ . *فرض‌کنیم تابع حسابی f متناوب به هنگ k باشد. دراین صورت، تابع حسابی منحصر بفردی مانند g هست، که آن نیز متناوب به هنگ k است، بطوری که*

$$f(m) = \sum_{n=0}^{k-1} g(n)e^{2\pi imn/k}.$$

درواقع، g از فرمول زیر بدست می‌آید:

$$g(n) = \frac{1}{k}\sum_{m=0}^{k-1} f(m)e^{-2\pi imn/k}.$$

برهان. فرض‌کنیم به‌ازای $m = 0, 1, 2, \ldots, k-1$، $w_m = f(m)$، و، با اعمال قضیهٔ ۳۰۸، اعداد $a_0, a_1, \ldots, a_{k-1}$ را معین می‌کنیم. تابع g را با روابط $g(m) = a_m$ به‌ازای $m = 0, 1, 2, \ldots, k-1$ تعریف کــرده و تعریف $g(m)$ را به‌وسیلهٔ تناوب به هنگ k به همهٔ اعداد صحیح m تعمیم می‌دهیم. دراین صورت، f به‌وسیلهٔ معادلات قضیه به g مربوط می‌شود.

تذکر. چون f و g هردو متناوب به هنگ k اند، می‌توان مجموعهای قضیهٔ ۴۰۸ را به صورت زیر نوشت:

$$f(m) = \sum_{n \bmod k} g(n)e^{2\pi imn/k} \tag{۳}$$

و

$$g(n) = \frac{1}{k} \sum_{m \bmod k} f(m) e^{-2\pi i mn/k}. \qquad (۴)$$

درهر حالت، مجموع را می‌توان روی هر دستگاه مانده‌ای تام به هنگ k گسترش داد. مجموع (۳) **بسط فوریهٔ متناهی** f نامیده و اعداد $g(n)$ تعریف شده با (۴) را **ضرایب فوریهٔ** f می‌نامند.

۳.۸ مجموع رامانوجان[1] و تعمیمهای آن

در تمرین ۱۴۰۲ (ب) نشان داده شد که تابع موبیوس $\mu(k)$ مجموع k ریشهٔ اولیهٔ واحد است. درایـن بخش، این نتیجه را تعمیم می‌دهیم. بخصوص، فرض کنیم n یک عدد صحیح مثبت ثابت بوده و مجموع تـوانـهای n م ریشه‌های k ام اولیهٔ واحد را درنظر می‌گیریم. این مجموع به **مجموع رامانوجان** معروف است و با $c_k(n)$ نموده می‌شود:

$$c_k(n) = \sum_{\substack{m \bmod k \\ (m,k)=1}} e^{2\pi i mn/k}.$$

قبلاً متذکر شدیم که این مجموع، وقتی $n = 1$، به تابع موبیوس تحویل می‌شود:

$$\mu(k) = c_k(1).$$

وقتی $k|n$، مجموع بـه تـابع φ اویلر تحویل می‌شود، زیرا هر جمله 1 است و تعداد جملات $\varphi(k)$ می‌باشد. رامانوجان‌نشان داد که $c_k(n)$ همواره یک عدد صحیح است ودارای خواص ضربی جالبی می‌باشد. وی این مطالب را از رابطهٔ

$$c_k(n) = \sum_{d|(n,k)} d\mu\left(\frac{k}{d}\right) \qquad (۵)$$

نتیجه گرفت. این فرمول دلیل تحویل $c_k(n)$ به $\mu(k)$ و $\varphi(k)$ را نشان می‌دهد. درواقع، وقتی $n = 1$، فقط یک جمله در مجموع وجود دارد و بدست می‌آوریم $c_k(1) = \mu(k)$. و وقتی $k|n$، داریم $(n, k) = k$ و $c_k(n) = \sum_{d|k} d\mu(k/d) = \varphi(k)$. رابطهٔ (۵) را به‌عنوان حالت خاصی از یک نتیجهٔ کلیتر (قضیهٔ ۵.۸) بدست می‌آوریم.

فرمول (۵) برای $c_k(n)$ پیشنهاد می‌کند که ما مجموعهای کلی به شکل

$$\sum_{d|(n,k)} f(d) g\left(\frac{k}{d}\right) \qquad (۶)$$

1. Ramanujan

رابررسی کنیم. این مجموعها شبیه مجموعهای پیچش دیریکلهٔ $f * g$ است جز آنکه مجموع روی زیرمجموعه‌ای از مقسوم‌علیه‌های k ، یعنی آن d هایی که n را نیز عاد می‌کنند، گرفته می‌شود.

مجموع (۶) را با $s_k(n)$ نشان می‌دهیم. چون n فقط در (n, k) بمعم می‌آید، داریم

$$s_k(n+k) = s_k(n);$$

درنتیجه، $s_k(n)$ یک تابع متناوب از n با دورهٔ تناوب k است. لذا، این مجموع یک بسط فوریهٔ متناهی دارد. قضیهٔ بعدی به‌ما می‌گوید که ضرایب فوریهٔ آن با مجموعی از همین نوع داده می‌شوند.

قضیهٔ ۵.۸ . فرض‌کنیم $s_k(n) = \sum_{d|(n,k)} f(d)g(k/d)$. دراین صورت، $s_k(n)$ دارای بسط فوریهٔ متناهی زیر است:

$$s_k(n) = \sum_{m \bmod k} a_k(m) e^{2\pi i m n/k} \qquad (۷)$$

که در آن

$$a_k(m) = \sum_{d|(m,k)} g(d) f\left(\frac{k}{d}\right) \frac{d}{k}. \qquad (۸)$$

برهان. بنابر قضیهٔ ۴.۸ ، ضرایب $a_k(m)$ از روابط زیر بدست می‌آیند:

$$a_k(m) = \frac{1}{k} \sum_{n \bmod k} s_k(n) e^{-2\pi i n m/k}$$
$$= \frac{1}{k} \sum_{n=1}^{k} \sum_{\substack{d|n \\ d|k}} f(d) g\left(\frac{k}{d}\right) e^{-2\pi i n m/k}.$$

حال می‌نویسیم $n = cd$ و توجه می‌کنیم که به‌ازای‌هر d ثابت، اندیس c از 1 تا k/d تغییر می‌کند و خواهیم داشت

$$a_k(m) = \frac{1}{k} \sum_{d|k} f(d) g\left(\frac{k}{d}\right) \sum_{c=1}^{k/d} e^{-2\pi i c d m/k}.$$

حال، اگر در مجموع طرف راست d را با k/d عوض کنیم، بدست می‌آید که

$$a_k(m) = \frac{1}{k} \sum_{d|k} f\left(\frac{k}{d}\right) g(d) \sum_{c=1}^{d} e^{-2\pi i c m/d}.$$

اما، طبق قضیهٔ ۱.۸ ، مجموع روی c مساوی 0 است، مگر آنکه $d|m$ که دراین حالت

مجموع مقدار d را خواهد داشت. بنابراین،

$$a_k(m) = \frac{1}{k} \sum_{\substack{d|k \\ d|m}} f\left(\frac{k}{d}\right) g(d) d$$

که (۸) را ثابت خواهد کرد.

حال، بـه‌ازای توابع خاص f و g، فرمول مجموع را مانوجان را که قبلاً" ذکر شد بدست می‌آوریم.

قضیهٔ ۶.۸ . داریم

$$c_k(n) = \sum_{d|(n,k)} d\mu\left(\frac{k}{d}\right).$$

برهان. با فرض $f(k) = k$ و $g(k) = \mu(k)$ در قضیهٔ ۵.۸، معلوم می‌شود که

$$\sum_{d|(n,k)} d\mu\left(\frac{k}{d}\right) = \sum_{m \bmod k} a_k(m) e^{2\pi imn/k}$$

که درآن

$$a_k(m) = \sum_{d|(m,k)} \mu(d) = \left[\frac{1}{(m,k)}\right] = \begin{cases} 1 & \text{اگر } (m,k) = 1 \\ 0 & \text{اگر } (m,k) > 1 \end{cases}$$

بنابراین،

$$\sum_{d|(n,k)} d\mu\left(\frac{k}{d}\right) = \sum_{\substack{m \bmod k \\ (m,k)=1}} e^{2\pi imn/k} = c_k(n).$$

۴.۸ خواص ضربی مجموعهای $s_k(n)$

قضیهٔ ۷.۸ . فرض کنیم

$$s_k(n) = \sum_{d|(n,k)} f(d) g\left(\frac{k}{d}\right)$$

که درآن f و g ضربی‌اند. دراین صورت،

(۹) اگر $(a,k) = (b,m) = 1$، $s_{mk}(ab) = s_m(a) s_k(b)$.

بخصوص،

(۱۰) اگر $(b,m) = 1$، $s_m(ab) = s_m(a)$.

و

اگر $(a, k) = 1$ ، $s_{mk}(a) = s_m(a)g(k)$. (۱۱)

برهان. روابط $(a, k) = (b, m) = 1$ ایجاب می‌کنند (ر.ک. تمرین ۲۴۰۱) که

$$(mk, ab) = (a, m)(k, b),$$

که درآن (a, m) و (b, k) نسبت بهم اول‌اند. بنابراین،

$$s_{mk}(ab) = \sum_{d|(mk, ab)} f(d)g\left(\frac{mk}{d}\right) = \sum_{d|(a, m)(b, k)} f(d)g\left(\frac{mk}{d}\right).$$

اگر درآخرین مجموع بنویسیم $d = d_1d_2$ ، خواهیم داشت

$$\begin{aligned} s_{mk}(ab) &= \sum_{d_1|(a, m)} \sum_{d_2|(b, k)} f(d_1d_2)g\left(\frac{mk}{d_1d_2}\right) \\ &= \sum_{d_1|(a, m)} f(d_1)g\left(\frac{m}{d_1}\right) \sum_{d_2|(b, k)} f(d_2)g\left(\frac{k}{d_2}\right) = s_m(a)s_k(b). \end{aligned}$$

این (۹) را ثابت می‌کند.

با فرض $k = 1$ در (۹) ، بدست می‌آوریم

$$s_m(ab) = s_m(a)s_1(b) = s_m(a),$$

زیرا $s_1(b) = f(1)g(1) = 1$. این (۱۰) را ثابت می‌کند. با فرض $b = 1$ در (۹) ، معلوم می‌شود که

$$s_{mk}(a) = s_m(a)s_k(1) = s_m(a)g(k),$$

زیرا $s_k(1) = f(1)g(k) = g(k)$. این (۱۱) را ثابت خواهد کرد.

مثال. برای مجموع رامانوجان خواص ضربی زیر را بدست می‌آوریم:

اگر $(a, k) = (b, m) = 1$ ، $c_{mk}(ab) = c_m(a)c_k(b)$ ؛

اگر $(b, m) = 1$ ، $c_m(ab) = c_m(a)$ ؛

و

اگر $(a, k) = 1$ ، $c_{mk}(a) = c_m(a)\mu(k)$.

گاهی مجموعهای $s_k(n)$ را می‌توان برحسب پیچش دیریکلهٔ $f * g$ حساب کرد. در این رابطه، داریم:

قضیهٔ ۸۰۸ . فرض‌کنیم f کاملا "ضربی بوده ، و $g(k) = \mu(k)h(k)$ ، که درآن h ضربی می‌باشد . همچنین ، به‌ازای هر عدد اول p ، $f(p) \neq 0$ و $f(p) \neq h(p)$ ، و نیز

$$s_k(n) = \sum_{d|(n,k)} f(d)g\left(\frac{k}{d}\right).$$

دراین صورت ، داریم

$$s_k(n) = \frac{F(k)g(N)}{F(N)},$$

که درآن $F = f * g$ و $N = k/(n,k)$.

برهان. ابتدا توجه می‌کنیم که

$$F(k) = \sum_{d|k} f(d)\mu\left(\frac{k}{d}\right)h\left(\frac{k}{d}\right) = \sum_{d|k} f\left(\frac{k}{d}\right)\mu(d)h(d) = f(k)\sum_{d|k}\mu(d)\frac{h(d)}{f(d)}$$
$$= f(k)\prod_{p|k}\left(1 - \frac{h(p)}{f(p)}\right).$$

حال می‌نویسیم $a = (n,k)$ ؛ درنتیجه ، $k = aN$. دراین صورت ، داریم

$$s_k(n) = \sum_{d|a} f(d)\mu\left(\frac{k}{d}\right)h\left(\frac{k}{d}\right) = \sum_{d|a} f(d)\mu\left(\frac{aN}{d}\right)h\left(\frac{aN}{d}\right)$$
$$= \sum_{d|a} f\left(\frac{a}{d}\right)\mu(Nd)h(Nd).$$

اما ،اگر $(N,d) = 1$ ، $\mu(Nd) = \mu(N)\mu(d)$ ،و ،اگر $(N,d) > 1$ ، $\mu(Nd) = 0$ ؛ درنتیجه ، معادلهٔ آخر نتیجه می‌دهد که

$$s_k(n) = \mu(N)h(N)\sum_{\substack{d|a\\(N,d)=1}} f\left(\frac{a}{d}\right)\mu(d)h(d) = f(a)\mu(N)h(N)\sum_{\substack{d|a\\(N,d)=1}}\mu(d)\frac{h(d)}{f(d)}$$
$$= f(a)\mu(N)h(N)\prod_{\substack{p|a\\p\nmid N}}\left(1 - \frac{h(p)}{f(p)}\right) = f(a)\mu(N)h(N)\frac{\prod_{p|aN}\left(1 - \frac{h(p)}{f(p)}\right)}{\prod_{p|N}\left(1 - \frac{h(p)}{f(p)}\right)}$$
$$= f(a)\mu(N)h(N)\frac{F(k)}{f(k)}\frac{f(N)}{F(N)} = \frac{F(k)\mu(N)h(N)}{F(N)} = \frac{F(k)g(N)}{F(N)}.$$

مثال. برای مجموع رامانوجان صورت سادهٔ زیر بدست می‌آید :

$$c_k(n) = \varphi(k)\mu(N)/\varphi(N) = \frac{\varphi(k)\mu\left(\dfrac{k}{(n, k)}\right)}{\varphi\left(\dfrac{k}{(n, k)}\right)}.$$

۵.۸ مجموعهای گاوس وابسته به مشخصهای دیریکله

تعریف. به‌ازای مشخص دیریکلهٔ χ به هنگ k ، مجموع

$$G(n, \chi) = \sum_{m=1}^{k} \chi(m)e^{2\pi imn/k}$$

را **مجموع گاوس وابسته به** χ می‌نامند.

هرگاه $\chi = \chi_1$ ، یعنی مشخص‌اصلی به هنگ k ، داریم $\chi_1(m) = 1$ اگر $(m, k) = 1$، و $\chi_1(m) = 0$ درغیر این‌صورت. دراین حالت، مجموع گاوس به مجموع‌رامانوجان تحویل می‌شود :

$$G(n, \chi_1) = \sum_{\substack{m=1 \\ (m,k)=1}}^{k} e^{2\pi imn/k} = c_k(n).$$

لذا، مجموعهای گاوس $G(n, \chi)$ را می‌توان تعمیمهای مجموع رامانوجان دانست. حال به بررسی مشروح خواص آنها می‌پردازیم.

اولین نتیجه یک خاصیت تجزیه است که نقش مهمی در مطالب بعدی دارد.

قضیهٔ ۹.۸ . هرگاه χ یک مشخص دیریکله به هنگ k باشد، آنگاه
هر وقت $(n, k) = 1$ ، $G(n, \chi) = \bar{\chi}(n)G(1, \chi)$.

برهان. وقتی $(n, k) = 1$ ، اعداد nr ، همانند r ، یک دستگاه مانده‌ای تام به هنگ k را تولید می‌کنند. همچنین، $|\chi(n)|^2 = \chi(n)\bar{\chi}(n) = 1$ ؛ درنتیجه،

$$\chi(r) = \bar{\chi}(n)\chi(n)\chi(r) = \bar{\chi}(n)\chi(nr).$$

لذا، مجموع معرف $G(n, \chi)$ را می‌توان به‌صورت زیر نوشت :

$$G(n, \chi) = \sum_{r \bmod k} \chi(r)e^{2\pi inr/k} = \bar{\chi}(n) \sum_{r \bmod k} \chi(nr)e^{2\pi inr/k}$$

$$= \bar{\chi}(n) \sum_{m \bmod k} \chi(m)e^{2\pi i m/k} = \bar{\chi}(n)G(1, \chi).$$

این قضیه را ثابت خواهد کرد.

تعریف. مجموع گاوس $G(n, \chi)$ را *جدایی پذیر* گوییم اگر

$$G(n, \chi) = \bar{\chi}(n)G(1, \chi). \qquad (۱۲)$$

قضیهٔ ۹.۸ می‌گوید که $G(n, \chi)$ وقتی n نسبت به هنگ k اول باشد جدایی پذیر است. برای اعداد صحیح nی که نسبت به k اول نیستند قضیهٔ زیر را داریم.

قضیهٔ ۱۰.۸ . *هرگاه χ یک مشخص به هنگ k باشد، مجموع گاوس $G(n, \chi)$ به‌ازای هر n جدایی پذیر است اگر و فقط اگر*

هر وقت $(n, k) > 1$ ، $G(n, \chi) = 0$.

برهان. اگر $(n, k) = 1$ ، جدایی‌پذیری همواره برقرار است. اما، اگر $(n, k) > 1$ ، داریم $\bar{\chi}(n) = 0$ ؛ درنتیجه، معادلهٔ (۱۲) برقرار است اگر و فقط اگر $G(n, \chi) = 0$.

قضیهٔ زیر نتیجهٔ مهم جدایی پذیری است.

قضیهٔ ۱۱.۸ . *هرگاه $G(n, \chi)$ به‌ازای هر n جدایی پذیر باشد، آنگاه*

$$|G(1, \chi)|^2 = k. \qquad (۱۳)$$

برهان. داریم

$$\begin{aligned}
|G(1, \chi)|^2 &= G(1, \chi)\overline{G(1, \chi)} = G(1, \chi)\sum_{m=1}^{k} \bar{\chi}(m)e^{-2\pi i m/k} \\
&= \sum_{m=1}^{k} G(m, \chi)e^{-2\pi i m/k} = \sum_{m=1}^{k}\sum_{r=1}^{k} \chi(r)e^{2\pi i m r/k}e^{-2\pi i m/k} \\
&= \sum_{r=1}^{k} \chi(r)\sum_{m=1}^{k} e^{2\pi i m(r-1)/k} = k\chi(1) = k,
\end{aligned}$$

زیرا آخرین مجموع روی m یک مجموع هندسی است که صفر است مگر آنکه $r = 1$.

۸.۶ مشخصهای دیریکله با مجموعهای گاوس صفر نشو

به‌ازای هر مشخص χ به هنگ k ، دیدیم که $G(n, \chi)$ جدایی پذیر است اگر $(n, k) = 1$ و جدایی‌پذیری $G(n, \chi)$ معادل صفر نشدن $G(n, \chi)$ به‌ازای $(n, k) > 1$ می‌باشد. حال خواص دیگر آن مشخصهایی را توصیف می‌کنیم که وقتی $(n, k) > 1$ ، $G(n, \chi) = 0$. درواقع ، ساده‌تر است که مجموعهٔ متمم را بررسی‌کنیم. قضیهٔ زیر شرطی لازم برای ناصفر بودن $G(n, \chi)$ به‌ازای $(n, k) > 1$ است.

قضیهٔ ۸.۱۲ . فرض‌کنیم χ یک مشخص‌دیریکله به هنگ k بوده و، به‌ازای n ی صادق در $(n, k) > 1$ ، $G(n, \chi) \neq 0$. دراین صورت ، مقسوم‌علیهی‌از k مانند d هست، که $d < k$ ، بطوری‌که

هر وقت $(a, k) = 1$ و $a \equiv 1 \pmod d$ ، $\chi(a) = 1$. (۱۴)

برهان. به‌ازای n داده شده، قرار می‌دهیم $q = (n, k)$ و $d = k/q$. دراین صورت، $d|k$ و، چون $q > 1$ ، داریم $d < k$. a ای صادق در $(a, k) = 1$ و $a \equiv 1 \pmod d$ اختیار می‌کنیم. ثابت می‌کنیم که $\chi(a) = 1$.

چون $(a, k) = 1$ ، در مجموع معرف $G(n, \chi)$ می‌توان اندیس جمعبندی m را با am عوض‌کرد و بدست آورد که

$$G(n, \chi) = \sum_{m \bmod k} \chi(m) e^{2\pi i n m/k} = \sum_{m \bmod k} \chi(am) e^{2\pi i n a m/k}$$

$$= \chi(a) \sum_{m \bmod k} \chi(m) e^{2\pi i n a m/k}.$$

چون $a \equiv 1 \pmod d$ و $d = k/q$ ، به‌ازای عدد صحیحی مانند b می‌توان نوشت $a = 1 + (bk/q)$ ، و خواهیم داشت

$$\frac{anm}{k} = \frac{nm}{k} + \frac{bknm}{qk} = \frac{nm}{k} + \frac{bnm}{q} \equiv \frac{nm}{k} \pmod 1$$

زیرا $q|n$. بنابراین، $e^{2\pi i n a m/k} = e^{2\pi i n m/k}$ و مجموع مربوط به $G(n, \chi)$ خواهد شد

$$G(n, \chi) = \chi(a) \sum_{m \bmod k} \chi(m) e^{2\pi i n m/k} = \chi(a) G(n, \chi).$$

چون $G(n, \chi) \neq 0$ ، این، همانطور که حکم شده، ایجاب می‌کند که $\chi(a) = 1$.

قضیهٔ قبل ما را به این امر هدایت می‌کند که مشخصهایی مانند χ به هنگ k را در نظر بگیریم که برای آنها مقسوم علیهی مانند $d < k$ صادق در (۱۴) وجود داشته باشد. این مشخصها ذیلاً بررسی می‌شوند.

۷.۸ هنگهای القایی و مشخصهای اولیه

تعریف هنگ القایی. فرض کنیم χ یک مشخص دیریکله به هنگ k، و d یک مقسوم علیه مثبت k باشد. عدد d یک هنگ ***القایی*** برای χ است اگر

هر وقت $(a, k) = 1$ و $a \equiv 1 \pmod{d}$، داشته باشیم $\chi(a) = 1$. (۱۵)

به‌عبارت دیگر، d یک هنگ القایی است اگر مشخص χ به هنگ k بر نمایندههای ردهٔ باقیماندهای $\hat{1}$ به هنگ d که نسبت به k اول است مثل یک مشخص به هنگ d عمل کند. توجه کنید که خود k همواره یک هنگ القایی برای χ است.

قضیهٔ ۱۳.۸. *فرض کنیم χ یک مشخص دیریکله به هنگ k باشد. در این صورت، 1 یک هنگ القایی برای χ است اگر و فقط اگر $\chi = \chi_1$.*

برهان. هرگاه $\chi = \chi_1$، آنگاه، به‌ازای هر a نسبت به k اول، $\chi(a) = 1$. اما چون هر a در $a \equiv 1 \pmod{1}$ صدق می‌کند، عدد 1 یک هنگ القایی است.

بعکس، هرگاه 1 یک هنگ القایی باشد، آنگاه، هر وقت $(a, k) = 1$، $\chi(a) = 1$؛ درنتیجه، $\chi = \chi_1$، زیرا χ بر اعدادی که نسبت به k اول نیستند صفر می‌شود.

به‌ازای هر مشخص دیریکله به هنگ k، خود هنگ k یک هنگ القایی است. اگر هنگ القایی دیگری نباشد، مشخص را ***اولیه*** می‌نامیم. یعنی،

تعریف مشخصهای اولیه. گوییم مشخص دیریکلهٔ χ به هنگ k ***اولیه*** به هنگ k است اگر هیچ هنگ القایی $d < k$ وجود نداشته باشد. به‌عبارت دیگر، χ اولیه به هنگ k است اگر و فقط اگر، به‌ازای هر مقسوم علیه d از k، که $0 < d < k$، عدد صحیحی مانند $a \equiv 1 \pmod{d}$، که $(a, k) = 1$، باشد بطوری که $\chi(a) \neq 1$.

اگر $1 < k$ ، مشخص اصلی χ_1 اولیه نیست ، زیرا 1 را به عنوان یک هنگ القایی دارد . حال نشان می‌دهیم که اگر هنگ، *اول* باشد ، هر مشخص غیر اصلی اولیه است .

قضیهٔ ۱۴۰۸ . هر مشخص غیر *اصلی* χ به هنگ عدد *اول* p یک مشخص *اولیه* به هنگ p *است* .

برهان . تنها مقسوم علیه‌های p عبارتند از 1 و p ؛ درنتیجه ، اینها تنها نامزدهای هنگهای القایی‌اند . اما ، اگر $\chi \neq \chi_1$ ، مقسوم علیه 1 یک هنگ القایی نیست ؛ درنتیجه ، χ هنگ القایی کوچکتر از p ندارد . بنابراین ، χ اولیه می‌باشد .

حال می‌توان قضایای ۱۰۰۸ تا ۱۲۰۸ را با مشخصهای اولیه بیان کرد .

قضیهٔ ۱۵۰۸ . فرض‌کنیم χ یک مشخص دیریکلهٔ *اولیه* به هنگ k باشد . دراین صورت ،

(آ) به‌ازای هر n که $(n, k) > 1$ ، $G(n, \chi) = 0$ ؛

(ب) به‌ازای هر n ، $G(n, \chi)$ جدایی پذیر *است* ؛

(پ) $|G(1, \chi)|^2 = k$.

برهان . هرگاه به‌ازای n ی که $(n, k) > 1$ ، $G(n, \chi) \neq 0$ ، آنگاه قضیهٔ ۱۲۰۸ نشان می‌دهد که χ یک هنگ القایی مانند $d < k$ دارد ؛ درنتیجه ، χ نمی‌تواند اولیه باشد . این (آ) را ثابت می‌کند .

قسمت (ب) از (آ) و قضیهٔ ۱۰۰۸ نتیجه می‌شود . قسمت (پ) از قسمت (ب) و قضیهٔ ۱۱۰۸ نتیجه می‌شود .

تذکر . قضیهٔ ۱۵۰۸ (ب) نشان می‌دهد که مجموع گاوس $G(n, \chi)$ در صورت اولیه بودن χ جدایی پذیر است . دریکی از بخشهای آتی عکس آن را ثابت می‌کنیم . یعنی ، هرگاه به‌ازای هر n ، $G(n, \chi)$ جدایی پذیر باشد ، آنگاه χ اولیه است . (ر.ک. قضیهٔ ۱۹۰۸ .)

۸۰۸ خواص دیگر هنگهای القایی

قضیهٔ زیر عمل χ بر اعداد همنهشت با یک هنگ القایی را نشان می‌دهد .

قضیهٔ ۱۶۰۸ . **فرض‌کنیم χ یک مشخص دیریکله به هنگ k بوده و $d > 0$ ، $d|k$.** **در این صورت ، d یک هنگ القایی برای χ است اگر و فقط اگر**

هر وقت $(a, k) = (b, k) = 1$ و $a \equiv b \pmod d$ ، $\chi(a) = \chi(b)$. (۱۶)

برهان . اگر (۱۶) برقرار باشد ، d یک هنگ القایی است ، زیرا می‌توان $b = 1$ را اختیار و به معادلهٔ (۱۵) رجوع کرد . حال عکس آن را ثابت می‌کنیم .

a و b را طوری می‌گیریم که $(a, k) = (b, k) = 1$ و $a \equiv b \pmod d$. نشان می‌دهیم که $\chi(a) = \chi(b)$. فرض‌کنیم a' متقابل a به هنگ k باشد ؛ یعنی ، $aa' \equiv 1 \pmod k$. متقابل وجود دارد ، زیرا $(a, k) = 1$. اما $aa' \equiv 1 \pmod d$ ، زیرا $d|k$. درنتیجه ، $\chi(aa') = 1$ ، زیرا d یک هنگ القایی است . اما $aa' \equiv ba' \equiv 1 \pmod d$ ، زیرا $a \equiv b \pmod d$ ، پس $\chi(aa') = \chi(ba')$ ؛ درنتیجه ،

$$\chi(a)\chi(a') = \chi(b)\chi(a').$$

اما $\chi(a') \neq 0$ ، زیرا $\chi(a)\chi(a') = 1$. با حذف $\chi(a')$ ، معلوم می‌شود که $\chi(a) = \chi(b)$ ، و این برهان را تمام خواهد کرد .

معادلهٔ (۱۶) می‌گوید که χ بر اعداد صحیح نسبت به k اول متناوب به هنگ d است . لذا ، χ خیلی شبیه یک مشخص به هنگ d عمل می‌کند . برای بررسی بیشتر این رابطه ، به چند مثال می‌پردازیم .

مثال ۱ . جدول زیر یکی از مشخصهای χ به هنگ 9 را توصیف می‌کند .

n	1	2	3	4	5	6	7	8	9
$\chi(n)$	1	-1	0	1	-1	0	1	-1	0

می‌بینیم که این جدول متناوب به هنگ 3 است ؛ درنتیجه ، 3 یک هنگ القایی برای χ است . درواقع ، χ شبیه مشخص ψ به هنگ 3 زیر عمل می‌کند :

n	1	2	3
$\psi(n)$	1	-1	0

چون به‌ازای هر n ، $\chi(n) = \psi(n)$ ، χ را یک توسیع ψ می‌نامیم . واضح است که هروقت χ یک توسیع مشخص ψ به هنگ d باشد ، d یک هنگ القایی برای χ خواهد بود .

مثال ۲ . حال مشخص χ به هنگ 6 زیر را امتحان می‌کنیم :

n	1	2	3	4	5	6
$\chi(n)$	1	0	0	0	-1	0

دراین‌حالت ، عدد 3 یک هنگ القایی است زیرا ، به‌ازای هر $n \equiv 1 \pmod 3$ که $(n, 6) = 1$ ، $\chi(n) = 1$. (فقط یک چنین n وجود دارد ، یعنی $n = 1$.) بااینحال ، χ یک توسیع مشخص ψ به هنگ 3 نیست ، زیرا تنها مشخصها به هنگ 3 که مشخص اصلی ψ_1 اند ، مشخصهای جدول زیر

n	1	2	3
$\psi_1(n)$	1	1	0

و مشخص ψ مثال 1 می‌باشند . چون $\chi(2) = 0$ ، این مشخص نمی‌تواند توسیع ψ یا ψ_1 باشد .

این مثالها پرتوی بر قضیهٔ زیر می‌افکنند .

قضیهٔ ۱۷۰۸ . ***فرض‌کنیم χ یک مشخص دیریکله به هنگ k بوده و $d|k, d > 0$. در این صورت ، احکام زیر با هم معادلند :***

(آ) d یک هنگ القایی برای χ است ؛

(ب) یک مشخص به هنگ d مانند ψ هست بطوری که ،

به‌ازای هر n ، $\chi(n) = \psi(n)\chi_1(n)$ ، (۱۷)

که درآن χ_1 مشخص اصلی به هنگ k است .

برهان . فرض‌کنیم (ب) برقرارباشد . n راطوری می‌گیریم که $(n, k) = 1, n \equiv 1 \pmod d$. پس $\chi_1(n) = \psi(n) = 1$ ؛ درنتیجه ، $\chi(n) = 1$ ؛ و لذا ، d یک هنگ القایی است . بنابر این ، (ب) حکم (آ) را ایجاب می‌کند .

حال فرض کنیم (آ) برقرار باشد . یک مشخص به هنگ d مانند ψ نشان می‌دهیم که به‌ازای‌آن (۱۷) برقرار باشد . $\psi(n)$ را به‌صورت زیر تعریف می‌کنیم : اگر $(n, d) > 1$ ، قرارمی‌دهیم $\psi(n) = 0$. دراین حالت نیز داریم $(n, k) > 1$ ؛ درنتیجه ، (۱۷) ، بدلیل صفر بودن طرفین ، برقرار است .

حال فرض کنیم $(n, d) = 1$. پس عدد صحیحی مانند m هست بطوری که $m \equiv n \pmod d, (m, k) = 1$. این مطلب را می‌توان با قضیهٔ دیریکله فورا " ثابت کرد .

تصاعد حسابی $xd + n$ شامل بی‌نهایت عدد اول است. یکی از آنها که k را عاد نکند اختیار کرده و آن را m می‌نامیم. بااینحال، نتیجه خیلی عمیق نیست؛ وجود چنین m ی را می‌توان به‌آسانی، بی استفاده از قضیهٔ دیریکله، ثابت کرد. (برای برهان دیگر، ر.ک. تمرین ۴۰۸ .) پس از اختیار m، که به هنگ d منحصر بفرد است، تعریف می‌کنیم

$$\psi(n) = \chi(m).$$

عدد $\psi(n)$ تعریف شده است، زیرا χ در اعدادی که همنهشت به هنگ d بوده و نسبت به k اولند مقادیر مساوی می‌گیرد.

خواننده می‌تواند به‌آسانی تحقیق کند که χ یک مشخص به هنگ d است. تحقیق می‌کنیم که معادلهٔ (۱۷) به‌ازای هر n برقرار است.

هرگاه $(n, k) = 1$، آنگاه $(n, d) = 1$؛ درنتیجه، به‌ازای $m \equiv n \pmod{d}$ ی، $\psi(n) = \chi(m)$. لذا، طبق قضیهٔ ۱۶۰۸،

$$\chi(n) = \chi(m) = \psi(n) = \psi(n)\chi_1(n)$$

زیرا $\chi_1(n) = 1$.

هرگاه $(n, k) > 1$، آنگاه $\chi(n) = \chi_1(n) = 0$ و طرفین (۱۷) مساوی 0 اند. لذا، (۱۷) به‌ازای هر n برقرار می‌باشد.

۹.۸ هادی یک مشخص

تعریف. فرض کنیم χ یک مشخص دیریکله به هنگ k باشد. کوچکترین هنگ القایی d برای χ **هادی** χ نامیده می‌شود.

قضیهٔ ۱۸۰۸ . *هر مشخص دیریکلهٔ χ به هنگ k را می‌توان به‌صورت حاصل ضرب بیان کرد:*

$$\text{به‌ازای هر } n\text{،}\quad \chi(n) = \psi(n)\chi_1(n) \tag{۱۸}$$

که در آن χ_1 مشخص اصلی به هنگ k بوده و ψ یک مشخص اولیه به هنگ هادی ψ می‌باشد.

برهان. فرض کنیم d هادی χ باشد. از قضیهٔ ۱۷۰۸ می‌دانیم که χ را می‌توان به‌صورت حاصل ضرب (۱۸) بیان کرد، که در آن ψ یک مشخص به هنگ d است. حال ثابت می‌کنیم ψ اولیه به هنگ d است.

فرض کنیم ψ اولیه به هنگ d نباشد و به تناقض می‌رسیم. اگر ψ اولیه به هنگ d نباشد، مقسوم علیهی از d مانند q هست، که $q < d$، و یک هنگ القایی برای ψ است. ثابت می‌کنیم این q، که k را عاد می‌کند، یک هنگ القایی برای χ نیز هست، که با کوچکترین هنگ القایی بودن d برای χ تناقض دارد.

$n \equiv 1 \pmod q|(n, k) = 1$ را اختیار می‌کنیم. دراین صورت،

$$\chi(n) = \psi(n)\chi_1(n) = \psi(n) = 1$$

زیرا q یک هنگ القایی برای ψ است. لذا، q نیز یک هنگ القایی برای χ است واین تناقض می‌باشد.

۱۰.۸ مشخصهای اولیه و مجموعهای گاوس جدایی پذیر

به‌عنوان کاربردی از قضایای پیش، توصیف دیگرزیر از مشخصهای اولیه را عرضه می‌کنیم.

قضیهٔ ۱۹.۸. *فرض کنیم χ یک مشخص به هنگ k باشد. دراین صورت، χ اولیه به هنگ k است اگر و فقط اگر مجموع گاوس*

$$G(n, \chi) = \sum_{m \bmod k} \chi(m) e^{2\pi i m n/k}$$

به‌ازای هر n جدایی پذیر باشد.

برهان. هرگاه χ اولیه‌باشد، $G(n, \chi)$ طبق قضیهٔ ۱۵.۸ (ب) جدایی پذیر است. حال عکس آن را ثابت می‌کنیم.

بخاطرقضایای ۹.۸و۱۰.۸، کافی است ثابت کنیم اگر χ اولیه به هنگ k نباشد، به‌ازای r ی صادق در $(r, k) > 1$ داریم $G(r, \chi) \neq 0$. پس فرض کنیم χ اولیه به هنگ k نباشد. این ایجاب می‌کند که $k > 1$. پس χ دارای هادیی مانند $d < k$ است. فرض کنیم $r = k/d$. پس $(r, k) > 1$، و ثابت می‌کنیم به‌ازای این r، $G(r, \chi) \neq 0$. بنابر قضیهٔ ۱۸.۸، یک مشخص اولیه به هنگ d مانند ψ هست بطوری که به ازای هر n، $\chi(n) = \psi(n)\chi_1(n)$. لذا، می‌توان نوشت

$$G(r, \chi) = \sum_{m \bmod k} \psi(m)\chi_1(m) e^{2\pi i r m/k} = \sum_{\substack{m \bmod k \\ (m, k) = 1}} \psi(m) e^{2\pi i r m/k}$$

$$= \sum_{\substack{m \bmod k \\ (m,k)=1}} \psi(m)e^{2\pi im/d} = \frac{\varphi(k)}{\varphi(d)} \sum_{\substack{m \bmod d \\ (m,d)=1}} \psi(m)e^{2\pi im/d},$$

که در آخرین مرحله از قضیهٔ ۳۳۰۵ (آ) استفاده شده است. بنابراین، داریم

$$G(r, \chi) = \frac{\varphi(k)}{\varphi(d)} G(1, \psi).$$

اما، طبق‌قضیهٔ ۱۵۰۸، $|G(1, \psi)|^2 = d$ (چون ψ اولیه به هنگ d است)؛ و درنتیجه، $G(r, \chi) \neq 0$. این برهان را تمام خواهد کرد.

۱۱۰۸ سریهای فوریهٔ متناهی مشخصهای دیریکله

چون هر مشخص دیریکلهٔ χ به هنگ k متناوب به هنگ k است، بسط فوریهٔ متناهی

$$\chi(m) = \sum_{n=1}^{k} a_k(n)e^{2\pi imn/k} \tag{۱۹}$$

را دارد، و قضیهٔ ۴۰۸ می‌گوید که ضرایبش از فرمول زیر بدست می‌آید:

$$a_k(n) = \frac{1}{k} \sum_{m=1}^{k} \chi(m)e^{-2\pi imn/k}.$$

مجموع سمت راست یک مجموع گاوس به‌صورت $G(-n, \chi)$ است؛ درنتیجه، داریم

$$a_k(n) = \frac{1}{k} G(-n, \chi). \tag{۲۰}$$

وقتی χ اولیه باشد، بسط فوریهٔ (۱۹) را می‌توان به‌صورت زیر بیان کرد:

قضیهٔ ۲۰۰۸ . *بسط فوریهٔ متناهی مشخص دیریکلهٔ اولیهٔ χ به هنگ k به شکل زیر است:*

$$\chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k} \bar{\chi}(n)e^{-2\pi imn/k}, \tag{۲۱}$$

که در آن

$$\tau_k(\chi) = \frac{G(1, \chi)}{\sqrt{k}} = \frac{1}{\sqrt{k}} \sum_{m=1}^{k} \chi(m)e^{2\pi im/k}. \tag{۲۲}$$

اعداد $\tau_k(\chi)$ دارای قدر مطلق 1 می‌باشند.

برهان. چون χ اولیه‌است، داریم $G(-n, \chi) = \bar{\chi}(-n)G(1, \chi)$، و (۲۰) ایجاب می‌کند که $a_k(n) = \bar{\chi}(-n)G(1, \chi)/k$. بنابراین، (۱۹) را می‌توان به‌صورت زیر نوشت:

$$\chi(m) = \frac{G(1, \chi)}{k} \sum_{n=1}^{k} \bar{\chi}(-n)e^{2\pi imn/k} = \frac{G(1, \chi)}{k} \sum_{n=1}^{k} \bar{\chi}(n)e^{-2\pi imn/k},$$

که همان (۲۱) می‌باشد. قضیهٔ ۱۱۰۸ نشان می‌دهد که اعداد $\tau_k(\chi)$ دارای قدر مطلق 1 هستند.

۱۲۰۸ نامساوی پولیا[1] برای مجموعه‌های جزئی مشخصهای اولیه

در برهان قضیهٔ دیریکله در فصل ۷ از رابطهٔ

$$\left| \sum_{m \le x} \chi(m) \right| \le \varphi(k)$$

استفاده شد، که به‌ازای هر مشخص دیریکلهٔ χ به هنگ k و هر عدد حقیقی $x \ge 1$ برقرار است. این را نمی‌توان وقتی $\chi = \chi_1$ ثابت کرد، زیرا $\sum_{m=1}^{k} \chi_1(m) = \varphi(k)$. با اینحال، پولیا نشان داد که وقتی χ یک مشخص اولیه باشد، این نامساوی را می‌توان به‌طور قابل ملاحظه‌ای اصلاح نمود.

قضیهٔ ۲۱۰۸. نامساوی پولیا. *هرگاه χ یک مشخص اولیه به هنگ k باشد، آنگاه به‌ازای هر $x \ge 1$ داریم*

$$\left| \sum_{m \le x} \chi(m) \right| < \sqrt{k} \log k. \tag{۲۳}$$

برهان. $\chi(m)$ را با بسط فوریهٔ متناهی‌اش، به‌صورت آمده در قضیهٔ ۲۰۰۸، بیان می‌کنیم:

$$\chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k} \bar{\chi}(n)e^{-2\pi imn/k},$$

و، با جمعبندی روی تمام $m \le x$ های، بدست می‌آوریم

$$\sum_{m \le x} \chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k-1} \bar{\chi}(n) \sum_{m \le x} e^{-2\pi imn/k}$$

---

1. Pólya

زیرا $\chi(k) = 0$. با قدر مطلق گرفتن و ضرب در $\sqrt{k}$ ، معلوم می‌شود که

$$\sqrt{k}\left|\sum_{m\le x}\chi(m)\right| \le \sum_{n=1}^{k-1}\left|\sum_{m\le x} e^{-2\pi imn/k}\right| = (\text{"مثلا"}) \sum_{n=1}^{k-1}|f(n)|, \qquad (۲۴)$$

که در آن

$$f(n) = \sum_{m\le x} e^{-2\pi imn/k}.$$

اما

$$f(k-n) = \sum_{m\le x} e^{-2\pi im(k-n)/k} = \sum_{m\le x} e^{2\pi imn/k} = \overline{f(n)};$$

درنتیجه، $|f(k-n)| = |f(n)|$. از اینرو، (۲۴) را می‌توان به‌صورت زیر نوشت :

$$\sqrt{k}\left|\sum_{m\le x}\chi(m)\right| \le 2\sum_{n\le k/2}|f(n)|. \qquad (۲۵)$$

اما $f(n)$ یک مجموع هندسی به شکل

$$f(n) = \sum_{m=1}^{r} y^m$$

است، که در آن $r = [x]$ و $y = e^{-2\pi in/k}$. اینجا $y \ne 1$ ، زیرا $1 \le n \le k-1$. با نوشتن $z = e^{-\pi in/k}$ ، داریم $y = z^2$ و $z^2 \ne 1$ ، زیرا $n \le k/2$. لذا، داریم

$$f(n) = y\,\frac{y^r - 1}{y - 1} = z^2\,\frac{z^{2r} - 1}{z^2 - 1} = z^{r+1}\,\frac{z^r - z^{-r}}{z - z^{-1}};$$

درنتیجه،

$$|f(n)| = \left|\frac{z^r - z^{-r}}{z - z^{-1}}\right| = \left|\frac{e^{-\pi irn/k} - e^{\pi irn/k}}{e^{-\pi in/k} - e^{\pi in/k}}\right| = \frac{\left|\sin\dfrac{\pi rn}{k}\right|}{\left|\sin\dfrac{\pi n}{k}\right|} \le \frac{1}{\sin\dfrac{\pi n}{k}}. \qquad (۲۶)$$

حال، با استفاده از نامساوی $\sin t \ge 2t/\pi$ ، که به‌ازای $0 \le t \le \pi/2$ معتبر است، و $t = \pi n/k$ بدست می‌آوریم

$$|f(n)| \le \frac{1}{\dfrac{2}{\pi}\dfrac{\pi n}{k}} = \frac{k}{2n}.$$

از اینرو، (۲۵) خواهد شد

$$\sqrt{k}\left|\sum_{m\le x}\chi(m)\right| \le k\sum_{n\le k/2}\frac{1}{n} < k\log k,$$

و این (۲۳) را ثابت خواهد کرد .

تذکر. در یکی از فصلهای آتی ثابت می‌کنیم نامساوی پولیا رامی‌توان به هر مشخص غیر اصلی تعمیم داد . این نامساوی برای مشخصهای غیر اولیه شکل زیر را خواهد گرفت :

$$\sum_{m\le x}\chi(m) = O(\sqrt{k}\log k).$$

(ر.ک. قضیهٔ ۱۳.۱۵.)

تمرین برای فصل ۸

۱ . فرض کنید $x = e^{2\pi i/n}$ و ثابت کنید

$$\sum_{k=1}^{n-1} kx^k = \frac{n}{x-1}.$$

۲ . فرض کنید $((x)) = x - [x] - \frac{1}{2}$ اگر x صحیح نباشد ، و درغیر این‌صورت قرار دهید $((x)) = 0$. توجه‌کنید که $((x))$ یک تابع متناوب از x با دورهٔ تناوب 1 است . اگر k و n صحیح بوده و $n > 0$ ، ثابت کنید

$$\left(\left(\frac{k}{n}\right)\right) = -\frac{1}{2n}\sum_{m=1}^{n-1}\cot\frac{\pi m}{n}\sin\frac{2\pi km}{n}.$$

۳ . فرض کنید $c_k(m)$ مجموع رامانوجان بوده ، و $M(x) = \sum_{n\le x}\mu(n)$ مجموعهای جزئی‌تابع موبیوس باشد .

(آ) ثابت کنید

$$\sum_{k=1}^{n} c_k(m) = \sum_{d|m} dM\left(\frac{n}{d}\right).$$

بخصوص، وقتی $n = m$ ،

$$\sum_{k=1}^{m} c_k(m) = \sum_{d|m} dM\left(\frac{m}{d}\right).$$

(ب) با استفاده از (آ) ، نتیجه بگیرید که

$$M(m) = m\sum_{d|m}\frac{\mu(m/d)}{d}\sum_{k=1}^{d} c_k(d).$$

(پ) ثابت کنید

$$\sum_{m=1}^{n} c_k(m) = \sum_{d|k} d\mu\left(\frac{k}{d}\right)\left[\frac{n}{d}\right].$$

۴ . فرض کنید n, a, d اعداد صحیحی باشند و $(a, d) = 1$. و نیز $m = a + qd$ ، که درآن q حاصل‌ضرب (احتمالا" تهی) از همهٔ اعدا اولی است که n را عاد می‌کنندولی a را عاد نمی‌کنند . ثابت کنید

$m \equiv a \pmod{d}$ و $(m, n) = 1$.

۵ . ثابت کنید هرگاه $k = 2m$ ، که در آن m فرد است ، آنگاه یک مشخص اولیهٔ حقیقی به هنگ k مانند χ وجود ندارد .

۶ . فرض کنید χ مشخصی به هنگ k باشد . هرگاه k_1 و k_2 هنگهایی القایی برای χ باشند ، ثابت کنید (k_1, k_2) ، یعنی بمعم آنها ، نیز چنین است .

۷ . ثابت کنید هادی χ هر هنگ القایی برای χ را عاد می‌کند .

در تمرینهای ۸ تا ۱۲ ، فرض کنید $k = k_1 k_2 \cdots k_r$ ، که درآن k_i اعداد صحیح مثبت دوبدو نسبت بهم اولند : اگر $i \neq j$ ، $(k_i, k_j) = 1$.

۸ . (آ) ثابت کنید بەازای هر عدد صحیح a ، عدد صحیحی چون a_i هست بطوری که

$a_i \equiv a \pmod{k_i}$ و بەازای هر $j \neq i$ ، $a_i \equiv 1 \pmod{k_j}$.

(ب) فرض کنید χ یک مشخص به هنگ k باشد . χ_i را با معادلهٔ

$$\chi_i(a) = \chi(a_i)$$

تعریف‌کنید ، که‌درآن a_i عددصحیح‌قسمت (آ) است . ثابت کنید χ_i یک‌مشخص به هنگ k_i است .

۹ . ثابت کنید هر مشخص به هنگ k مانند χ را می‌توان بەطور منحصر بفرد به شکل حاصل ضرب $\chi = \chi_1 \chi_2 \cdots \chi_r$ تجزیه کرد ، که در آن χ_i یک مشخص به هنگ k_i است .

۱۰ . فرض کنید $f(\chi)$ هادی χ باشد . هرگاه χ تجزیهٔ تمرین ۹ را داشته باشد ، ثابت کنید $f(\chi) = f(\chi_1) \cdots f(\chi_r)$.

۱۱ . هرگاه χ تجزیهٔ تمرین ۹ را داشته باشد ، ثابت کنید بەازای هر عدد صحیح a ،

$$G(a, \chi) = \prod_{i=1}^{r} \chi_i\left(\frac{k}{k_i}\right) G(a_i, \chi_i),$$

که درآن a_i عدد صحیح تمرین ۸ است .

۱۲ . هرگاه χ تجزیهٔ تمرین ۹ را داشته باشد ، ثابت کنید χ اولیه به هنگ k است‌اگر و فقط‌اگر هر χ_i اولیه به هنگ k_i باشد . [**راهنمایی** . قضیهٔ ۸.۱۹ .]

۱۳ . فرض‌کنید χ یک مشخص اولیه به هنگ k باشد . ثابت کنید اگر $N < M$ ،

$$\left|\sum_{m=N+1}^{M} \frac{\chi(m)}{m}\right| < \frac{2}{N+1}\sqrt{k}\log k.$$

۱۴ . این تمرین اصلاح جزئی نامساوی پولیا را به‌اختصار شرح می‌دهد . به برهان قضیهٔ ۲۱۰۸ رجوع کنید . بعد از نامساوی (۲۶) بنویسید

$$\sum_{n\le k/2} |f(n)| \le \sum_{n\le k/2} \frac{1}{\sin\frac{\pi n}{k}} < \frac{1}{\sin\frac{\pi}{k}} + \int_1^{k/2} \frac{dt}{\sin\frac{\pi t}{k}}.$$

نشان‌دهید که انتگرال از $-(k/\pi)\log(\sin(\pi/2k))$ کمتر است ، و نتیجه بگیرید که

$$\left|\sum_{n\le x} \chi(n)\right| < \sqrt{k} + \frac{2}{\pi}\sqrt{k}\log k.$$

این نامساوی پولیا را به‌قدر سازهٔ $2/\pi$ در جملهٔ اصلی اصلاح می‌کند .

۱۵ . مجموع کلوسترمان[1] $K(m, n; k)$ به‌صورت زیر تعریف می‌شود :

$$K(m, n; k) = \sum_{\substack{h \bmod k \\ (h,k)=1}} e^{2\pi i(mh+nh')/k}$$

که در آن h' متقابل h به هنگ k است . وقتی $k|n$ ، این مجموع به مجموع رامانوجان $c_k(m)$ تحویل می‌شود . خواص زیر از مجموعهای کلوسترمان را نتیجه بگیرید :

(آ) $K(m, n; k) = K(n, m; k)$ ؛

(ب) هر وقت $(m, k) = 1$ ، $K(m, n; k) = K(1, mn; k)$ ؛

(پ) به‌ازای اعداد صحیح n, k_1, k_2 که $(k_1, k_2) = 1$ ، نشان دهید که اعداد صحیحی مانند n_1 و n_2 هستند بطوری که

$$n \equiv n_1 k_2^2 + n_2 k_1^2 \pmod{k_1 k_2},$$

و برای این اعداد صحیح داریم

$$K(m, n; k_1k_2) = K(m, n_1; k_1)K(m, n_2; k_2).$$

این امر بررسی مجموعهای کلوسترمان را به‌حالت خاص $K(m, n; p^2)$ ، که در آن p اول است ، منحصر می‌سازد .

۱۶ . هرگاه n و k اعدادی صحیح بوده و $n > 0$ ، مجموع

---

1. Kloosterman

$$G(k;n)=\sum_{r=1}^{n} e^{2\pi ikr^2/n}$$

یک مجموع گاوس درجهٔ دوم نامیده می‌شود. خواص زیر از مجموعهای گاوس درجهٔ دوم را نتیجه بگیرید:

(آ) هر وقت $(m,n)=1$ ، $G(k;mn)=G(km;n)G(kn;m)$. این امر بررسی مجموعهای گاوس را به‌حالت خاص $G(k;p^\alpha)$ ، که در آن p اول است، منحصر می‌سازد.

(ب) فرض کنید p یک عدد اول فرد باشد، $p\nmid k$ ، و $\alpha\ge 2$. ثابت‌کنید $G(k;p^\alpha)=pG(k;p^{\alpha-2})$ ، و نتیجه بگیرید که

$$G(k;p^\alpha)=\begin{cases}p^{\alpha/2} & \text{اگر } \alpha \text{ زوج باشد،}\\ p^{(\alpha-1)/2}G(k;p) & \text{اگر } \alpha \text{ فرد باشد،}\end{cases}$$

خواص دیگر مجموع گاوس $G(k;p)$ در فصل بعد می‌آیند، که نشان می‌دهیم $G(k;p)$ همان مجموع گاوس $G(k,\chi)$ وابسته به مشخص دیریکلهٔ χ به هنگ p است. (ر.ک. تمرین ۹.۰۹.)

۹
مانده‌های مربعی
و
قانون تقابل مربعی

۱.۹ مانده‌های مربعی

همانطور که در فصل ۵ نشان دادیم ، مسئلهٔ حل یک همنهشت چندجمله‌ای

$$f(x) \equiv 0 \pmod{m}$$

را می‌توان به همنهشتیهای چندجمله‌ای باهنگهای اول و مجموعه‌ای از همنهشتیهای خطی تحویل کرد . این فصل مربوط می‌شود به همنهشتیهای مربعی به شکل

$$x^2 \equiv n \pmod{p}, \tag{۱}$$

که‌درآن p عدد اول فردی است و $n \not\equiv 0 \pmod{p}$. چون هنگ‌اول است ، (۱) حداکثر دوجواب دارد . بعلاوه ، اگر x یک جواب باشد ، $-x$ نیز هست ؛ درنتیجه ، تعدادجوابها 0 یا 2 است .

تعریف . اگر همنهشتی (۱) جواب داشته باشد ، گوییم n یک ***ماندهٔ*** **مربعی به هنگ** p است و می‌نویسیم nRp . اگر (۱) جواب نداشته‌باشد ، گوییم n یک ***ناماندهٔ*** **مربعی به هنگ** p است و می‌نویسیم $n\bar{R}p$.

دو مسئلهٔ اساسی بر نظریهٔ مانده‌های مربعی سایه افکنده است :

۱ . به‌ازای عدد اول p ، تعیین n هایی که مانده‌های مربعی به هنگ p اند و آنهایی که نامانده‌های مربعی به هنگ p می‌باشند ؛

۲ . به‌ازای عدد n ، تعیین اعداد اول p که به‌ازای آنها n یک ماندهٔ مربعی به‌هنگ p است و آنهایی که به‌ازای آنها n یک ناماندهٔ مربعی به هنگ p است .

با چند روش برای حل مسئلهٔ ۱ آغاز می‌کنیم .

مثال . برای یافتن مانده‌های مربعی به هنگ 11 ، اعداد $1, 2, \ldots, 10$ را مربع کرده و به هنگ 11 تحویل می‌کنیم . خواهیم داشت

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9, \quad 4^2 \equiv 5, \quad 5^2 \equiv 3 \pmod{11}.$$

کافی است فقط نیمهٔ اول اعداد را مربع کنیم ، زیرا

$$6^2 \equiv (-5)^2 \equiv 3, \quad 7^2 \equiv (-4)^2 \equiv 5, \ldots, 10^2 \equiv (-1)^2 \equiv 1 \pmod{11}.$$

درنتیجه ، مانده‌های مربعی به هنگ 11 عبارتند از $1, 3, 4, 5, 9$ ، و نامانده‌ها عبارتند از $2, 6, 7, 8, 10$.

این مثال قضیهٔ زیر را توضیح می‌دهد .

***قضیهٔ ۱۰۹ .* فرض کنیم p یک عدد اول فرد باشد . دراین صورت ، هر دستگاه مانده‌ای تحویل یافته به هنگ p شامل دقیقاً $(p-1)/2$ ماندهٔ مربعی و دقیقاً $(p-1)/2$ نامانده‌ٔ مربعی به هنگ p است . مانده‌های مربعی متعلق به رده‌های مانده‌ای شامل اعداد**

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2 \qquad (۲)$$

می‌باشند .

برهان . ابتدا توجه می‌کنیم که اعداد (۲) متمایز به هنگ p اند . درواقع ، هرگاه $x^2 \equiv y^2 \pmod{p}$ با $1 \le x \le (p-1)/2$ و $1 \le y \le (p-1)/2$ ، آنگاه

$$(x-y)(x+y) \equiv 0 \pmod{p}.$$

اما $1 < x + y < p$ ؛ درنتیجه ، $x - y \equiv 0 \pmod{p}$. بنابراین ، $x = y$. چون

$$(p-k)^2 \equiv k^2 \pmod{p},$$

هر ماندهٔ مربعی همنهشت دقیقاً یکی از اعداد (۲) به هنگ p است . این برهان را تمام می‌کند .

جدول مختصر زیر از مانده‌های مربعی R و نامانده‌های $\bar{R}$ به کمک قضیهٔ ۱۰۹ بدست آمده است .

	$p=3$	$p=5$	$p=7$	$p=11$	$p=13$
R:	1	1, 4	1, 2, 4	1, 3, 4, 5, 9	1, 3, 4, 9, 10, 12
$\bar{R}$:	2	2, 3	3, 5, 6	2, 6, 7, 8, 10	2, 5, 6, 7, 8, 11

۲.۹ علامت لژاندر و خواص آن

تعریف. فرض‌کنیم p یک عدد اول فرد باشد. هرگاه $n \not\equiv 0 \pmod p$، علامت لژاندر $(n|p)$ را به‌صورت زیر تعریف می‌کنیم:

$$(n|p) = \begin{cases} +1 & \text{اگر } nRp \\ -1 & \text{اگر } n\bar{R}p \end{cases}$$

هرگاه $n \equiv 0 \pmod p$، تعریف می‌کنیم $(n|p) = 0$.

چند مثال. $(1|p) = 1, (m^2|p) = 1, (7|11) = -1, (22|11) = 0$.

تذکر. بعضی از مولفان به‌جای $(n|p)$ می‌نویسند $\left(\dfrac{n}{p}\right)$.

واضح است که هر وقت $m \equiv n \pmod p$، $(m|p) = (n|p)$؛ درنتیجه، $(n|p)$ یک تابع متناوب از n با دورهٔ تناوب p است.

قضیهٔ فرمای کوچک می‌گوید که اگر $p \nmid n$، $n^{p-1} \equiv 1 \pmod p$. چون

$$n^{p-1} - 1 = (n^{(p-1)/2} - 1)(n^{(p-1)/2} + 1),$$

نتیجه می‌شود که $n^{(p-1)/2} \equiv \pm 1 \pmod p$. قضیهٔ زیر می‌گوید که اگر nRp، $+1$ و، اگر $n\bar{R}p$، -1 خواهیم داشت.

قضیهٔ ۲.۹. محک اویلر. فرض‌کنیم p یک عدد اول فرد باشد. در این صورت، به‌ازای هر n داریم

$$(n|p) \equiv n^{(p-1)/2} \pmod p.$$

برهان. اگر $n \equiv 0 \pmod p$، نتیجه بدیهی است زیرا هردو طرف همنهشت 0 به هنگ p اند. حال فرض‌کنیم $(n|p) = 1$. در این صورت، x ی هست بطوری‌که $x^2 \equiv n \pmod p$؛

و درنتیجه،

$$n^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 = (n|p) \pmod p.$$

این قضیه را درحالتی که $(n|p) = 1$ ثابت می‌کند.

حال فرض‌کنیم $(n|p) = -1$ و چندجمله‌ای

$$f(x) = x^{(p-1)/2} - 1$$

را درنظر می‌گیریم. چون $f(x)$ از درجهٔ $(p-1)/2$ است، همنهشتی

$$f(x) \equiv 0 \pmod p$$

حداکثر $(p-1)/2$ جواب‌دارد. اما $(p-1)/2$ ماندهٔ‌مربعی به هنگ p جوابند؛ درنتیجه، نامانده‌ها جواب نمی‌باشند. بنابراین،

اگر $(n|p) = -1$، $n^{(p-1)/2} \not\equiv 1 \pmod p$.

اما $n^{(p-1)/2} \equiv \pm 1 \pmod p$؛ درنتیجه، $n^{(p-1)/2} \equiv -1 \equiv (n|p) \pmod p$. این برهان را تمام خواهد کرد.

قضیهٔ ۳.۹. *علامت لژاندر $(n|p)$ یک تابع کاملاً ضربی از n است.*

برهان. هرگاه $p|m$ یا $p|n$، آنگاه $p|mn$؛ درنتیجه، $(mn|p) = 0$ و $(m|p) = 0$ یا $(n|p) = 0$. لذا، اگر $p|m$ یا $p|n$، $(mn|p) = (m|p)(n|p)$.

هرگاه $p \nmid m$ و $p \nmid n$، آنگاه $p \nmid mn$ و داریم

$$(mn|p) \equiv (mn)^{(p-1)/2} = m^{(p-1)/2} n^{(p-1)/2} \equiv (m|p)(n|p) \pmod p.$$

اما هریک از $(mn|p)$، $(m|p)$، و $(n|p)$ مساوی 1 یا -1 است؛ درنتیجه، تفاضل

$$(mn|p) - (m|p)(n|p)$$

0، 2، یا -2 می‌باشد. چون این تفاضل بر p بخشپذیر است، باید 0 باشد.

تذکر. چون $(n|p)$ یک تابع کاملاً ضربی از n است که متناوب با دورهٔ تناوب p بوده و وقتی $p|n$ صفر می‌شود، داریم $(n|p) = \chi(n)$، که در آن χ یکی از مشخصهای دیریکله به هنگ p است، علامت لژاندر مشخص مربعی به هنگ p نامیده می‌شود.

۳.۹ محاسبهٔ $(-1|p)$ و $(2|p)$

قضیهٔ ۴.۹ . *به‌ازای هر عدد اول فرد* p ،

$$(-1|p) = (-1)^{(p-1)/2} = \begin{cases} 1 \text{ ، } & p \equiv 1 \pmod 4 \text{ اگر} \\ -1 \text{ ، } & p \equiv 3 \pmod 4 \text{ اگر} \end{cases}$$

برهان. بنابر محک اویلر، داریم $(-1|p) \equiv (-1)^{(p-1)/2} \pmod p$. چون هرطرف این همنهشتی 1 یا -1 است، دو طرف مساوی می‌باشند.

قضیهٔ ۵.۹ . *به‌ازای هر عدد اول فرد* p ،

$$(2|p) = (-1)^{(p^2-1)/8} = \begin{cases} 1 \text{ ، } & p \equiv \pm 1 \pmod 8 \text{ اگر} \\ -1 \text{ ، } & p \equiv \pm 3 \pmod 8 \text{ اگر} \end{cases}$$

برهان. $(p-1)/2$ همنهشتی زیر را درنظر می‌گیریم:

$$\begin{aligned} p-1 &\equiv 1(-1)^1 && \pmod p \\ 2 &\equiv 2(-1)^2 && \pmod p \\ p-3 &\equiv 3(-1)^3 && \pmod p \\ 4 &\equiv 4(-1)^4 && \pmod p \\ &\vdots \\ r &\equiv \frac{p-1}{2}(-1)^{(p-1)/2} && \pmod p, \end{aligned}$$

که در آن r مساوی $p-(p-1)/2$ یا $(p-1)/2$ است. با ضرب اینها در هم و توجه به اینکه هر عدد صحیح سمت چپ زوج است، داریم

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+(p-1)/2} \pmod p.$$

از این نتیجه می‌شود که

$$2^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{(p^2-1)/8} \pmod p.$$

چون $((p-1)/2)! \not\equiv 0 \pmod p$ ، این ایجاب می‌کند که

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} \pmod p.$$

طبق محک اویلر، داریم $2^{(p-1)/2} \equiv (2|p) \pmod p$ ، و چون هر طرف 1 یا -1 است، طرفین مساوی می‌باشند. این برهان را تمام خواهد کرد.

۴.۹ لم گاوس

گرچه محک اویلر روش سرراستی برای محاسبهٔ $(n|p)$ است، ممکن است برای n بزرگ مناسب نباشد زیرا باید n را به توان $(p-1)/2$ رسانید. گاوس محک دیگری یافت که محاسبات ساده‌تری را می‌طلبد.

قضیهٔ ۶.۹ . لم گاوس. *فرض‌کنیم $n \not\equiv 0 \pmod p$ و کمترین مانده‌های مثبت به هنگ p مرکب از $(p-1)/2$ مضرب n زیر را درنظر می‌گیریم:*

$$n, 2n, 3n, \ldots, \frac{p-1}{2}n. \tag{۳}$$

اگر m تعداد این مانده‌ها که از $p/2$ متجاوزند باشد،

$$(n|p) = (-1)^m.$$

برهان. اعداد (۳) ناهمنهشت به هنگ p اند. کمترین مانده‌های مثبت آنها را درنظر گرفته و آنهـا را، برحسب اینکه از $p/2$ کوچکتر یا از $p/2$ بزرگترند، به دو مجموعهٔ ازهم جدای A و B تقسیم می‌کنیم. بنابراین،

$$A = \{a_1, a_2, \ldots, a_k\},$$

که در آن به‌ازای $t \le (p-1)/2$ ای و $0 < a_i < p/2$ ، $a_i \equiv tn \pmod p$ ، و

$$B = \{b_1, b_2, \ldots, b_m\},$$

که در آن به‌ازای $s \le (p-1)/2$ ای و $p/2 < b_i < p$ ، $b_i \equiv sn \pmod p$. توجه کنیدکه چون A و B از هم جدایند، $m + k = (p-1)/2$. تعداد عناصر B ، یعنی m ، دراین قضیه مهم است. مجموعهٔ جدید C از m عنصر را با تفریق هر b_i از p می‌سازیم. لذا،

$C = \{c_1, c_2, \ldots, c_m\}$ ، که در آن $c_i = p - b_i$.

اما $0 < c_i < p/2$ ؛ درنتیجه، عناصر C دربازه‌ای که عناصر A قرار دارند واقع‌اند. حال نشان می‌دهیم A و C از هم جدایند.

فرض‌کنیم به‌ازای جفتی‌از i و j ، $c_i = a_j$. پس $p - b_i = a_j$ یا $a_j + b_i \equiv 0 \pmod p$. لذا، به‌ازای s و t ای که $1 \le t < p/2, 1 \le s < p/2$ ،

$$tn + sn = (t + s)n \equiv 0 \pmod p).$$

اما این غیــر ممکن اســت ، زیــرا $p \nmid n$ و p $0 < s + t < p$. پس A و C از هم جدایند ؛ درنتیجــه ، اجتمــاعشــان $A \cup C$ شامــل $m + k = (p-1)/2$ عــدد صحیــح در بازهٔ $[1, (p-1)/2]$ است . بنابراین ،

$$A \cup C = \{a_1, a_2, \ldots, a_k, c_1, c_2, \ldots, c_m\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}.$$

حال حاصل ضرب تمام عناصر در $A \cup C$ را تشکیل می‌دهیم ؛ خواهیم داشت

$$a_1 a_2 \cdots a_k c_1 c_2 \cdots c_m = \left(\frac{p-1}{2}\right)!.$$

چون $c_i = p - b_i$ ، این نتیجه می‌دهد که

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= a_1 a_2 \cdots a_k (p - b_1)(p - b_2) \cdots (p - b_m)\\ &\equiv (-1)^m a_1 a_2 \cdots a_k b_1 b_2 \cdots b_m \pmod p\\ &\equiv (-1)^m n(2n)(3n) \cdots \left(\frac{p-1}{2} n\right) \pmod p\\ &\equiv (-1)^m n^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod p.\end{aligned}$$

با حذف فاکتوریل بدست می‌آوریم

$$n^{(p-1)/2} \equiv (-1)^m \pmod p.$$

محک اویلر نشــان مــی‌دهد که $(-1)^m \equiv (n|p) \pmod p$ ؛ درنتیجه ، $(-1)^m = (n|p)$ و برهان لم گاوس تمام است .

برای استفاده از لــم گاوس در عمل ، باید مقدار دقیق m را بدانیم ؛ البته ، فقط جفتی آن را ، یعنی اینکه m فرد یا زوج است . قضیهٔ زیر راه نسبتاً" ساده‌ای برای تعیین جفتی m بدست می‌دهد .

قضیهٔ ۹ . ۷ . فرض کنیم m عدد تعریف شده در لم گاوس باشد . در این صورت ،

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] + (n-1)\frac{p^2-1}{8} \pmod 2.$$

بالاخص، اگر n فرد باشد، داریم

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] \pmod 2.$$

برهان. به‌یاد می‌آوریم که m تعداد کمترین مانده‌های مثبت اعداد

$$n, 2n, 3n, \ldots, \frac{p-1}{2} n$$

است که از $p/2$ متجاوزند. یک عدد نوعی، مثلاً tn، را اختیار، آن را بر p تقسیم، و اندازهٔ مانده را بررسی می‌کنیم. داریم

$$\frac{tn}{p} = \left[\frac{tn}{p}\right] + \left\{\frac{tn}{p}\right\}$$ ، که درآن $0 < \left\{\frac{tn}{p}\right\} < 1$ ؛

درنتیجه، مثلاً،

$$tn = p\left[\frac{tn}{p}\right] + p\left\{\frac{tn}{p}\right\} = p\left[\frac{tn}{p}\right] + r_t,$$

که درآن $0 < r_t < p$. عدد $r_t = tn - p[tn/p]$ کمترین ماندهٔ مثبت tn به هنگ p است. با مراجعهٔ مجدد به مجموعه‌های A و B در برهان لم گاوس، داریم

$$\{r_1, r_2, \ldots, r_{(p-1)/2}\} = \{a_1, a_2, \ldots, a_k, b_1, \ldots, b_m\}.$$

همچنین، به‌یاد می‌آوریم که

$$\left\{1, 2, \ldots, \frac{p-1}{2}\right\} = \{a_1, a_2, \ldots, a_k, c_1, \ldots, c_m\},$$

که درآن هر $c_i = p - b_i$. حال، با محاسبهٔ مجموعهای عناصر دراین مجموعه‌ها، دو معادلهٔ زیر بدست می‌آیند:

$$\sum_{t=1}^{(p-1)/2} r_t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j$$

و

$$\sum_{t=1}^{(p-1)/2} t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} c_j = \sum_{i=1}^{k} a_i + mp - \sum_{j=1}^{m} b_j.$$

در معادلهٔ اول r_t را با تعریفش عوض کرده بدست می‌آوریم

$$\sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j = n\sum_{t=1}^{(p-1)/2} t - p\sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right].$$

معادلهٔ دوم عبارت است از

$$mp+\sum_{i=1}^{k}a_i-\sum_{j=1}^{n}b_j=\sum_{t=1}^{(p-1)/2}t.$$

از جمع این با معادلهٔ قبل خواهیم داشت

$$\begin{aligned}mp+2\sum_{i=1}^{k}a_i&=(n+1)\sum_{t=1}^{(p-1)/2}t-p\sum_{t=1}^{(p-1)/2}\left[\frac{tn}{p}\right]\\&=(n+1)\frac{p^2-1}{8}-p\sum_{t=1}^{(p-1)/2}\left[\frac{tn}{p}\right].\end{aligned}$$

حال، با توجه به $p\equiv 1 \pmod 2$ و $n+1\equiv n-1 \pmod 2$، این‌را به هنگ 2 تحویل کرده، بدست می‌آوریم

$$m\equiv(n-1)\frac{p^2-1}{8}+\sum_{t=1}^{(p-1)/2}\left[\frac{tn}{p}\right] \pmod 2,$$

که برهان را تمام می‌کند.

۵.۹ قانون تقابل مربعی

محک اویلر و لم گاوس هردوروشهایی، اگرچه گاهی طولانی، برای حل اولین مسئلهٔ اساسی نظریهٔ مـانده‌های مربعی‌اند. دومین مسئله بسیار مشکلتر است. حل آن به قضیهٔ جالبی به‌نام ***قانون‌تقابل مربعی*** بستگی دارد، که ابتدا به‌وسیلهٔ اویلر به‌شکل پیچیده در فاصله سالهای ۱۷۴۶ ــ ۱۷۴۴ بیان شد، و بعد در ۱۷۸۵ توسط لژاندر مجدداً کشف گردید و وی برهان ناقصی برای آن ارائه داد. گاوس قانون تقابل را مستقلاً در هجده سالگی کشف کرد و یک سال بعد در ۱۷۹۶ اولین برهان کامل آن را ارائه داد.

قانون تقابل مربعی می‌گوید که اگر p و q اعداد اول متمایزی باشند، $(p|q)=(q|p)$ مگر آنکه $p\equiv q\equiv 3 \pmod 4$، که در این حالت $(p|q)=-(q|p)$. قضیه معمولاً به شکل متقارن زیر که توسط لژاندر داده شده بیان می‌شود.

قضیهٔ ۸.۹ (قانون تقابل مربعی). ***هرگاه p و q اعداد اول فرد متمایزی باشند، آنگاه***

$$(p|q)(q|p)=(-1)^{(p-1)(q-1)/4}. \qquad (۴)$$

برهان. طبق لم گاوس و قضیهٔ ۷.۹، داریم

$$(q|p)=(-1)^m,$$

که درآن

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tq}{p}\right] \pmod 2.$$

بهمین نحو ،

$$(p|q) = (-1)^n,$$

که در آن

$$n \equiv \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q}\right] \pmod 2.$$

لذا ، $(p|q)(q|p) = (-1)^{m+n}$ ، و (۴) فوراً از اتحاد زیر نتیجه می‌شود :

$$\sum_{t=1}^{(p-1)/2} \left[\frac{tq}{p}\right] + \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}. \tag{۵}$$

برای اثبات (۵) ، تابع

$$f(x, y) = qx - py$$

را درنظر می‌گیریم . هرگاه x و y اعداد صحیح ناصفری باشند ، $f(x, y)$ یک عدد صحیح ناصفراست . بعلاوه ،وقتی x مقادیر $1, 2, \ldots, (p-1)/2$ و y مقادیر $1, 2, \ldots, (q-1)/2$ را بگیرد ، $f(x, y)$

$$\frac{p-1}{2}\frac{q-1}{2}$$

مقدار می‌گیرد ، که هیچ دوتای آنها مساوی نیستند ، زیرا

$$f(x, y) - f(x', y') = f(x - x', y - y') \neq 0.$$

حال تعداد مقادیر $f(x, y)$ که مثبت‌اند و تعدادی که منفی‌اند را حساب می‌کنیم .

بەازای‌هر x ثابت ، $f(x, y) > 0$ اگر و فقط اگر $y < qx/p$ یا $y \leq [qx/p]$. لذا ، تعداد کل مقادیر مثبت مساوی است با

$$\sum_{x=1}^{(p-1)/2} \left[\frac{qx}{p}\right].$$

بهمین نحو ، تعداد مقادیر منفی برابر است با

$$\sum_{y=1}^{(q-1)/2} \left[\frac{py}{q}\right].$$

چون تعداد مقادیر مثبت و منفی با هم مساوی

$$\frac{p-1}{2}\frac{q-1}{2}$$

است ، این (۵) ، و درنتیجه (۴) ، را ثابت می‌کند .

تذکر. خواننده ممکن است تعبیر هندسی برهان (۵) را ، با استفاده از نقاط مشبکه در صفحه ، آموزنده بداند .

دست کم 150 برهان قانون تقابل مربعی منتشر شده‌اند . خود گاوس حداقل هشت‌تا ازآنها ، و ازجمله صورتی از برهانی که هم‌اینک داده شد ، را بدست آورد . برهان کوتاهی از قانون تقابل مربعی در مقاله‌ای توسط ام . گراشتنهابر[1] [۲۵] توصیف شده است .

۶.۹ کاربردهای قانون تقابل

مثالهای زیر طرز استفاده از قانون تقابل مربعی را در حل دو نوع اساسی از مسائل نظریهٔ مانده‌های مربعی نشان می‌دهند .

مثال ۱ . معین کنید 219 یک ماندهٔ مربعی به هنگ 383 است یا نامانده‌ٔ مربعی .

حل . علامت‌لژاندر $(219|383)$ را ، با استفاده از خاصیت ضربی ، قانون تقابل ، تناوب ، و مقادیر خاص $(-1|p)$ و $(2|p)$ که قبلاً "حساب شدند ، محاسبه می‌کنیم .

چون $219 = 3\cdot 73$ ، خاصیت ضربی ایجاب می‌کند که

$$(219|383) = (3|383)(73|383).$$

با استفاده از قانون تقابل و تناوب ، داریم

$$(3|383) = (383|3)(-1)^{(383-1)(3-1)/4} = -(-1|3) = -(-1)^{(3-1)/2} = 1,$$

و

$$\begin{aligned}(73|383) &= (383|73)(-1)^{(383-1)(73-1)/4} = (18|73) = (2|73)(9|73)\\ &= (-1)^{((73)^2-1)/8} = 1.\end{aligned}$$

لذا ، $(219|383) = 1$ ؛ درنتیجه ، 219 یک ماندهٔ مربعی به هنگ 383 است .

---

1. M. Gerstenhaber

مثال ۲ . p های اول فردی را تعیین کنید که به‌ازای آنها 3 یک ماندهٔ مربعی باشد و آنهایی که به‌ازای آنها این عدد یک نامانده باشد .

حل . مجدداً ، طبق قانون تقابل ، داریم

$$(3|p) = (p|3)(-1)^{(p-1)(3-1)/4} = (-1)^{(p-1)/2}(p|3).$$

برای تعیین $(p|3)$ ، باید مقدار p به هنگ 3 را بدانیم ، و برای تعیین $(-1)^{(p-1)/2}$ ، باید مقدار $(p-1)/2$ به هنگ 2 ، یا مقدار p به هنگ 4 را بدانیم . لذا ، p به هنگ 12 را درنظر می‌گیریم . تنها این چهار حالت باید درنظر گرفته شوند : $p \equiv 1, 5, 7, 11 \pmod{12}$ ، بقیه بدلیل فرد بودن p حذف می‌شوند .

حالت ۱ . $p \equiv 1 \pmod{12}$. دراین حالت $p \equiv 1 \pmod 3$ ؛ در نتیجه ، $(p|3) = (1|3) = 1$. همچنین ، $p \equiv 1 \pmod 4$ ؛ درنتیجه ، $(p-1)/2$ زوج است . بنابراین ، $(3|p) = 1$.

حالت ۲ . $p \equiv 5 \pmod{12}$. دراین حالت $p \equiv 2 \pmod 3$ ؛ در نتیجه ، $(p|3) = (2|3) = (-1)^{(3^2-1)/8} = -1$. مجدداً ، $(p-1)/2$ زوج است ، زیرا $p \equiv 1 \pmod 4$ ؛ درنتیجه ، $(3|p) = -1$.

حالت ۳ . $p \equiv 7 \pmod{12}$. دراین حالت $p \equiv 1 \pmod 3$ ؛ در نتیجه ، $(p|3) = (1|3) = 1$. همچنین ، $(p-1)/2$ فرد است ، زیرا $p \equiv 3 \pmod 4$. بنابراین ، $(3|p) = -1$.

حالت ۴ . $p \equiv 11 \pmod{12}$. دراین حالت $p \equiv 2 \pmod 3$ ؛ درنتیجه ، $(p|3) = (2|3) = -1$. مجدداً ، $(p-1)/2$ فرداست ، زیرا $p \equiv 3 \pmod 4$. بنابراین ، $(3|p) = 1$.

با تلخیص نتایج این چهار حالت ، درمی‌یابیم که

اگر $p \equiv \pm 1 \pmod{12}$ ، $3Rp$ ؛

اگر $p \equiv \pm 5 \pmod{12}$ ، $3\bar{R}p$.

۷.۹ علامت ژاکوبی[1]

در تعیین اینکه یک عدد مرکب یک مانده یا ناماندهٔ مربعی به هنگ p است باید بسته به

1. Jacobi

مشخص مــربعی عاملـها چنــدحالت درنظر گرفته شود . بعضی از محاسبات را می‌توان ، با استفاده از تعمیم علامت لژاندر که توسط ژاکوبی عرضه شده ، ساده کرد.

تعریف . هرگاه P یک عدد صحیح فرد مثبت با تجزیه به اعداد اول

$$P = \prod_{i=1}^{r} p_i^{a_i}$$

باشد ، علامت ژاکوبی $(n|P)$ به‌ازای جمیع اعداد صحیح n با معادلهٔ

$$(n|P) = \prod_{i=1}^{r} (n|p_i)^{a_i} \qquad (۶)$$

تعریف می‌شود ،که‌درآن $(n|p_i)$ علامت لژاندر است . همچنین ، تعریف می‌کنیم $(n|1) = 1$. مــقــادیــر ممکن $(n|P)$ عبــارتند از 1 ، -1 ، یا 0 ، با $(n|P) = 0$ اگر و فقط اگر $(n, P) > 1$.

اگر همنهشتی

$$x^2 \equiv n \pmod{P}$$

جواب داشته بــاشد . بــه‌ازای هــر عــدد اول p_i در (۶) ، $(n|p_i) = 1$ ؛ و درنتیجــه ، $(n|P) = 1$. اما عکس این درست نیست ، چونکه اگر تعداد زوجی عامل -1 در (۶) ظاهر شوند ، $(n|P)$ می‌تواند 1 باشد .

خواننده می‌تواندتحقیق کندکه خواص زیراز علامت ژاکوبی به‌آسانی از خواص‌علامت لژاندر نتیجه می‌شوند .

قضیهٔ ۹.۹ . *اگر P و Q اعداد فرد مثبتی باشند ، داریم*

(آ) $(m|P)(n|P) = (mn|P)$ ؛

(ب) $(n|P)(n|Q) = (n|PQ)$ ؛

(پ) **هروقت** $m \equiv n \pmod{P}$ ، $(m|P) = (n|P)$ ؛

(ت) **هروقت** $(a, P) = 1$ ، $(a^2n|P) = (n|P)$.

فرمولهای خاص برای محاسبهٔ علامات لژاندر $(-1|p)$ و $(2|p)$ برای علامت‌ژاکوبی نیز برقرارند .

قضیهٔ ۱۰.۹ . *اگر P عدد فرد مثبتی باشد ، داریم*

$$(-1|P) = (-1)^{(P-1)/2} \tag{۷}$$

و

$$(2|P) = (-1)^{(P^2-1)/8}. \tag{۸}$$

برهان . می‌نویسیم $P = p_1 p_2 \cdots p_m$ ، که درآن عاملهای اول p_i لزوما" متمایز نیستند . این را می‌توان به صورت زیر نیز نوشت :

$$P = \prod_{i=1}^{m}(1 + p_i - 1) = 1 + \sum_{i=1}^{m}(p_i - 1) + \sum_{i \neq j}(p_i - 1)(p_j - 1) + \cdots.$$

اما هر عامل $p_i - 1$ زوج است ؛ درنتیجه ، هر مجموع بعد از اولی بر 4 بخشپذیر است . از اینرو ،

$$P \equiv 1 + \sum_{i=1}^{m}(p_i - 1) \pmod 4,$$

یا

$$\frac{1}{2}(P-1) \equiv \sum_{i=1}^{m}\frac{1}{2}(p_i - 1) \pmod 2.$$

بنابراین ،

$$(-1|P) = \prod_{i=1}^{m}(-1|p_i) = \prod_{i=1}^{m}(-1)^{(p_i-1)/2} = (-1)^{(P-1)/2},$$

که (۷) را ثابت می‌کند .

برای اثبات (۸) ، می‌نویسیم

$$P^2 = \prod_{i=1}^{m}(1 + p_i^2 - 1) = 1 + \sum_{i=1}^{m}(p_i^2 - 1) + \sum_{i \neq j}(p_i^2 - 1)(p_j^2 - 1) + \cdots.$$

چون p_i فرد است ، داریم $p_i^2 - 1 \equiv 0 \pmod 8$ ؛ درنتیجه ،

$$P^2 \equiv 1 + \sum_{i=1}^{m}(p_i^2 - 1) \pmod{64}\cdot$$

ازاینرو ،

$$\frac{1}{8}(P^2-1) = \sum_{i=1}^{m}\frac{1}{8}(p_i^2 - 1) \pmod 8.$$

این به هنگ 2 نیز برقرار است. بنابراین،

$$(2|P) = \prod_{i=1}^{m}(2|p_i) = \prod_{i=1}^{m}(-1)^{(p_i{}^2-1)/8} = (-1)^{(P^2-1)/8},$$

که (۸) را ثابت خواهد کرد.

قضیهٔ ۱۱.۹ . قانون تقابل برای علامات ژاکوبی. *هرگاه P و Q اعداد فرد مثبتی بوده و $(P, Q) = 1$، آنگاه*

$$(P|Q)(Q|P) = (-1)^{(P-1)(Q-1)/4}.$$

برهان. می‌نویسیم $P = p_1 \cdots p_m,\ Q = q_1 \cdots q_n$، که در آن p_i و q_i اولند. دراین صورت، مثلاً"،

$$(P|Q)(Q|P) = \prod_{i=1}^{m}\prod_{j=1}^{n}(p_i|q_j)(q_j|p_i) = (-1)^r,$$

با اعمال قانون تقابل مربعی بر هر عامل، معلوم می‌شود که

$$r = \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{1}{2}(p_i-1)\frac{1}{2}(q_j-1) = \sum_{i=1}^{m}\frac{1}{2}(p_i-1)\sum_{j=1}^{n}\frac{1}{2}(q_j-1).$$

در برهان قضیهٔ ۱۰.۹ نشان دادیم که

$$\sum_{i=1}^{m}\frac{1}{2}(p_i-1) \equiv \frac{1}{2}(P-1) \pmod 2,$$

و همنهشتی نظیر برای $\sum \frac{1}{2}(q_j-1)$ برقرار است. لذا،

$$r \equiv \frac{P-1}{2}\frac{Q-1}{2} \pmod 2,$$

که برهان را تمام می‌کند.

مثال ۱. معین کنید 888 ماندهٔ مربعی عدد اول 1999 است یا نامانده‌ٔ مربعی.

حل. داریم

$$(888|1999) = (4|1999)(2|1999)(111|1999) = (111|1999).$$

برای محاسبهٔ $(111|1999)$، با استفاده از علامات لژاندار می‌نویسیم

$$(111|1999) = (3|1999)(37|1999)$$

و قانون تقابل مربعی را بر هر عامل سمت راست اعمال می‌کنیم . با علامات ژاکوبی محاسبات ساده‌تر است ، زیرا داریم

$$(111|1999) = -(1999|111) = -(1|111) = -1.$$

لذا ، 888 یک نامانده‌ٔ مربعی 1999 است .

مثال ۲ . معین کنید -104 ماندهٔ مربعی عدد اول 997 است یا نامانده .

حل . چون $104 = 2 \cdot 4 \cdot 13$ ، داریم

$$\begin{aligned}(-104|997) &= (-1|997)(2|997)(13|997) = -(13|997)\\ &= -(997|13) = -(9|13) = -1.\end{aligned}$$

بنابراین ، -104 یک نامانده‌ٔ مربعی از 997 است .

۸.۹ کاربردهایی در معادلات دیوفانتینی

معادلاتی که برای جوابهای صحیح حل می‌شوند ، بخاطر دیوفانتوس اسکندری ، ***معادلات دیوفانتینی*** نام دارند . یک نمونه معادلهٔ

$$y^2 = x^3 + k \qquad (۹)$$

است ، کـه در آن k عدد صحیح مفـروضی است . مسئله این است که بگوییم ، به‌ازای k مفروض ، معادله جوابهای صحیح x, y دارد یا نه و ، اگر دارد ، همهٔ آنها را نشان دهیم .

بحث این معادله در اینجا از یک جهت بخاطر سابقهٔ طولانی آن است ، که به قرن هفده باز می‌گردد ، و از جهتی بخاطر آنکه بعضی حالات را می‌توان به کمک مانده‌های مربعی بررسی کرد . یک قضیهٔ کلی می‌گوید که معادلهٔ دیوفانتینی

$$y^2 = f(x),$$

درصورتی که $f(x)$ یک چندجمله‌ای از درجهٔ ناکمتر از 3 با ضرایب صحیح و صفرهای متمایز باشد ، حداکثر تعدادی متناهی جواب دارد . (ر.ک. قضایای ۴ تا ۱۸ در لووک [۴۴] ، جلد ۲ .) بـا اینحال ، هیـچ روشی برای تعیین جوابها (یا حتی *تعداد* جوابها) جز در حالاتی بسیار خاص در دست نیست . قضیهٔ زیر مجموعه‌ای نامتناهی از مقادیر k را توصیف می‌کند که به‌ازای آنها (۹) جواب *ندارد* .

قضیهٔ ۱۲.۹ . *معادلهٔ دیوفانتینی*

$$y^2 = x^3 + k \qquad (۱۰)$$

درصورتی که k به شکل

$$k = (4n - 1)^3 - 4m^2 \tag{۱۱}$$

باشد ،که در آن اعداد صحیح m و n چنان باشند که هیچ عدد اول $p \equiv -1 \pmod 4$ ، m را عاد نکند ، جواب نخواهد داشت .

برهان . فرض کنیم جواب x, y موجود باشد و ، با درنظر گرفتن معادله به هنگ 4 ، تناقض بدست می‌آوریم . چون $k \equiv -1 \pmod 4$ ، داریم

$$y^2 \equiv x^3 - 1 \pmod 4. \tag{۱۲}$$

اما به‌ازای‌هر y ، $y^2 \equiv 0$ یا $1 \pmod 4$ ؛ درنتیجه ،اگر x زوج باشد یا $x \equiv -1 \pmod 4$ ، (۱۲) نمی‌تواند برقرار باشد . لذا ، باید داشته باشیم $x \equiv 1 \pmod 4$. حال فرض کنیم

$$a = 4n - 1;$$

درنتیجه ، $k = a^3 - 4m^2$ ، و (۱۰) را به شکل زیر می‌نویسیم :

$$y^2 + 4m^2 = x^3 + a^3 = (x + a)(x^2 - ax + a^2). \tag{۱۳}$$

چون $x \equiv 1 \pmod 4$ و $a \equiv -1 \pmod 4$ ، داریم

$$x^2 - ax + a^2 \equiv 1 - a + a^2 \equiv -1 \pmod 4. \tag{۱۴}$$

لذا ، $x^2 - ax + a^2$ فرد است ،و (۱۴) نشان می‌دهدکه همهٔ عاملهای اول آن نمی‌توانند همنهشت 1 به هنگ 4 باشند . بنابراین ،$p \equiv -1 \pmod 4$ ای $x^2 - ax + a^2$ را عاد می‌کند ، و (۱۳) نشان می‌دهد که این $y^2 + 4m^2$ را نیز عاد می‌کند . به عبارت دیگـــر ،

$$\text{به‌ازای } p \equiv -1 \pmod 4\text{ ای}،\quad y^2 \equiv -4m^2 \pmod p. \tag{۱۵}$$

اما ،طبق فرض، $p \nmid m$ ؛ درنتیجه ، $(-4m^2|p) = (-1|p) = -1$ ، که با (۱۵) متناقض است .این ثابت می‌کندکه معادلهٔ دیوفانتینی (۱۰) ، وقتی k به شکل (۱۱) است ،جواب ندارد .

جدول زیر چند مقدار از k که قضیهٔ ۱۲۰۹ بدست می‌دهد را نشان می‌دهد .

n	0	0	0	0	1	1	1	1	2	2	2	2
m	1	2	4	5	1	2	4	5	1	2	4	5
k	−5	−17	−65	−100	23	11	−37	−73	339	327	279	243

تذکر . تمام جوابهای (۱۰) ،وقتی k دربازهٔ $-100 \le k \le 100$ است ، حساب شده‌اند . (ر.ک. کتاب مرجع [۳۲] .) هیچ جوابی برای مقادیر مثبت زیر از $k \le 100$ وجودندارد :

$$k = 6, 7, 11, 13, 14, 20, 21, 23, 29, 32, 34, 39, 42, 45, 46, 47, 51, 53, 58;$$
$$59, 60, 61, 62, 66, 67, 69, 70, 74, 75, 77, 78, 83, 84, 85, 86, 87, 88, 90,$$
$$93, 95, 96.$$

۹.۹ مجموعهای گاوس و قانون تقابل مربعی

در این بخش برهان دیگری از قانون تقابل مربعی عرضه می‌شود که به کمک مجموعهای گاوس

$$G(n, \chi) = \sum_{r \bmod p} \chi(r) e^{2\pi i n r/p} \tag{۱۶}$$

صورت می‌گیرد، که در آن $\chi(r) = (r|p)$ مشخص مربعی به هنگ p است. چون هنگ اول است، χ یک مشخص اولیه است و خاصیت‌جدایی پذیری

$$G(n, \chi) = (n|p) G(1, \chi) \tag{۱۷}$$

را به‌ازای‌هر n داریم. همچنین، قضیهٔ ۱۱.۸ ایجاب می‌کند که $|G(1, \chi)|^2 = p$. قضیهٔ زیر نشان می‌دهد که $G(1, \chi)^2$ مساوی $\pm p$ است.

قضیهٔ ۱۳.۹ . اگر p عدد اول فردی بوده و $\chi(r) = (r|p)$ ، داریم

$$G(1, \chi)^2 = (-1|p) p. \tag{۱۸}$$

برهان. داریم

$$G(1, \chi)^2 = \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} (r|p)(s|p) e^{2\pi i (r+s)/p}.$$

به‌ازای‌هر جفت r, s یک t به‌هنگ p منحصربفرد وجود دارد بطوری‌که $s \equiv tr \pmod p$، و $(r|p)(s|p) = (r|p)(tr|p) = (r^2|p)(t|p) = (t|p)$. از اینرو،

$$G(1, \chi)^2 = \sum_{t=1}^{p-1} \sum_{r=1}^{p-1} (t|p) e^{2\pi i r(1+t)/p} = \sum_{t=1}^{p-1} (t|p) \sum_{r=1}^{p-1} e^{2\pi i r(1+t)/p}.$$

آخرین مجموع روی r یک مجموع هندسی است که از روابط زیر بدست می‌آید:

$$\sum_{r=1}^{p-1} e^{2\pi i r(1+t)/p} = \begin{cases} -1 & \text{اگر } p \nmid (1+t) \\ p-1 & \text{اگر } p \mid (1+t) \end{cases}$$

بنابراین،

$$G(1,\chi)^2 = -\sum_{t=1}^{p-2}(t|p) + (p-1)(p-1|p) = -\sum_{t=1}^{p-1}(t|p) + p(-1|p)$$
$$= (-1|p)p$$

زیرا $\sum_{t=1}^{p-1}(t|p) = 0$. این (۱۸) را ثابت می‌کند .

معادلهٔ (۱۸) نشـان مـی‌دهد کـه $G(1,\chi)^2$ یک عـدد صحیـح است ؛ درنتیجه، $G(1,\chi)^{q-1}$ نیز به‌ازای هر q فرد عددی صحیح است . قضیهٔ زیر نشان می‌دهد که قانون تقابل مربعی به مقدار این عدد صحیح به هنگ q ارتباط دارد .

قضیهٔ ۱۴.۹ . فرض‌کنیـم p و q اعداد اول فرد متمایزی بوده و χ مشخص مربعی به هنگ p باشد . دراین صورت ، قانون تقابل مربعی

$$(q|p) = (-1)^{(p-1)(q-1)/4}(p|q) \tag{۱۹}$$

معادل همنهشتی

$$G(1,\chi)^{q-1} \equiv (q|p) \pmod q \tag{۲۰}$$

است .

برهان . از (۱۸) داریم

$$G(1,\chi)^{q-1} = (-1|p)^{(q-1)/2}p^{(q-1)/2} = (-1)^{(p-1)(q-1)/4}p^{(q-1)/2}. \tag{۲۱}$$

بنابر محک اویلر ، داریم $p^{(q-1)/2} \equiv (p|q) \pmod q$ ؛ درنتیجه ، (۲۱) ایجاب می‌کندکه

$$G(1,\chi)^{q-1} \equiv (-1)^{(p-1)(q-1)/4}(p|q) \pmod q. \tag{۲۲}$$

اگر (۲۰) برقرار باشد ، داریم

$$(q|p) \equiv (-1)^{(p-1)(q-1)/4}(p|q) \pmod q$$

که (۱۹) را ایجـاب می‌کند ، زیرا هر دو طرف مساوی ± 1 اند . بعکس، اگر (۱۹) برقرار باشد ، (۲۲) رابطهٔ (۲۰) را ایجاب خواهد کرد .

قضیهٔ زیر اتحادی بدست می‌دهد که با استفاده از آن (۲۰) را نتیجه خواهیم‌گرفت .

قضیهٔ ۱۵.۹ . اگر p و q اعداد اول فرد متمایزی بوده و χ مشخص مربعی به هنگ p باشد ، داریم

$$G(1,\chi)^{q-1}=(q|p)\sum_{\substack{r_1 \bmod p\\ r_1+\cdots+r_q\equiv q \pmod p}}\cdots\sum_{r_q \bmod p}(r_1\cdots r_q|p). \qquad (۲۳)$$

برهان. مجموع گاوس $G(n,\chi)$ یک تابع متناوب از n با دورهٔ تناوب p است. همین امر در مورد $G(n,\chi)^q$ درست است؛ درنتیجه، بسط فوریهٔ متناهی زیر را داریم:

$$G(n,\chi)^q=\sum_{m \bmod p}a_q(m)e^{2\pi imn/p},$$

که در آن ضرایب از رابطهٔ زیر بدست می‌آیند:

$$a_q(m)=\frac{1}{p}\sum_{n \bmod p}G(n,\chi)^q e^{-2\pi imn/p}. \qquad (۲۴)$$

از تعریف $G(n,\chi)$ داریم

$$G(n,\chi)^q=\sum_{r_1 \bmod p}(r_1|p)e^{2\pi inr_1/p}\cdots\sum_{r_q \bmod p}(r_q|p)e^{2\pi inr_q/p}$$
$$=\sum_{r_1 \bmod p}\cdots\sum_{r_q \bmod p}(r_1\cdots r_q|p)e^{2\pi in(r_1+\cdots+r_q)/p};$$

درنتیجه، (۲۴) خواهد شد

$$a_q(m)=\frac{1}{p}\sum_{r_1 \bmod p}\cdots\sum_{r_q \bmod p}(r_1\cdots r_q|p)\sum_{n \bmod p}e^{2\pi in(r_1+\cdots+r_q-m)/p}.$$

مجموع روی n یک مجموع هندسی است که صفر است مگر آنکه $r_1+\cdots+r_q\equiv m \pmod p$، که در این حالت مجموع مساوی p است. بنابراین،

$$a_q(m)=\sum_{\substack{r_1 \bmod p\\ r_1+\cdots+r_q\equiv m \pmod p}}\cdots\sum_{r_q \bmod p}(r_1\cdots r_q|p). \qquad (۲۵)$$

حال به (۲۴) بازگشته و عبارت دیگری برای $a_q(m)$ بدست می‌آوریم. با استفاده از جدایی پذیری $G(n,\chi)$ و رابطهٔ $(n|p)^q=(n|p)$ به‌ازای q فرد، معلوم می‌شود که

$$a_q(m)=\frac{1}{p}G(1,\chi)^q\sum_{n \bmod p}(n|p)e^{-2\pi imn/p}=\frac{1}{p}G(1,\chi)^qG(-m,\chi)$$
$$=\frac{1}{p}G(1,\chi)^q(m|p)G(-1,\chi)=(m|p)G(1,\chi)^{q-1},$$

زیرا

$$G(1,\chi)G(-1,\chi)=G(1,\chi)\overline{G(1,\chi)}=|G(1,\chi)|^2=p.$$

به عبارت دیگر، $G(1,\chi)^{q-1}=(m|p)a_q(m)$. با فرض $m=q$ و استفاده از (۲۵)، رابطهٔ

(۲۳) بدَست می‌آید .

برهان قانون تقابل. برای آنکه قانــون تقــابل مربعی را از (۲۳) نتیجه بگیریم ، کافی است نشان دهیم که

$$\sum_{r_1 \bmod p} \cdots \sum_{r_q \bmod p} (r_1 \cdots r_q|p) \equiv 1 \pmod q, \tag{۲۶}$$

که در آن اندیسهای جمعبندی $r_1, \ldots, r_q$ مقید به آنند که

$$r_1 + \cdots + r_q \equiv q \pmod p. \tag{۲۷}$$

اگر همــهٔ انــدیسهای $r_1, \ldots, r_q$ همنهشت یکدیگر به هنگ p باشند ، مجموعشان همنهشت qr_j بەازای‌هر $j = 1, 2, \ldots, q$ است ؛ درنتیجه ، (۲۷) برقرار است اگر و فقط اگر

$$qr_j \equiv q \pmod p;$$

یعنی ، اگـر و فقط اگر بەازای هر j ، $r_j \equiv 1 \pmod p$. دراین حالت ، جمعوند نظیر در (۲۶) مساوی‌است با $(1|p) = 1$. بەازای‌همهٔ اندیسهای دیگر صادق در (۲۷) ، باید دست‌کم دواندیس‌ناهمنهشت‌بین $r_1, \ldots, r_q$ موجودباشند . لذا ، هر جایگشت دوری از $r_1, \ldots, r_q$ جواب جدیدی‌از (۲۷) بدست می‌دهد که همان جمعوند ، یعنی $(r_1 \cdots r_q|p)$ ، را خواهد داد . بنابراین ، هرچنین جمعوند q بار ظاهر می‌شود و 0 به هنگ q به مجموع‌می‌افزاید . از اینرو ، تنها جمله در مجموع (۲۶) که به هنگ q ناصفر است $(1|p) = 1$ می‌باشد . این برهان را تمام خواهد کرد .

۹.۱۰ قانون تقابل برای مجموعـهای گاوس مربعی

این بخش برهــان دیگری از قانون تقابل مربعی را توصیف می‌کند که بر مجموعـهای گاوس مربعی

$$G(n; m) = \sum_{r=1}^{m} e^{2\pi i n r^2/m} \tag{۲۸}$$

استوار است . اگر p عدد اول فردی بوده و $p \nmid n$ ، فرمول زیر را داریم :

$$G(n; p) = (n|p)G(1; p), \tag{۲۹}$$

که بررسی مجموعـهای $G(n; p)$ را بەحالت $n = 1$ تحویل می‌کند . معادلهٔ (۲۹) به‌آسانی از (۲۸) یا بــا توجه به $G(n; p) = G(n, \chi)$ ، که درآن $\chi(n) = (n|p)$ ، و اینکه $G(n, \chi)$ جدایی پذیر است نتیجه می‌شود .

با آنکه هر جملهٔ مجموع $G(1;p)$ دارای قدر مطلق 1 است، خود مجموع قدر مطلق 0 ، $\sqrt{p}$ ، یا $\sqrt{2p}$ دارد. در واقع، گاوس فرمول جالب زیر را ثابت کرد: به‌ازای هر $m \geq 1$ ،

$$G(1;m) = \frac{1}{2}\sqrt{m}(1+i)(1+e^{-\pi i m/2}) = \begin{cases} \sqrt{m} & \text{اگر } m \equiv 1 \pmod 4 \text{ ،} \\ 0 & \text{اگر } m \equiv 2 \pmod 4 \text{ ،} \\ i\sqrt{m} & \text{اگر } m \equiv 3 \pmod 4 \text{ ،} \\ (1+i)\sqrt{m} & \text{اگر } m \equiv 0 \pmod 4 \text{ ،} \end{cases} \qquad (۳۰)$$

برهانهای مختلفی از (۳۰) بدست آمده‌اند. فرمول (۳۰) را با بررسی مجموع مربوطهٔ

$$S(a, m) = \sum_{r=0}^{m-1} e^{\pi i a r^2/m},$$

که در آن a و m اعداد صحیح مثبتی‌اند، نتیجه خواهیم گرفت. هرگاه $a = 2$ ، آنگاه $S(2, m) = G(1; m)$.

مجموعهای $S(a, m)$ از یک قانون تقابل تبعیت می‌کنند (ذیلا" در قضیهٔ ۹.۱۶ بیان شده است) که فرمول گاوس (۳۰) را ایجاب می‌کند و نیز به برهان دیگری از قانون تقابل مربعی منجر می‌شود.

قضیهٔ ۹.۱۶ . *اگر حاصل ضرب ma زوج باشد، داریم*

$$S(a, m) = \sqrt{\frac{m}{a}}\left(\frac{1+i}{\sqrt{2}}\right)\overline{S(m, a)}, \qquad (۳۱)$$

که در آن خط مزدوج مختلط را نشان می‌دهد.

تذکر. برای بدست‌آوردن فرمول گاوس (۳۰) ، در (۳۱) $a = 2$ را اختیار کرده وملاحظه می‌کنیم که $\overline{S(m, 2)} = 1 + e^{-\pi i m/2}$.

برهان. این برهان مبتنی بر حساب مانده‌هاست. فرض کنیم تابع g با معادلهٔ زیر تعریف شده باشد:

$$g(z) = \sum_{r=0}^{m-1} e^{\pi i a (z+r)^2/m}. \qquad (۳۲)$$

دراین صورت، g همه‌جا تحلیلی است، و $g(0) = S(a, m)$. چون ma زوج است، درمی‌یابیم که

$$g(z+1) - g(z) = e^{\pi i a z^2/m}(e^{2\pi i a z} - 1) = e^{\pi i a z^2/m}(e^{2\pi i z} - 1)\sum_{n=0}^{a-1} e^{2\pi i n z}.$$

حال f را با معادلهٔ زیر تعریف می‌کنیم :

$$f(z) = \frac{g(z)}{e^{2\pi i z} - 1}.$$

دراین صورت ، f همه‌جا جـز به‌ازای قطب مرتبهٔ اول در هر عدد صحیح تحلیلی است ، و f در معادلهٔ زیر صدق می‌کند :

$$f(z+1) = f(z) + \varphi(z), \tag{۳۳}$$

که در آن

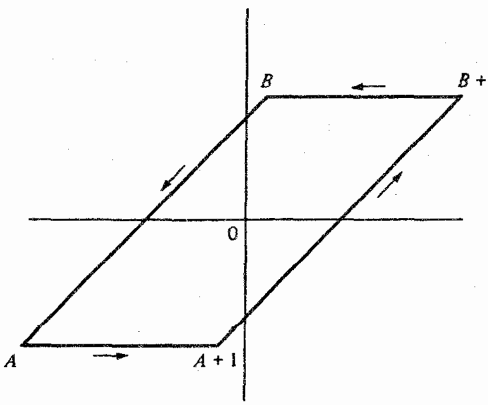
$$\varphi(z) = e^{\pi i a z^2/m}\sum_{n=0}^{a-1} e^{2\pi i n z}. \tag{۳۴}$$

تابع φ همه‌جا تحلیلی است .

در $z = 0$ ، ماندهٔ f مساوی $g(0)/(2\pi i)$ است ؛ و درنتیجه ،

$$S(a, m) = g(0) = 2\pi i \operatorname*{Res}_{z=0} f(z) = \int_\gamma f(z)\, dz, \tag{۳۵}$$

که در آن γ یک مسیر بستهٔ سادهٔ جهت‌پذیر با جهت مثبت است که نمودارش درناحیهٔ درونی خـود فقط شامل قطب $z = 0$ می‌باشد . γ را طوری می‌گیریم که متوازی‌الاضلاعی به راسهای $A, A+1, B+1, B$ را توصیف کند ، که ، همانطور که شکل ۱۰۹ نشان داده ،



شکل ۱۰۹

$A = -\frac{1}{2} - Re^{\pi i/4}$ و $B = -\frac{1}{2} + Re^{\pi i/4}$.

با انتگرالگیری از f در امتداد γ ، داریم

$$\int_{\gamma} f = \int_{A}^{A+1} f + \int_{A+1}^{B+1} f + \int_{B+1}^{B} f + \int_{B}^{A} f.$$

در انتگرال f $|_{A+1}^{B+1}$ تغییر متغیر $w = z + 1$ داده و سپس، با استفاده از (۳۳) ، بدست می‌آوریم

$$\int_{A+1}^{B+1} f(w)\,dw = \int_{A}^{B} f(z+1)\,dz = \int_{A}^{B} f(z)\,dz + \int_{A}^{B} \varphi(z)\,dz.$$

لذا ، (۳۵) خواهد شد

$$S(a, m) = \int_{A}^{B} \varphi(z)\,dz + \int_{A}^{A+1} f(z)\,dz - \int_{B}^{B+1} f(z)\,dz. \qquad (۳۶)$$

حال نشان می‌دهیم که انتگرالها در امتداد پاره خطهای افقی از A تا $A+1$ و از B تا $B+1$ ، وقتی $R \to +\infty$ ، به 0 میل می‌کنند . برای این‌کار ، انتگرالده را روی این پاره خطها تخمین می‌زنیم . می‌نویسیم

$$|f(z)| = \frac{|g(z)|}{|e^{2\pi i z} - 1|}, \qquad (۳۷)$$

و صورت و مخرج را جداگانه تخمین می‌زنیم .

بر پاره خط بین B و $B+1$ ، قرار می‌دهیم

$\gamma(t) = t + Re^{\pi i/4}$ ، که درآن $-\frac{1}{2} \le t \le \frac{1}{2}$.

از (۳۲) معلوم می‌شود که

$$|g[\gamma(t)]| \le \sum_{r=0}^{m-1} \left| \exp\left\{ \frac{\pi i a(t + Re^{\pi i/4} + r)^2}{m} \right\} \right|, \qquad (۳۸)$$

که درآن $z = e^z$ $\exp$. عبارت داخل دو ابرو دارای قسمت صحیح

$$\frac{-\pi a(\sqrt{2}tR + R^2 + \sqrt{2}rR)}{m}$$

است . چون $|e^{x+iy}| = e^x$ و $\exp\{-\pi a\sqrt{2}rR/m\} \le 1$ ، هر جمله در (۳۸) قدر مطلق نامتجاوزاز $\exp\{-\pi aR^2/m\}\exp\{-\sqrt{2}\pi atR/m\}$ دارد .اما $-1/2 \le t \le 1/2$ ؛درنتیجه، تخمین زیر را خواهیم داشت :

$$|g[\gamma(t)]| \le me^{\pi\sqrt{2}aR/(2m)}e^{-\pi aR^2/m}.$$

برای مخرج در (۳۷) ، از نامساوی مثلثی به شکل

$$|e^{2\pi iz} - 1| \geq ||e^{2\pi iz}| - 1|$$

استفاده می‌کنیم . چون

$$|\exp\{2\pi i\gamma(t)\}| = \exp\{-2\pi R\sin(\pi/4)\} = \exp\{-\sqrt{2}\pi R\},$$

معلوم می‌شود که

$$|e^{2\pi i\gamma(t)} - 1| \geq 1 - e^{-\sqrt{2}\pi R}.$$

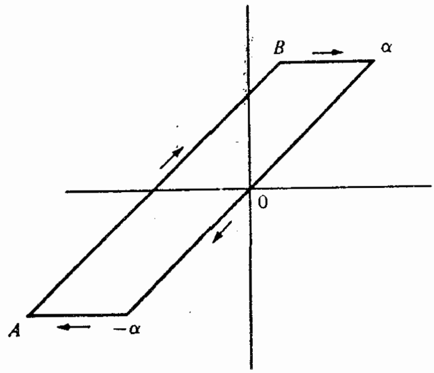
لذا ، بر پاره خط بین B و $B+1$ ، تخمین زیر را خواهیم داشت :

$$|f(z)| \leq \frac{me^{\pi\sqrt{2}aR/(2m)}e^{-\pi aR^2/m}}{1 - e^{-\sqrt{2}\pi R}} = o(1)$$ وقتی $R \to +\infty$.

استدلال مشابهی نشان می‌دهد که بر پاره خط بین A و $A+1$ ، انتگرالده، وقتی $R \to +\infty$ ، به 0 میل می‌کند . چون طول مسیر انتگرالگیری در هر حالت 1 است ، این نشان می‌دهد که انتگرالهای دوم و سوم سمت راست (۳۶) ، وقتی $R \to +\infty$ ، به 0 میل می‌کنند . لذا ، (۳۶) را می‌توان به شکل زیر نوشت :

$$S(a, m) = \int_A^B \varphi(z)\,dz + o(1) \quad (۳۹)$$ وقتی $R \to +\infty$.

برای انتگرال $\int_A^B \varphi$ ، قضیهٔ کشی را بکار می‌بریم ، از φ حول متوازی الاضلاع به راسهای $A, B, \alpha, -\alpha$ ، که $\alpha = B + \frac{1}{2} = Re^{\pi i/4}$ ، انتگرال می‌گیریم . (ر.ک. شکل ۹.۲) .



شکل ۹.۲

چون φ همه‌جا تحلیلی است ، انتگرالش حول این متوازی الاضلاع 0 است؛ درنتیجه ،

$$\int_A^B \varphi + \int_B^\alpha \varphi + \int_\alpha^{-\alpha} \varphi + \int_{-\alpha}^A \varphi = 0. \quad (۴۰)$$

بخاطر عامل نمایی $e^{\pi iaz^2/m}$ در (۳۴) ، استدلالی مشابه فوق نشان می‌دهد که انتگرال

φ درامتداد هرپاره خط افقی، وقتی $R \to +\infty$، به 0 میل می‌کند. لذا، (۴۰) نتیجه می‌دهد که

$$\text{وقتی } R \to +\infty ,\quad \int_A^B \varphi = \int_{-\alpha}^{\alpha} \varphi + o(1) ,$$

و (۳۹) خواهد شد:

$$\text{وقتی } R \to +\infty ,\quad S(a, m) = \int_{-\alpha}^{\alpha} \varphi(z)\, dz + o(1) , \tag{۴۱}$$

که درآن $\alpha = Re^{\pi i/4}$. با استفاده از (۳۴)، معلوم می‌شود که

$$\int_{-\alpha}^{\alpha} \varphi(z)\, dz = \sum_{n=0}^{a-1} \int_{-\alpha}^{\alpha} e^{\pi i a z^2/m} e^{2\pi i n z}\, dz = \sum_{n=0}^{a-1} e^{-\pi i m n^2/a} I(a, m, n, R),$$

که درآن

$$I(a, m, n, R) = \int_{-\alpha}^{\alpha} \exp\left\{\frac{\pi i a}{m}\left(z + \frac{nm}{a}\right)^2\right\} dz.$$

با اعمال مجدد قضیهٔ کشی بر متوازی‌الاضلاع به راسهای $-\alpha$، α، $\alpha - (nm/a)$، و $-\alpha - (nm/a)$، مثل قبل می‌بینیم که انتگرالها در امتداد پاره خطهای افقی، وقتی $R \to +\infty$، به 0 میل می‌کنند؛ درنتیجه،

$$\text{وقتی } R \to +\infty ,\quad I(a, m, n, R) = \int_{-\alpha - nm/a}^{\alpha - mn/a} \exp\left\{\frac{\pi i a}{m}\left(z + \frac{nm}{a}\right)^2\right\} dz + o(1) .$$

تغییر متغیر $w = \sqrt{a/m}(z + (nm/a))$ رابطهٔ فوق را به شکل زیر درمی‌آورد:

$$\text{وقتی } R \to +\infty ,\quad I(a, m, n, R) = \sqrt{\frac{m}{a}} \int_{-\alpha\sqrt{a/m}}^{\alpha\sqrt{a/m}} e^{\pi i w^2}\, dw + o(1) .$$

با فرض $R \to +\infty$ در (۴۱)، درمی‌یابیم که

$$S(a, m) = \sum_{n=0}^{a-1} e^{-\pi i m n^2/a} \sqrt{\frac{m}{a}} \lim_{R \to +\infty} \int_{-R\sqrt{a/m}e^{\pi i/4}}^{R\sqrt{a/m}e^{\pi i/4}} e^{\pi i w^2}\, dw. \tag{۴۲}$$

و با نوشتن $T = \sqrt{a/m}R$، می‌بینیم که آخرین حد مساوی است با، مثلاً،

$$\lim_{T \to +\infty} \int_{-Te^{\pi i/4}}^{Te^{\pi i/4}} e^{\pi i w^2}\, dw = I ,$$

که درآن I عددی مستقل از a و m است. لذا، (۴۲) نتیجه می‌دهد که

$$S(a, m) = \sqrt{\frac{m}{a}}\, I\overline{S(m, a)}. \tag{۴۳}$$

برای محاسبهٔ I ، در (۴۳) $a = 1$ و $m = 2$ را اختیار می‌کنیم . دراین صورت ، $S(1, 2) = 1 + i$ و $S(2, 1) = 1$ ؛ درنتیجه ، (۴۳) ایجاب می‌کند که $I = (1 + i)/\sqrt{2}$ ، و (۴۳) به (۳۱) تحویل خواهد شد .

از قضیهٔ ۱۶.۹ یک قانون تقابل برای مجموعهای گاوس مربعی نتیجه می‌شود .

قضیهٔ ۱۷.۹ . *هرگاه $h > 0, k > 0$ و h فرد باشد ، آنگاه*

$$G(h; k) = \sqrt{\frac{k}{h}}\frac{1 + i}{2}(1 + e^{-\pi ihk/2})\overline{G(k; h)}. \tag{۴۴}$$

برهان . با اختیار $a = 2h, m = k$ در قضیهٔ ۱۶.۹ ، بدست می‌آوریم

$$G(h; k) = S(2h, k) = \sqrt{\frac{k}{2h}}\frac{1 + i}{\sqrt{2}}\overline{S(k, 2h)} = \sqrt{\frac{k}{h}}\frac{1 + i}{2}\sum_{r=0}^{2h-1} e^{-\pi ikr^2/(2h)}. \tag{۴۵}$$

مجموع روی r را ، بسته به زوج و فرد بودن r ، به دو بخش تجزیه می‌کنیم . به‌ازای r زوج ، می‌نویسیم $r = 2s$ که درآن $s = 0, 1, 2, \ldots, h - 1$. به‌ازای r فرد ، توجه‌می‌کنیم که $(r + 2h)^2 \equiv r^2 \pmod{4h}$ ؛ درنتیجه ، مجموع‌را می‌توان‌روی اعداد فرد در یک‌دستگاه مانده‌ای‌تام به‌هنگ $2h$ گسترش داد . ما روی اعداد فرد در بازهٔ $h \le r < 3h$ جمعبندی کرده ، می‌نویسیم $r = 2s + h$ ، که درآن $s = 0, 1, 2, \ldots, h - 1$. (اعداد $2s + h$ فرد و متمایز به هنگ $2h$ اند .) این نتیجه می‌دهد که

$$\begin{aligned}\sum_{r=0}^{2h-1} e^{-\pi ikr^2/(2h)} &= \sum_{s=0}^{h-1} e^{-\pi ik(2s)^2/(2h)} + \sum_{s=0}^{h-1} e^{-\pi ik(2s+h)^2/(2h)}\\ &= \sum_{s=0}^{h-1} e^{-2\pi iks^2/h}(1 + e^{-\pi ihk/2})\\ &= (1 + e^{-\pi ihk/2})\overline{G(k; h)}.\end{aligned}$$

با استفاده از این در (۴۵) ، رابطهٔ (۴۴) بدست می‌آید .

۱۱.۹ برهان دیگری از قانون تقابل مربعی

فرمول‌گاوس (۳۰) به‌برهان سریعی از قانون تقابل مربعی ختم می‌شود . ابتدا توجه می‌کنیم

که (۳۰) رابطهٔ

$$G(1;k) = i^{(k-1)^2/4}\sqrt{k}$$

را، درصورت فرد بودن k ، ایجاب می‌کند. همچنین، خاصیت ضربی زیر را داریم (ر.ک. تمرین ۱۶۰۸ (آ)):

اگر $(m, n) = 1$ ، $G(m;n)G(n;m) = G(1;mn)$.

لذا، اگر p و q اعداد اول فرد متمایزی باشند، خواهیم داشت

$$G(p;q) = (p|q)G(1;q) = (p|q)i^{(q-1)^2/4}\sqrt{q}$$
$$G(q;p) = (q|p)G(1;p) = (q|p)i^{(p-1)^2/4}\sqrt{p}$$

و

$$G(p;q)G(q;p) = G(1;pq) = i^{(pq-1)^2/4}\sqrt{pq}.$$

از مقایسهٔ آخرین معادله با دو معادلهٔ پیش از آن، معلوم می‌شود که

$$(p|q)(q|p)i^{\{(q-1)^2+(p-1)^2\}/4} = i^{(pq-1)^2/4},$$

و قانون تقابل مربعی با توجه به

$$i^{\{(pq-1)^2-(q-1)^2-(p-1)^2\}/4} = (-1)^{(p-1)(q-1)/4}$$

نتیجه خواهد شد.

تمرین برای فصل ۹

۱. اعداد اول فرد p را تعیین کنید که به‌ازای آنها $(-3|p) = 1$ و آنهایی که به‌ازای آنها $(-3|p) = -1$.

۲. ثابت کنید 5 یک ماندهٔ مربعی از عدد اول فرد p است اگر $p \equiv \pm 1 \pmod{10}$ ، و 5 یک نامانده است اگر $p \equiv \pm 3 \pmod{10}$.

۳. فرض‌کنید p یک عدد اول فرد باشد. همچنین، مجموعهٔ $\{1, 2, \ldots, p-1\}$ را بتوان به‌صورت اجتماعی از دو زیرمجموعهٔ ناتهی S و T ، که $S \neq T$ ، بیان کرد بطوری که حاصل ضرب (به هنگ p) هر دو عنصر در یکی از زیرمجموعه‌ها در S قرار داشته‌باشد، ولی حاصل ضرب (به هنگ p) هر عنصر در S و هر عنصر در T در T واقع باشد. ثابت کنید S از مانده‌های مربعی و T از نامانده‌ها به‌هنگ p تشکیل شده است.

۴ . فرض‌کنید $f(x)$ یک چند جمله‌ای باشد که، وقتی x صحیح است، مقدار صحیح می‌گیرد.

(آ) هرگاه a و b صحیح باشند، ثابت کنید که

اگر $(a, p) = 1$ ، $\sum_{x \bmod p} (f(ax + b)|p) = \sum_{x \bmod p} (f(x)|p)$

و

به‌ازای هر a ، $\sum_{x \bmod p} (af(x)|p) = (a|p) \sum_{x \bmod p} (f(x)|p)$.

(ب) ثابت کنید که

اگر $(a, p) = 1$ ، $\sum_{x \bmod p} (ax + b|p) = 0$.

(پ) فرض کنید $f(x) = x(ax + b)$ ، که در آن $(a, p) = (b, p) = 1$. ثابت کنید

$$\sum_{x=1}^{p-1} (f(x)|p) = \sum_{x=1}^{p-1} (a + bx|p) = -(a|p).$$

[**راهنمایی.** وقتی x در یک دستگاه مانده‌ای تحویل یافته به هنگ p تغییر کند، x' ، یعنی متقابل x به هنگ p ، نیز چنین خواهد کرد.]

۵ . فرض کنید α و β اعدادی صحیح باشند که مقادیر ممکن آنها ± 1 اند. همچنین، $N(\alpha, \beta)$ تعداد اعداد صحیح x بین $1, 2, \ldots, p-2$ باشد بطوری که

$(x|p) = \alpha$ و $(x + 1|p) = \beta$ ،

که در آن p یک عدد اول فرد است. ثابت کنید

$$4N(\alpha, \beta) = \sum_{x=1}^{p-2} \{1 + \alpha(x|p)\}\{1 + \beta(x + 1|p)\},$$

و، با استفاده از تمرین ۴، نتیجه بگیرید که

$$4N(\alpha, \beta) = p - 2 - \beta - \alpha\beta - \alpha(-1|p).$$

در حالت خاص، این نتیجه می‌دهد که

$$N(1, 1) = \frac{p - 4 - (-1|p)}{4},$$

$$N(-1, -1) = N(-1, 1) = \frac{p - 2 + (-1|p)}{4},$$

$$N(1, -1) = 1 + N(1, 1).$$

۶ . با استفاده از تمرین ۵، نشان دهید که به‌ازای هر عدد اول p ، اعداد صحیحی

مانند x و y وجود دارند بطوری که $x^2 + y^2 + 1 \equiv 0 \pmod p$.

۷ . فرض کنید p عدد اول فردی باشد . هریک از احکام زیر را ثابت کنید :

(آ) اگر $p \equiv 1 \pmod 4$ ، $\sum_{r=1}^{p-1} r(r|p) = 0$ ؛

(ب) اگر $p \equiv 1 \pmod 4$ ، $\sum_{\substack{r=1 \\ (r|p)=1}}^{p-1} r = \frac{p(p-1)}{4}$ ؛

(پ) اگر $p \equiv 3 \pmod 4$ ، $\sum_{r=1}^{p-1} r^2(r|p) = p\sum_{r=1}^{p-1} r(r|p)$ ؛

(ت) اگر $p \equiv 1 \pmod 4$ ، $\sum_{r=1}^{p-1} r^3(r|p) = \frac{3}{2}p\sum_{r=1}^{p-1} r^2(r|p)$ ؛

(ث) اگر $p \equiv 3 \pmod 4$ ، $\sum_{r=1}^{p-1} r^4(r|p) = 2p\sum_{r=1}^{p-1} r^3(r|p) - p^2\sum_{r=1}^{p-1} r^2(r|p)$.

[**راهنمایی .** $p - r$ اعداد $1, 2, \ldots, p - 1$ را با r می‌گیرد .]

۸ . فرض‌کنید p یک عدد اول‌فرد بوده ، $p \equiv 3 \pmod 4$ ، و قرار دهید $q = (p-1)/2$.

(آ) ثابت کنید که

$$\{1 - 2(2|p)\}\sum_{r=1}^{q} r(r|p) = p\,\frac{1-(2|p)}{2}\sum_{r=1}^{q}(r|p).$$

[**راهنمایی .** وقتی r اعداد $1, 2, \ldots, q$ را بگیرد ، r و $p - r$ با هم اعداد $1, 2, \ldots, p - 1$ را می‌گیرند ، همچنین $2r$ و $p - 2r$ چنین می‌کنند .]

(ب) ثابت کنید که

$$\{(2|p) - 2\}\sum_{r=1}^{p-1} r(r|p) = p\sum_{r=1}^{q}(r|p).$$

۹ . اگر p عدد اول فردی باشد ، قرار دهید $\chi(n) = (n|p)$. ثابت کنید هرگاه $(n, p) = 1$ ، مجموع گاوس $G(n, \chi)$ وابسته به χ همان مجموع گاوس مربعی $G(n; p)$ است که در تمرین ۱۶.۸ معرفی شد . به عبارت دیگر ، اگر $p \nmid n$ ، داریم

$$G(n, \chi) = \sum_{m \bmod p} \chi(m)e^{2\pi imn/p} = \sum_{r=1}^{p} e^{2\pi inr^2/p} = G(n; p).$$

باید توجه کرد که اگر $p|n$ ، $G(n, \chi) \neq G(n; p)$ ، زیرا $G(p, \chi) = 0$ ولی $G(p; p) = p$.

۱۰ . مجموع گاوس مربعی $G(2; p)$ را با استعمال یکی از قوانین تقابل حساب کنید . نتیجه را با فرمول $G(2; p) = (2|p)G(1; p)$ مقایسه کرده و نتیجه بگیرید که اگر p عدد اول فردی باشد ، $(2|p) = (-1)^{(p^2-1)/8}$.

ریشه‌های اولیه ۱۰

۱۰.۱ نمای یک عدد به هنگ m، ریشه‌های اولیه

فرض کنیم a و $m \geq 1$ اعداد صحیح نسبت بهم اول باشند، و همهٔ توانهای مثبت a را درنظر می‌گیریم :

$$a, a^2, a^3, \ldots$$

از قضیهٔ اویلر ــ فرما می‌دانیم که $a^{\varphi(m)} \equiv 1 \pmod m$. با اینحال، ممکن است توان پیشتری مانند a^f باشد بطوری که $a^f \equiv 1 \pmod m$. کوچکترین f مثبت با این خاصیت مورد توجه ماست .

تعریف . کوچکترین عدد صحیح مثبت f که

$$a^f \equiv 1 \pmod m$$

نمای a به هنگ m نامیده و با

$$f = \exp_m(a)$$

نموده می‌شود . اگر $\exp_m(a) = \varphi(m)$ ، a یک ریشهٔ اولیه به هنگ m نام دارد .

قضیهٔ اویلر ــ فرما می‌گوید که $\exp_m(a) \leq \varphi(m)$. قضیهٔ زیر نشان می‌دهد که $\exp_m(a)$ ، $\varphi(m)$ را عاد می‌کند .

قضیهٔ ۱۰.۱ . *به‌ازای* $m \geq 1$ ، $(a, m) = 1$ ، و $f = \exp_m(a)$. *درا‌ین صورت ،*

(آ) $a^k \equiv a^h \pmod m$ *اگر و فقط اگر* $k \equiv h \pmod f$ ؛

(ب) $a^k \equiv 1 \pmod m$ *اگر و فقط اگر* $k \equiv 0 \pmod f$. *درحالت خاص،* $f \mid \varphi(m)$ ؛

(پ) *اعداد* $1, a, a^2, \ldots, a^{f-1}$ *ناهمنهشت به هنگ* m *اند* .

برهان. قسمتهای (ب) و (پ) فوراً از (آ) نتیجه می‌شوند؛ درنتیجه، فقط کافی است (آ) را ثابت کنیم. هرگاه $a^k \equiv a^h \pmod{m}$، آنگاه $a^{k-h} \equiv 1 \pmod{m}$. می‌نویسیم $k - h = qf + r$، درآن $0 \le r < f$.

دراین‌صورت، $1 \equiv a^{k-h} = a^{qf+r} \equiv a^r \pmod{m}$؛ درنتیجه، $r = 0$ و $k \equiv h \pmod{f}$.

بعکس، هرگاه $k \equiv h \pmod{f}$، آنگاه $k - h = qf$؛ درنتیجه، $a^{k-h} \equiv 1 \pmod{m}$؛ ولذا، $a^k \equiv a^h \pmod{m}$.

۲.۱۰ ریشه‌های اولیه و دستگاههای مانده‌ای تحویل یافته

قضیهٔ ۲.۱۰. *فرض کنیم $(a, m) = 1$. دراین صورت، a یک ریشهٔ اولیه به هنگ m است اگر و فقط اگر اعداد*

$$a, a^2, \ldots, a^{\varphi(m)} \tag{1}$$

یک دستگاه مانده‌ای تحویل یافته به هنگ m تشکیل دهند.

برهان. اگر a یک ریشهٔ اولیه باشد، طبق قضیهٔ ۱.۱۰ (پ)، اعداد (۱) ناهمنهشت به هنگ m اند. چون از این اعداد $\varphi(m)$ تا وجود دارند، اینها یک دستگاه مانده‌ای تحویل یافته به هنگ m تشکیل می‌دهند.

بعکس، اگر اعداد (۱) یک دستگاه مانده‌ای تحویل یافته تشکیل دهند، $a^{\varphi(m)} \equiv 1 \pmod{m}$ ولی هیچ توان کوچکتری همنهشت 1 نیست؛ درنتیجه، a یک ریشهٔ اولیه می‌باشد.

تذکر. در فصل ۶ دیدیم که رده‌های مانده‌ای تحویل یافته به هنگ m گروه تشکیل می‌دهند. اگر m ریشهٔ اولیه‌ای چون a داشته باشد، قضیهٔ ۲.۱۰ نشان می‌دهد که این گروه یک گروه دوری است که به وسیلهٔ ردهٔ مانده‌ای $\hat{a}$ تولید می‌شود.

اهمیت ریشه‌های اولیه را قضیهٔ ۲.۱۰ توضیح می‌دهد. اگر m یک ریشهٔ اولیه باشد، هر دستگاه مانده‌ای تحویل یافته به هنگ m را می‌توان به صورت یک تصاعد هندسی بیان کرد. این ابزاری قوی بدست می‌دهد که می‌توان آن را در مسائل مربوط به دستگاههای مانده‌ای تحویل یافته بکار برد. متاسفانه، همهٔ هنگها ریشه‌های اولیه ندارند. در چند بخش بعد ثابت می‌کنیم ریشه‌های اولیه فقط برای هنگهای زیر وجود دارند:

$$m = 1, 2, 4, p^\alpha, 2p^\alpha,$$

که درآنها p یک عدد اول فرد بوده و $\alpha \ge 1$،

سه حالت اول به آسانی سامان می‌یابند. حالت $m = 1$ بدیهی است. به‌ازای $m = 2$، عدد 1 یک ریشهٔ اولیه است. به‌ازای $m = 4$، داریم $\varphi(4) = 2$ و $3^2 \equiv 1 \pmod 4$؛ درنتیجه، 3 یک ریشهٔ اولیه است. حال نشان می‌دهیم که اگر $\alpha \geq 3$، ریشهٔ اولیه‌ای به هنگ 2^α وجود ندارد.

۳.۱۰ عدم وجود ریشه‌های اولیه به هنگ 2^α به ازای $\alpha \geq 3$

قضیهٔ ۳.۱۰. *فرض کنیم x یک عدد صحیح فرد باشد. به‌ازای $\alpha \geq 3$، داریم*

$$x^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}; \qquad (۲)$$

درنتیجه، ریشه‌های اولیه به هنگ 2^α وجود ندارند.

برهان. اگر $\alpha = 3$، همنهشتی (۲) می‌گوید که به‌ازای x فرد، $x^2 \equiv 1 \pmod 8$. این با امتحان $x = 1, 3, 5, 7$، یا با توجه به اینکه

$$(2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$$

و زوج بودن $k(k + 1)$، به‌آسانی تحقیق می‌شود.

حال قضیه را به استقرا روی α ثابت می‌کنیم. فرض کنیم (۲) به‌ازای α برقرار باشد، و ثابت می‌کنیم به‌ازای $\alpha + 1$ نیز چنین است. فرض استقرا این است که

$$x^{\varphi(2^\alpha)/2} = 1 + 2^\alpha t,$$

که در آن t یک عدد صحیح است. با مربع کردن طرفین، بدست می‌آوریم

$$x^{\varphi(2^\alpha)} = 1 + 2^{\alpha+1}t + 2^{2\alpha}t^2 \equiv 1 \pmod{2^{\alpha-1}}$$

زیرا $2\alpha \geq \alpha + 1$. این برهان را تمام می‌کند، زیرا $\varphi(2^{\alpha+1})/2 = 2^{\alpha-1} = \varphi(2^\alpha)$.

۴.۱۰ وجود ریشه‌های اولیه به هنگ p به‌ازای p های اول فرد

ابتدا لم زیر را ثابت می‌کنیم.

لم ۱. *به فرض $(a, m) = 1$، قرار می‌دهیم $f = \exp_m(a)$. دراین صورت،*

$$\exp_m(a^k) = \frac{\exp_m(a)}{(k, f)}.$$

درحالت خاص، $\exp_m(a^k) = \exp_m(a)$ اگر و فقط اگر $(k, f) = 1$.

برهان. نمای a^k کوچکترین عدد مثبت x است بطوری که

$$a^{xk} \equiv 1 \pmod{m}.$$

این‌کوچکترین $x > 0$ که $kx \equiv 0 \pmod{f}$ نیزهست. اما همنهشتی اخیر معادل‌همنهشتی

$$x \equiv 0 \left(\bmod \frac{f}{d}\right)$$

است، که‌در‌آن $d = (k, f)$. کوچکترین‌جواب‌مثبت این همنهشتی f/d است؛ درنتیجه، همانطور که حکم شده، $\exp_m(a^k) = f/d$.

لم ۱ برای اثبات‌وجود ریشه‌های‌اولیه برای هنگهای اول بکار خواهد رفت. درواقع، تعداد دقیق ریشه‌های اولیه به هنگ p را معین خواهیم کرد.

قضیهٔ ۴۰۱۰ . فرض‌کنیم p یک‌عدد‌اول فرد بوده، و d مقسوم علیه مثبتی‌از $p-1$ باشد. دراین صورت، در هر دستگاه مانده‌ای تحویل یافته به هنگ p دقیقاً "$\varphi(d)$" عدد مانند a وجود دارند بطوری که

$$\exp_p(a) = d.$$

درحالت‌خاص، وقتی $d = \varphi(p) = p - 1$، دقیقاً "$\varphi(p-1)$" ریشهٔ‌اولیه‌به هنگ p وجود دارند.

برهان. با استفاده از روش بکار رفته در فصل ۲، رابطهٔ

$$\sum_{d|n} \varphi(d) = n$$

را ثابت‌می‌کنیم. اعداد $1, 2, \ldots, p-1$ در مجموعه‌های‌ازهم جدای $A(d)$ توزیع شده‌اند، که هر مجموعه نظیر به مقسوم علیه d از $p-1$ است. در اینجا تعریف می‌کنیم

$$A(d) = \{x : 1 \le x \le p-1, \exp_p(x) = d\}.$$

فرض‌کنیم $f(d)$ تعداد عناصر در $A(d)$ باشد. دراین صورت، به‌ازای هر d، $f(d) \ge 0$. هدف ما اثبات این است که $f(d) = \varphi(d)$.

چون مجموعه‌های $A(d)$ از هم جدایند و هر $x = 1, 2, \ldots, p-1$ در $A(d)$ ای قرار دارد، داریم

$$\sum_{d|p-1} f(d) = p - 1.$$

اما نیز داریم

$$\sum_{d|p-1} \varphi(d) = p - 1;$$

درنتیجه ،

$$\sum_{d|p-1} \{\varphi(d) - f(d)\} = 0.$$

برای نشان دادن اینکه هر جمله دراین مجموع صفر است ، کافی است ثابت کنیم $f(d) \leq \varphi(d)$. این را با نشان دادن اینکه $f(d) = 0$ یا $f(d) = \varphi(d)$ انجام می‌دهیم ؛یا ،به‌عبارت دیگر ، نشان می‌دهیم که $f(d) \neq 0$ تساوی $f(d) = \varphi(d)$ راایجاب می‌کند .

فرض‌کنیم $f(d) \neq 0$. پس $A(d)$ ناتهی‌است؛ درنتیجه، به‌ازای a ای، $a \in A(d)$. لذا،

$\exp_p(a) = d$ ؛ درنتیجه، $a^d \equiv 1 \pmod{p}$.

اما هر توان a در همان همنهشتی صدق می‌کند ؛ درنتیجه، d عدد

$$a, a^2, \ldots, a^d \tag{۳}$$

جوابهای همنهشتی چندجمله‌ای

$$x^d - 1 \equiv 0 \pmod{p} \tag{۴}$$

می‌باشند . این جوابها ناهمنهشت به هنگ p اند ، زیرا $d = \exp_p(a)$. اما (۴) حداکثر d جواب دارد ، زیرا هنگ اول است ؛ درنتیجه، d عدد در (۳) همه باید جواب (۴) باشند . لذا ، هر عدد در $A(d)$ باید به‌ازای $k = 1, 2, \ldots, d$ ای به شکل a^k باشد . چه وقت $\exp_p(a^k) = d$ ؟ طبق لم ۱ ، این رخ می‌دهد اگر و فقط اگر $(k, d) = 1$. به عبارت دیگر ،دربین d عدددر (۳) $\varphi(d)$ عدد هستند که دارای نمای d به هنگ p می‌باشند . یعنی ، نشان داده‌ایم که اگر $f(d) \neq 0$ ، $f(d) = \varphi(d)$. همانطور که قبلاً" گفتیم ، این برهان را تمام خواهد کرد .

۵.۱۰ ریشه‌های اولیه و مانده‌های مربعی

قضیهٔ ۵.۱۰ . فرض‌کنیم g یک ریشهٔ اولیه به هنگ p باشد ، که در آن p عدد اول فردی است . دراین صورت ، توانهای زوج

$$g^2, g^4, \ldots, g^{p-1}$$

مانده‌های مربعی به هنگ p اند ، و توانهای فرد

$$g, g^3, \ldots, g^{p-2}$$

نامانده‌های مربعی به هنگ p می‌باشند .

برهان . هرگاه n زوج باشد ، مثلا" $n = 2m$ ، آنگاه $g^n = (g^m)^2$ ؛ درنتیجه ، $g^n \equiv x^2 \pmod p$ ، که درآن $x = g^m$. لذا ، g^nRp . اما $(p-1)/2$ توان زوج متمایز $g^2, \ldots, g^{p-1}$ به هنگ p و همین تعداد ماندهٔ مربعی به هنگ p وجود دارند . لذا ، توانهای زوج مانده‌های مربعی و توانهای فرد نامانده می‌باشند .

۶.۱۰ وجود ریشه‌های اولیه به هنگ p^α

اینک به حالت $m = p^\alpha$ می‌پردازیم ، که در آن p عدد اول فردی است و $\alpha \geq 2$. در جستجوی ریشه‌های اولیه به هنگ p^α ، طبیعی است ریشه‌های اولیه به هنگ p را امتحان کنیم . فرض کنیم g چنین ریشهٔ اولیه‌ای بوده و می‌پرسیم g نیز یک ریشهٔ اولیه به‌هنگ p^2 است یا نه . داریم $g^{p-1} \equiv 1 \pmod p$ و ، چون $\varphi(p^2) = p(p-1) > p-1$ ، اگر $g^{p-1} \equiv 1 \pmod{p^2}$ ، این g محققا" یک ریشهٔ اولیه نیست . لذا ، رابطهٔ

$$g^{p-1} \not\equiv 1 \pmod{p^2}$$

شرط لازم است برای آنکه ریشهٔ اولیهٔ g به هنگ p ریشهٔ اولیه به هنگ p^2 نیز باشد . اما این شرط کافی برای آنکه g ریشهٔ اولیه به هنگ p^2 و ، بطور کلی ، هنگ p^α به‌ازای همهٔ توانهای $\alpha \geq 2$ ، باشد نیز هست . درواقع ، قضیهٔ زیر را داریم .

قضیهٔ ۶.۱۰ . *فرض کنیم p یک عدد اول فرد باشد . دراین صورت ، داریم*

(آ) هرگاه g یک ریشهٔ اولیه به هنگ p باشد ، آنگاه g یک ریشهٔ اولیه به هنگ p^α به‌ازای هر $\alpha \geq 1$ است اگر و فقط اگر

$$g^{p-1} \not\equiv 1 \pmod{p^2}. \tag{۵}$$

(ب) دست کم یک ریشهٔ اولیه به هنگ p مانند g هست که در (۵) صدق می‌کند ؛ درنتیجه ، اگر $\alpha \geq 2$ ، دست کم یک ریشهٔ اولیه به هنگ p^α وجود دارد .

برهان . ابتدا (ب) را ثابت می‌کنیم . فرض کنیم g یک ریشهٔ اولیه به هنگ p باشد . اگر $g^{p-1} \not\equiv 1 \pmod{p^2}$ ، چیزی برای اثبات وجود ندارد . اما ، اگر $g^{p-1} \equiv 1 \pmod{p^2}$ ، می‌توان نشان داد که $g_1 = g + p$ ، که ریشهٔ اولیهٔ دیگری به هنگ p است که در شرط

$$g_1{}^{p-1} \not\equiv 1 \pmod{p^2}$$

صدق می‌کند. درواقع، داریم

$$\begin{aligned} g_1{}^{p-1} &= (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + tp^2 \\ &\equiv g^{p-1} + (p^2-p)g^{p-2} \pmod{p^2} \\ &\equiv 1 - pg^{p-2} \pmod{p^2}. \end{aligned}$$

امانمی‌توان‌داشت $pg^{p-2} \equiv 0 \pmod{p^2}$، زیرااین‌ایجاب‌می‌کندکه $g^{p-2} \equiv 0 \pmod{p}$ که با ریشهٔ اولیه به هنگ p بودن g متناقض است. بنابراین، $g_1{}^{p-1} \not\equiv 1 \pmod{p^2}$ درنتیجه، (ب) ثابت شده است.

حال (آ) را ثابت می‌کنیم. فرض کنیم g یک ریشهٔ اولیه به هنگ p باشد. اگر این g ریشهٔ اولیه به هنگ p^α به‌ازای هر $\alpha \geq 1$ باشد، بالاخص ریشهٔ اولیه به هنگ p^2 است و، همانطور که قبلاً گفتیم، این (۵) را ایجاب خواهد کرد.

حال عکس این مطلب را ثابت می‌کنیم. فرض کنیم g یک ریشهٔ اولیه به هنگ p و صادق در (۵) باشد. باید نشان دهیم که g یک ریشهٔ اولیه به هنگ p^α به‌ازای هر $\alpha \geq 2$ نیز هست. فرض‌کنیم t نمای g به هنگ p^α باشد. می‌خواهیم نشان دهیم که $t = \varphi(p^\alpha)$. چون $g^t \equiv 1 \pmod{p^\alpha}$، نیز داریم $g^t \equiv 1 \pmod{p}$؛ درنتیجه، $\varphi(p)|t$ و می‌توان نوشت

$$t = q\varphi(p). \tag{۶}$$

اما $t|\varphi(p^\alpha)$؛ درنتیجه، $q\varphi(p)|\varphi(p^\alpha)$. اما $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. لذا،

$$q(p-1)|p^{\alpha-1}(p-1),$$

که به معنی $q|p^{\alpha-1}$ است. بنابراین، $q = p^\beta$، که در آن $\beta \leq \alpha - 1$، و (۶) خواهد شد

$$t = p^\beta(p-1).$$

اگر ثابت کنیم $\beta = \alpha - 1$، $t = \varphi(p^\alpha)$ و برهان تمام خواهد بود.

فرض کنیم، بعکس، $\beta < \alpha - 1$. پس $\beta \leq \alpha - 2$ و داریم

$$t = p^\beta(p-1)|p^{\alpha-2}(p-1) = \varphi(p^{\alpha-1}).$$

لذا، چون $\varphi(p^{\alpha-1})$ مضربی از t است، این ایجاب می‌کند که

$$g^{\varphi(p^{\alpha-1})} \equiv 1 \pmod{p^\alpha}. \tag{۷}$$

حال با استفاده از لم زیر نشان می‌دهیم که (۷) یک تناقض است. این تناقض برهان قضیهٔ ۶.۱۰ را تمام می‌کند.

لم ۲ . **فرض کنیم g یک ریشهٔ اولیه به هنگ p باشد بطوری که**

$$g^{p-1} \not\equiv 1 \pmod{p^2}. \tag{۸}$$

دراین صورت ، به‌ازای هر $\alpha \geq 2$ ، داریم

$$g^{\varphi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}. \tag{۹}$$

برهان لم ۲ . از استقرا روی α استفاده می‌کنیم . به‌ازای $\alpha = 2$ ، رابطهٔ (۹) به (۸) تحویل مـی‌شود . پس فرض کنیم (۹) به‌ازای α برقرار باشد . طبق قضیهٔ اویلر ــ فرما ، داریم

$$g^{\varphi(p^{\alpha-1})} \equiv 1 \pmod{p^{\alpha-1}}\,;$$

درنتیجه ،

$$g^{\varphi(p^{\alpha-1})} = 1 + kp^{\alpha-1},$$

که درآن ، بخـاطر (۹) ، $p \nmid k$. اگر طرفین رابطهٔ اخیررا به‌توان p برسانیم ، معلوم می‌شود که

$$g^{\varphi(p^\alpha)} = (1 + kp^{\alpha-1})^p = 1 + kp^\alpha + k^2\frac{p(p-1)}{2}p^{2(\alpha-1)} + rp^{3(\alpha-1)}.$$

اما $2\alpha - 1 \geq \alpha + 1$ و $3\alpha - 3 \geq \alpha + 1$ ، زیـرا $\alpha \geq 2$. لذا ، معادلهٔ اخیرهمنهشتی

$$g^{\varphi(p^\alpha)} \equiv 1 + kp^\alpha \pmod{p^{\alpha+1}}$$

رابدست می‌دهد ، که‌درآن $p \nmid k$. به‌عبارت دیگر ، $g^{\varphi(p^\alpha)} \not\equiv 1 \pmod{p^{\alpha+1}}$ ؛ درنتیجه ، (۹) ، درصورت برقراری به‌ازای α ، به‌ازای $\alpha + 1$ برقرار است . این برهان لم ۲ و نیز قضیهٔ ۶.۱۰ را تمام خواهد کرد .

۷.۱۰ وجود ریشه‌های اولیه به هنگ $2p^\alpha$

قضیهٔ ۷.۱۰ . ***اگر p یک عدد اول فرد بوده و $\alpha \geq 1$ ، ریشه‌های اولیهٔ فرد به هنگ p^α مانند g وجود دارند . هرچنین g یک ریشهٔ اولیه به هنگ $2p^\alpha$ نیز هست .***

برهان . اگر g ریشهٔ اولیه‌به‌هنگ p^α باشد ، $g + p^\alpha$ نیز هست . اما g یا $g + p^\alpha$ فرد است ؛ درنتیجه ، ریشه‌های اولیهٔ فرد به‌هنگ p^α همیشه وجود دارند . فرض کنیم g یک ریشهٔ اولیهٔ فـرد به هنگ p^α بوده و f نمای g به هنگ $2p^\alpha$ باشد . می‌خواهیم نشان

دهیم کـه $f = \varphi(2p^\alpha)$. اما $f|\varphi(2p^\alpha)$ ، و $\varphi(2p^\alpha) = \varphi(2)\varphi(p^\alpha) = \varphi(p^\alpha)$ ؛ درنتیجه، $f|\varphi(p^\alpha)$. از آن‌سـو، $g^f \equiv 1 \pmod{2p^\alpha}$ ؛ درنتیجـه، $g^f \equiv 1 \pmod{p^\alpha}$ ؛ از اینرو ، $\varphi(p^\alpha)|f$ ، زیرا g ریشهٔ اولیه به هنگ p^α است . بنابراین ، $f = \varphi(p^\alpha) = \varphi(2p^\alpha)$ ؛ درنتیجه ، g ریشهٔ اولیه به هنگ $2p^\alpha$ می‌باشد .

۸.۱۰ عدم وجود ریشه‌های اولیه در حالات دیگر

قضیهٔ ۸.۱۰ . فرض کنیـم $m \geq 1$ ، که در آن m به شکل $m = 1, 2, 4, p^\alpha, 2p^\alpha$ ، که p عدد اول فـردی است ، نبـاشد . دراین صورت ، به‌ازای هر a که $(a, m) = 1$ ، داریم

$$a^{\varphi(m)/2} \equiv 1 \pmod{m};$$

درنتیجه ، ریشه‌های اولیه به هنگ m وجود ندارند .

برهان . قبلاً نشان داده‌ایم که اگر $\alpha \geq 3$ ، ریشه‌های اولیه به هنگ 2^α وجود ندارند . لذا ، می‌توان فرض کرد m دارای تجزیهٔ

$$m = 2^\alpha p_1^{\alpha_1} \cdots p_s^{\alpha_s}$$

باشد ، که در آن p_i اعداد اول فـردی بـوده ، $s \geq 1$ ، و $\alpha \geq 0$. چـون m به شکل $1, 2, 4, p^\alpha$ یا $2p^\alpha$ نیست ، $\alpha \geq 2$ اگر $s = 1$ ، و $s \geq 2$ اگر 0 یا $1 = \alpha$. توجه کنید که

$$\varphi(m) = \varphi(2^\alpha)\varphi(p_1^{\alpha_1}) \cdots \varphi(p_s^{\alpha_s}).$$

حال فرض کنیم a عدد صحیحی و نسبت به m اول باشد . می‌خواهیم ثابت کنیم

$$a^{\varphi(m)/2} \equiv 1 \pmod{m}.$$

فرض کنیم g یک ریشهٔ اولیه به هنگ $p_1^{\alpha_1}$ بوده ، و k را طوری می‌گیریم که

$$a \equiv g^k \pmod{p_1^{\alpha_1}}.$$

دراین صورت ، داریم

$$a^{\varphi(m)/2} \equiv g^{k\varphi(m)/2} \equiv g^{t\varphi(p_1^{\alpha_1})} \pmod{p_1^{\alpha_1}}, \tag{۱۰}$$

که در آن

$$t = k\varphi(2^\alpha)\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s})/2.$$

نشان می‌دهیم‌که t یک عددصحیح است . اگر $\alpha \geq 2$ ، عامل $\varphi(2^\alpha)$ زوج‌است ؛ ودرنتیجه، t یک عددصحیح است . اگر 0 یا $1 = \alpha$ ، $s \geq 2$ و عامل $\varphi(p_2^{\alpha_2})$ زوج است ؛ درنتیجه ، t دراین حالت نیز عددی صحیح است . لذا ، همنهشتی (۱۰) نتیجه می‌دهد که

$$a^{\varphi(m)/2} \equiv 1 \pmod{p_1^{\alpha_1}}.$$

بهمین نحو ، معلوم می‌شود که ، به‌ازای هر $i = 1, 2, \ldots, s$ ،

$$a^{\varphi(m)/2} \equiv 1 \pmod{p_i^{\alpha_i}} . \tag{۱۱}$$

حال نشان می‌دهیم این همنهشتی به هنگ 2^α نیز برقرار است. اگر $\alpha \geq 3$ ، شرط $(a, m) = 1$ فرد بودن a را ایجاب می‌کند و می‌توان قضیهٔ ۳۰۱۰ بکار برد و نوشت

$$a^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}.$$

چون $\varphi(2^\alpha) | \varphi(m)$ ، این نتیجه می‌دهد که، به‌ازای $\alpha \geq 3$ ،

$$a^{\varphi(m)/2} \equiv 1 \pmod{2^\alpha} . \tag{۱۲}$$

اگر $\alpha \leq 2$ ، داریم

$$a^{\varphi(2^\alpha)} \equiv 1 \pmod{2^\alpha}. \tag{۱۳}$$

اما $s \geq 1$ ؛ درنتیجه، $\varphi(m) = \varphi(2^\alpha)\varphi(p_1^{\alpha_1}) \cdots \varphi(p_s^{\alpha_s}) = 2r\varphi(2^\alpha)$ ، که در آن r یک عدد صحیح است. لذا، $\varphi(2^\alpha) | \varphi(m)/2$ و (۱۳) رابطهٔ (۱۲) را به‌ازای $\alpha \leq 2$ ایجاب می‌کند. ازاینرو، (۱۲) به‌ازای هر α برقرار است. با ضرب همنهشتیهای (۱۱) و (۱۲) درهم، بدست می‌آوریم

$$a^{\varphi(m)/2} \equiv 1 \pmod{m},$$

و این نشان می‌دهد که a نمی‌تواند یک ریشهٔ اولیه به هنگ m باشد.

۹.۱۰ تعداد ریشه‌های اولیه به هنگ m

نشان داده‌ایم که عدد صحیح $m \geq 1$ ریشهٔ اولیه دارد اگر و فقط اگر

$$m = 1, 2, 4, p^\alpha , 2p^\alpha,$$

که p یک عدد اول فرد بوده و $\alpha \geq 1$. قضیهٔ زیر به‌ما می‌گوید که، به‌ازای هرچنین m ، چند ریشهٔ اولیه وجود دارند.

قضیهٔ ۹.۱۰ . *هرگاه m دارای ریشهٔ اولیهٔ g باشد، آنگاه m دقیقاً "$\varphi(\varphi(m))$ ریشهٔ اولیهٔ ناهمنهشت دارد و اینها به‌وسیلهٔ اعداد مجموعهٔ*

$$S = \{g^n : 1 \leq n \leq \varphi(m), (n, \varphi(m)) = 1\}$$

داده می‌شوند.

برهان. داریم $\exp_m(g) = \varphi(m)$ ، و لم ۱ نشان می‌دهد که $\exp_m(g^n) = \exp_m(g)$ اگر و فقط اگر $(n, \varphi(m)) = 1$. لذا، هر عنصر از S ریشهٔ اولیه به هنگ m می‌باشد.

بعکس، اگر a ریشهٔ اولیه به هنگ m باشد، به‌ازای $k = 1, 2, \ldots, \varphi(m)$ ای، $a \equiv g^k \pmod{m}$. لذا، $\exp_m(g^k) = \exp_m(a) = \varphi(m)$ ، و لم ۱ ایجاب می‌کند که

$(k, \varphi(m)) = 1$. بنابراین ، هر ریشهٔ اولیه عضوی از S است . چون S شامل $\varphi(\varphi(m))$ عضو ناهمنهشت به هنگ m است ، برهان تمام خواهد بود .

با آنکه وجود ریشه‌های اولیه را برای بعضی هنگها نشان داده‌ایم ، در حالت کلی هیچ روش مستقیمی برای محاسبهٔ این ریشه‌ها بدون محاسبات زیاد ، بویژه برای هنگهای بزرگ ، وجود ندارد . فرض کنیم $g(p)$ کوچکترین ریشهٔ اولیه به هنگ p باشد . در جدول ۱۰۱۰ ، $g(p)$ به‌ازای جمیع اعداد اول فرد $p < 1000$ لیست شده است .

جدول ۱۰۱۰ $g(p)$ کوچکترین ریشهٔ اولیهٔ عدد اول p است .

p	$g(p)$	p	$g(p)$	p	$g(p)$	p	$g(p)$	p	$g(p)$	p	$g(p)$
2	1	109	6	269	2	439	15	617	3	811	3
3	2	113	3	271	6	443	2	619	2	821	2
5	2	127	3	277	5	449	3	631	3	823	3
7	3	131	2	281	3	457	13	641	3	827	2
11	2	137	3	283	3	461	2	643	11	829	2
13	2	139	2	293	2	463	3	647	5	839	11
17	3	149	2	307	5	467	2	653	2	853	2
19	2	151	6	311	17	479	13	659	2	857	3
23	5	157	5	313	10	487	3	661	2	859	2
29	2	163	2	317	2	491	2	673	5	863	5
31	3	167	5	331	3	499	7	677	2	877	2
37	2	173	2	337	10	503	5	683	5	881	3
41	6	179	2	347	2	509	2	691	3	883	2
43	3	181	2	349	2	521	3	701	2	887	5
47	5	191	19	353	3	523	2	709	2	907	2
53	2	193	5	359	7	541	2	719	11	911	17
59	2	197	2	367	6	547	2	727	5	919	7
61	2	199	3	373	2	557	2	733	6	929	3
67	2	211	2	379	2	563	2	739	3	937	5
71	7	223	3	383	5	569	3	743	5	941	2
73	5	227	2	389	2	571	3	751	3	947	2
79	3	229	6	397	5	577	5	757	2	953	3
83	2	233	3	401	3	587	2	761	6	967	5
89	3	239	7	409	21	593	3	769	11	971	6
97	5	241	7	419	2	599	7	773	2	977	3
101	2	251	6	421	2	601	7	787	2	983	5
103	5	257	3	431	7	607	3	797	2	997	7
107	2	263	5	433	5	613	2	809	3		

۱۰.۱۰ حساب اندیسها

اگر m دارای ریشهٔ اولیهٔ g باشد، اعداد $1, g, g^2, \ldots, g^{\varphi(m)-1}$ یک دستگاه مانده‌ای تحویل یافته به هنگ m تشکیل می‌دهند. اگر $(a, m) = 1$، عدد صحیح منحصر بفردی مانند k در بازهٔ $0 \le k \le \varphi(m) - 1$ هست بطوری که

$$a \equiv g^k \pmod{m}.$$

این عدد صحیح را *اندیس* a در پایهٔ g (به هنگ m) نامیده، و می‌نویسیم

$$k = \operatorname{ind}_g a$$

یا، اگر پایهٔ g معلوم باشد، $k = \operatorname{ind} a$.

قضیهٔ زیر نشان می‌دهد که اندیسها خواصی مشابه خواص لگاریتمها دارند. اثبات به عنوان تمرین به خواننده محول می‌شود.

قضیهٔ ۱۰.۱۰ . فرض کنیم g یک ریشهٔ اولیه به هنگ m باشد. اگر $(a, m) = (b, m) = 1$، **داریم**

(آ) $\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{\varphi(m)}$؛

(ب) *اگر* $n \ge 1$، $\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod{\varphi(m)}$؛

(پ) $\operatorname{ind} 1 = 0$ و $\operatorname{ind} g = 1$؛

(ت) *اگر* $m > 2$، $\operatorname{ind}(-1) = \varphi(m)/2$؛

(ث) *هرگاه g' نیز یک ریشهٔ اولیه به هنگ m باشد، آنگاه*

$$\operatorname{ind}_g a \equiv \operatorname{ind}_{g'} a \cdot \operatorname{ind}_g g' \pmod{\varphi(m)}.$$

جدول ۲.۱۰ در صفحات ۲۵۲ تا ۲۵۳ اندیسها را به‌ازای جمیع اعداد $a \not\equiv 0 \pmod{p}$ و همهٔ اعداد اول فرد $p < 50$ ذکر کرده است. پایهٔ g کوچکترین ریشهٔ اولیهٔ p می‌باشد.

مثالهای زیر کاربرد اندیسها در حل همنهشتیها را نشان می‌دهد.

مثال ۱ . همنهشتیهای خطی . فرض کنیم m یک ریشهٔ اولیه بوده، و $(a, m) = (b, m) = 1$. دراین صورت، همنهشتی خطی

$$ax \equiv b \pmod{m} \tag{۱۴}$$

معادل همنهشتی

$$\operatorname{ind} a + \operatorname{ind} x \equiv \operatorname{ind} b \pmod{\varphi(m)}$$

است؛ درنتیجه، جواب منحصر بفرد (۱۴) در همنهشتی

جدول ۱۰.۲ اندیسهای همهٔ اعداد $a \not\equiv 0 \pmod{p}$ به‌ازای اعداد اول فرد $p < 50$.
پایهٔ g کوچکترین ریشهٔ اولیهٔ p است.

a	اعداد اول 3	5	7	11	13	17	19	23	29	31	37	41	43	47
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	2	1	1	14	1	2	1	24	1	26	27	18
3		3	1	8	4	1	13	16	5	1	26	15	1	20
4		2	4	2	2	12	2	4	2	18	2	12	12	36
5			5	4	9	5	16	1	22	20	23	22	25	1
6			3	9	5	15	14	18	6	25	27	1	28	38
7				7	11	11	6	19	12	28	32	39	35	32
8				3	3	10	3	6	3	12	3	38	39	8
9				6	8	2	8	10	10	2	16	30	2	40
10				5	10	3	17	3	23	14	24	8	10	19
11					7	7	12	9	25	23	30	3	30	7
12					6	13	15	20	7	19	28	27	13	10
13						4	5	14	18	11	11	31	32	11
14						9	7	21	13	22	33	25	20	4
15						6	11	17	27	21	13	37	26	21
16						8	4	8	4	6	4	24	24	26
17							10	7	21	7	7	33	38	16
18							9	12	11	26	17	16	29	12
19								15	9	4	35	9	19	45
20								5	24	8	25	34	37	37

21	13	17	29	22	14	36	6
22	11	26	17	31	29	15	25
23		20	27	15	36	16	5
24		8	13	29	13	40	28
25		16	10	10	4	8	2
26		19	5	12	17	17	29
27		15	3	6	5	3	14
28		14	16	34	11	5	22
29			9	21	7	41	35
30			15	14	23	11	39
31				9	28	34	3
32				5	10	9	44
33				20	18	31	27
34				8	19	23	34
35				19	21	18	33
36				18	2	14	30
37					32	7	42
38					35	4	17
39					6	33	31
40					20	22	9
41						6	15
42						21	24
43							13
44							43
45							41
46							23

$$\text{ind } x \equiv \text{ind } b - \text{ind } a \pmod{\varphi(m)}$$

صدق می‌کند.

به عنوان یک مثال عددی، همنهشتی خطی

$$9x \equiv 13 \pmod{47}$$

را درنظر می‌گیریم. رابطهٔ اندیسی نظیر عبارت است از

$$\text{ind } x \equiv \text{ind } 13 - \text{ind } 9 \pmod{46}.$$

از جدول ۲۰۱۰ معلوم می‌شود که $\text{ind } 13 = 11$ و $\text{ind } 9 = 40$ (به‌ازای $p = 47$)؛ درنتیجه،

$$\text{ind } x \equiv 11 - 40 \equiv -29 \equiv 17 \pmod{46}.$$

مجددا"، از جدول ۲۰۱۰ معلوم می‌شود که $x \equiv 38 \pmod{47}$.

مثال ۲ همنهشتیهای دوجمله‌ای. یک همنهشتی به شکل

$$x^n \equiv a \pmod{m}$$

یک همنهشتی دوجمله‌ای نام دارد. اگر m ریشهٔ اولیه داشته و $(a, m) = 1$، این معادل همنهشتی

$$n \text{ ind } x \equiv \text{ind } a \pmod{\varphi(m)}$$

است، که خطی نسبت به مجهول $\text{ind } x$ است. دراین صورت، دارای جواب است اگر وفقط اگر $\text{ind } a$ بر $d = (n, \varphi(m))$ بخشپذیر باشد، که در این حالت دقیقا" d جواب دارد.

به عنوان یک مثال عددی، همنهشتی دوجمله‌ای

$$x^8 \equiv a \pmod{17} \tag{۱۵}$$

را درنظر می‌گیریم. رابطهٔ اندیسی نظیر خواهد بود

$$8 \text{ ind } x \equiv \text{ind } a \pmod{16}. \tag{۱۶}$$

دراین مثال، $d = (8, 16) = 8$. جدول ۲۰۱۰ نشان می‌دهد که 1 و 16 تنها اعداد به هنگ 17 هستند که اندیس آنها بر 8 بخشپذیر است. درواقع، $\text{ind } 1 = 0$ و $\text{ind } 16 = 8$. از اینرو، (۱۵) درصورتی که $a \not\equiv 16 \pmod{17}$ یا $a \not\equiv 1$ جواب ندارد.

به‌ازای $a = 1$، همنهشتی (۱۶) می‌شود

$$8 \text{ ind } x \equiv 0 \pmod{16}, \tag{۱۷}$$

و، به‌ازای $a = 16$، خواهد شد

$$8 \text{ ind } x \equiv 8 \pmod{16}. \tag{۱۸}$$

هریک‌ازاینها دقیقا" هشت جواب به هنگ 16 دارند. جوابهای (۱۷) آن x هایی‌هستند

که اندیسشان زوج است :

$$x \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}.$$

این ، البته ، مانده‌های مربعی 17 هستند . جوابهای (۱۸) آن x هایی هستند که‌اندیسشان فرد است ، یعنی نامانده‌های مربعی 17 :

$$x \equiv 3, 5, 6, 7, 10, 11, 12, 14 \pmod{17}.$$

مثال ۳ . همنهشتیهای نمایی . یک همنهشتی نمایی به شکل

$$a^x \equiv b \pmod m$$

است . اگر m ریشهٔ اولیه‌داشته‌و $(a, m) = (b, m) = 1$ ، این معادل همنهشتی خطی

$$x \operatorname{ind} a \equiv \operatorname{ind} b \pmod{\varphi(m)} \qquad (۱۹)$$

است . فرض کنیم $d = (\operatorname{ind} a, \varphi(m))$ دراین‌صورت ، (۱۹) جواب دارد اگر و فقط اگر $d | \operatorname{ind} b$ ، که دراین حالت دقیقاً d جواب وجود دارند . در مثال عددی

$$25^x \equiv 17 \pmod{47} \qquad (۲۰)$$

داریم $\operatorname{ind} 25 = 2$ ، $\operatorname{ind} 17 = 16$ ، و $d = (2, 46) = 2$. لذا ، (۱۹) خواهد شد

$$2x \equiv 16 \pmod{46},$$

با دو جواب $x \equiv 8, 31 \pmod{46}$. اینها جوابهای (۲۰) به هنگ 47 هستند .

۱۱۰۱۰ ریشه‌های اولیه و مشخصهای دیریکله

از ریشه‌های اولیه و اندیسها می‌توان برای ساختن صریح همهٔ مشخصهای دیریکله به هنگ m استفاده کرد . ابتدا هنگ p^α ، که توان عددی اول است و p عدد اول فردی بوده و $\alpha \geq 1$ ، را درنظر می‌گیریم .

فرض کنیم g ریشهٔ اولیه‌ای به‌هنگ p باشد که ریشهٔ اولیه به هنگ p^β به‌ازای هر $\beta \geq 1$ نیز باشد . چنین g طبق قضیهٔ ۱۰۰۶ وجود دارد . اگر $(n, p) = 1$ ، قرارمی‌دهیم $b(n) = \operatorname{ind}_g n \pmod{p^\alpha}$ ؛ درنتیجه ، $b(n)$ عدد صحیح منحصر بفرد صادق در شرایط

$$n \equiv g^{b(n)} \pmod{p^\alpha}, \quad 0 \leq b(n) < \varphi(p^\alpha)$$

است به ازای $h = 0, 1, 2, \ldots, \varphi(p^\alpha) - 1$ ، χ_h را با روابط زیر تعریف می‌کنیم :

$$\chi_h(n) = \begin{cases} e^{2\pi i h b(n)/\varphi(p^\alpha)} & \text{اگر } p \nmid n \text{ ،} \\ 0 & \text{اگر } p | n \text{ ،} \end{cases} \qquad (۲۱)$$

با استفاده از خواص اندیسها ، به آسانی تحقیق می‌شود که χ_h کاملاً ضربی و متناوب با دورهٔ تناوب p^α است ؛ درنتیجه ، χ_h یک مشخص دیریکله به هنگ p^α است ، که χ_0

مشخص اصلی می‌باشد. این تحقیق را به عنوان تمرین به خواننده وامی‌گذاریم.

چون

$$\chi_h(g) = e^{2\pi i h/\varphi(p^\alpha)}$$

مشخصهای $\chi_0, \chi_1, \ldots, \chi_{\varphi(p^\alpha)-1}$ متمایزند، زیرا در g مقادیر متمایز می‌گیرند. لذا، چون ازاین توابع $\varphi(p^\alpha)$ تا وجود دارند، اینها تمام مشخصهای دیریکله به هنگ p^α را نمایش می‌دهند. همین ساختن برای هنگ 2^α، درصورتی که $\alpha = 1$ یا $\alpha = 2$، با استفاده از $g = 3$ به عنوان ریشهٔ اولیه، قابل انجام است.

حال‌اگر $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$، که‌درآن p_i اعداد اول فرد متمایزند، و χ_i یک‌مشخص دیریکله بـــه هنگ $p_i^{\alpha_i}$ باشد، حــاصل ضرب $\chi = \chi_1 \cdots \chi_r$ یک مشخص دیریکله به هنگ m می‌باشد. چون $\varphi(m) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r})$، وقتی هر χ_i، $\varphi(p_i^{\alpha_i})$ تا مشخص به هنگ $p_i^{\alpha_i}$ را بگیرد، $\varphi(m)$ تا از این مشخصها بدست می‌آوریم. لذا، به‌ازای هر هنگ فرد m، همهٔ مشخصها به هنگ m به‌طور صریح ساخته شده‌اند.

اگر $\alpha \geq 3$، هنگ 2^α ریشهٔ اولیه ندارد، و برای بدست آوردن مشخصها به هنگ 2^α به ساختنی‌کمی متفاوت نیاز اســت. قضیهٔ زیر نشان می‌دهد که 5 جانشین مناسبی برای یک ریشهٔ اولیه به هنگ 2^α است.

قضیهٔ ۱۱.۱۰ . فرض‌کنیـــم $\alpha \geq 3$. دراین صورت، به‌ازای هر عدد صحیح فرد n عدد صحیح منحصر بفردی مانند $b(n)$ هست بطوری که

$$n \equiv (-1)^{(n-1)/2} 5^{b(n)} \pmod{2^\alpha}$$ ، که درآن $1 \leq b(n) \leq \varphi(2^\alpha)/2$.

برهان. فرض کنیم $f = \exp_{2^\alpha}(5)$؛ درنتیجه، $5^f \equiv 1 \pmod{2^\alpha}$. نشان می‌دهیم که $f = \varphi(2^\alpha)/2$. گوییم $f | \varphi(2^\alpha) = 2^{\alpha-1}$؛ درنتیجه، به‌ازای $\beta \leq \alpha - 1$ ای، $f = 2^\beta$.از قضیهٔ ۸.۱۰ می‌دانیم که

$$5^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}.$$

ازاینرو، $f \leq \varphi(2^\alpha)/2 = 2^{\alpha-2}$. بنابراین، $\beta \leq \alpha - 2$.نشان‌می‌دهیم‌که $\beta = \alpha - 2$.

طرفین معادلهٔ $5 = 1 + 2^2$ را به‌توان $f = 2^\beta$ می‌رسانیم، خواهیم داشت

$$5^f = (1 + 2^2)^{2^\beta} = 1 + 2^{\beta+2} + r2^{\beta+3} = 1 + 2^{\beta+2}(1 + 2r),$$

که درآن r عددی صحیح است. از اینرو، $5^f - 1 = 2^{\beta+2}t$ ، که درآن t فرد است.

اما $2^\alpha|(5^f - 1)$ ؛ درنتیجه، $\alpha \le \beta + 2$ ، یا $\beta \ge \alpha - 2$. لذا، $\beta = \alpha - 2$ و $f = 2^{\alpha-2} = \varphi(2^\alpha)/2$. بنابراین، اعداد

$$5, 5^2, \dots, 5^f \tag{۲۲}$$

ناهمنهشت به هنگ 2^α اند. همچنین، هریک همنهشت 1 به هنگ 4 است، زیرا $5 \equiv 1 \pmod 4$. بهمین نحو، اعداد

$$-5, -5^2, \dots, -5^f \tag{۲۳}$$

ناهمنهشت به هنگ 2^α اند و هریک همنهشت 3 به هنگ 4 می‌باشد، زیرا $-5 \equiv 3 \pmod 4$. $2f = \varphi(2^\alpha)$ عدد در (۲۲) و (۲۳) با هم وجود دارند. بعلاوه، نمی‌توان داشت $5^a \equiv -5^b \pmod{2^\alpha}$ ، زیرا این ایجاب می‌کند که $1 \equiv -1 \pmod 4$. لذا، اعداد (۲۲) همراه با اعداد (۲۳) $\varphi(2^\alpha)$ عدد فرد ناهمنهشت به هنگ 2^α را نمایش می‌دهند. هر عدد فرد $n \equiv 1 \pmod 4$ با یکی از اعداد (۲۲) همنهشت به هنگ 2^α است، و هر عدد فرد $n \equiv 3 \pmod 4$ با یکی از اعداد (۲۳) همنهشت است. این قضیه را ثابت خواهد کرد.

به کمک قضیهٔ ۱۱۰۱۰ ، می‌توان همهٔ مشخصها به هنگ 2^α را در صورت $\alpha \geq 3$ ساخت. فرض کنیم

$$f(n) = \begin{cases} (-1)^{(n-1)/2} & \text{اگر } n \text{ فرد باشد،} \\ 0 & \text{اگر } n \text{ زوج باشد،} \end{cases} \tag{۲۴}$$

و نیز

$$g(n) = \begin{cases} e^{2\pi i b(n)/2^{\alpha-2}} & \text{اگر } n \text{ فرد باشد،} \\ 0 & \text{اگر } n \text{ زوج باشد،} \end{cases}$$

که درآن $b(n)$ عدد صحیحی است که قضیهٔ ۱۱۰۱۰ بدست می‌دهد. به‌آسانی تحقیق می‌شود که هریک از f و g یک مشخص به هنگ 2^α است. همچنین است هر حاصلضرب

$$\chi_{a,c}(n) = f(n)^a g(n)^c, \tag{۲۵}$$

که درآن $a = 1, 2$ و $c = 1, 2, \dots, \varphi(2^\alpha)/2$. بعلاوه، این $\varphi(2^\alpha)$ مشخص متمایزند؛ در نتیجه، همهٔ مشخصها به هنگ 2^α را نمایش می‌دهند.

حال اگر $m = 2^\alpha Q$ ، که درآن Q فرد است، حاصل ضربهای $\chi = \chi_1\chi_2$ را تشکیل می‌دهیم، که درآنها χ_1 ، $\varphi(2^\alpha)$ مشخص به هنگ 2^α و χ_2 ، $\varphi(Q)$ مشخص به هنگ Q بگیرند تا همهٔ مشخصها به هنگ m بدست آیند.

۱۲.۱۰ مشخصهای دیریکلهٔ حقیقی به هنگ p^α

اگر χ یک مشخص دیریکلهٔ حقیقی به هنگ m بوده و $(n, m) = 1$ ، عدد $\chi(n)$ هم یک ریشهٔ واحد است و هم حقیقی است ؛ در نتیجه ، $\chi(n) = \pm 1$. از ساختن در بخش پیش می‌توان همهٔ مشخصهای دیریکلهٔ حقیقی به هنگ p^α را معین کرد .

قضیهٔ ۱۲.۱۰ . *به‌ازای عدد اول فرد p و $\alpha \geq 1$ ، $\varphi(p^\alpha)$ مشخص دیریکله به هنگ p^α راکه به‌وسیله (۲۱) داده شده‌اند درنظر می‌گیریم . دراین صورت ، χ_h حقیقی است اگر و فقط اگر $h = 0$ یا $h = \varphi(p^\alpha)/2$. بنابراین ، دقیقاً" دو مشخص حقیقی به هنگ p^α وجود دارند .*

برهان. داریم $e^{\pi i z} = \pm 1$ اگر و فقط اگر z صحیح باشد . اگر $p \nmid n$ ، داریم

$$\chi_h(n) = e^{2\pi i h b(n)/\varphi(p^\alpha)};$$

درنتیجه ، $\chi_h(n) = \pm 1$ اگر و فقط اگر $\varphi(p^\alpha) | 2hb(n)$. این شرط، اگر $h = 0$ یا اگر $h = \varphi(p^\alpha)/2$ ، به‌ازای هر n برقرار است . بعکس، اگر به‌ازای هر n ، $\varphi(p^\alpha) | 2hb(n)$ ، وقتی $b(n) = 1$ ، خواهیم داشت $\varphi(p^\alpha) | 2h$ یا $\varphi(p^\alpha)/2 | h$. بنابراین ، $h = 0$ یا $h = \varphi(p^\alpha)/2$ ، زیرا اینها تنها مضارب $\varphi(p^\alpha)/2$ کوچکتر از $\varphi(p^\alpha)$ اند .

تذکر. مشخص نظیر به $h = 0$ مشخص اصلی است . وقتی $\alpha = 1$ ، مشخص مربعی $\chi(n) = (n|p)$ تنها مشخص حقیقی به هنگ p می‌باشد .

به‌ازای هنگهای $m = 1, 2, 4$ ، همهٔ مشخصهای دیریکله حقیقی‌اند . قضیهٔ زیر مشخصهای حقیقی به هنگ 2^α ، وقتی $\alpha \geq 3$ ، را توصیف می‌کند .

قضیهٔ ۱۳.۱۰ . *اگر $\alpha \geq 3$ ، $\varphi(2^\alpha)$ مشخص دیریکلهٔ $\chi_{a,c}$ به هنگ 2^α که توسط (۲۵) داده شده‌اند را درنظر می‌گیریم . $\chi_{a,c}$ حقیقی است اگر و فقط اگر $c = \varphi(2^\alpha)/2$ یا $c = \varphi(2^\alpha)/4$. لذا ، اگر $\alpha \geq 3$ ، دقیقاً "چهارمشخص حقیقی به هنگ 2^α وجود دارند .*

برهان. اگر $\alpha \geq 3$ و n فرد باشد ، طبق (۲۵) داریم

$$\chi_{a,c}(n) = f(n)^a g(n)^c ,$$

که در آن $f(n) = \pm 1$ و

$$g(n)^c = e^{2\pi i c b(n)/2^{\alpha-2}},$$

که در آن $1 \le c \le 2^{\alpha-2}$. این $1\pm$ است اگر و فقط اگر $2^{\alpha-2}|2cb(n)$ یا $2^{\alpha-3}|cb(n)$. چون $\varphi(2^\alpha) = 2^{\alpha-1}$ ، این شرط برقرار است اگر $c = \varphi(2^\alpha)/2 = 2^{\alpha-2}$ یا اگر $c = \varphi(2^\alpha)/4 = 2^{\alpha-3}$. بعکس، اگر به‌ازای هر n ، $2^{\alpha-3}|cb(n)$ ، از $b(n) = 1$ نتیجه می‌شود که $2^{\alpha-3}|c$ ؛ درنتیجه، $2^{\alpha-2}$ یا $c = 2^{\alpha-3}$ ، زیرا $1 \le c \le 2^{\alpha-2}$.

۱۳.۱۰ مشخصهای دیریکلهٔ اولیه به هنگ p^α

در قضیهٔ ۱۴.۸ ثابت شد که هر مشخص غیر اصلی χ به هنگ p اولیه است اگر p اول باشد . حال جمیع مشخصهای دیریکلهٔ اولیه به هنگ p^α را معین می‌کنیم .

به‌یاد می‌آوریم (بخش ۷.۸) کـه χ اولیه به هنگ k است اگر و فقط اگر χ هنگ القایی $d < k$ نداشته باشد . یک هنگ القایی یک مقسوم علیه k مانند d است بطوری‌که هر وقت $(n, k) = 1$ و $n \equiv 1 \pmod d$ ، $\chi(n) = 1$.

اگر $k = p^\alpha$ و χ غیر اولیه بـه هنگ p^α باشد ، یکی از مقسوم علیه‌های $1, p, \ldots, p^{\alpha-1}$ یک هنگ القایی است ؛ و درنتیجه، $p^{\alpha-1}$ یک هنگ القایی است . از اینرو، χ اولیه به هنگ p^α است اگر و فقط اگر $p^{\alpha-1}$ یک هنگ القایی برای χ نباشد.

قضیهٔ ۱۴.۱۰ . به‌ازای عدد اول فرد p و $\alpha \ge 2$ ، $\varphi(p^\alpha)$ مشخص دیریکلهٔ χ_h به‌هنگ p^α که توسط (۳۱) داده شده‌اند را درنظر می‌گیریم . دراین صورت ، χ_h اولیه به هنگ p^α است اگر و فقط اگر $p \nmid h$.

برهان . نشان‌می‌دهیم‌که $p^{\alpha-1}$ یک هنگ‌القایی است اگر و فقط اگر $p|h$. اگر $p \nmid n$ ، طبق (۲۱) داریم

$$\chi_h(n) = e^{2\pi i h b(n)/\varphi(p^\alpha)},$$

که در آن $n \equiv g^{b(n)} \pmod{p^\alpha}$ و g یک ریشهٔ اولیه به هنگ p^β ، به ازای هر $\beta \ge 1$ ، است . بنابراین ،

$$g^{b(n)} \equiv n \pmod{p^{\alpha-1}}.$$

حال‌اگر $n \equiv 1 \pmod{p^{\alpha-1}}$ ، $g^{b(n)} \equiv 1 \pmod{p^{\alpha-1}}$ و ، چون g یک‌ریشهٔ اولیهٔ $p^{\alpha-1}$ است ، داریم $\varphi(p^{\alpha-1})|b(n)$ ، یا ، به‌ازای عدد صحیحی مانند t ،

$$b(n) = t\varphi(p^{\alpha-1}) = t\varphi(p^\alpha)/p .$$

بنابراین ،

$$\chi_h(n) = e^{2\pi i h t/p}.$$

اگر $p|h$ ، این مساوی 1 است؛ و درنتیجه، χ_h غیر اولیه به هنگ p^α است. اگر $p \nmid h$ ، $n = 1 + p^{\alpha-1}$ را اختیار می‌کنیم. در این صورت، $n \equiv 1 \pmod{p^{\alpha-1}}$ ولی $n \not\equiv 1 \pmod{p^\alpha}$؛ درنتیجه، $0 < b(n) < \varphi(p^\alpha)$. لذا، $p \nmid t$ ، $p \nmid ht$ ، و $\chi_h(n) \neq 1$. این نشان می‌دهد که اگر $p \nmid h$ ، χ_h اولیه می‌باشد.

وقتی 1 یا $m = 2$ ، فقط یک مشخص χ به هنگ m ، یعنی مشخص اصلی، وجود دارد. اگر $m = 4$ ، دو مشخص به هنگ 4 وجود دارند؛ یعنی، مشخص اصلی و مشخص اولیهٔ f که با (۲۴) داده‌شده‌است. قضیهٔ زیر همهٔ مشخصهای اولیه به هنگ 2^α به‌ازای $\alpha \geq 3$ را توصیف می‌کند. اثبات مشابه اثبات قضیهٔ ۱۴.۱۰ است و به خواننده محول می‌شود.

قضیهٔ ۱۵.۱۰ . ***اگر $\alpha \geq 3$ ، $\varphi(2^\alpha)$ مشخص دیریکلهٔ $\chi_{a,c}$ به هنگ 2^α که توسط (۲۵) داده شده‌اند را درنظر می‌گیریم. در این صورت، $\chi_{a,c}$ اولیه به هنگ 2^α است اگر و فقط اگر c فرد باشد.***

نتایج پیشگفته همهٔ مشخصهای اولیه به هنگ p^α را به‌ازای همهٔ توانهای اول توصیف می‌کنند. برای تعیین مشخصهای اولیه به‌ازای هنگ مرکب k ، می‌نویسیم

$$k = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

در این صورت، هر مشخص χ به هنگ k را می‌توان به شکل زیر تجزیه کرد:

$$\chi = \chi_1 \cdots \chi_r ,$$

که در آن هر χ_i یک مشخص به هنگ $p_i^{\alpha_i}$ است. بعلاوه، طبق تمرین ۱۲.۸ ، χ اولیه به هنگ k است اگر و فقط اگر هر χ_i اولیه به هنگ $p_i^{\alpha_i}$ باشد. لذا، توصیف کاملی از همهٔ مشخصهای اولیه به هنگ k خواهیم داشت.

تمرین برای فصل ۱۰

۱ . ثابت کنید m اول است اگر و فقط اگر به‌ازای a ای، $\exp_m(a) = m - 1$.

۲ . هرگاه $(a, m) = (b, m) = 1$ و $(\exp_m(a), \exp_m(b)) = 1$ ، ثابت کنید

$$\exp_m(ab) = \exp_m(a)\exp_m(b).$$

۳ . فرض کنید g ریشهٔ اولیهٔ عدد اول فرد p باشد. ثابت کنید $-g$ نیز ریشهٔ اولیهٔ p است اگر $p \equiv 1 \pmod 4$ ، ولی $\exp_p(-g) = (p-1)/2$ اگر $p \equiv 3 \pmod 4$.

۴ . (آ) ثابت کنید 3 یک ریشهٔ اولیه به هنگ p است اگر p عدد اولی به شکل

$n > 1$ ، $2^n + 1$ باشد .

(ب) ثابت کنید 2 یک ریشهٔ اولیه به هنگ p است اگر p عدد اولی به شکل $4q + 1$ باشد ، که در آن q یک عدد اول فرد است .

۵ . فرض کنید $m > 2$ عددی‌صحیح و دارای‌ریشهٔ‌اولیه بوده ، و $(a, m) = 1$. می‌نویسیم aRm اگر x ی وجود داشته باشد بطوری که $a \equiv x^2 \pmod{m}$. ثابت کنید

(آ) aRm اگر و فقط اگر $a^{\varphi(m)/2} \equiv 1 \pmod{m}$ ؛

(ب) اگر aRm ، همنهشتی $x^2 \equiv a \pmod{m}$ دقیقاً " دو جواب دارد ؛

(پ) دقیقاً " $\varphi(m)/2$ عددصحیح مانند a وجود دارند ، ناهمنهشت به هنگ m ، بطوری که $(a, m) = 1$ و aRm .

۶ . فرض کنید $m > 2$, $(a, m) = 1$, aRm . ثابت کنید همنهشتی $x^2 \equiv a \pmod{m}$ دقیقاً " دو جواب دارد اگر و فقط اگر m ریشهٔ اولیه داشته باشد .

۷ . فرض کنید $S_n(p) = \sum_{k=1}^{p-1} k^n$ ، که در آن p عدد اول فردی بوده و $n > 1$. ثابت کنید

$$S_n(p) \equiv \begin{cases} 0 \pmod{p} & \text{اگر } n \not\equiv 0 \pmod{p-1} \\ -1 \pmod{p} & \text{اگر } n \equiv 0 \pmod{p-1} \end{cases}$$

۸ . ثابت کنید مجموع ریشه‌های اولیه به هنگ p همنهشت $\mu(p-1)$ به هنگ p است .

۹ . هرگاه p عدد اول فردی بزرگتراز 3 باشد ، ثابت کنید حاصل ضرب ریشه‌های‌اولیه به هنگ p همنهشت 1 به هنگ p است .

۱۰ . فرض کنید p عدد اول فردی‌به شکل $2^{2^k} + 1$ باشد . ثابت کنید مجموعهٔ ریشه‌های اولیه به هنگ p مساوی‌مجموعهٔ نامانده‌های مربعی‌به هنگ p است . با استفاده از این نتیجه ، ثابت کنید 7 ریشهٔ اولیهٔ هرچنین عدد اول می‌باشد .

۱۱ . فرض کنید $d|\varphi(m)$ ، اگر $d = \exp_m(a)$ ، گوییم a یک ریشهٔ اولیهٔ همنهشتی

$$x^d \equiv 1 \pmod{m}$$

است . ثابت کنید اگر همنهشتی

$$x^{\varphi(m)} \equiv 1 \pmod{m}$$

ریشهٔ اولیه داشته باشد ، $\varphi(\varphi(m))$ ریشهٔ اولیه ، ناهمنهشت به هنگ m ، دارد .

۱۲ . خواص اندیسها را که در قضیهٔ ۱۰.۱۰ ذکر شدند اثبات کنید .

۱۳ . فرض کنید p یک عدد اول فرد باشد . اگر $(h, p) = 1$ ، قرار دهید

$$S(h) = \{h^n : 1 \le n \le \varphi(p-1), (n, p-1) = 1\}.$$

اگر h یک ریشهٔ اولیهٔ p باشد، اعداد موجود در مجموعهٔ $S(h)$ متمایز به هنگ p اند (اینها، در واقع، ریشه‌های اولیهٔ p اند). ثابت کنید عدد صحیحی مانند h هست، که ریشهٔ اولیهٔ p نیست، بطوری که اعداد موجود در $S(h)$ متمایز به هنگ p اند اگر و فقط اگر $p \equiv 3 \pmod 4$.

۱۴. اگر $m > 1$، $p_1, \ldots, p_k$ را مقسوم علیه‌های اول متمایز $\varphi(m)$ می‌گیریم. اگر $(g, m) = 1$، ثابت کنید g ریشهٔ اولیهٔ m است اگر و فقط اگر g در هیچیک از همنهشتیهای $g^{\varphi(m)/p_i} \equiv 1 \pmod m$ به‌ازای $i = 1, 2, \ldots, k$ صدق نکند.

۱۵. عدد اول $p = 71$، 7 را به عنوان یک ریشهٔ اولیه دارد. همهٔ ریشه‌های اولیهٔ 71 و نیز یک ریشهٔ اولیه برای p^2 و یک ریشهٔ اولیه برای $2p^2$ بیابید.

۱۶. هریک از همنهشتیهای زیر را حل کنید:

(آ) $8x \equiv 7 \pmod{43}$؛

(ب) $x^8 \equiv 17 \pmod{43}$؛

(پ) $8^x \equiv 3 \pmod{43}$.

۱۷. فرض کنید q یک عدد اول فرد بوده، و $p = 4q + 1$ نیز اول باشد.

(آ) ثابت کنید همنهشتی $x^2 \equiv -1 \pmod p$ دقیقاً" دو جواب دارد، که هریک نامانده‌ٔ مربعی از p است.

(ب) ثابت کنید هر نامانده‌ٔ مربعی از p یک ریشهٔ اولیهٔ p است، به استثنای دونامانده در (آ).

(پ) همهٔ ریشه‌های اولیهٔ 29 را بیابید.

۱۸. (تعمیم تمرین ۱۷). فرض کنید q عدد اول فردی بوده، و $p = 2^n q + 1$ نیز اول باشد. ثابت کنید هر نامانده‌ٔ مربعی a از p یک ریشهٔ اولیهٔ p است اگر $a^{2^n} \not\equiv 1 \pmod p$.

۱۹. ثابت کنید تنها دو مشخص اولیهٔ حقیقی به هنگ 8 وجود دارند و جدولی ازمقادیر آنها بسازید.

۲۰. فرض کنید χ یک مشخص‌اولیهٔ حقیقی به هنگ m باشد. اگر m توانی از 2 نباشد، ثابت کنید m به شکل

$$m = 2^\alpha p_1 \cdots p_r$$

است، که درآن p_i ها اعداد اول فرد متمایزی بوده و $\alpha = 0, 2, 3$. اگر $\alpha = 0$، نشان دهید که

$$\chi(-1) = \prod_{p|m}(-1)^{(p-1)/2}$$

و فرمول نظیری برای $\chi(-i)$ ، وقتی $\alpha = 2$ ، پیدا کنید .

۱۱
سریهای دیریکله و حاصل ضربهای اویلر

۱۰۱۱ مقدمه

درسال ۱۷۳۷ اویلــر قضیهٔ اقلیدس در باب وجود بی‌نهایت عدد اول را با نشان دادن واگرایی $\sum p^{-1}$ ، که روی همهٔ اعداد اول گرفته شده، ثابت کرد. وی این قضیه را ازاین امر که تابع زتای $\zeta(s)$ ، که به‌ازای $s > 1$ حقیقی با

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad (۱)$$

داده مــی‌شود، وقتــی $s \to 1$ ، به ∞ میل می‌کند نتیجه گرفت. در سال ۱۸۳۷ دیریکله قضیهٔ مشهور خود در باب اعداد اول در تصاعدهای حسابی را با بررسی سری

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad (۲)$$

که در آن χ یک مشخص دیریکله بوده و $s > 1$ ، ثابت کرد.

سریهای (۱) و (۲) نمونه‌هایی هستند از سری

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \qquad (۳)$$

که در آن $f(n)$ یک‌تابع حسابی است. اینها را سریهای دیریکله با ضرایب $f(n)$ می‌نامند، و یکی از مفیدترین ابزارها در نظریهٔ تحلیلی اعداد را تشکیل می‌دهند.

دراین‌فصل به مطالعهٔ خواص عمومی سریهای دیریکله می‌پردازیم. در فصل بعد به بررسی مشروحتر تابع زتای ریمان $\zeta(s)$ و Lــ توابع دیریکلهٔ $L(s, \chi)$ خواهیم پرداخت.

نمادگذاری. به تقلید از ریمان، فرض‌کنیم s متغیری مختلط باشد، و می‌نویسیم

$$s = \sigma + it,$$

که در آن σ و t حقیقی‌اند. درایـن صورت، $n^s = e^{s \log n} = e^{(\sigma+it)\log n} = n^\sigma e^{it \log n}$.
این نشان می‌دهد که $|n^s| = n^\sigma$ ، زیرا به‌ازای θ حقیقی، $|e^{i\theta}| = 1$.

مجموعهٔ نقـاط $s = \sigma + it$ که $\sigma > a$ **نیمصفحه** نام دارد. نشان خواهیم داد که، برای هـر سری دیریکله، یک نیمصفحه مانند $\sigma > \sigma_c$ هست که در آن سری همگراست، و نیمصفحهٔ دیگری مانند $\sigma > \sigma_a$ هست که در آن به‌طور مطلق همگراست. همچنین، نشان می‌دهیم که سری در نیمصفحهٔ همگرایی یک تابع تحلیلی از متغیر مختلط s را نمایش می‌دهد.

۲.۱۱ نیمصفحهٔ همگرایی مطلق یک سری دیریکله

ابتدا توجه می‌کنیم که اگر $\sigma \geq a$ ، داریم $|n^s| = n^\sigma \geq n^a$ ؛ درنتیجه،

$$\left|\frac{f(n)}{n^s}\right| \leq \frac{|f(n)|}{n^a}.$$

لذا، اگـر سری دیریکلهٔ $\sum f(n)n^{-s}$ به‌ازای $s = a + ib$ به‌طور مطلق همگرا باشد، طبق آزمون مقایسه‌ای، به‌ازای هر s که $\sigma \geq a$ نیز به‌طور مطلق همگراست. این نکات قضیهٔ زیر را ایجاب می‌کنند.

قضیهٔ ۱.۱۱ . فرض‌کنیـم سری $\sum |f(n)n^{-s}|$ به‌ازای هر s همگرا یا به‌ازای هر s واگرا نباشد. درایـن صـورت، عددی حقیقی مانند σ_a ، به‌نام طول همگرایی مطلق، هست بطوری که سری $\sum f(n)n^{-s}$ به‌طور مطلق همگراست اگر $\sigma > \sigma_a$ ، ولی به‌طور مطلق همگرا نیست اگر $\sigma < \sigma_a$.

برهان. فرض‌کنیـم D مجموعهٔ تمام σ های حقیقی باشد که $\sum |f(n)n^{-s}|$ واگراست. D تهی نیست، زیرا این سری به‌ازای هر s همگرا نیست، و D از بالا کراندار است، زیرا سری بـه‌ازای هر s واگرا نمـی‌باشد. لذا، D کوچکترین کران بالایی دارد، که ما آن را σ_a می‌نامیم. هرگاه $\sigma < \sigma_a$، آنگاه $\sigma \in D$ ؛ درغیر این‌صورت، σ یک کران بالایی‌برای D کوچکتر از کوچکترین کران بالایی است. هرگاه $\sigma > \sigma_a$ ، آنگاه $\sigma \notin D$ ، زیرا σ_a یک کران بالایی برای D است. این قضیه را ثابت خواهد کرد.

تذکر. اگر $\sum |f(n)n^{-s}|$ همه‌جا همگـرا باشد، تعریف می‌کنیم $\sigma_a = -\infty$. اگـر سری $\sum |f(n)n^{-s}|$ هیچ جا همگرا نباشد، تعریف می‌کنیم $\sigma_a = +\infty$.

مثال ۱ . تابع زتای ریمان . سری دیریکلهٔ $\sum_{n=1}^{\infty} n^{-s}$ به‌ازای $\sigma > 1$ به‌طور مطلق همگراست . وقتی $s = 1$ ، سری واگراست ؛ درنتیجه ، $\sigma_a = 1$. مجموع این سری با $\zeta(s)$ نموده و تابع زتای ریمان نامیده می‌شود .

مثال ۲ . اگر f کراندار باشد ، مثلاً " به‌ازای هر $n \geq 1$ ، $|f(n)| \leq M$ ، $\sum f(n)n^{-s}$ به‌ازای $\sigma > 1$ به‌طور مطلق همگراست ؛ درنتیجه ، $\sigma_a \leq 1$. بویژه ، اگر χ یک مشخص دیریکله باشد ، L ــ سری $L(s, \chi) = \sum \chi(n)n^{-s}$ به‌ازای $\sigma > 1$ به‌طور مطلق همگراست .

مثال ۳ . سری $\sum n^n n^{-s}$ به‌ازای هر s واگراست ؛ درنتیجه ، $\sigma_a = +\infty$.

مثال ۴ . سری $\sum n^{-n} n^{-s}$ به‌ازای‌هر s به‌طورمطلق همگراست ؛ درنتیجه ، $\sigma_a = -\infty$.

۳.۱۱ تابع تعریف شده با یک سری دیریکله

فرض‌کنیم $\sum f(n)n^{-s}$ به‌ازای $\sigma > \sigma_a$ به‌طور مطلق همگرا بوده ، و $F(s)$ تابع مجموع زیر باشد :

$$\text{به‌ازای } \sigma > \sigma_a \text{ ، } F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} . \tag{۴}$$

دراین بخش چند خاصیت $F(s)$ را بدست می‌آوریم . ابتدا لم زیر را ثابت می‌کنیم .

لم ۱ . *اگر* $N \geq 1$ *و* $\sigma \geq c > \sigma_a$ ، *داریم*

$$\left| \sum_{n=N}^{\infty} f(n)n^{-s} \right| \leq N^{-(\sigma-c)} \sum_{n=N}^{\infty} |f(n)|n^{-c}.$$

برهان . داریم

$$\left| \sum_{n=N}^{\infty} f(n)n^{-s} \right| \leq \sum_{n=N}^{\infty} |f(n)|n^{-\sigma} = \sum_{n=N}^{\infty} |f(n)|n^{-c}n^{-(\sigma-c)}$$
$$\leq N^{-(\sigma-c)} \sum_{n=N}^{\infty} |f(n)|n^{-c}.$$

قضیهٔ زیر رفتار $F(s)$ را ، وقتی $\sigma \to +\infty$ ، توصیف می‌کند .

قضیهٔ ۲.۱۱ . هرگاه $F(s)$ با (۴) داده شده باشد ، آنگاه به‌طور یکنواخت به‌ازای $-\infty < t < +\infty$ ،

$$\lim_{\sigma \to +\infty} F(\sigma + it) = f(1) \cdot$$

برهان. چون $F(s) = f(1) + \sum_{n=2}^{\infty} f(n)n^{-s}$ ، فقط باید ثابت‌کرد که جملهٔ دوم ، وقتی $\sigma \to +\infty$ ، به 0 میل‌می‌کند . $c > \sigma_a$ رااختیارمی‌کنیم . دراین صورت ، به‌ازای $\sigma \geq c$ ، لم فوق ایجاب می‌کند که

$$\left|\sum_{n=2}^{\infty} \frac{f(n)}{n^s}\right| \leq 2^{-(\sigma-c)} \sum_{n=2}^{\infty} |f(n)| n^{-c} = \frac{A}{2^\sigma} ,$$

که‌درآن A مستقل از σ و t است . چون وقتی $\sigma \to +\infty$ ، $A/2^\sigma \to 0$ ، این قضیه را ثابت خواهد کرد .

چند مثال. وقتی $\sigma \to +\infty$ ، $\zeta(\sigma + it) \to 1$ و $L(\sigma + it, \chi) \to 1$.

حال ثابت می‌کنیم که همهٔ ضرایب به‌طور منحصر بفرد به‌وسیلهٔ تابع مجموع معین می‌شوند .

قضیهٔ ۳.۱۱ . قضیهٔ یکتایی. فرض‌کنیم

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \quad \text{و} \quad F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

هردو به‌ازای $\sigma > \sigma_a$ به‌طورمطلق همگرا باشند . هرگاه به‌ازای هر s در یک دنبالهٔ نامتناهی $\{s_k\}$ که وقتی $k \to \infty$ ، $\sigma_k \to +\infty$ ، داشته باشیم $F(s) = G(s)$ ، آنگاه به‌ازای هر n ، $f(n) = g(n)$.

برهان. فرض‌کنیم $h(n) = f(n) - g(n)$ و $H(s) = F(s) - G(s)$. دراین صورت ، به‌ازای هر k ، $H(s_k) = 0$. برای اثبات اینکه به‌ازای هر n ، $h(n) = 0$ ، فرض کنیم به‌ازای n ی $h(n) \neq 0$ ، و تناقض بدست می‌آوریم .

فرض‌کنیم N کوچکترین عدد صحیحی باشد که به‌ازای آن $h(n) \neq 0$. دراین‌صورت،

$$H(s) = \sum_{n=N}^{\infty} \frac{h(n)}{n^s} = \frac{h(N)}{N^s} + \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}.$$

لذا،

$$h(N) = N^s H(s) - N^s \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}.$$

با قرار دادن $s = s_k$ ، داریم $H(s_k) = 0$ ؛ درنتیجه،

$$h(N) = -N^{s_k} \sum_{n=N+1}^{\infty} h(n) n^{-s_k}.$$

k را طوری می‌گیریم که $\sigma_k > c$ ، که‌درآن $c > \sigma_a$. دراین صورت، لم ۱ ایجاب می‌کند که

$$|h(N)| \leq N^{\sigma_k}(N+1)^{-(\sigma_k - c)} \sum_{n=N+1}^{\infty} |h(n)| n^{-c} = \left(\frac{N}{N+1}\right)^{\sigma_k} A,$$

که‌درآن A مستقل‌از k است. با فرض $k \to \infty$ ، معلوم می‌شود که $(N/(N+1))^{\sigma_k} \to 0$ ؛ درنتیجه، $h(N) = 0$ ، که یک تناقض است.

قضیهٔ یکتایی وجود نیمصفحه‌ای‌را ایجاب می‌کند که در آن یک سری دیریکله صفر نمی‌شود (البته، مگر آنکه سری متحد صفر باشد).

قضیهٔ ۴۰۱۱ . فرض‌کنیم $F(s) = \sum f(n) n^{-s}$ و، به‌ازای s ی که $\sigma > \sigma_a$ ، $F(s) \neq 0$. دراین صورت، نیمصفحه‌ای مانند $\sigma > c \geq \sigma_a$ وجود دارد که درآن $F(s)$ هرگز صفر نمی‌شود.

برهان. فرض کنیم چنین نیمصفحه‌ای موجود نباشد. دراین صورت، به‌ازای هر $k = 1, 2, \ldots$ ، نقطه‌ای‌مانند s_k باخاصیت $\sigma_k > k$ هست بطوری که $F(s_k) = 0$. چون وقتی $k \to \infty$ ، $\sigma_k \to +\infty$ ، قضیهٔ یکتایی‌نشان می‌دهدکه به‌ازای هر n ، $f(n) = 0$ ، که فرض اینکه به‌ازای s ی $F(s) \neq 0$ را نقض می‌کند.

۴۰۱۱ ضرب سریهای دیریکله

قضیهٔ زیرحاصل ضرب سریهای دیریکله را با پیچش دیریکلهٔ ضرایب آنها پیوند می‌دهد.

قضیهٔ ۱۱‎.۵ . فرض‌کنیم دو تابع $F(s)$ و $G(s)$ با سریهای دیریکلهٔ زیر نمایش داده شده باشند :

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{،} \quad \sigma > a \text{ به‌ازای}$$

و

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \quad \text{،} \quad \sigma > b \text{ به‌ازای} .$$

دراین صورت ، در نیمصفحه‌ای که هردو سری به‌طور مطلق همگرایند ، داریم

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}, \tag{۵}$$

که در آن $h = f * g$ ، یعنی پیچش دیریکلهٔ f و g :

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

بعکس، هرگاه بـه‌ازای هر s در دنباله‌ای مانند $\{s_k\}$ که وقتی $k \to \infty$ ، $\sigma_k \to +\infty$ ، داشته باشیم $F(s)G(s) = \sum \alpha(n)n^{-s}$ ، آنگاه $\alpha = f * g$.

برهان. به‌ازای هر s که در آن هر دو سری به‌طور مطلق همگراست ، داریم

$$F(s)G(s) = \sum_{n=1}^{\infty} f(n)n^{-s} \sum_{m=1}^{\infty} g(m)m^{-s} = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} f(n)g(m)(mn)^{-s}.$$

بخاطر همگـرایی مطلق، می‌توان این سریها را درهم ضرب کرد و جملات را بدون تغییر مجموع هرطور کـه بخواهیم تغییر آرایش‌داد . جملات را طوری دسته‌بندی می‌کنیم که در هر دسته mn ثابت‌باشد ، مثلاً $mn = k$. مقادیرممکن برای k عبارتند از $1, 2, \ldots$ ؛ درنتیجه ،

$$F(s)G(s) = \sum_{k=1}^{\infty}\left(\sum_{mn=k} f(n)g(m)\right)k^{-s} = \sum_{k=1}^{\infty} h(k)k^{-s},$$

که در آن $h(k) = \sum_{mn=k} f(n)g(m) = (f * g)(k)$. این اولیـن حکم را ثابت می‌کند ، و حکم دوم از قضیهٔ یکتایی نتیجه می‌شود .

مثال ۱ . هردوسری $\sum n^{-s}$ و $\sum \mu(n)n^{-s}$ به‌ازای $\sigma > 1$ به‌طورمطلق‌همگرایند . بااختیار $f(n) = 1$ و $g(n) = \mu(n)$ در (۵) ، معلوم می‌شود که $h(n) = [1/n]$ ؛ درنتیجه ،

$$\text{اگر } \sigma > 1 \text{ ، } \zeta(s)\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = 1 .$$

بالاخص، این نشان می‌دهد که به‌ازای $\sigma > 1$ ، $\zeta(s) \neq 0$ ، و

$$\text{اگر } \sigma > 1 \text{ ، } \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)} .$$

مثال ۲ . بطورکلی، فرض کنیم $f(1) \neq 0$ و $g = f^{-1}$ ، یعنی معکوس دیریکله‌ٔ f . در این صورت ، در هر نیمصفحه که هر دو سری $F(s) = \sum f(n)n^{-s}$ و $G(s) = \sum g(n)n^{-s}$ به طور مطلق همگرایند ، داریم $F(s) \neq 0$ و $G(s) = 1/F(s)$.

مثال ۳ . فرض کنیم $F(s) = \sum f(n)n^{-s}$ به‌ازای $\sigma > \sigma_a$ به‌طور مطلق همگراباشد . اگر f کاملا" ضربی باشد ، داریم $f^{-1}(n) = \mu(n)f(n)$. چون $|f^{-1}(n)| \leq |f(n)|$ ، سری $\sum \mu(n)f(n)n^{-s}$ نیز به‌ازای $\sigma > \sigma_a$ به‌طور مطلق همگراست و داریم :

$$\text{اگر } \sigma > \sigma_a \text{ ، } \sum_{n=1}^{\infty}\frac{\mu(n)f(n)}{n^s} = \frac{1}{F(s)} .$$

بالاخص، به‌ازای هر مشخص دیریکله‌ٔ χ ، داریم :

$$\text{اگر } \sigma > 1 \text{ ، } \sum_{n=1}^{\infty}\frac{\mu(n)\chi(n)}{n^s} = \frac{1}{L(s,\chi)} .$$

مثال ۴ . فرض کنیم $f(n) = 1$ و $g(n) = \varphi(n)$ (کامل اویلر) . چون $\varphi(n) \leq n$ ، سری $\sum \varphi(n)n^{-s}$ به‌ازای $\sigma > 2$ به‌طور مطلق همگراست . همچنین ، $h(n) = \sum_{d|n}\varphi(d) = n$ ؛ درنتیجه، (۵) ایجاب می‌کند که

$$\text{اگر } \sigma > 2 \text{ ، } \zeta(s)\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s} = \sum_{n=1}^{\infty}\frac{n}{n^s} = \zeta(s-1) .$$

لذا،

$$\text{اگر } \sigma > 2 \text{ ، } \sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} .$$

مثال ۵. فرض کنیم $f(n) = 1$ و $g(n) = n^\alpha$. پس $h(n) = \sum_{d|n} d^\alpha = \sigma_\alpha(n)$ ، و (۵) نتیجه می‌دهد که

$$\zeta(s)\zeta(s-\alpha) = \sum_{n=1}^{\infty} \frac{\sigma_\alpha(n)}{n^s} \text{ ، } \sigma > \max\{1, 1+\operatorname{Re}(\alpha)\} \text{ اگر } .$$

مثال ۶. فرض کنیم $f(n) = 1$ و $g(n) = \lambda(n)$ (تابع لیوویل) . پس

$$h(n) = \sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{ ،} n = m^2 \text{ اگر به‌ازای } m \text{ ی} \\ 0 & \text{ ، درغیر این‌صورت} \end{cases}$$

لذا ، (۵) نتیجه می‌دهد که

$$\zeta(s)\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \sum_{\substack{n=1 \\ n = \text{مربع}}}^{\infty} \frac{1}{n^s} = \sum_{m=1}^{\infty} \frac{1}{m^{2s}} = \zeta(2s).$$

لذا ،

$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)} \text{ ، } \sigma > 1 \text{ اگر } .$$

۱۱.۵ حاصل ضربهای اویلر

قضیهٔ زیر ،که توسط اویلردر ۱۷۳۷ کشف شده ، گاهی صورت تحلیلی قضیهٔ اساسی حساب نامیده می‌شود .

قضیهٔ ۶.۱۱ . *فرض‌کنیم f یک تابع حسابی ضربی باشد بطوری‌که سری $\sum f(n)$ به‌طور مطلق‌همگرا ست . در این صورت ، مجموع سری را می‌توان به‌صورت یک حاصل ضرب‌نامتناهی به‌طور مطلق همگرایی بیان کرد :*

$$\sum_{n=1}^{\infty} f(n) = \prod_p \{1 + f(p) + f(p^2) + \cdots\}, \tag{۶}$$

که روی همهٔ اعداد اول گرفته شده‌است . اگر f کاملاً" ضربی باشد ، این حاصل ضرب ساده شده و خواهیم داشت

$$\sum_{n=1}^{\infty} f(n) = \prod_p \frac{1}{1-f(p)}. \tag{۷}$$

تذکر. در هر حالت، حاصل ضرب *حاصل ضرب اویلر* سری نامیده می‌شود.

برهان. حاصل ضرب متناهی

$$P(x) = \prod_{p \le x} \{1 + f(p) + f(p^2) + \cdots\}$$

را درنظر می‌گیریم، که روی همهٔ اعداد اول $p \le x$ گرفته شده است. چون این حاصل ضرب تعدادی متناهی سری به‌طور مطلق همگراست، می‌توان سریها را در هم ضرب کرده و جملات را بدون تغییر مجموع تجدید آرایش کرد. یک جملهٔ نوعی به شکل زیر است:

$$f(p_1^{a_1})f(p_2^{a_2}) \cdots f(p_r^{a_r}) = f(p_1^{a_1}p_2^{a_2} \cdots p_r^{a_r})$$

زیرا f ضربی است. طبق قضیهٔ اساسی حساب، می‌توان نوشت

$$P(x) = \sum_{n \in A} f(n),$$

که در آن A از n هایی تشکیل شده که همهٔ عوامل اولشان نابیشتر از x اند. بنابراین،

$$\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n \in B} f(n),$$

که‌درآن B مجموعهٔ n هایی‌است‌که‌دست‌کم یک‌عامل‌اول بزرگتر از x دارند. بنابراین،

$$\left| \sum_{n=1}^{\infty} f(n) - P(x) \right| \le \sum_{n \in B} |f(n)| \le \sum_{n > x} |f(n)|.$$

وقتی $x \to \infty$، آخرین مجموع سمت راست به 0 میل می‌کند، زیرا $\sum |f(n)|$ همگراست. لذا، وقتی $x \to \infty$، $P(x) \to \sum f(n)$.

اما یک حاصل ضرب نامتناهی به شکل $\prod (1 + a_n)$ به‌طور مطلق همگراست هروقت سری نظیر $\sum a_n$ به‌طور مطلق همگرا باشد. دراین حالت، داریم

$$\sum_{p \le x} |f(p) + f(p^2) + \cdots| \le \sum_{p \le x} (|f(p)| + |f(p^2)| + \cdots) \le \sum_{n=2}^{\infty} |f(n)|.$$

چون همهٔ مجموعهای جزئی کراندار هستند، سری با جملات مثبت

$$\sum_{p} |f(p) + f(p^2) + \cdots|$$

همگراست، و این همگرایی مطلق حاصل ضرب (۶) را ایجاب می‌کند.

بالاخره، وقتی f کاملاً ضربی باشد، داریم $f(p^n) = f(p)^n$ و هر سری سمت راست

(۶) یک سری هندسی همگرا با مجموع $(1 - f(p))^{-1}$ است .

با اعمال قضیهٔ ۶۰۱۱ بر سری دیریکلهٔ به‌طور مطلق همگرا ، فورا" خواهیم داشت

قضیهٔ ۷۰۱۱ . *فرض‌کنیم $\sum f(n)n^{-s}$ به‌ازای $\sigma > \sigma_a$ به‌طور مطلق همگرا باشد . هرگاه f ضربی باشد ، داریم :*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left\{1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\right\} \quad \text{،} \quad \sigma > \sigma_a \text{ اگر} \tag{۸}$$

و هرگاه f کاملا" ضربی باشد ، داریم

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \frac{1}{1 - f(p)p^{-s}} \quad \text{،} \quad \sigma > \sigma_a \text{ اگر} \ .$$

باید توجه داشت که‌جملهٔ عمومی حاصل ضرب (۸) سری بل $f_p(x)$ تابع f به‌ازای $x = p^{-s}$ است . (ر.ک. بخش ۱۶۰۲ .)

چند مثال. اگـر بترتیب $f(n)$ را 1 ، $\mu(n)$ ، $\varphi(n)$ ، $\sigma_\alpha(n)$ ، $\lambda(n)$ ، و $\chi(n)$ اختیار کنیم ، حاصل ضربهای اویلر زیر بدست خواهند آمد :

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}} \quad \text{،} \quad \sigma > 1 \text{ اگر}$$

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p (1 - p^{-s}) \quad \text{،} \quad \sigma > 1 \text{ اگر}$$

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \prod_p \frac{1 - p^{-s}}{1 - p^{1-s}} \quad \text{،} \quad \sigma > 2 \text{ اگر}$$

$$\zeta(s)\zeta(s-\alpha) = \sum_{n=1}^{\infty} \frac{\sigma_\alpha(n)}{n^s} = \prod_p \frac{1}{(1 - p^{-s})(1 - p^{\alpha-s})} \quad \text{،} \sigma > \max\{1, 1 + \mathrm{Re}(\alpha)\} \text{ اگر}$$

$$\frac{\zeta(2s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \prod_p \frac{1}{1+p^{-s}}$$ ، $\sigma > 1$ اگر

$$\cdot L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)p^{-s}}$$ ، $\sigma > 1$ اگر

تذکر. هرگاه $\chi = \chi_1$ ، یعنی مشخص اصلـی به هنگ k باشد، $\chi_1(p) = 0$ اگر $p|k$ و $\chi_1(p) = 1$ اگر $p \nmid k$ ؛ درنتیجه، حاصل ضرب اویلر برای $L(s, \chi_1)$ خواهد شد

$$L(s, \chi_1) = \prod_{p \nmid k} \frac{1}{1-p^{-s}} = \prod_p \frac{1}{1-p^{-s}} \cdot \prod_{p|k} (1-p^{-s}) = \zeta(s) \prod_{p|k} (1-p^{-s}).$$

لذا، L ـ تابع $L(s, \chi_1)$ مساوی تـابع زتای $\zeta(s)$ است که در تعدادی متناهی عامل ضرب شده است.

۱۱ . ۶ نیمصفحهٔ همگرایی یک سری دیریکله

برای اثبات وجود نیمصفحهٔ همگرایی، از لم زیر استفاده می‌کنیم.

لم ۲. فرض کنیـم $s_0 = \sigma_0 + it_0$ ، و سری دیـریکلهٔ $\sum f(n)n^{-s_0}$ دارای مجموعهای جزئی کراندار باشد؛ *مثلاً*، به‌ازای هر $x \geq 1$ ،

$$\left| \sum_{n \leq x} f(n)n^{-s_0} \right| \leq M \cdot$$

دراین صورت، به‌ازای هر s که $\sigma > \sigma_0$ ، داریم

$$\left| \sum_{a<n\leq b} f(n)n^{-s} \right| \leq 2Ma^{\sigma_0-\sigma}\left(1 + \frac{|s-s_0|}{\sigma-\sigma_0}\right). \tag{۹}$$

برهان. فـرض کنیـم $a(n) = f(n)n^{-s_0}$ و $A(x) = \sum_{n\leq x} a(n)$. درایـن صـورت، $f(n)n^{-s} = a(n)n^{s_0-s}$ ؛ درنتیجه، می‌توان با اعمال قضیهٔ ۲.۴ (به‌ازای $f(x) = x^{s_0-s}$) بدست آورد که

$$\sum_{a<n\leq b} f(n)n^{-s} = A(b)b^{s_0-s} - A(a)a^{s_0-s} + (s-s_0)\int_a^b A(t)t^{s_0-s-1}\,dt.$$

چون $|A(x)| \leq M$ ، این نتیجه می‌دهد که

$$\left|\sum_{a<n\le b} f(n)n^{-s}\right| \le Mb^{\sigma_0-\sigma} + Ma^{\sigma_0-\sigma} + |s-s_0|M\int_a^b t^{\sigma_0-\sigma-1}\,dt$$
$$\le 2Ma^{\sigma_0-\sigma} + |s-s_0|M\left|\frac{b^{\sigma_0-\sigma}-a^{\sigma_0-\sigma}}{\sigma_0-\sigma}\right|$$
$$\le 2Ma^{\sigma_0-\sigma}\left(1+\frac{|s-s_0|}{\sigma-\sigma_0}\right).$$

چند مثال. اگر مجموعهای جزئی $\sum_{n\le x} f(n)$ کراندار باشند، لم ۲ ایجاب می‌کند که $\sum f(n)n^{-s}$ به‌ازای $\sigma>0$ همگرا باشد. درواقع، اگردر (۹) اختیار کنیم $s_0=\sigma_0=0$، به‌ازای $\sigma>0$ خواهیم داشت

$$\left|\sum_{a<n\le b} f(n)n^{-s}\right| \le Ka^{-\sigma},$$

که در آن K مستقل از a است. با فرض $a\to+\infty$، معلوم می‌شود که اگر $\sigma>0$، $\sum f(n)n^{-s}$ همگراست. این، درحالت خاص، نشان می‌دهد که سری دیریکلهٔ

$$\sum_{n=1}^{\infty}\frac{(-1)^n}{n^s}$$

به‌ازای $\sigma>0$ همگراست، زیرا $|\sum_{n\le x}(-1)^n|\le 1$. بهمین نحو، اگر χ یک مشخص دیریکلهٔ غیر اصلی به هنگ k باشد، داریم $|\sum_{n\le x}\chi(n)|\le\varphi(k)$؛ درنتیجه،

$$\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

به‌ازای $\sigma>0$ همگراست. همین نوع استدلال قضیهٔ زیر را بدست می‌دهد.

قضیهٔ ۸.۱۱. *هرگاه سری $\sum f(n)n^{-s}$ به‌ازای $s=\sigma_0+it_0$ همگرا باشد، به‌ازای هر s که در آن $\sigma>\sigma_0$ نیز همگراست. هرگاه به‌ازای $s=\sigma_0+it_0$ واگرا باشد، به‌ازای هر s که در آن $\sigma<\sigma_0$ نیز واگراست.*

برهان. حکم دوم از حکم اول نتیجه می‌شود. برای اثبات حکم اول، s ی با $\sigma>\sigma_0$ اختیار می‌کنیم. لم ۲ نشان می‌دهد که

$$\left|\sum_{a<n\le b} f(n)n^{-s}\right| \le K a^{\sigma_0-\sigma},$$

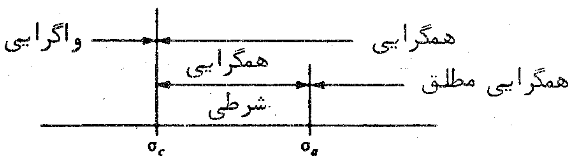
که در آن K مستقل از a است. چون وقتی $a \to +\infty$ ، $a^{\sigma_0-\sigma} \to 0$ ، شرط کشی نشان می‌دهد که $\sum f(n)n^{-s}$ همگرا می‌باشد.

قضیهٔ ۹.۱۱ . هرگاه سری $\sum f(n)n^{-s}$ هیچ جا همگرا یا هیچ جا واگرا نباشد، عددی حقیقی مانند σ_c ، به‌نام طول همگرایی، وجود دارد بطوری که سری به‌ازای هر s در نیمصفحهٔ $\sigma > \sigma_c$ همگرا است و به‌ازای هر s در نیمصفحهٔ $\sigma < \sigma_c$ واگرا می‌باشد.

برهان. مثل برهان قضیهٔ ۱.۱۱ استدلال کرده، σ_c را کوچکترین کران بالایی همهٔ σ هایی می‌گیریم که به‌ازای آنها $\sum f(n)n^{-s}$ واگراست.

تذکر. اگر سری همه‌جا همگرا باشد تعریف می‌کنیم $\sigma_c = -\infty$ ، واگر هیچ جا همگرا نباشد، تعریف می‌کنیم $\sigma_c = +\infty$.

چون همگرایی مطلق همگرایی را ایجاب می‌کند، همواره داریم $\sigma_a \ge \sigma_c$. اگر $\sigma_a > \sigma_c$ ، نواری نامتناهی مانند $\sigma_c < \sigma < \sigma_a$ هست که در آن سری به‌طور مشروط همگراست (ر.ک. شکل ۱.۱۱).



شکل ۱.۱۱

قضیهٔ زیر نشان می‌دهد که پهنای این نوار از 1 بیشتر نیست.

قضیهٔ ۱۰.۱۱ . به‌ازای هر سری دیریکله با σ_c متناهی، داریم

$$0 \le \sigma_a - \sigma_c \le 1.$$

برهان. کافی است نشان دهیم که اگر $\sum |f(n)n^{-s}|$ به‌ازای s_0 ای همگرا باشد، به‌ازای

هر s که در آن $\sigma > \sigma_0 + 1$ به‌طور مطلق همگراست. فرض کنیم A یک کران بالایی برای اعداد $|f(n)n^{-s_0}|$ باشد. دراین صورت،

$$\left|\frac{f(n)}{n^s}\right| = \left|\frac{f(n)}{n^{s_0}}\right| \left|\frac{1}{n^{s-s_0}}\right| \leq \frac{A}{n^{\sigma-\sigma_0}};$$

درنتیجه، $\sum f(n)n^{-s_0}$ در مقایسه با $\sum n^{\sigma_0-\sigma}$ همگراست.

مثال. سری

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$$

همگراست اگر $\sigma > 0$، ولی همگرایی فقط وقتی مطلق است که $\sigma > 1$. لذا، دراین‌مثال $\sigma_c = 0$ و $\sigma_a = 1$.

خواص همگرایی سریهای‌دیریکله را می‌توان با خواص همگرایی سریهای توانی مقایسه کرد. هرسری‌توانی دارای‌یک قرص همگرایی‌است، حال آنکه هر سری دیریکله یک‌نیمصفحهٔ همگرایی دارد. در سریهای توانی، درون قرص همگرایی قلمرو همگرایی مطلق نیز هست. در سریهای دیریکله، قلمرو همگرایی مطلق ممکن است زیرمجموعهٔ حقیقی قلمرو همگرایی باشد. هر سری توانی یک تابع تحلیلی را داخل قرص همگرایی خود نمایش می‌دهد. حال نشان می‌دهیم که هر سری دیریکله نمایش یک تابع تحلیلی در داخل نیمصفحهٔ همگرایی خود است.

۷.۱۱ خواص تحلیلی سریهای دیریکله

خواص تحلیلی سریهای دیریکله از قضیهٔ عمومی زیر در نظریهٔ توابع مختلط که ما آن را به‌صورت لم بیان می‌کنیم نتیجه می‌شوند.

لم ۳. *فرض کنیم $\{f_n\}$ دنباله‌ای‌ازتوابع باشد که بر زیرمجموعهٔ باز S از صفحهٔ مختلط تحلیلی‌اند، و $\{f_n\}$ بر هر زیر مجموعهٔ فشردهٔ S به‌طور یکنواخت به تابع حدی f همگرا باشد. دراین صورت، f بر S تحلیلی است و دنبالهٔ مشتقات $\{f'_n\}$ بر هر زیرمجموعهٔ فشرده از S به‌طور یکنواخت به مشتق f' همگرا می‌باشد.*

برهان. چون f_n بر S تحلیلی است، فرمول انتگرال کشی را داریم:

$$f_n(a) = \frac{1}{2\pi i}\int_{\partial D}\frac{f_n(z)}{z-a}\,dz ,$$

که در آن D یک قرص فشرده در S است، ∂D کرانهٔ جهتدار آن با جهت مثبت است، و a یک نقطهٔ درونی D می‌باشد. بخاطر همگرایی یکنواخت، می‌توان زیر علامت انتگرال به حد رفت و بدست آورد

$$f(a) = \frac{1}{2\pi i}\int_{\partial D}\frac{f(z)}{z-a}\,dz ,$$

که تحلیلی بودن f در داخل D را ایجاب می‌کند. برای مشتقها، داریم

$$f_n'(a) = \frac{1}{2\pi i}\int_{\partial D}\frac{f_n(z)}{(z-a)^2}\,dz \quad \text{و} \quad f'(a) = \frac{1}{2\pi i}\int_{\partial D}\frac{f(z)}{(z-a)^2}\,dz ,$$

که از آنها به‌آسانی نتیجه می‌شود که بر هر زیر مجموعهٔ فشرده از S، وقتی $n \to \infty$، به‌طور یکنواخت $f_n'(a) \to f'(a)$.

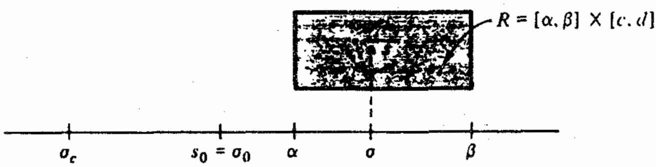
برای اعمال لم بر سریهای دیریکله، ابتدا نشان می‌دهیم که بر زیرمجموعه‌های فشردهٔ نیمصفحهٔ همگرایی همگرایی یکنواخت داریم.

قضیهٔ ۱۱۰۱۱ . سری دیریکلهٔ $\sum f(n)n^{-s}$ بر هر زیر مجموعهٔ فشردهٔ واقع در درون نیمصفحهٔ همگرایی $\sigma > \sigma_c$ به‌طور یکنواخت همگراست.

برهان. کافی است نشان دهیم که $\sum f(n)n^{-s}$ برهرمستطیل فشردهٔ $R = [\alpha, \beta] \times [c, d]$، که $\alpha > \sigma_c$، به‌طور یکنواخت همگراست. برای این کار، از تخمین حاصل از لم ۲ استفاده می‌کنیم:

$$\left|\sum_{a<n\le b} f(n)n^{-s}\right| \le 2Ma^{\sigma_0-\sigma}\left(1 + \frac{|s-s_0|}{\sigma-\sigma_0}\right), \tag{۱۰}$$

که در آن $s_0 = \sigma_0 + it_0$ نقطه‌ای در نیمصفحهٔ $\sigma > \sigma_c$ بوده و s نقطه‌ای با $\sigma > \sigma_0$



شکل ۲۰۱۱

می‌باشد. $s_0 = \sigma_0$ را اختیار می‌کنیم، که درآن $\sigma_c < \sigma_0 < \alpha$. (ر.ک. شکل ۱۱ ۰ ۲ ۰ .)
دراین صورت، اگر $s \in R$ ، داریم $\sigma - \sigma_0 \geq \alpha - \sigma_0$ و $|s_0 - s| < C$ ، که درآن C ثابتی است وابسته به s_0 و R ولی نه به s . پس (۱۰) ایجاب می‌کند که

$$\left|\sum_{a<n\leq b} f(n)n^{-s}\right| \leq 2Ma^{\sigma_0-\alpha}\left(1+\frac{C}{\alpha-\sigma_0}\right) = Ba^{\sigma_0-\alpha} ,$$

که درآن B مستقل از s است. چون وقتی $a \to +\infty$ ، $a^{\sigma_0-\alpha} \to 0$ ، شرط کشی برای همگرایی یکنواخت برقرار است.

قضیهٔ ۱۲.۱۱ . تابع مجموع $F(s) = \sum f(n)n^{-s}$ یک سری دیریکله درنیمصفحهٔ همگرایی $\sigma > \sigma_c$ تحلیلی است، و مشتقش $F'(s)$ در این نیمصفحه با سری دیریکلهٔ

$$F'(s) = -\sum_{n=1}^{\infty} \frac{f(n)\log n}{n^s} \tag{۱۱}$$

نمایش داده می‌شود، که از مشتقگیری جمله به جمله بدست می‌آید.

برهان. قضیهٔ ۱۱.۱۱ ولم ۳ را بر دنبالهٔ مجموعهای جزئی اعمال می‌کنیم.

چند تذکر. سری حاصل در (۱۱) همان طول همگرایی و همان طول همگرایی مطلق سری مربوط به $F(s)$ را دارد.

با اعمال مکرر قضیهٔ ۱۲.۱۱ ، معلوم می‌شود که مشتق k ام از رابطهٔ زیر بدست می‌آید:

$$\text{به‌ازای } \sigma > \sigma_c ، \quad F^{(k)}(s) = (-1)^k \sum_{n=1}^{\infty} \frac{f(n)(\log n)^k}{n^s} .$$

چند مثال. به‌ازای $\sigma > 1$ ، داریم

$$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s} \tag{۱۲}$$

و

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}. \tag{۱۳}$$

معادلهٔ (۱۲) با مشتقگیری جمله به جمله از سری مربوط به تابع زتا بدست می‌آید، و (۱۳) با ضرب دو سری دیریکلهٔ $\sum \Lambda(n)n^{-s}$ و $\sum n^{-s}$ و استفاده از اتحاد $\sum_{d|n} \Lambda(d) = \log n$ حاصل می‌شود.

۸.۱۱ سریهای دیریکله با ضرایب نامنفی

بعضی از توابع تعریف شده با سریهای دیریکله در نیمصفحهٔ همگرایی آنها $\sigma > \sigma_c$ را می‌توان به‌طور تحلیلی ورای خط $\sigma = \sigma_c$ ادامه داد. مثلاً، در فصل بعد نشان می‌دهیم که تابع زتای ریمان $\zeta(s)$ را می‌توان به‌طور تحلیلی ورای خط $\sigma = 1$ به تابعی ادامه داد که به‌ازای هر s جز یک قطب ساده در $s = 1$ تحلیلی باشد. بهمین نحو، اگر χ یک مشخص دیریکلهٔ غیر اصلی باشد، Lــ تابع $L(s, \chi)$ را می‌توان به‌طور تحلیلی ورای خط $\sigma = 1$ به یک تابع تمام (تحلیلی به‌ازای هر s) ادامه داد. انفراد برای تابع زتا به‌وسیلهٔ قضیهٔ زیر از لاندو توضیح داده می‌شود، که در باب سریهای دیریکله با ضرایب نامنفی می‌باشد.

قضیهٔ ۱۳.۱۱ . فرض کنیم $F(s)$ در نیمصفحهٔ $\sigma > c$ با سری دیریکلهٔ

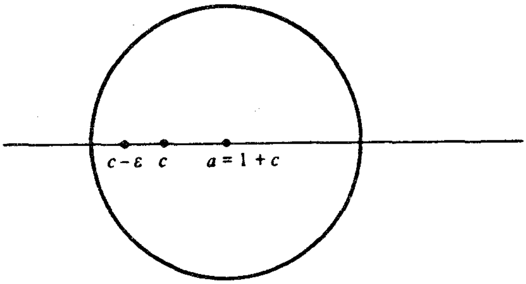
$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \tag{۱۴}$$

نمایش داده می‌شود، که در آن c متناهی است، و نیز به‌ازای هر $n \geq n_0$، $f(n) \geq 0$. هرگاه $F(s)$ در قرصی حول نقطهٔ $s = c$ تحلیلی باشد، سری دیریکله در نیمصفحهٔ $\sigma > c - \varepsilon$ به‌ازای $\varepsilon > 0$ ی همگراست. در نتیجه، هرگاه سری دیریکله طول همگرایی متناهی σ_c داشته باشد، $F(s)$ بر محور حقیقی در نقطهٔ $s = \sigma_c$ انفراد دارد.

برهان. فرض کنیم $a = 1 + c$. چون F در a تحلیلی است، می‌توان آن را با یک بسط به‌صورت سری توانی به‌طور مطلق همگرا حول a نمایش داد:

$$F(s) = \sum_{k=0}^{\infty} \frac{F^{(k)}(a)}{k!}(s-a)^k, \tag{۱۵}$$

و شعاع همگرایی این سری توانی از 1 متجاوز است، زیرا F در c تحلیلی است. (ر.ک. شکل ۳.۱۱). طبق قضیهٔ ۱۲.۱۱، مشتقات $F^{(k)}(a)$ را می‌توان با مشتقگیری مکرر از (۱۴) تعیین کرد. این نتیجه می‌دهد که



شکل ۳۰۱۱

$$F^{(k)}(a) = (-1)^k \sum_{n=1}^{\infty} f(n)(\log n)^k n^{-a};$$

درنتیجه، (۱۵) را می‌توان به‌صورت زیر نوشت:

$$F(s) = \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} \frac{(a-s)^k}{k!} f(n)(\log n)^k n^{-a}. \qquad (۱۶)$$

چون شعاع همگرایی‌از 1 متجاوزاست، این فرمول به‌ازای $s = c - \varepsilon$ ی حقیقی که $\varepsilon > 0$ معتبراست (ر.ک. شکل ۳۰۱۱). پس به‌ازای این s، $a - s = 1 + \varepsilon$، و سری‌مضاعف در (۱۶) دارای جملات نامنفی به‌ازای $n \geq n_0$ است. لذا، می‌توان ترتیب جمعبندی را عوض کرد و بدست آورد

$$F(c-\varepsilon) = \sum_{n=1}^{\infty} \frac{f(n)}{n^a} \sum_{k=0}^{\infty} \frac{\{(1+\varepsilon)\log n\}^k}{k!} = \sum_{n=1}^{\infty} \frac{f(n)}{n^a} e^{(1+\varepsilon)\log n} = \sum_{n=1}^{\infty} \frac{f(n)}{n^{c-\varepsilon}}.$$

به عبارت دیگر، سری دیریکلهٔ $\sum f(n)n^{-s}$ به‌ازای $s = c - \varepsilon$ همگراست؛ درنتیجه، در نیمصفحهٔ $\sigma > c - \varepsilon$ نیز همگرا می‌باشد.

۹۰۱۱ سریهای دیریکلهٔ بیان شده به صورت نماییهای سریهای دیریکله

یک سری‌دیریکلهٔ $F(s) = \sum f(n)n^{-s}$ که متحد صفر نباشد دارای نیمصفحه‌ای است که در آن هرگزصفرنمی‌شود. قضیهٔ بعد نشان می‌دهد که اگر $f(1) \neq 0$، $F(s)$ در این‌نیمصفحه نمایی سری دیریکلهٔ دیگری است.

قضیهٔ ۱۴۰۱۱ . فرض‌کنیم $F(s) = \sum f(n)n^{-s}$ به‌ازای $\sigma > \sigma_a$ به‌طور مطلق همگرا بوده و $f(1) \neq 0$. هرگاه به‌ازای $\sigma > \sigma_0 \geq \sigma_a$ ، $F(s) \neq 0$ ، آنگاه به‌ازای $\sigma > \sigma_0$ داریم

با

$$F(s) = e^{G(s)}$$

$$G(s) = \log f(1) + \sum_{n=2}^{\infty} \frac{(f' * f^{-1})(n)}{\log n} n^{-s},$$

که در آن f^{-1} معکوس دیریکلهٔ f بوده و $f'(n) = f(n)\log n$.

تذکر. به‌ازای $z \neq 0$ مختلط ، $\log z$ آن شاخهٔ لگاریتم است که وقتی $z > 0$ حقیقی است .

برهان. چون $F(s) \neq 0$ ، به‌ازای تابعی چون $G(s)$ که به‌ازای $\sigma > \sigma_0$ تحلیلی است ، می‌توان نوشت $F(s) = e^{G(s)}$. مشتقگیری نتیجه می‌دهد که

$$F'(s) = e^{G(s)}G'(s) = F(s)G'(s);$$

درنتیجه ، $G'(s) = F'(s)/F(s)$. اما

$$F'(s) = -\sum_{n=1}^{\infty} \frac{f(n)\log n}{n^s} = -\sum_{n=1}^{\infty} \frac{f'(n)}{n^s} \quad و \quad \frac{1}{F(s)} = \sum_{n=1}^{\infty} \frac{f^{-1}(n)}{n^s};$$

لذا ،

$$G'(s) = F'(s) \cdot \frac{1}{F(s)} = -\sum_{n=2}^{\infty} \frac{(f' * f^{-1})(n)}{n^s}.$$

انتگرالگیری نتیجه می‌دهد

$$G(s) = C + \sum_{n=2}^{\infty} \frac{(f' * f^{-1})(n)}{\log n} n^{-s},$$

که در آن C ثابت است . با فرض $\sigma \to +\infty$ ، درمی‌یابیم که $\lim_{\sigma \to \infty} G(\sigma + it) = C$ ؛ از اینرو ،

$$f(1) = \lim_{\sigma \to \infty} F(\sigma + it) = e^C;$$

درنتیجه ، $C = \log f(1)$. این برهان را تمام می‌کند . این برهان همچنین نشان می‌دهد که سری مربوط به $G(s)$ به‌ازای $\sigma > \sigma_0$ به‌طور مطلق همگراست .

مثال ۱. وقتی $f(n) = 1$ ، داریم $f'(n) = \log n$ و $f^{-1}(n) = \mu(n)$ ؛ درنتیجه ،

$$(f' * f^{-1})(n) = \sum_{d|n} \log d\mu\left(\frac{n}{d}\right) = \Lambda(n).$$

لذا، اگر $\sigma > 1$ ، داریم

$$\zeta(s) = e^{G(s)}, \tag{۱۷}$$

که در آن

$$G(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} n^{-s}.$$

مثال ۲. استدلال مشابهی نشان می‌دهد که اگر f کاملاً ضربی بوده و $F(s) = \sum f(n)n^{-s}$ ، در نیمصفحهٔ همگرایی مطلق $\sigma > \sigma_a$ داریم

$$F(s) = e^{G(s)},$$

که در آن

$$G(s) = \sum_{n=2}^{\infty} \frac{f(n)\Lambda(n)}{\log n} n^{-s}$$

زیرا $(f' * f^{-1})(n) = \sum_{d|n} f(d)\log d\mu(n/d)f(n/d) = f(n)\Lambda(n)$.

فرمولهای امثلهٔ پیش را می‌توان به‌کمک حاصل ضربهای اویلر نیز نتیجه گرفت. مثلاً، برای تابع زتای ریمان داریم

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

s را حقیقی و بزرگتر از 1 می‌گیریم؛ درنتیجه، $\zeta(s)$ مثبت است. با گرفتن لگاریتم و استفاده از سری توانی $-\log(1 - x) = \sum x^m/m$ ، معلوم می‌شود که

$$\log \zeta(s) = -\sum_p \log(1 - p^{-s}) = \sum_p \sum_{m=1}^{\infty} \frac{p^{-ms}}{m} = \sum_{n=1}^{\infty} \Lambda_1(n)n^{-s},$$

که در آن

$$\Lambda_1(n) = \begin{cases} \dfrac{1}{m} & \text{اگر به‌ازای عدد اولی چون } p \text{ ، } n = p^m \text{ ،} \\ 0 & \text{درغیر این‌صورت،} \end{cases}$$

اما اگر $n = p^m$ ، $\log n = m \log p = m\Lambda(n)$ ؛ درنتیجه، $1/m = \Lambda(n)/\log n$. بنابراین،

$$\log \zeta(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} n^{-s},$$

که (۱۷) را بــه‌ازای $s > 1$ حقیقی ایجــاب مــی‌کند . اما هر طرف (۱۷) در نیمصفحهٔ $\sigma > 1$ تحلیلی است ؛ درنتیجه ، بــا ادامــهٔ تحلیلی ، (۱۷) به‌ازای $\sigma > 1$ نیز برقرار است .

۱۰۰۱۱ فرمولهای مقدار میانگین برای سریهای دیریکله

قضیهٔ ۱۵۰۱۱ . *فرض کنیم دو سری دیریکلهٔ $F(s) = \sum f(n)n^{-s}$ و $G(s) = \sum g(n)n^{-s}$ بترتیب دارای طولهای همگرایی مطلق σ_1 و σ_2 باشند . دراین صورت ، به‌ازای $a > \sigma_1$ و $b > \sigma_2$ داریم*

$$\lim_{T\to\infty} \frac{1}{2T}\int_{-T}^{T} F(a+it)G(b-it)\,dt = \sum_{n=1}^{\infty} \frac{f(n)g(n)}{n^{a+b}}.$$

برهان . داریم

$$F(a+it)G(b-it) = \left(\sum_{m=1}^{\infty}\frac{f(m)}{m^{a+it}}\right)\left(\sum_{n=1}^{\infty}\frac{g(n)}{n^{b-it}}\right) = \sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\frac{f(m)g(n)}{m^a n^b}\left(\frac{n}{m}\right)^{it}$$
$$= \sum_{n=1}^{\infty}\frac{f(n)g(n)}{n^{a+b}} + \sum_{\substack{m=1\\ m\neq n}}^{\infty}\sum_{n=1}^{\infty}\frac{f(m)g(n)}{m^a n^b}\left(\frac{n}{m}\right)^{it}.$$

امــا

$$\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\left|\frac{f(m)g(n)}{m^a n^b}\left(\frac{n}{m}\right)^{it}\right| \le \sum_{m=1}^{\infty}\frac{|f(m)|}{m^a}\sum_{n=1}^{\infty}\frac{|g(n)|}{n^b};$$

درنتیجه ، سری به‌طورمطلق همگراست ، و این همگرایی به‌ازای هر t *یکنواخت* نیزهست . لذا ، می‌توان جمله به جمله انتگرال گرفت و بر $2T$ تقسیم کرد تا بدست آید که

$$\frac{1}{2T}\int_{-T}^{T} F(a+it)G(b-it)\,dt$$
$$= \sum_{n=1}^{\infty}\frac{f(n)g(n)}{n^{a+b}} + \sum_{\substack{m,n=1\\ m\neq n}}^{\infty}\frac{f(m)g(n)}{m^a n^b}\frac{1}{2T}\int_{-T}^{T} e^{it\log(n/m)}\,dt.$$

اما ، به‌ازای $m \neq n$ ، داریم

$$\int_{-T}^{T} e^{it\log(n/m)}\,dt = \frac{e^{it\log(n/m)}}{i\log(n/m)}\bigg|_{-T}^{T} = \frac{2\sin\left[T\log\left(\frac{n}{m}\right)\right]}{\log\left(\frac{n}{m}\right)};$$

درنتیجه، خواهیم داشت

$$\frac{1}{2T}\int_{-T}^{T} F(a+it)G(b-it)\,dt$$

$$= \sum_{n=1}^{\infty}\frac{f(n)g(n)}{n^{a+b}} + \sum_{\substack{m,n=1\\ m\neq n}}^{\infty}\frac{f(m)g(n)}{m^a n^b}\frac{\sin\left[T\log\left(\frac{n}{m}\right)\right]}{T\log\left(\frac{n}{m}\right)}.$$

مجدداً، سری مضاعف نسبت به T به‌طور یکنواخت همگراست، زیرا $(\sin x)/x$ به‌ازای‌هر x کراندار است. لذا، می‌توان جمله به جمله به حد رفت و حکم قضیه را بدست آورد.

قضیهٔ ۱۶.۱۱ . هرگاه $F(s)=\sum_{n=1}^{\infty} f(n)n^{-s}$ به‌طورمطلق‌به‌ازای $\sigma > \sigma_a$ همگرا باشد، آنگاه به‌ازای $\sigma > \sigma_a$ داریم

$$\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}|F(\sigma+it)|^2\,dt = \sum_{n=1}^{\infty}\frac{|f(n)|^2}{n^{2\sigma}}. \tag{۱۸}$$

بالاخص، اگر $\sigma > 1$ ، خواهیم داشت

(آ) $\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}|\zeta(\sigma+it)|^2\,dt = \sum_{n=1}^{\infty}\frac{1}{n^{2\sigma}} = \zeta(2\sigma)$ ؛

(ب) $\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}|\zeta^{(k)}(\sigma+it)|^2\,dt = \sum_{n=1}^{\infty}\frac{\log^{2k} n}{n^{2\sigma}} = \zeta^{(2k)}(2\sigma)$ ؛

(پ) $\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}|\zeta(\sigma+it)|^{-2}\,dt = \sum_{n=1}^{\infty}\frac{\mu^2(n)}{n^{2\sigma}} = \frac{\zeta(2\sigma)}{\zeta(4\sigma)}$ ؛

(ت) $\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}|\zeta(\sigma+it)|^4\,dt = \sum_{n=1}^{\infty}\frac{\sigma_0{}^2(n)}{n^{2\sigma}} = \frac{\zeta^4(2\sigma)}{\zeta(4\sigma)}$.

برهان. فرمول (۱۸) با فرض $g(n)=\overline{f(n)}$ در قضیهٔ ۱۵.۱۱ نتیجه می‌شود. برای اثبات فرمولهای‌خاص (آ) تا (ت) ، کافی است سری دیریکلهٔ $\sum |f(n)|^2 n^{-2\sigma}$ را به‌ازای انتخابهای‌زیر از $f(n)$ حساب کنیم : (آ) $f(n)=1$ ؛ (ب) $f(n)=(-1)^k\log^k n$ ؛ (پ) $f(n)=\mu(n)$ ؛ (ت) $f(n)=\sigma_0(n)$. فرمول (آ) واضح است، و فرمول (ب) از رابطهٔ زیر بدست می‌آید :

$$\zeta^{(k)}(s) = (-1)^k \sum_{n=1}^{\infty} \frac{\log^k n}{n^s}.$$

برای اثبات (پ) و (ت)، از حاصل ضربهای اویلر استفاده می‌کنیم. درمورد (پ)، داریم

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} = \prod_p (1 + p^{-s}) = \prod_p \frac{1 - p^{-2s}}{1 - p^{-s}} = \frac{\zeta(s)}{\zeta(2s)}.$$

از تعویض s با 2σ قسمت (پ) بدست می‌آید. در مورد (ت)، می‌نویسیم

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{\sigma_0{}^2(n)}{n^s} &= \prod_p \{1 + \sigma_0{}^2(p)p^{-s} + \sigma_0{}^2(p^2)p^{-2s} + \cdots\} \\ &= \prod_p \{1 + 2^2p^{-s} + 3^2p^{-2s} + \cdots\} \\ &= \prod_p \left\{\sum_{n=0}^{\infty}(n+1)^2p^{-ns}\right\} = \prod_p \frac{1 - p^{-2s}}{(1 - p^{-s})^4} = \frac{\zeta^4(s)}{\zeta(2s)},\end{aligned}$$

زیرا $\sum_{n=0}^{\infty} (n+1)^2x^n = \frac{x+1}{(x-1)^3} = \frac{1-x^2}{(1-x)^4}$. حال از تعویض s با 2σ قسمت (ت) بدست می‌آید.

۱۱۰۱۱ فرمول انتگرال برای ضرایب یک سری دیریکله

قضیهٔ ۱۷۰۱۱. فرض کنیم سری $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ به‌ازای $\sigma > \sigma_a$ به‌طور مطلق همگرا باشد. دراین صورت، به‌ازای $\sigma > \sigma_a$ و $x > 0$ داریم

$$\lim_{T\to\infty} \frac{1}{2T}\int_{-T}^{T} F(\sigma + it)x^{\sigma+it}\,dt = \begin{cases} f(n) & \text{، } x = n \text{ اگر} \\ 0 & \text{، درغیر این‌صورت} \end{cases}$$

برهان. به‌ازای $\sigma > \sigma_a$، داریم

$$\frac{1}{2T}\int_{-T}^{T} F(\sigma + it)x^{\sigma+it}\,dt = \frac{x^\sigma}{2T}\int_{-T}^{T}\sum_{n=1}^{\infty}\frac{f(n)}{n^\sigma}\left(\frac{x}{n}\right)^{it}dt \tag{۱۹}$$

$$= \frac{x^\sigma}{2T}\sum_{n=1}^{\infty}\frac{f(n)}{n^\sigma}\int_{-T}^{T} e^{it\log(x/n)}\,dt,$$

زیرا سری به‌ازای هر t در هر بازهٔ $[-T,T]$ به‌طور یکنواخت همگراست. اگر x عددی صحیح نباشد، به‌ازای هر n، $x/n \neq 1$، و داریم

$$\int_{-T}^{T} e^{it\log(x/n)}\,dt = \frac{2\sin\left[T\log\left(\frac{x}{n}\right)\right]}{\log\left(\frac{x}{n}\right)},$$

و سری خواهد شد

$$\frac{x^\sigma}{T}\sum_{n=1}^{\infty}\frac{f(n)}{n^\sigma}\frac{\sin\left[T\log\left(\frac{x}{n}\right)\right]}{\log\left(\frac{x}{n}\right)},$$

که‌وقتی $T\to\infty$ ، به 0 میل می‌کند . اما ، اگر x صحیح باشد ، مثلا" $x=k$ ، جمله‌ای در (۱۹) که در آن $n=k$ عبارت است از

$$\int_{-T}^{T}\left(\frac{x}{n}\right)^{it}dt = \int_{-T}^{T}\left(\frac{k}{k}\right)^{it}dt = \int_{-T}^{T}dt = 2T;$$

و درنتیجه ،

$$\frac{x^\sigma}{2T}\sum_{n=1}^{\infty}\frac{f(n)}{n^\sigma}\int_{-T}^{T}\left(\frac{x}{n}\right)^{it}dt = f(k) + \frac{k^\sigma}{2T}\sum_{\substack{n=1\\ n\neq k}}^{\infty}\frac{f(n)}{n^\sigma}\int_{-T}^{T}\left(\frac{k}{n}\right)^{it}dt.$$

همانطور که در قسمت اول استدلال نشان دادیم ، جملهٔ دوم وقتی $T\to\infty$ به 0 میل می‌کند .

۱۲۰۱۱ فرمول انتگرال برای مجموعهای جزئی یک سری دیریکله

دراین بخش فرمولی از پرون[1] برای بیان مجموعهای جزئی یک سری دیریکله به صورت انتگرالی از تابع مجموع بدست می‌آوریم . به یک لم درباب انتگرالهای کنتوری نیاز خواهیم داشت

لم ۴ . هرگاه $c>0$ ، آنگاه $\int_{c-\infty i}^{c+\infty i}$ یعنی $\lim_{T\to\infty}\int_{c-iT}^{c+iT}$. دراین صورت ، هرگاه a عدد حقیقی مثبتی باشد ،

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} a^z\frac{dz}{z} = \begin{cases} 1 & \text{اگر } a>1\text{ ،}\\ \frac{1}{2} & \text{اگر } a=1\text{ ،}\\ 0 & \text{اگر } 0<a<1\text{ ،}\end{cases}$$

بعلاوه ،

---

1. Perron

اگر $0 < a < 1$ ، $\left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT} a^z \frac{dz}{z}\right| \le \frac{a^c}{\pi T \log\left(\frac{1}{a}\right)}$ ؛ (۲۰)

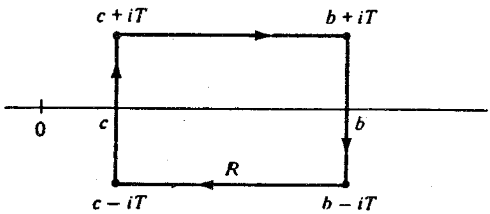
اگر $a > 1$ ، $\left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT} a^z \frac{dz}{z} - 1\right| \le \frac{a^c}{\pi T \log a}$ ؛ (۲۱)

و

اگر $a = 1$ ، $\left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{dz}{z} - \frac{1}{2}\right| \le \frac{c}{\pi T}$. (۲۲)

برهان. ابتدا فرض کنیم $0 < a < 1$ ، و کنتوری مستطیلی شکل R در شکل ۴۰۱۱ رادر نظر می‌گیریم . چون a^z/z داخل R تحلیلی است ، داریم $\int_R a^z/z\, dz = 0$. لذا ،

$$\int_{c-iT}^{c+iT} = \int_{b+iT}^{c+iT} + \int_{b-iT}^{b+iT} + \int_{c-iT}^{b-iT};$$



شکل ۴۰۱۱

درنتیجه ،

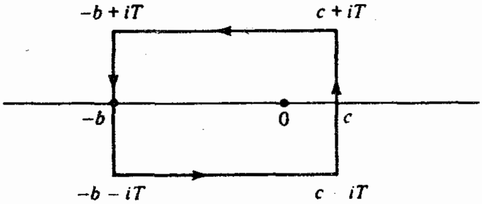
$$\left|\int_{c-iT}^{c+iT} a^z \frac{dz}{z}\right| \le \int_c^b \frac{a^x}{T}\, dx + \frac{2Ta^b}{b} + \int_c^b \frac{a^x}{T}\, dx$$
$$\le \frac{2}{T}\int_c^\infty a^x\, dx + \frac{2Ta^b}{b} = \frac{2}{T}\left(\frac{-a^c}{\log a}\right) + \frac{2Ta^b}{b}.$$

فرض کنیم $b \to \infty$. پس $a^b \to 0$ ؛ درنتیجه ،

$$\left|\int_{c-iT}^{c+iT} a^z \frac{dz}{z}\right| \le \frac{2a^c}{T \log\left(\frac{1}{a}\right)}.$$

این (۲۰) را ثابت می‌کند.

اگر $a > 1$ ، از کنتور R شکل ۵.۱۱ استفاده می‌کنیم. در اینجا $b > c > 0$ و



شکل ۵.۱۱

$T > c$. اما a^z/z در $z = 0$ قطب مرتبهٔ اول با ماندهٔ 1 دارد، زیرا وقتی $z \to 0$ ، $a^z = e^{z \log a} = 1 + z \log a + O(|z|^2)$.

لذا،

$$2\pi i = \left(\int_{c-iT}^{c+iT} + \int_{c+iT}^{-b+iT} + \int_{-b+iT}^{-b-iT} + \int_{-b-iT}^{c-iT}\right) a^z \frac{dz}{z};$$

درنتیجه،

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} a^z \frac{dz}{z} - 1 = \frac{1}{2\pi i}\left(\int_{-b+iT}^{c+iT} + \int_{-b-iT}^{-b+iT} + \int_{c-iT}^{-b-iT}\right) a^z \frac{dz}{z}.$$

حال انتگرالهای سمت راست را تخمین می‌زنیم. داریم

$$\left|\int_{-b+iT}^{c+iT} a^z \frac{dz}{z}\right| \le \int_{-b}^{c} \frac{a^x\,dx}{T} \le \frac{1}{T}\int_{-\infty}^{c} a^x\,dx = \frac{1}{T}\frac{a^c}{\log a},$$

$$\left|\int_{-b-iT}^{-b+iT} a^z \frac{dz}{z}\right| \le 2T\frac{a^{-b}}{b},$$

$$\left|\int_{c-iT}^{-b-iT} a^z \frac{dz}{z}\right| \le \int_{-b}^{c} \frac{a^x\,dx}{T} \le \frac{1}{T}\frac{a^c}{\log a}.$$

وقتی $b \to \infty$ ، انتگرال دوم به 0 میل می‌کند و (۲۱) بدست می‌آید.

وقتی $a = 1$ ، می‌توان مستقیماً به انتگرال پرداخت. داریم

$$\int_{c-iT}^{c+iT} \frac{dz}{z} = \int_{-T}^{T} \frac{i\,dy}{c+iy} = \int_{-T}^{T} \frac{y}{c^2+y^2}\,dy + ic\int_{-T}^{T} \frac{dy}{c^2+y^2}$$

$$= 2ic\int_{0}^{T} \frac{dy}{c^2+y^2},$$

و انتگرال دیگر صفر است ، زیرا انتگرالده یک تابع فرد است . لذا ،

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\frac{dz}{z}=\frac{c}{\pi}\int_0^T\frac{dy}{c^2+y^2}=\frac{1}{\pi}\arctan\frac{T}{c}=\frac{1}{2}-\frac{1}{\pi}\arctan\frac{c}{T}.$$

چون $\arctan\ c/T < c/T$، این (۲۲) را ثابت می‌کند ، و برهان لم ۴ تمام خواهد بود .

قضیهٔ ۱۸۰۱۱ . فرمول پرون . فرض‌کنیم $F(s)=\sum_{n=1}^{\infty} f(n)/n^s$ **به‌ازای** $\sigma > \sigma_a$ **به‌طور مطلق همگرا بوده ، و** $c > 0; x > 0$ **دلخواه باشند . دراین صورت ، اگر** $\sigma > \sigma_a - c$ ، **داریم**

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}F(s+z)\frac{x^z}{z}\,dz=\sum_{n\le x}{}^{*}\frac{f(n)}{n^s},$$

که درآن $\sum^*$ **یعنی ، وقتی** x **صحیح باشد ، آخرین جمله در مجموع باید در** $1/2$ **ضرب شود .**

برهان . درانتگرال ، c قسمت حقیقی z است ؛ درنتیجه ، سری مربوط به $F(s+z)$ بر زیر مجموعه‌های فشرده‌ازنیمصفحهٔ $\sigma + c > \sigma_a$ به‌طور مطلق و به‌طور یکنواخت همگراست . بنابراین ،

$$\begin{aligned}\int_{c-iT}^{c+iT}F(s+z)\frac{x^z}{z}\,dz&=\int_{c-iT}^{c+iT}\sum_{n=1}^{\infty}\frac{f(n)}{n^{s+z}}\frac{x^z}{z}\,dz\\&=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^z\frac{dz}{z}\\&=\sum_{n<x}\frac{f(n)}{n^s}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^z\frac{dz}{z}+\sum_{n>x}\frac{f(n)}{n^s}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^z\frac{dz}{z}\\&\quad+'\frac{f(x)}{x^s}\int_{c-iT}^{c+iT}\frac{dz}{z},\end{aligned}$$

که درآن علامت $+'$ نشان می‌دهد که آخرین جمله فقط وقتی ظاهر می‌شود که x صحیح باشد . درمجموع متناهی $\sum_{n<x}$ می‌توان جمله به جمله به حد $T\to\infty$ رفت ، و انتگرال ، طبق لم ۴ ، مساوی $2\pi i$ است . (دراینجا $a = x/n, a > 1$.) آخرین جمله (در صورت ظاهر شدن) $\pi i f(x)x^{-s}$ را بدست می‌دهد ، و اگر نشان دهیم

$$\lim_{T\to\infty}\sum_{n>x}\frac{f(n)}{n^s}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^z\frac{dz}{z}=0, \qquad (۲۳)$$

قضیه ثابت خواهد شد. می‌دانیم کـه اگر $n > x$ ، $\int_{c-i\infty}^{c+i\infty}(x/n)^z(dz/z) = 0$ ، ولی برای اثبات (۲۳) باید میزان تمایل $\int_{c-iT}^{c+iT}$ به صفر را تخمین بزنیم.

از لم ۴ تخمین زیر را داریم:

$$\left|\int_{c-iT}^{c+iT}a^z\frac{dz}{z}\right|\le\frac{2}{T}\frac{a^c}{\left(\log\frac{1}{a}\right)} \text{ ، } 0<a<1 \text{ اگر}$$

در اینجـــا $a = x/n$ بـــا $n > x$. در واقـــع ، $n \geq [x]+1$ ؛ درنتیجـــــه ، $1/a = n/x \geq ([x]+1)/x$. از اینرو، وقتی $T\to\infty$ ،

$$\left|\sum_{n>x}\frac{f(n)}{n^s}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^z\frac{dz}{z}\right|\le\sum_{n>x}\frac{|f(n)|}{n^\sigma}\frac{2}{T}\left(\frac{x}{n}\right)^c\frac{1}{\log\left(\frac{[x]+1}{x}\right)}$$

$$=\frac{2}{T}\frac{x^c}{\log\left(\frac{[x]+1}{x}\right)}\sum_{n>x}\frac{|f(n)|}{n^{\sigma+c}}\to 0 \;.$$

این فرمول پرون را ثابت می‌کند.

تذکر. اگر $c > \sigma_a$ ، فرمول‌پرون به‌ازای $s = 0$ معتبر است، و نمایش انتگرالی زیربرای مجموعهای جزئی ضرایب بدست می‌آید:

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}F(z)\frac{x^z}{z}\,dz=\sum_{n\le x}{}^{*} f(n).$$

تمرین برای فصل ۱۱

۱. اتحادهای زیر را بدست آورید، که به‌ازای $\sigma > 1$ معتبرند:

(آ) $\zeta(s) = s\int_1^\infty \frac{[x]}{x^{s+1}}\,dx$ ؛

(ب) $\sum_p \frac{1}{p^s} = s\int_1^\infty \frac{\pi(x)}{x^{s+1}}dx$ ، که درآن مجموع روی تمام اعداد اول گرفته‌شده‌است ؛

(پ) $\frac{1}{\zeta(s)} = s\int_1^\infty \frac{M(x)}{x^{s+1}}dx$ ، که درآن $M(x) = \sum_{n\le x}\mu(n)$ ؛

(ت) $-\frac{\zeta'(s)}{\zeta(s)} = s\int_1^\infty \frac{\psi(x)}{x^{s+1}}dx$ ، که درآن $\psi(x) = \sum_{n\le x}\Lambda(n)$ ؛

(ث) $L(s,\chi) = s\int_1^\infty \frac{A(x)}{x^{s+1}}dx$ ، که درآن $A(x) = \sum_{n\le x}\chi(n)$.

نشان دهید که اگر χ یک مشخص غیراصلی باشد ، (ث) به‌ازای $\sigma > 0$ نیز معتبر است . [**راهنمایی .** قضیهٔ ۲.۴ .]

۲ . فرض کنید سری $\sum_{n=1}^\infty f(n)$ همگرا با مجموع A بوده ، و $A(x) = \sum_{n\le x} f(n)$.

(آ) ثابت کنید سری دیریکلهٔ $F(s) = \sum_{n=1}^\infty f(n)n^{-s}$ به‌ازای هر s همگراست با $\sigma > 0$ و

$$\sum_{n=1}^\infty \frac{f(n)}{n^s} = A - s\int_1^\infty \frac{R(x)}{x^{s+1}}dx,$$

که درآن $R(x) = A - A(x)$. [**راهنمایی .** قضیهٔ ۲.۴ .]

(ب) نتیجه بگیرید که وقتی $\sigma \to 0+$ ، $F(\sigma) \to A$.

(پ) اگر $\sigma > 0$ و $N \ge 1$ صحیح باشد ، ثابت کنید

$$F(s) = \sum_{n=1}^N \frac{f(n)}{n^s} - \frac{A(N)}{N^s} + s\int_N^\infty \frac{A(y)}{y^{s+1}}dy.$$

(ت) بنویسید $s = \sigma + it$ ، در قسمت (پ) $N = 1 + [|t|]$ را اختیار کنید ، و نشان دهید که

اگر $0 < \sigma < 1$ ، $|F(\sigma + it)| = O(|t|^{1-\sigma})$.

۳ . (آ) ثابت کنید که اگر $t \ne 0$ ، سری $\sum n^{-1-it}$ دارای مجموعهای جزئی کراندار است . وقتی $t = 0$ ، مجموعهای جزئی بی‌کران می‌باشند .

(ب) ثابت‌کنید سری $\sum n^{-1-it}$ به‌ازای هر t حقیقی واگراست . به عبارت‌دیگر ، سری دیریکلهٔ مربوط به $\zeta(s)$ همه‌جا بر خط $\sigma = 1$ واگراست .

۴ . فرض کنید $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ ، که در آن $f(n)$ کاملا" ضربی بوده و سری به‌ازای $\sigma > \sigma_a$ به‌طور مطلق همگراست . ثابت کنید که اگر $\sigma > \sigma_a$ ، داریم

$$\frac{F'(s)}{F(s)} = -\sum_{n=1}^{\infty} \frac{f(n)\Lambda(n)}{n^s}.$$

در تمرینهای زیر ، $\lambda(n)$ تابع لیوویل بوده ، $d(n)$ تعداد مقسوم علیه‌های n است ، و $\nu(n)$ و $\kappa(n)$ به صورت زیر تعریف می‌شوند : $\nu(1) = 0,\ \kappa(1) = 1$ ؛ اگر $n = p_1^{a_1} \cdots p_k^{a_k}$ ، $\nu(n) = k$ و $\kappa(n) = a_1 a_2 \cdots a_k$.

ثابت کنید اتحادهای تمرینهای ۵ تا ۱۰ به‌ازای $\sigma > 1$ معتبرند .

۵ . $\sum_{n=1}^{\infty} \frac{d(n^2)}{n^s} = \frac{\zeta^3(s)}{\zeta(2s)}$.

۶ . $\sum_{n=1}^{\infty} \frac{\nu(n)}{n^s} = \zeta(s) \sum_p \frac{1}{p^s}$.

۷ . $\sum_{n=1}^{\infty} \frac{2^{\nu(n)}}{n^s} = \frac{\zeta^2(s)}{\zeta(2s)}$.

۸ . $\sum_{n=1}^{\infty} \frac{2^{\nu(n)}\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta^2(s)}$.

۹ . $\sum_{n=1}^{\infty} \frac{\kappa(n)}{n^s} = \frac{\zeta(s)\zeta(2s)\zeta(3s)}{\zeta(6s)}$.

۱۰ . $\sum_{n=1}^{\infty} \frac{3^{\nu(n)}\kappa(n)}{n^s} = \frac{\zeta^3(s)}{\zeta(3s)}$.

۱۱ . مجموع سری $\sum_{n=1}^{\infty} 3^{\nu(n)}\kappa(n)\lambda(n)n^{-s}$ را برحسب تابع زتای ریمان بیان کنید .

۱۲ . فرض کنید f یک تابع کاملا" ضربی باشد بطوری که به‌ازای هر عدد اول p ، $f(p) = f(p)^2$. اگر سری $\sum f(n)n^{-s}$ به‌ازای $\sigma > \sigma_a$ به‌طور مطلق همگرا بوده و دارای مجموع $F(s)$ باشد ، ثابت کنید $F(s) \neq 0$ و ، اگر $\sigma > \sigma_a$ ،

$$\sum_{n=1}^{\infty} \frac{f(n)\lambda(n)}{n^s} = \frac{F(2s)}{F(s)}.$$

۱۳ . فرض کنید f یک تابع ضربی باشد بطوری که به‌ازای هر عدد اول p ، $f(p) = f(p)^2$. اگر سری $\sum \mu(n)f(n)n^{-s}$ به‌ازای $\sigma > \sigma_a$ به‌طور مطلق همگرا بوده و دارای مجموع $F(s)$ باشد ، ثابت کنید $F(s) \neq 0$ و ، اگر $\sigma > \sigma_a$ ،

$$\sum_{n=1}^{\infty} \frac{f(n)|\mu(n)|}{n^s} = \frac{F(2s)}{F(s)}.$$

۱۴ . فرض کنید f یک تابع ضربی باشد بطوری که $\sum f(n)n^{-s}$ به‌ازای $\sigma > \sigma_a$ به‌طور مطلق همگراست . اگر p اول بوده و $\sigma > \sigma_a$ ، ثابت کنید

$$(1+f(p)p^{-s})\sum_{n=1}^{\infty}\frac{f(n)\mu(n)}{n^s}=(1-f(p)p^{-s})\sum_{n=1}^{\infty}\frac{f(n)\mu(n)\mu(p,n)}{n^s},$$

که در آن $\mu(p,n)$ تابع موبیوس است که در بمعم p و n حساب شده است.

[**راهنمایی.** حاصل ضربهای اویلر.]

۱۵ . ثابت کنید

$$\sum_{\substack{m=1\\(m,n)=1}}^{\infty}\sum_{n=1}^{\infty}\frac{1}{m^2n^2}=\frac{\zeta^2(2)}{\zeta(4)}.$$

بطور کلی، اگر هر s_i دارای جزء حقیقی $\sigma_i > 1$ باشد، مجموع چندگانهٔ

$$\sum_{\substack{m_1=1\\(m_1,\ldots,m_r)=1}}^{\infty}\cdots\sum_{m_r=1}^{\infty}m_1^{-s_1}\cdots m_r^{-s_r}$$

را برحسب تابع زتای ریمان بیان نمایید.

۱۶ . انتگرالهای به شکل

$$f(s)=\int_1^{\infty}\frac{A(x)}{x^s}\,dx, \qquad (۲۴)$$

که در آن $A(x)$ برهربازهٔ فشردهٔ $[1,a]$ انتگرال ریمان دارد، خواصی دارند شبیه خواص سریهای دیریکله. مثلا"، دارای نیمصفحهٔ همگرایی مطلق $\sigma > \sigma_a$ و نیمصفحهٔ همگرایی $\sigma > \sigma_c$ اند که در آن $f(s)$ تحلیلی است. این تمرین مشابهی از قضیهٔ ۱۱.۱۳ را توصیف می‌کند (قضیهٔ لاندو). فرض کنید $f(s)$ در نیمصفحهٔ $\sigma > \sigma_c$ با (۲۴) نمایش داده‌شده باشد، که در آن σ_c متناهی است، و نیز $A(x)$ حقیقی بوده و به‌ازای $x \geq x_0$ تغییر علامت ندهد. ثابت کنید $f(s)$ بر محور حقیقی در نقطهٔ $s=\sigma_c$ انفراد دارد.

۱۷ . فرض کنید $\lambda_a(n)=\sum_{d|n}d^a\lambda(d)$، که در آن $\lambda(n)$ تابع لیوویل است. ثابت کنید که اگر $\sigma > \max\{1, \mathrm{Re}(a)+1\}$، داریم

$$\sum_{n=1}^{\infty}\frac{\lambda(n)\lambda_a(n)}{n^s}=\frac{\zeta(2s)\zeta(s-a)}{\zeta(s)}$$

و

$$\sum_{n=1}^{\infty}\frac{\lambda_a(n)}{n^s}=\frac{\zeta(s)\zeta(2s-2a)}{\zeta(s-a)}.$$

۱۲ توابع $\zeta(s)$ و $L(s, \chi)$

۱.۱۲ مقدمه

دراین فصل چند خاصیت تابع زتای ریمان $\zeta(s)$ و L ـ توابع دیریکلهٔ $L(s, \chi)$ که به‌ازای $\sigma > 1$ با سریهای

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad \text{و} \quad \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

تعریف شده‌اند را مطرح می‌کنیم. همانند فصل اخیر، می‌نویسیم $s = \sigma + it$. بحث $\zeta(s)$ و $L(s, \chi)$ را می‌توان با معرفی تابع زتای هرویتس[1] $\zeta(s, a)$، که به‌ازای $\sigma > 1$ با سری

$$\zeta(s, a) = \sum_{n=0}^{\infty} \frac{1}{(n+a)^s}$$

تعریف‌شده، یک کاسه کرد. در اینجا a یک عدد حقیقی ثابت بوده و $0 < a \le 1$. وقتی $a = 1$، این بـه تابع زتای ریمان تحویل می‌شود، $\zeta(s) = \zeta(s, 1)$. همچنین، می‌توان $L(s, \chi)$ را برحسب توابع زتای هرویتس بیان کرد. اگر χ یک مشخص به هنگ k باشد، جملات سری مربوط‌به $L(s, \chi)$ را برطبق ردهٔ مانده‌ای به هنگ k تجدید آرایش می‌کنیم. یعنی، می‌نویسیم

$n = qk + r$، که در آن $1 \le r \le k$ و $q = 0, 1, 2, \ldots$

و بدست می‌آوریم

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{r=1}^{k} \sum_{q=0}^{\infty} \frac{\chi(qk+r)}{(qk+r)^s} = \frac{1}{k^s} \sum_{r=1}^{k} \chi(r) \sum_{q=0}^{\infty} \frac{1}{\left(q + \frac{r}{k}\right)^s}$$

---

1. Hurwitz

$$= k^{-s} \sum_{r=1}^{k} \chi(r)\zeta\left(s, \frac{r}{k}\right).$$

این نمایش $L(s, \chi)$ به صورت ترکیبی خطی از توابع زتای هرویتس نشان می‌دهد که خواص L ـ توابع مآلا " به خواص $\zeta(s, a)$ وابسته‌اند.

اولین هدف بدست آوردن ادامهٔ تحلیلی $\zeta(s, a)$ ورای خط $\sigma = 1$ است. این عمل با یک نمایش انتگرالی برای $\zeta(s, a)$ انجام می‌شود که از فرمول انتگرالی برای تابع گامای $\Gamma(s)$ بدست می‌آید.

۲.۱۲ خواص تابع گاما

سراسر این فصل به چند خاصیت اساسی تابع گامای $\Gamma(s)$ نیاز داریم. برای تسهیل مراجعه، این خواص را در اینجا ذکر می‌کنیم، گرچه همهٔ آنها مورد حاجت نیستند. برهانهای آنها را می‌توان در اکثر کتب درسی در نظریهٔ توابع مختلط یافت.

به‌ازای $\sigma > 0$، نمایش انتگرالی زیر را داریم:

$$\Gamma(s) = \int_0^\infty x^{s-1} e^{-x}\, dx. \qquad (۱)$$

تابعی که به‌این طریق به‌ازای $\sigma > 0$ تعریف شود را می‌توان ورای خط $\sigma = 0$ ادامه داد، و $\Gamma(s)$ به‌عنوان تابعی که همه‌جا در صفحهٔ s جز در نقاط سادهٔ

$$s = 0, -1, -2, -3, \ldots,$$

با مانده $(-1)^n/n!$ در $s = -n$، تحلیلی است وجود دارد. همچنین، نمایش زیر را داریم:

$$\Gamma(s) = \lim_{n\to\infty} \frac{n^s n!}{s(s+1)\cdots(s+n)}$$ ، به‌ازای $s \neq 0, -1, -2, \ldots$ ،

و فرمول حاصل ضربی زیر:

$$\frac{1}{\Gamma(s)} = s e^{Cs} \prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right) e^{-s/n}$$ ، به‌ازای هر s ،

که در آن C ثابت اویلر است. چون این حاصل ضرب به‌ازای هر s همگراست، $\Gamma(s)$ هرگز صفر نیست. تابع گاما در دو معادلهٔ تابعی زیر صدق می‌کند:

$$\Gamma(s+1) = s\Gamma(s) \qquad (۲)$$

و

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}, \tag{۳}$$

که به‌ازای هر s معتبرند ، و فرمول ضرب

$$\Gamma(s)\Gamma\left(s+\frac{1}{m}\right)\cdots\Gamma\left(s+\frac{m-1}{m}\right) = (2\pi)^{(m-1)/2} m^{(1/2)-ms}\Gamma(ms), \tag{۴}$$

که به‌ازای هر s و هر عدد صحیح $m \geq 1$ معتبر است .

ما ازنمایش انتگرالی (۱) ، معادلات تابعی (۲) و (۳) ، و موجودیت $\Gamma(s)$ درتمام صفحه باقطبهای ساده‌دراعداد صحیح $s = 0, -1, -2, \ldots$ استفاده می‌کنیم . همچنین ، توجه می‌کنیم که اگر n عدد صحیح نامنفیی باشد ، $\Gamma(n+1) = n!$.

۳۰۱۲ نمایش انتگرالی برای تابع زتای هرویتس

تابع زتای هرویتس $\zeta(s, a)$ اساسا" به‌ازای $\sigma > 1$ با سری

$$\zeta(s, a) = \sum_{n=0}^{\infty} \frac{1}{(n+a)^s}$$

تعریف شده است .

قضیهٔ ۱۰۱۲ . سری مربوط‌به $\zeta(s, a)$ به‌ازای $\sigma > 1$ به‌طور مطلق همگرا است . همگرایی درهرنیمصفحهٔ $\sigma \geq 1 + \delta, \delta > 0$ یکنواخت است؛ درنتیجه ، $\zeta(s, a)$ یک تابع تحلیلی از s در نیمصفحهٔ $\sigma > 1$ می‌باشد .

برهان . همهٔ این احکام از نامساویهای زیر نتیجه می‌شوند :

$$\sum_{n=1}^{\infty} |(n+a)^{-s}| = \sum_{n=1}^{\infty} (n+a)^{-\sigma} \leq \sum_{n=1}^{\infty} (n+a)^{-(1+\delta)}.$$

قضیهٔ ۲۰۱۲ . به‌ازای $\sigma > 1$ ، نمایش انتگرالی زیر را داریم :

$$\Gamma(s)\zeta(s, a) = \int_0^{\infty} \frac{x^{s-1}e^{-ax}}{1-e^{-x}}\, dx. \tag{۵}$$

بویژه ، وقتی $a = 1$ ، خواهیم داشت

$$\Gamma(s)\zeta(s) = \int_0^{\infty} \frac{x^{s-1}e^{-x}}{1-e^{-x}}\, dx.$$

برهان. ابتدا s را حقیقی و بزرگتر از یک می‌گیریم، و بعد نتیجه را با ادامهٔ تحلیلی به s مختلط تعمیم می‌دهیم.

در انتگرال مربوط به $\Gamma(s)$ تغییر متغیر $x = (n+a)t$، که $n \geq 0$، می‌دهیم تا بدست آید

$$\Gamma(s) = \int_0^\infty e^{-x}x^{s-1}\,dx = (n+a)^s \int_0^\infty e^{-(n+a)t}t^{s-1}\,dt,$$

یا

$$(n+a)^{-s}\Gamma(s) = \int_0^\infty e^{-nt}e^{-at}t^{s-1}\,dt.$$

با جمعبندی روی همهٔ $n \geq 0$ ها، معلوم می‌شود که

$$\zeta(s,a)\Gamma(s) = \sum_{n=0}^{\infty}\int_0^\infty e^{-nt}e^{-at}t^{s-1}\,dt,$$

که در آن سری سمت راست به‌ازای $\sigma > 1$ همگراست. حال می‌خواهیم مجموع و انتگرال را با هم عوض کنیم. ساده‌ترین راه توجیه این امر گرفتن انتگرال به‌عنوان یک انتگرال لبگ[1] است. چون انتگرالده نامنفی است، قضیهٔ همگرایی لوی[2] (قضیهٔ ۱۰.۲۵ در کتاب مرجع [۲]) می‌گوید که سری

$$\sum_{n=0}^{\infty} e^{-nt}e^{-at}t^{s-1}$$

تقریبا" همه‌جا به یک تابع مجموع که بر $[0, +\infty)$ انتگرال لبگ دارد همگراست و

$$\zeta(s,a)\Gamma(s) = \sum_{n=0}^{\infty}\int_0^\infty e^{-nt}e^{-at}t^{s-1}\,dt = \int_0^\infty \sum_{n=0}^{\infty} e^{-nt}e^{-at}t^{s-1}\,dt.$$

اما اگر $t > 0$، داریم $0 < e^{-t} < 1$؛ و درنتیجه،

$$\sum_{n=0}^{\infty} e^{-nt} = \frac{1}{1-e^{-t}},$$

زیرا سری یک سری هندسی است. از اینرو، تقریبا" همه‌جا بر $[0, +\infty)$، درواقع همه جا جز در 0، داریم

$$\sum_{n=0}^{\infty} e^{-nt}e^{-at}t^{s-1} = \frac{e^{-at}t^{s-1}}{1-e^{-t}};$$

---

1. Lebesgue 2. Levi

درنتیجه،

$$\zeta(s, a)\Gamma(s) = \int_0^\infty \sum_{n=0}^\infty e^{-nt}e^{-at}t^{s-1}\, dt = \int_0^\infty \frac{e^{-at}t^{s-1}}{1-e^{-t}}\, dt.$$

این (۵) را به‌ازای $s > 1$ حقیقی ثابت می‌کند. برای تعمیم آن به همهٔ s های مختلط با $\sigma > 1$، توجه می‌کنیم که هر دو طرف به‌ازای $\sigma > 1$ تحلیلی‌اند. برای اثبات اینکه طرف راست تحلیلی است، فرض می‌کنیم $1 + \delta \le \sigma \le c$، که در آن $c > 1$ و $\delta > 0$، و می‌نویسیم

$$\int_0^\infty \left|\frac{e^{-at}t^{s-1}}{1-e^{-t}}\right| dt \le \int_0^\infty \frac{e^{-at}t^{\sigma-1}}{1-e^{-t}}\, dt = \left(\int_0^1 + \int_1^\infty\right)\frac{e^{-at}t^{\sigma-1}}{1-e^{-t}}\, dt.$$

اگر $0 \le t \le 1$، داریم $t^{\sigma-1} \le t^\delta$، و اگر $t \ge 1$، داریم $t^{\sigma-1} \le t^{c-1}$. همچنین، چون به‌ازای $t \ge 0$، $e^t - 1 \ge t$، داریم

$$\int_0^1 \frac{e^{-at}t^{\sigma-1}}{1-e^{-t}}\, dt \le \int_0^1 \frac{e^{(1-a)t}t^\delta}{e^t - 1}\, dt \le e^{(1-a)} \int_0^1 t^{\delta-1}\, dt = \frac{e^{1-a}}{\delta},$$

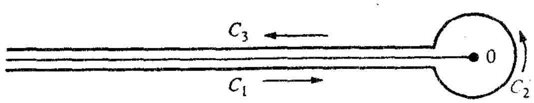
و

$$\int_1^\infty \frac{e^{-at}t^{\sigma-1}}{1-e^{-t}}\, dt \le \int_1^\infty \frac{e^{-at}t^{c-1}}{1-e^{-t}}\, dt \le \int_0^\infty \frac{e^{-at}t^{c-1}}{1-e^{-t}}\, dt = \Gamma(c)\zeta(c, a).$$

این نشان می‌دهد که انتگرال (۵) در هر نوار $1 + \delta \le \sigma \le c$، که $\delta > 0$، به‌طور یکنواخت همگراست؛ و لذا، در هر چنین نوار، و درنتیجه در نیمصفحهٔ $\sigma > 1$، یک تابع‌تحلیلی‌رانمایش می‌دهد. لذا، طبق ادامهٔ تحلیلی، (۵) به‌ازای هر s با $\sigma > 1$ برقرار می‌باشد.

۴۰۱۲ نمایش انتگرال کنتوری برای تابع زتای هرویتس

برای‌توسیع $\zeta(s, a)$ ورای خط $\sigma = 1$، نمایش دیگری برحسب یک انتگرال کنتوری بدست می‌آوریم. کنتور C یک حلقه حول محور حقیقی منفی، مثل شکل ۱۰۱۲، است. این



شکل ۱۰۱۲

حلقه از سه قسمت C_1, C_2, C_3 تشکیل شده است. C_2 یک دایرهٔ جهتدار با جهت

مثبت به‌شعاع $c < 2\pi$ حول مبداء است، و C_1, C_3 لبه‌های پایینی و بالایی یک "بریدگی" در صفحهٔ z در امتداد محور حقیقی منفی است، که طبق شکل ۱۲.۱ پیموده می‌شوند.

این یعنی ما از پارامتری سازیهای $z = re^{-\pi i}$ بر C_1 و $z = re^{\pi i}$ بر C_3، که درآنها r از c تا $+\infty$ تغییر می‌کند، استفاده می‌کنیم.

قضیهٔ ۳.۱۲ . *هرگاه $0 < a \leq 1$، تابع تعریف شده با انتگرال کنتوری*

$$I(s, a) = \frac{1}{2\pi i} \int_C \frac{z^{s-1} e^{az}}{1 - e^z} \, dz$$

یک تابع تمام از s است. بعلاوه،

اگر $\sigma > 1$، $\zeta(s, a) = \Gamma(1 - s) I(s, a)$. (۶)

برهان. در اینجا z^s یعنی $r^s e^{-\pi i s}$ بر C_1 و $r^s e^{\pi i s}$ بر C_3. قرص فشردهٔ دلخواه $|s| \leq M$ را درنظرگرفته، و ثابت می‌کنیم انتگرالها در امتداد C_1 و C_3 بر هرچنین قرص به‌طور یکنواخت همگراست. چون انتگرالده یک تابع تمام از s است، این ثابت خواهد کرد که $I(s, a)$ تمام است.

در امتداد C_1، به‌ازای $r \geq 1$ داریم

$$|z^{s-1}| = r^{\sigma-1} |e^{-\pi i(\sigma - 1 + it)}| = r^{\sigma-1} e^{\pi t} \leq r^{M-1} e^{\pi M}$$

زیرا $|s| \leq M$. بهمین نحو، در امتداد C_3، به‌ازای $r \geq 1$ داریم

$$|z^{s-1}| = r^{\sigma-1} |e^{\pi i(\sigma - 1 + it)}| = r^{\sigma-1} e^{-\pi t} \leq r^{M-1} e^{\pi M}.$$

لذا، بر C_1 یا C_3، به‌ازای $r \geq 1$ داریم

$$\left| \frac{z^{s-1} e^{az}}{1 - e^z} \right| \leq \frac{r^{M-1} e^{\pi M} e^{-ar}}{1 - e^{-r}} = \frac{r^{M-1} e^{\pi M} e^{(1-a)r}}{e^r - 1}.$$

اما وقتی $r > \log 2$، $e^r - 1 > e^r/2$ ؛ درنتیجه، انتگرالده به‌وسیلهٔ $A r^{M-1} e^{-ar}$ کراندار است، که درآن A ثابتی است وابسته به M ولی از r مستقل است. چون $\int_c^\infty r^{M-1} e^{-ar} \, dr$ به‌ازای $c > 0$ همگراست، این نشان می‌دهد که انتگرالها در امتداد C_1 و C_3 بر هر قرص فشردهٔ $|s| \leq M$ به‌طور یکنواخت همگراست؛ و درنتیجه، $I(s, a)$ یک تابع تمام از s می‌باشد.

برای اثبات (۶)، می‌نویسیم

$$2\pi i I(s, a) = \left(\int_{C_1} + \int_{C_2} + \int_{C_3}\right) z^{s-1} g(z)\, dz ,$$

که در آن $g(z) = e^{az}/(1 - e^z)$. بر C_1 و C_3 داریم $g(z) = g(-r)$ ، و بر C_2 می‌نویسیم $z = ce^{i\theta}$ ، که در آن $-\pi \le \theta \le \pi$. این نتیجه می‌دهد که

$$\begin{aligned} 2\pi i I(s, a) &= \int_{\infty}^{c} r^{s-1} e^{-\pi i s} g(-r)\, dr + i \int_{-\pi}^{\pi} c^{s-1} e^{(s-1)i\theta} c e^{i\theta} g(ce^{i\theta})\, d\theta \\ &\quad + \int_{c}^{\infty} r^{s-1} e^{\pi i s} g(-r)\, dr \\ &= 2i \sin(\pi s) \int_{c}^{\infty} r^{s-1} g(-r)\, dr + ic^s \int_{-\pi}^{\pi} e^{is\theta} g(ce^{i\theta})\, d\theta. \end{aligned}$$

با تقسیم بر $2i$ ، مثلاً" خواهیم داشت

$$\pi I(s, a) = \sin(\pi s) I_1(s, c) + I_2(s, c) \cdot$$

حال فرض‌کنیم $c \to 0$. دراین صورت ، اگر $\sigma > 1$ ،

$$\lim_{c \to 0} I_1(s, c) = \int_0^{\infty} \frac{r^{s-1} e^{-ar}}{1 - e^{-r}}\, dr = \Gamma(s)\zeta(s, a).$$

اینک نشان می‌دهیم که $\lim_{c \to 0} I_2(s, c) = 0$. برای این کار ، توجه می‌کنیم که $g(z)$ در $|z| < 2\pi$ جز به‌ازای یک قطب مرتبهٔ اول در $z = 0$ تحلیلی است . لذا ، $zg(z)$ همه‌جا در داخل $|z| < 2\pi$ تحلیلی است ؛ و درنتیجه ، درآن کراندار است ؛ مثلاً" ، $|g(z)| \le A/|z|$ ، که درآن $|z| = c < 2\pi$ و A ثابت است . بنابراین ، داریم

$$|I_2(s, c)| \le \frac{c^\sigma}{2} \int_{-\pi}^{\pi} e^{-t\theta} \frac{A}{c}\, d\theta \le Ae^{\pi|t|} c^{\sigma-1}.$$

اگر $\sigma > 1$ و $c \to 0$ ، معلوم می‌شود که $I_2(s, c) \to 0$ ؛ درنتیجه، $\pi I(s, a) = \sin(\pi s)\Gamma(s)\zeta(s, a)$.

چون $\Gamma(s)\Gamma(1 - s) = \pi/\sin \pi s$ ، این (۶) را ثابت خواهد کرد .

۱۲.۵ ادامهٔ تحلیلی تابع زتای هرویتس

در معادلهٔ $\zeta(s, a) = \Gamma(1 - s) I(s, a)$ ، که به‌ازای $\sigma > 1$ معتبر است ، توابع $I(s, a)$ و $\Gamma(1 - s)$ به‌ازای هر s مختلط با معنی‌اند . پس، با استفاده از این معادله، می‌توان $\zeta(s, a)$ را به‌ازای $\sigma \le 1$ تعریف کرد .

تعریف . اگر $\sigma \le 1$ ، $\zeta(s, a)$ را با معادلهٔ

$$\zeta(s, a) = \Gamma(1 - s)I(s, a) \tag{۷}$$

تعریف می‌کنیم. این معادله ادامهٔ تحلیلی $\zeta(s, a)$ را در تمام صفحهٔ s بدست می‌دهد.

قضیهٔ ۴۰۱۲. تابع $\zeta(s, a)$ که این‌طور تعریف می‌شود به‌ازای هر s جز یک قطب ساده در $s = 1$ با ماندهٔ 1 تحلیلی است.

برهان. چون $I(s, a)$ تمام است، تنها انفرادهای ممکن $\zeta(s, a)$ قطبهای $\Gamma(1 - s)$ اند؛ یعنی، نقاط $s = 1, 2, 3, \ldots$. اما قضیهٔ ۱۰۱۲ نشان می‌دهد که $\zeta(s, a)$ در $s = 2, 3, \ldots$ تحلیلی است؛ درنتیجه، $s = 1$ تنها قطب ممکن $\zeta(s, a)$ می‌باشد.

حال نشان می‌دهیم که یک قطب در $s = 1$ با ماندهٔ 1 وجود دارد. اگر s عددی صحیح باشد، مثلاً $s = n$، انتگرالده در انتگرال کنتوری مربوط به $I(s, a)$ بر C_1 و C_3 مقادیر یکسان می‌گیرد؛ و درنتیجه، انتگرالها در امتداد C_1 و C_3 حذف شده، وآنچه می‌ماند عبارت است از

$$I(n, a) = \frac{1}{2\pi i}\int_{C_2} \frac{z^{n-1}e^{az}}{1 - e^z}\,dz = \operatorname*{Res}_{z=0} \frac{z^{n-1}e^{az}}{1 - e^z}.$$

درحالت خاص، وقتی $s = 1$، داریم

$$I(1, a) = \operatorname*{Res}_{z=0} \frac{e^{az}}{1 - e^z} = \lim_{z\to 0} \frac{ze^{az}}{1 - e^z} = \lim_{z\to 0} \frac{z}{1 - e^z} = \lim_{z\to 0} \frac{-1}{e^z} = -1.$$

برای یافتن ماندهٔ $\zeta(s, a)$ در $s = 1$، حد زیر را حساب می‌کنیم:

$$\begin{aligned}\lim_{s\to 1}(s - 1)\zeta(s, a) &= -\lim_{s\to 1}(1 - s)\Gamma(1 - s)I(s, a) = -I(1, a)\lim_{s\to 1}\Gamma(2 - s)\\ &= \Gamma(1) = 1.\end{aligned}$$

این ثابت می‌کند که $\zeta(s, a)$ یک قطب ساده در $s = 1$ با ماندهٔ 1 دارد.

تذکر. چون $\zeta(s, a)$ در $s = 2, 3, \ldots$ تحلیلی است و $\Gamma(1 - s)$ در این نقاط قطب دارد، معادلهٔ (۷) ایجاب می‌کند که $I(s, a)$ در این نقاط صفر می‌شود.

۶۰۱۲ ادامهٔ تحلیلی $\zeta(s)$ و $L(s, \chi)$

در مقدمه ثابت شد که به‌ازای $\sigma > 1$ داریم

$$\zeta(s) = \zeta(s, 1)$$

و

$$L(s, \chi) = k^{-s} \sum_{r=1}^{k} \chi(r) \zeta\left(s, \frac{r}{k}\right), \tag{۸}$$

که در آن χ یک مشخص دیریکله به هنگ k است. حال این فرمولها را به‌عنوان تعاریف توابع $\zeta(s)$ و $L(s, \chi)$ به‌ازای $\sigma \leq 1$ بکار می‌بریم. بدین طریق، ادامهٔ تحلیلی $\zeta(s)$ و $L(s, \chi)$ را ورای خط $\sigma = 1$ بدست می‌آوریم.

قضیهٔ ۵۰۱۲. *(آ) تابع زتای ریمان $\zeta(s)$ همه‌جا جزبه‌ازای یک قطب ساده در $s = 1$ با ماندهٔ 1 تحلیلی است.*

(ب) به‌ازای مشخص اصلی χ_1 به هنگ k، L ـ تابع $L(s, \chi_1)$ همه‌جا جز به‌ازای یک قطب ساده در $s = 1$ با ماندهٔ $\varphi(k)/k$ تحلیلی است.

(پ) اگر $\chi \neq \chi_1$، $L(s, \chi)$ یک تابع تمام از s است.

برهان. قسمت (آ) فوراً از قضیهٔ ۴۰۱۲ نتیجه می‌شود. برای اثبات (ب) و (پ)، از رابطهٔ زیر استفاده می‌کنیم:

$$\sum_{r \bmod k} \chi(r) = \begin{cases} 0 & \text{اگر } \chi \neq \chi_1 \text{ ،} \\ \varphi(k) & \text{اگر } \chi = \chi_1 \text{ ،} \end{cases}$$

چون $\zeta(s, r/k)$ یک قطب ساده در $s = 1$ با ماندهٔ 1 دارد، تابع $\chi(r)\zeta(s, r/k)$ یک قطب ساده در $s = 1$ با ماندهٔ $\chi(r)$ دارد. بنابراین،

$$\operatorname*{Res}_{s=1} L(s, \chi) = \lim_{s \to 1}(s-1)L(s, \chi) = \lim_{s \to 1}(s-1)k^{-s} \sum_{r=1}^{k} \chi(r)\zeta\left(s, \frac{r}{k}\right)$$

$$= \frac{1}{k} \sum_{r=1}^{k} \chi(r) = \begin{cases} 0 & \text{اگر } \chi \neq \chi_1 \text{ ،} \\ \dfrac{\varphi(k)}{k} & \text{اگر } \chi = \chi_1 \text{ ،} \end{cases}$$

۷۰۱۲ فرمول هرویتس برای $\zeta(s, a)$

تابع $\zeta(s, a)$ در اصل به‌ازای $\sigma > 1$ با یک سری نامتناهی تعریف شده بود. هرویتس نمایش به‌صورت سری دیگری برای $\zeta(s, a)$ بدست آورد که در نیمصفحهٔ $\sigma < 0$ معتبر است. پیش از بیان این فرمول، لمی را ثابت می‌کنیم که بعداً در اثبات آن بکار خواهدرفت.

لم ۱. *فرض‌کنیم $S(r)$ ناحیهٔ حاصل از حذف تمام قرصهای مستدیر باز به شعاع*

$r,\ 0 < r < \pi$ و به مرکز $z = 2n\pi i, n = 0, \pm 1, \pm 2, \ldots$ از صفحهٔ z باشد. دراین صورت، اگر $0 < a \leq 1$، تابع

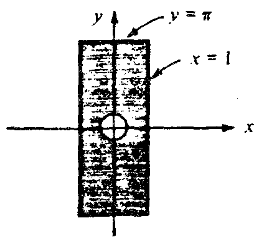
$$g(z) = \frac{e^{az}}{1 - e^z}$$

در $S(r)$ کراندار است. (کران به r بستگی دارد.)

برهان. می‌نویسیم $z = x + iy$، و مستطیل سوراخ شدهٔ

$$Q(r) = \{z : |x| \leq 1, |y| \leq \pi, |z| \geq r\}$$

در شکل ۲۰۱۲ را درنظر می‌گیریم.



شکل ۲۰۱۲

این یک مجموعهٔ فشرده است؛ درنتیجه، g بر $Q(r)$ کراندار است. همچنین، از اینکه $|g(z + 2\pi i)| = |g(z)|$، g در نوار نامتناهی سوراخ شدهٔ

$$\{z : |x| \leq 1, |z - 2n\pi i| \geq r, n = 0, \pm 1, \pm 2, \ldots\}$$

کراندار است. حال نشان می‌دهیم که g خارج این نوار کراندار است. فرض کنیم $|x| \geq 1$، ومی‌نویسیم

$$|g(z)| = \left|\frac{e^{az}}{1 - e^z}\right| = \frac{e^{ax}}{|1 - e^z|} \leq \frac{e^{ax}}{|1 - e^x|}.$$

به‌ازای $x \geq 1$، داریم $|1 - e^x| = e^x - 1$ و $e^{ax} \leq e^x$؛ درنتیجه،

$$|g(z)| \leq \frac{e^x}{e^x - 1} = \frac{1}{1 - e^{-x}} \leq \frac{1}{1 - e^{-1}} = \frac{e}{e - 1}.$$

همچنین، وقتی $x \leq -1$، داریم $|1 - e^x| = 1 - e^x$؛ درنتیجه،

$$|g(z)| \leq \frac{e^{ax}}{1 - e^x} \leq \frac{1}{1 - e^x} \leq \frac{1}{1 - e^{-1}} = \frac{e}{e - 1}.$$

از اینرو، به‌ازای $|x| \geq 1$ ، $|g(z)| \leq e/(e-1)$ ، و برهان لم تمام می‌باشد .

حال به فرمول هرویتس می‌پردازیم . این مستلزم سری دیریکلهٔ دیگر $F(x, s)$ است که با

$$F(x, s) = \sum_{n=1}^{\infty} \frac{e^{2\pi inx}}{n^s}, \tag{۹}$$

داده می‌شود ،که در آن x حقیقی است و $\sigma > 1$. توجه کنید که $F(x, s)$ یک تابع متناوب از x با دورهٔ تناوب 1 است و $F(1, s) = \zeta(s)$. این سری به ازای $\sigma > 1$ به‌طور مطلق همگراست . اگر x صحیح نباشد ، سری به‌ازای $\sigma > 0$ نیز (به‌طور مشروط) همگراست ،زیرا به‌ازای هر x غیر صحیح ثابت ، ضرایب دارای مجموعهای جزئی کراندار می‌باشند .

تذکر. ما $F(x, s)$ را ***تابع زتای متناوب*** می‌نامیم .

قضیهٔ ۶۰۱۲ . فرمول هرویتس. *اگر $0 < a \leq 1$ و $\sigma > 1$ ، داریم*

$$\zeta(1-s, a) = \frac{\Gamma(s)}{(2\pi)^s} \{e^{-\pi is/2}F(a, s) + e^{\pi is/2}F(-a, s)\}. \tag{۱۰}$$

اگر $a \neq 1$ ، این نمایش به‌ازای $\sigma > 0$ نیز معتبر است .

برهان. تابع

$$I_N(s, a) = \frac{1}{2\pi i} \int_{C(N)} \frac{z^{s-1}e^{az}}{1-e^z}\, dz$$

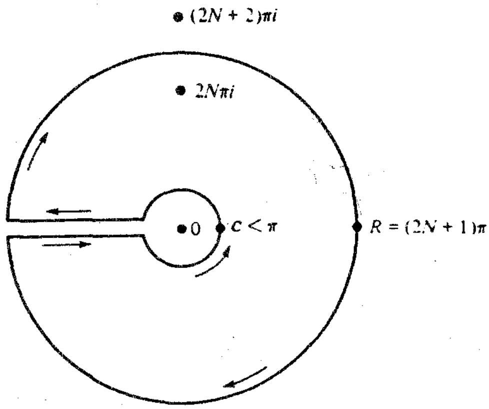
را درنظر می‌گیریم ، که در آن $C(N)$ کنتور شکل ۳۰۱۲ بوده و N عددی صحیح است .

ابتدا ثابت می‌کنیم که اگر $\sigma < 0$ ، $\lim_{N\to\infty} I_N(s, a) = I(s, a)$. برای این‌کار ، کافی‌است نشان دهیم که ، وقتی $N \to \infty$ ، انتگرال در امتداد دایرهٔ خارجی به 0 میل می‌کند .

بر دایرهٔ خارجی داریم $z = Re^{i\theta}, -\pi \leq \theta \leq \pi$ ؛ درنتیجه ،

$$|z^{s-1}| = |R^{s-1}e^{i\theta(s-1)}| = R^{\sigma-1}e^{-t\theta} \leq R^{\sigma-1}e^{\pi|t|}$$

چون دایرهٔ خارجی در مجموعهٔ $S(r)$ از لم ۱ قرار دارد ، انتگرالده به وسیلهٔ



شکل ۱۲ ۰ ۳

$Ae^{\pi|t|}R^{\sigma-1}$ کرانداراست ، که درآن کران A برای $|g(z)|$ است که از لم ۱ بدست‌می‌آید؛ درنتیجه ، انتگرال به‌وسیلهٔ

$$2\pi A e^{\pi|t|}R^{\sigma}$$

کرانداراست ، واین ، وقتی $R \to \infty$ ، اگر $\sigma < 0$ ، به 0 میل خواهد کرد . لذا ، ازتعویض s با $1-s$ معلوم می‌شود که

$$\lim_{N\to\infty} I_N(1-s, a) = I(1-s, a) \quad \text{اگر } \sigma > 1 \tag{11}$$

حال $I_N(1-s, a)$ را به‌وسیلهٔ قضیهٔ ماندهٔ کشی صریحاً حساب می‌کنیم . داریم

$$I_N(1-s, a) = -\sum_{\substack{n=-N\\ n\neq 0}}^{N} R(n) = -\sum_{n=1}^{N}\{R(n) + R(-n)\},$$

که در آن

$$R(n) = \operatorname*{Res}_{z=2n\pi i}\left(\frac{z^{-s}e^{az}}{1-e^{z}}\right).$$

اما

$$R(n) = \lim_{z\to 2n\pi i}(z-2n\pi i)\frac{z^{-s}e^{az}}{1-e^{z}} = \frac{e^{2n\pi i a}}{(2n\pi i)^s}\lim_{z\to 2n\pi i}\frac{z-2n\pi i}{1-e^{z}} = -\frac{e^{2n\pi i a}}{(2n\pi i)^s};$$

درنتیجه ،

$$I_N(1-s, a) = \sum_{n=1}^{N}\frac{e^{2n\pi i a}}{(2n\pi i)^s} + \sum_{n=1}^{N}\frac{e^{-2n\pi i a}}{(-2n\pi i)^s}$$

اما $i^{-s} = e^{-\pi is/2}$ و $(-i)^{-s} = e^{\pi is/2}$ ؛ درنتیجه،

$$I_N(1-s, a) = \frac{e^{-\pi is/2}}{(2\pi)^s} \sum_{n=1}^{N} \frac{e^{2n\pi ia}}{n^s} + \frac{e^{\pi is/2}}{(2\pi)^s} \sum_{n=1}^{N} \frac{e^{-2n\pi ia}}{n^s}.$$

با فرض $N \to \infty$ و استفاده از (۱۱)، بدست می‌آوریم

$$I(1-s, a) = \frac{e^{-\pi is/2}}{(2\pi)^s} F(a, s) + \frac{e^{\pi is/2}}{(2\pi)^s} F(-a, s).$$

بنابراین،

$$\zeta(1-s, a) = \Gamma(s) I(1-s, a) = \frac{\Gamma(s)}{(2\pi)^s} \{e^{-\pi is/2} F(a, s) + e^{\pi is/2} F(-a, s)\}.$$

۸.۱۲ معادلهٔ تابعی برای تابع زتای ریمان

اولین کاربرد فرمول هرویتس در معادلهٔ تابعی ریمان برای $\zeta(s)$ است.

قضیهٔ ۷.۱۲ . *برای هر s، داریم*

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s) \tag{۱۲}$$

یا، معادلاً"،

$$\zeta(s) = 2(2\pi)^{s-1}\Gamma(1-s)\sin\left(\frac{\pi s}{2}\right)\zeta(1-s). \tag{۱۳}$$

برهان. با فرض $a = 1$ در فرمول هرویتس، به‌ازای $\sigma > 1$ بدست می‌آوریم

$$\zeta(1-s) = \frac{\Gamma(s)}{(2\pi)^s} \{e^{-\pi is/2}\zeta(s) + e^{\pi is/2}\zeta(s)\} = \frac{\Gamma(s)}{(2\pi)^s} 2\cos\left(\frac{\pi s}{2}\right)\zeta(s).$$

این (۱۲) را به‌ازای $\sigma > 1$ ثابت می‌کند، و نتیجه طبق ادامهٔ تحلیلی به‌ازای هر s برقرار است. برای استنتاج (۱۳) از (۱۲)، s را با $1 - s$ عوض می‌کنیم.

تذکر. با فرض $s = 2n + 1$ در (۱۲) که $n = 1, 2, 3, \ldots$ ، عامل $\cos(\pi s/2)$ صفر می‌شود، و ما **صفرهای بدیهی** $\zeta(s)$ را می‌یابیم:

$$\zeta(-2n) = 0 \quad \text{، به‌ازای } n = 1, 2, 3, \ldots$$

اگر از فرمول المثنای لژاندر برای تابع گاما، یعنی

$$2\pi^{1/2}2^{-2s}\Gamma(2s) = \Gamma(s)\Gamma\left(s+\frac{1}{2}\right),$$

که حالت خاص $m = 2$ معادلهٔ (۴) است، استفاده کنیم، می‌توانیم معادلهٔ تابعی را به شکل ساده‌تری درآوریم. وقتی s با $(1-s)/2$ عوض شود، این خواهد شد

$$2^{s}\pi^{1/2}\Gamma(1-s) = \Gamma\left(\frac{1-s}{2}\right)\Gamma\left(1-\frac{s}{2}\right).$$

چون

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(1-\frac{s}{2}\right) = \frac{\pi}{\sin\frac{\pi s}{2}}$$

این نتیجه می‌دهد که

$$\Gamma(1-s)\sin\frac{\pi s}{2} = \frac{2^{-s}\pi^{1/2}\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}.$$

با استفاده از این برای تعویض حاصل ضرب $\Gamma(1-s)\sin(\pi s/2)$ در (۱۳)، خواهیم داشت

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

به عبارت دیگر، معادلهٔ تابعی شکل زیر را بخود می‌گیرد:

$$\Phi(s) = \Phi(1-s),$$

که در آن

$$\Phi(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

تابع $\Phi(s)$ دارای قطبهای ساده در $s = 0$ و $s = 1$ است. به تقلید از ریمان، برای حذف قطبها $\Phi(s)$ را در $s(s-1)/2$ ضرب و تعریف می‌کنیم

$$\xi(s) = \frac{1}{2}s(s-1)\Phi(s).$$

در این صورت، $\xi(s)$ یک تابع تمام از s است و در معادلهٔ تابعی

$$\xi(s) = \xi(1-s)$$

صدق می‌کند.

۹.۱۲ معادلهٔ تابعی برای تابع زتای هرویتس

معادلهٔ تابعی مربوط به $\zeta(s)$ حالت خاصی از معادلهٔ تابعی مربوط به $\zeta(s, a)$ ، وقتی a گویاست ، می‌باشد .

قضیهٔ ۸.۱۲ . هرگاه h و k صحیح باشند و $1 \le h \le k$ ، آنگاه به‌ازای هر s داریم

$$\zeta\left(1 - s, \frac{h}{k}\right) = \frac{2\Gamma(s)}{(2\pi k)^s} \sum_{r=1}^{k} \cos\left(\frac{\pi s}{2} - \frac{2\pi rh}{k}\right) \zeta\left(s, \frac{r}{k}\right). \tag{۱۴}$$

برهان. این ناشی از آن است که ، وقتی x گویا باشد ، تابع $F(x, s)$ ترکیبی خطی از توابع زتای هرویتس می‌باشد . درواقع ، اگر $x = h/k$ ، می‌توان جملات (۹) را طبق رده‌های مانده‌ای به هنگ k تجدید آرایش کرد به این‌ترتیب که نوشت

$n = qk + r$ ، که در آن $1 \le r \le k$ و $q = 0, 1, 2, \ldots$.

این نتیجه می‌دهد که به‌ازای $\sigma > 1$ ،

$$F\left(\frac{h}{k}, s\right) = \sum_{n=1}^{\infty} \frac{e^{2\pi inh/k}}{n^s} = \sum_{r=1}^{k} \sum_{q=0}^{\infty} \frac{e^{2\pi irh/k}}{(qk + r)^s} = \frac{1}{k^s} \sum_{r=1}^{k} e^{2\pi irh/k} \sum_{q=0}^{\infty} \frac{1}{\left(q + \frac{r}{k}\right)^s}$$

$$= k^{-s} \sum_{r=1}^{k} e^{2\pi irh/k} \zeta\left(s, \frac{r}{k}\right).$$

لذا ، اگر در فرمول هرویتس $a = h/k$ را اختیار کنیم ، خواهیم داشت

$$\zeta\left(1 - s, \frac{h}{k}\right) = \frac{\Gamma(s)}{(2\pi k)^s} \sum_{r=1}^{k} (e^{-\pi is/2} e^{2\pi irh/k} + e^{\pi is/2} e^{-2\pi irh/k}) \zeta\left(s, \frac{r}{k}\right)$$

$$= \frac{2\Gamma(s)}{(2\pi k)^s} \sum_{r=1}^{k} \cos\left(\frac{\pi s}{2} - \frac{2\pi rh}{k}\right) \zeta\left(s, \frac{r}{k}\right),$$

که (۱۴) را به‌ازای $\sigma > 1$ ثابت می‌کند . این نتیجه طبق ادامهٔ تحلیلی به‌ازای هر s برقرار است .

بایستی توجه داشت که‌وقتی $h = k = 1$ ، فقط یک جمله در مجموع (۱۴) وجود دارد ، و معادلهٔ تابعی ریمان بدست می‌آید .

۱۰.۱۲ معادلهٔ تابعی برای L ـ تابعها

فرمول هرویتس را می‌توان برای استنتاج یک معادلهٔ تابعی برای L ـ تابعهای دیریکله نیز

بکاربرد . ابتدا نشان می‌دهیم که کافی است فقط مشخصهای اولیه به هنگ k درنظرگرفته شونـــد .

قضیهٔ ۹.۱۲ . فرض‌کنیم χ یک مشخص دیریکله به هنگ k بوده، d یک هنگ القایی باشد ، و می‌نویسیم

$$\chi(n) = \psi(n)\chi_1(n),$$

که درآن ψ یک مشخص بــه هنــگ d بوده و χ_1 مشخص‌اصلی به هنگ k باشد . دراین صورت ، به‌ازای هر s داریم

$$L(s, \chi) = L(s, \psi)\prod_{p|k}\left(1 - \frac{\psi(p)}{p^s}\right).$$

برهان. ابتدا σ را بزرگتر از 1 گرفته و از حاصل ضرب اویلر

$$L(s, \chi) = \prod_p \frac{1}{1 - \dfrac{\chi(p)}{p^s}}$$

استفاده می‌کنیم . چون $\chi(p) = \psi(p)\chi_1(p)$ و چون $\chi_1(p) = 0$ اگر $p|k$ و $\chi_1(p) = 1$ اگر $p \nmid k$ ، خواهیم داشت

$$L(s, \chi) = \prod_{p\nmid k} \frac{1}{1 - \dfrac{\psi(p)}{p^s}} = \prod_p \frac{1}{1 - \dfrac{\psi(p)}{p^s}} \cdot \prod_{p|k}\left(1 - \frac{\psi(p)}{p^s}\right)$$
$$= L(s, \psi)\prod_{p|k}\left(1 - \frac{\psi(p)}{p^s}\right).$$

این قضیه را به‌ازای $\sigma > 1$ ثابت می‌کند ، و با ادامهٔ تحلیلی آن را به همهٔ s ها تعمیم می‌دهیم .

تذکر. اگر درقضیهٔفوق d راهادی χ بگیریم ، ψ یک‌مشخص اولیه به هنگ d می‌شود . این‌نشان می‌دهد که هر L ــ سری $L(s, \chi)$ مساوی L ــ سری $L(s, \psi)$ یک مشخص اولیه‌است که در تعدادی متناهی عامل ضرب شده است .

برای استنتاج معادلهٔ تابعی برای L ــ توابع از تابعها هرویتس، ابتدا $L(s, \chi)$ را برحسب ~~تابع~~ زتای متناوب $F(x, s)$ بیان می‌کنیم .

قضیهٔ ۱۰.۱۲ . فرض‌کنیم χ یک‌مشخص اولیه به هنگ k باشد . در این صورت ، به‌ازای $\sigma > 1$ داریم

$$G(1, \bar{\chi})L(s, \chi) = \sum_{h=1}^{k} \bar{\chi}(h)F\left(\frac{h}{k}, s\right), \tag{۱۵}$$

که در آن $G(m, \chi)$ مجموع گاوس مربوط به χ است :

$$G(m, \chi) = \sum_{r=1}^{k} \chi(r)e^{2\pi irm/k}.$$

برهان . با فرض $x = h/k$ در (۹) ، ضرب در $\bar{\chi}(h)$ ، و جمعبندی روی h ، خواهیم داشت

$$\sum_{h=1}^{k} \bar{\chi}(h)F\left(\frac{h}{k}, s\right) = \sum_{h=1}^{k}\sum_{n=1}^{\infty} \bar{\chi}(h)e^{2\pi inh/k}n^{-s} = \sum_{n=1}^{\infty} n^{-s}\sum_{h=1}^{k} \bar{\chi}(h)e^{2\pi inh/k}$$
$$= \sum_{n=1}^{\infty} n^{-s}G(n, \bar{\chi}).$$

اما $G(n, \bar{\chi})$ بخاطر اولیه بودن $\bar{\chi}$ جدایی‌پذیر است ؛ درنتیجه ، $G(n, \bar{\chi}) = \chi(n)G(1, \bar{\chi})$. بنابراین ،

$$\sum_{h=1}^{k} \bar{\chi}(h)F\left(\frac{h}{k}, s\right) = G(1, \bar{\chi})\sum_{n=1}^{\infty} \chi(n)n^{-s} = G(1, \bar{\chi})L(s, \chi).$$

قضیهٔ ۱۱.۱۲ . معادلهٔ تابعی برای L ـ تابعهای دیریکله . هرگاه χ یک مشخص اولیه به هنگ k باشد ، آنگاه به‌ازای هر s داریم

$$L(1 - s, \chi) = \frac{k^{s-1}\Gamma(s)}{(2\pi)^s}\{e^{-\pi is/2} + \chi(-1)e^{\pi is/2}\}G(1, \chi)L(s, \bar{\chi}). \tag{۱۶}$$

برهان . در فرمول هرویتس قرار می‌دهیم $x = h/k$ ، سپس طرفین را در $\chi(h)$ ضرب کرده و روی h جمع می‌بندیم . این نتیجه می‌دهد که

$$\sum_{h=1}^{k} \chi(h)\zeta\left(1 - s, \frac{h}{k}\right) = \frac{\Gamma(s)}{(2\pi)^s}\left\{e^{-\pi is/2}\sum_{h=1}^{k} \chi(h)F\left(\frac{h}{k}, s\right)\right.$$
$$\left. + e^{\pi is/2}\sum_{h=1}^{k} \chi(h)F\left(\frac{-h}{k}, s\right)\right\}.$$

چون $F(x, s)$ نسبت‌به x متناوب‌با دورهٔ تناوب 1 بوده و $\chi(h) = \chi(-1)\chi(-h)$ ، می‌توان

نوشت

$$\sum_{h \bmod k} \chi(h) F\left(\frac{-h}{k}, s\right) = \chi(-1) \sum_{h \bmod k} \chi(-h) F\left(\frac{-h}{k}, s\right)$$
$$= \chi(-1) \sum_{h \bmod k} \chi(k-h) F\left(\frac{k-h}{k}, s\right)$$
$$= \chi(-1) \sum_{h \bmod k} \chi(h) F\left(\frac{h}{k}, s\right),$$

و فرمول قبل خواهد شد

$$\sum_{h=1}^{k} \chi(h) \zeta\left(1-s, \frac{h}{k}\right) = \frac{\Gamma(s)}{(2\pi)^s} \{e^{-\pi i s/2} + \chi(-1) e^{\pi i s/2}\} \sum_{h=1}^{k} \chi(h) F\left(\frac{h}{k}, s\right).$$

حال طرفین را در k^{s-1} ضرب کرده و، با استفاده از (۱۵)، (۱۶) را بدست می‌آوریم.

۱۱.۱۲ محاسبهٔ $\zeta(-n, a)$

اگر n عدد صحیح نامنفیی‌باشد، مقدار $\zeta(-n, a)$ را می‌توان صریحاً حساب کرد. با فرض $s = -n$ در رابطهٔ $\zeta(s, a) = \Gamma(1-s) I(s, a)$، معلوم می‌شود که

$$\zeta(-n, a) = \Gamma(1+n) I(-n, a) = n!\, I(-n, a).$$

همچنین، داریم

$$I(-n, a) = \operatorname*{Res}_{z=0} \left(\frac{z^{-n-1} e^{az}}{1-e^z}\right).$$

محاسبهٔ این مانده به ردهٔ جالبی از توابع منجر می‌شود که به **چندجمله‌ایهای برنولی**[1] معروفند.

تعریف. به‌ازای‌هر x مختلط، توابع $B_n(x)$ را با معادلهٔ $\frac{ze^{xz}}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n$ تعریف می‌کنیم، که در آن $|z| < 2\pi$. اعداد $B_n(0)$ *اعداد برنولی* نام دارند و با B_n نموده می‌شوند. بنابراین،

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} z^n \text{، که در آن } |z| < 2\pi.$$

---

1. Bernoulli

قضیهٔ ۱۲۰۱۲ . توابع $B_n(x)$ چندجمله‌ایهایی از x اند که با

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$$

داده می‌شوند .

برهان . داریم

$$\sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n = \frac{z}{e^z - 1} \cdot e^{xz} = \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n\right)\left(\sum_{n=0}^{\infty} \frac{x^n}{n!} z^n\right).$$

با متحد کردن ضرایب z^n ، معلوم می‌شود که

$$\frac{B_n(x)}{n!} = \sum_{k=0}^{n} \frac{B_k}{k!} \frac{x^{n-k}}{(n-k)!},$$

که از آن قضیه نتیجه می‌شود .

قضیهٔ ۱۳۰۱۲ . به‌ازای هر عدد صحیح $n \geq 0$ ، داریم

$$\zeta(-n, a) = -\frac{B_{n+1}(a)}{n+1}. \qquad (۱۷)$$

برهان . همانطور که قبلاً گفتیم ، داریم $\zeta(-n, a) = n!I(-n, a)$. اما

$$I(-n, a) = \operatorname*{Res}_{z=0}\left(\frac{z^{-n-1}e^{az}}{1 - e^z}\right) = -\operatorname*{Res}_{z=0}\left(z^{-n-2}\frac{ze^{az}}{e^z - 1}\right)$$
$$= -\operatorname*{Res}_{z=0}\left(z^{-n-2}\sum_{m=0}^{\infty}\frac{B_m(a)}{m!}z^m\right) = -\frac{B_{n+1}(a)}{(n+1)!},$$

که از آن (۱۷) بدست می‌آید .

۱۲۰۱۲ خواص اعداد برنولی و چندجمله‌ایهای برنولی

قضیهٔ ۱۴۰۱۲ . چندجمله‌ایهای برنولی $B_n(x)$ در معادلهٔ تفاضلی زیر صدق می‌کند :

اگر $n \geq 1$ ، $B_n(x+1) - B_n(x) = nx^{n-1}$. (۱۸)

لذا

اگر $n \geq 2$ ، $B_n(0) = B_n(1)$. (۱۹)

برهان. اتحاد زیر را داریم

$$z\frac{e^{(x+1)z}}{e^z-1}-z\frac{e^{xz}}{e^z-1}=ze^{xz},$$

که از آن معلوم می‌شود که

$$\sum_{n=0}^{\infty}\frac{B_n(x+1)-B_n(x)}{n!}z^n=\sum_{n=0}^{\infty}\frac{x^n}{n!}z^{n+1}.$$

با متحدگرفتن ضرایب z^n ، (۱۸) بدست می‌آید. و با اختیار $x=0$ در (۱۸)، (۱۹) را خواهیم داشت.

قضیهٔ ۱۵.۱۲ . *اگر* $n \geq 2$ ، *داریم*

$$B_n=\sum_{k=0}^{n}\binom{n}{k}B_k.$$

برهان. این با فرض $x=1$ در قضیهٔ ۱۲.۱۲ و استفاده از (۱۹)، نتیجه می‌شود.

قضیهٔ ۱۵.۱۲ یک فرمول بازگشتی برای محاسبهٔ اعداد برنولی بدست می‌دهد. از تعریف نتیجه می‌شود که $B_0=1$ ، و قضیهٔ ۱۵.۱۲ مقادیر زیر را متوالیا" به‌ما می‌دهد:

$$B_0=1,\quad B_1=-\frac{1}{2},\quad B_2=\frac{1}{6},\quad B_3=0,\quad B_4=-\frac{1}{30},$$

$$B_5=0,\quad B_6=\frac{1}{42},\quad B_7=0,\quad B_8=-\frac{1}{30},\quad B_9=0,$$

$$B_{10}=\frac{5}{66},\quad B_{11}=0.$$

با اطلاعاتی از B_k می‌توان چندجمله‌ایهای $B_n(x)$ را با استفاده از قضیهٔ ۱۲.۱۲ حساب کرد. چندتای اول عبارتند از

$$B_0(x)=1,\quad B_1(x)=x-\frac{1}{2},\quad B_2(x)=x^2-x+\frac{1}{6},$$

$$B_3(x)=x^3-\frac{3}{2}x^2+\frac{1}{2}x,\quad B_4(x)=x^4-2x^3+x^2-\frac{1}{30}.$$

ملاحظه می‌شود که قضایای ۱۲.۱۲ و ۱۵.۱۲ را می‌توان به‌طور صوری چنین نوشت:

$$B_n(x)=(B+x)^n,\quad B_n=(B+1)^n.$$

با این علامات، فرمولهای طرفهای راست را باید به‌وسیلهٔ قضیهٔ دوجمله‌ای بسط داد، و سپس هر توان B^k را با B_k عوض کرد.

قضیهٔ ۱۶.۱۲ . *اگر* $n \geq 0$ *، داریم*

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}. \tag{۲۰}$$

همچنین، اگر $n \geq 1$ **، داریم** $\zeta(-2n) = 0$ **؛ درنتیجه،** $B_{2n+1} = 0$.

برهان. برای محاسبهٔ $\zeta(-n)$ ، کافی است در قضیهٔ ۱۳.۱۲ فرض کنیم $a = 1$. قبلاً گفتیم که معادلهٔ تابعی

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s) \tag{۲۱}$$

ایجاب می‌کند که به‌ازای $n \geq 1$ ، $\zeta(-2n) = 0$ ؛ درنتیجه، بنابر (۲۰)، $B_{2n+1} = 0$.

تذکر. نتیجهٔ $B_{2n+1} = 0$ با توجه به اینکه طرف چپ

$$\frac{z}{e^z - 1} + \frac{1}{2}z = 1 + \sum_{n=2}^{\infty} \frac{B_n}{n!} z^n$$

تابع زوجی از z است نیز بدست می‌آید.

قضیهٔ ۱۷.۱۲ . *اگر* k *عدد صحیح مثبتی باشد، داریم*

$$\zeta(2k) = (-1)^{k+1}\frac{(2\pi)^{2k}B_{2k}}{2(2k)!}. \tag{۲۲}$$

برهان. با فرض $s = 2k$ در معادلهٔ تابعی مربوط به $\zeta(s)$ ، بدست می‌آید

$$\zeta(1-2k) = 2(2\pi)^{-2k}\Gamma(2k)\cos(\pi k)\zeta(2k),$$

یا

$$-\frac{B_{2k}}{2k} = 2(2\pi)^{-2k}(2k-1)!(-1)^k\zeta(2k).$$

این (۲۲) را ایجاب خواهد کرد.

تذکر. اگـر در (۲۱) $s = 2k + 1$ را قرار دهیم ، طرفین صفر شده و هیچ اطلاعی از $\zeta(2k + 1)$ بدست نمـی‌آوریم . تاکنون هیچ فرمول ساده‌ای شبیه (۲۲) برای $\zeta(2k + 1)$ یا حتی برای حالت خاصی نظیر $\zeta(3)$ بدست نیامده است . حتی نمی‌دانیم که $\zeta(2k + 1)$ به‌ازای هر k گویاست یا گنگ .

قضیهٔ ۱۸۰۱۲ . *اعداد برنولی B_{2k} متناوبا " تغییر علامت می‌دهند . یعنی ،*

$$(-1)^{k+1}B_{2k} > 0.$$

بعلاوه ، وقتی $k \to \infty$ ، $|B_{2k}| \to \infty$. درواقع ،

$$\text{وقتی } k \to \infty \text{ ، } (-1)^{k+1}B_{2k} \sim \frac{2(2k)!}{(2\pi)^{2k}} . \qquad (۲۳)$$

برهان . چون $\zeta(2k) > 0$ ، (۲۲) نشان می‌دهد که اعداد B_{2k} متناوبا " تغییر علامت می‌دهند . رابطـهٔ مجانبی (۲۳) از این امر که وقتی $k \to \infty$ ، $\zeta(2k) \to 1$ نتیجه خواهد شـد .

تذکر . از (۲۳) نتیجه مـی‌شود که وقتی $k \to \infty$ ، $|B_{2k+2}/B_{2k}| \sim k^2/\pi^2$. همچنین ، به‌یاری فرمول استرلینگ[1] ، یعنی $n! \sim (n/e)^n\sqrt{2\pi n}$ ، درمی‌یابیم که

$$\text{وقتی } k \to \infty \text{ ، } (-1)^{k+1}B_{2k} \sim 4\pi\sqrt{e}\left(\frac{k}{\pi e}\right)^{2k+1/2} .$$

قضیهٔ زیـر بسـط‌فوریهٔ چندجمله‌ای $B_n(x)$ را در بازهٔ $0 < x \le 1$ به‌ما می‌دهد .

قضیهٔ ۱۹۰۱۲ . *اگر $0 < x \le 1$ ، داریم*

$$B_n(x) = -\frac{n!}{(2\pi i)^n}\sum_{\substack{k=-\infty \\ k\neq 0}}^{+\infty}\frac{e^{2\pi ikx}}{k^n}; \qquad (۲۴)$$

و درنتیجه ،

$$B_{2n}(x) = (-1)^{n+1}\frac{2(2n)!}{(2\pi)^{2n}}\sum_{k=1}^{\infty}\frac{\cos 2\pi kx}{k^{2n}},$$

---

1. Stirling

$$B_{2n+1}(x) = (-1)^{n+1} \frac{2(2n+1)!}{(2\pi)^{2n+1}} \sum_{k=1}^{\infty} \frac{\sin 2\pi kx}{k^{2n+1}}.$$

برهان. معادلهٔ (۲۴)، با اختیار $s = n$ در فرمول هرویتس و اعمال قضیهٔ ۱۳۰۱۲، فوراً نتیجه می‌شود. دو فرمول دیگر حالات خاص (۲۴) می‌باشند.

تذکر. تابع $\bar{B}_n(x)$ که به‌ازای هر x حقیقی به وسیلهٔ طرف راست (۲۴) تعریف می‌شود، *تابع متناوب برنولی* n م نام دارد. این تابع متناوب با دورهٔ تناوب 1 است و باچند جمله‌ای برنولی $B_n(x)$ در بازهٔ $0 < x \le 1$ یکی است. لذا، داریم

$$\bar{B}_n(x) = B_n(x - [x]).$$

۱۳۰۱۲ فرمولهایی برای $L(0, \chi)$

قضیهٔ ۱۳۰۱۲ ایجاب می‌کند که

$$\zeta(0, a) = -B_1(a) = \frac{1}{2} - a.$$

بخصوص، $\zeta(0) = \zeta(0, 1) = -1/2$. همچنین، می‌توان $L(0, \chi)$ را به‌ازای هر مشخص دیریکلهٔ χ حساب کرد.

قضیهٔ ۲۰۰۱۲ . فرض کنیم χ یک مشخص دیریکله به هنگ k باشد.

(آ) اگر (مشخص اصلی) $\chi = \chi_1$، $L(0, \chi_1) = 0$.

(ب) اگر $\chi \neq \chi_1$، داریم

$$L(0, \chi) = -\frac{1}{k} \sum_{r=1}^{k} r\chi(r).$$

بعلاوه، اگر $\chi(-1) = 1$، $L(0, \chi) = 0$.

برهان. اگر $\chi = \chi_1$، از فرمول

$$L(s, \chi_1) = \zeta(s) \prod_{p|k} (1 - p^{-s})$$

که درفصل ۱۱ به‌ازای $\sigma > 1$ ثابت شد استفاده می‌کنیم. این فرمول طبق ادامهٔ تحلیلی به‌ازای هر s برقراراست. وقتی $s = 0$، حاصل ضرب صفراست؛ درنتیجه، $L(0, \chi_1) = 0$.

اگر $\chi \neq \chi_1$ ، داریم

$$L(0, \chi) = \sum_{r=1}^{k} \chi(r)\zeta\left(0, \frac{r}{k}\right) = \sum_{r=1}^{k} \chi(r)\left(\frac{1}{2} - \frac{r}{k}\right) = -\frac{1}{k}\sum_{r=1}^{k} r\chi(r).$$

اما

$$\sum_{r=1}^{k} r\chi(r) = \sum_{r=1}^{k} (k-r)\chi(k-r) = k\sum_{r=1}^{k} \chi(k-r) - \sum_{r=1}^{k} r\chi(-r)$$
$$= -\chi(-1)\sum_{r=1}^{k} r\chi(r).$$

لذا، اگر $\chi(-1) = 1$ ، خواهیم داشت $\sum_{r=1}^{k} r\chi(r) = 0$.

۱۴۰۱۲ تقریب $\zeta(s, a)$ به‌وسیلهٔ مجموعهای متناهی

بعضی از کاربردها نیاز به تخمینهایی از میزان رشد $\zeta(\sigma + it, a)$ به‌عنوان تابعی از t دارند. آنها را می‌توان از نمایش دیگری از $\zeta(s, a)$ که از فرمول جمعبندی اویلر حاصل می‌شود نتیجه گرفت. این نمایش $\zeta(s, a)$ را به مجموعهای جزئی سری خود در نیمصفحهٔ $\sigma > 0$ ربط داده و نیز راه دیگری برای توسیع تحلیلی $\zeta(s, a)$ و رای خط $\sigma = 1$ بدست می‌دهد.

قضیهٔ ۲۱۰۱۲ . به‌ازای هر عدد صحیح $N \geq 0$ و $\sigma > 0$ ، داریم

$$\zeta(s, a) = \sum_{n=0}^{N} \frac{1}{(n+a)^s} + \frac{(N+a)^{1-s}}{s-1} - s\int_N^{\infty} \frac{x - [x]}{(x+a)^{s+1}}\,dx. \qquad (۲۵)$$

برهان. فرمول‌جمعبندی‌اویلر (قضیهٔ ۱۰۳) را به‌ازای $f(t) = (t+a)^{-s}$ و اعدادصحیح x و y بکار برده، بدست می‌آوریم

$$\sum_{y<n\leq x} \frac{1}{(n+a)^s} = \int_y^x \frac{dt}{(t+a)^s} - s\int_y^x \frac{t-[t]}{(t+a)^{s+1}}\,dt.$$

$y = N$ را اختیار و، با حفظ $\sigma > 1$ ، فرض می‌کنیم $x \to \infty$. این نتیجه می‌دهد که

$$\sum_{n=N+1}^{\infty} \frac{1}{(n+a)^s} = \int_N^{\infty} \frac{dt}{(t+a)^s} - s\int_N^{\infty} \frac{t-[t]}{(t+a)^{s+1}}\,dt,$$

یا

$$\zeta(s, a) - \sum_{n=0}^{N} \frac{1}{(n+a)^s} = \frac{(N+a)^{1-s}}{s-1} - s\int_N^\infty \frac{t-[t]}{(t+a)^{s+1}}\,dt.$$

این (۲۵) را بـه‌ازای $\sigma > 1$ ثـابـت می‌کنـد. اگر $0 < \delta \le \sigma$، انتگرال تحت تسلط $\int_N^\infty (t+a)^{-\delta-1}\,dt$ است؛ درنتیجه، به‌ازای $\sigma \ge \delta$ به‌طور یکنواخت همگراست؛ و لذا، درنیمصفحهٔ $\sigma > 0$ یک تابع تحلیلی را نمایش می‌دهد. لذا، طبق ادامهٔ تحلیلی، (۲۵) به‌ازای $\sigma > 0$ برقرار می‌باشد.

انتگرال طرف راست (۲۵) را می‌توان به صورت یک سری نیز نوشت. انتگرال را به مجموعی از انتگـرالـها کـه در آنـهـا $[x]$ ثابت است، مثلاً $[x] = n$، تجزیه کرده، و بدست می‌آوریم

$$\int_N^\infty \frac{x-[x]}{(x+a)^{s+1}}\,dx = \sum_{n=N}^{\infty} \int_n^{n+1} \frac{x-n}{(x+a)^{s+1}}\,dx = \sum_{n=N}^{\infty} \int_0^1 \frac{u}{(u+n+a)^{s+1}}\,du.$$

لذا، اگر $\sigma > 0$، (۲۵) را می‌توان به شکل زیر نیز نوشت:

$$\zeta(s, a) - \sum_{n=0}^{N} \frac{1}{(n+a)^s} = \frac{(N+a)^{1-s}}{s-1} - s\sum_{n=N}^{\infty} \int_0^1 \frac{u}{(u+n+a)^{s+1}}\,du. \qquad (۲۶)$$

همانطورکه قضیهٔ زیرنشان داده، انتگرالگیری به طریقهٔ جزء به جزء به نمایشهای‌مشابهی بترتیب در نیمصفحه‌های بزرگتر منجر می‌شود.

قضیهٔ ۲۲.۱۲ . *اگر $\sigma > -1$، داریم*

$$\begin{aligned}\zeta(s, a) - \sum_{n=0}^{N} \frac{1}{(n+a)^s} &= \frac{(N+a)^{1-s}}{s-1} \\ &\quad - \frac{s}{2!}\left\{\zeta(s+1, a) - \sum_{n=0}^{N} \frac{1}{(n+a)^{s+1}}\right\} \\ &\quad - \frac{s(s+1)}{2!} \sum_{n=N}^{\infty} \int_0^1 \frac{u^2}{(n+a+u)^{s+2}}\,du.\end{aligned} \qquad (۲۷)$$

بطور کلی، اگر $\sigma > -m$، که در آن $m = 1, 2, 3, \ldots$، داریم

$$\begin{aligned}\zeta(s, a) - \sum_{n=0}^{N} \frac{1}{(n+a)^s} &= \frac{(N+a)^{1-s}}{s-1} - \sum_{r=1}^{m} \frac{s(s+1)\cdots(s+r-1)}{(r+1)!} \\ &\quad \times \left\{\zeta(s+r, a) - \sum_{n=0}^{N} \frac{1}{(n+a)^{s+r}}\right\}\end{aligned} \qquad (۲۸)$$

$$-\frac{s(s+1)\cdots(s+m)}{(m+1)!}$$
$$\times \sum_{n=N}^{\infty}\int_0^1 \frac{u^{m+1}}{(n+a+u)^{s+m+1}}\,du.$$

برهان. انتگرالگیری به طریقهٔ جزء به جزء نتیجه می‌دهد که

$$\int \frac{u\,du}{(n+a+u)^{s+1}} = \frac{u^2}{2(n+a+u)^{s+1}} + \frac{s+1}{2}\int \frac{u^2\,du}{(n+a+u)^{s+2}};$$

درنتیجه، اگر $\sigma > 0$، داریم

$$\sum_{n=N}^{\infty}\int_0^1 \frac{u\,du}{(n+a+u)^{s+1}} = \frac{1}{2}\sum_{n=N}^{\infty}\frac{1}{(n+a+1)^{s+1}}$$
$$+\frac{s+1}{2}\sum_{n=N}^{\infty}\int_0^1 \frac{u^2\,du}{(n+a+u)^{s+2}}.$$

اما، اگر $\sigma > 0$، مجموع اول سمت راست $\zeta(s+1,a) - \sum_{n=0}^{N}(n+a)^{-s-1}$ است، و (۲۶) رابطهٔ (۲۷) را ایجاب می‌کند. این نتیجه، طبق ادامهٔ تحلیلی، به‌ازای $\sigma > -1$ نیز معتبر است. با تکرار انتگرالگیری به طریقهٔ جزء به جزء، نمایش کلیتر (۲۸) بدست خواهد آمد.

۱۵.۱۲ نامساویهایی برای $|\zeta(s, a)|$

فرمولهای بخش‌پیش کرانهایی بالابی برای $|\zeta(\sigma+it,a)|$ به عنوان تابعی از t بدست می‌دهند.

قضیهٔ ۲۳.۱۲ . (آ) هرگاه $\delta > 0$،

به‌ازای $\sigma \ge 1+\delta$، $|\zeta(s,a) - a^{-s}| \le \zeta(1+\delta)$. (۲۹)

(ب) هرگاه $0 < \delta < 1$، ثابت مثبتی مانند $A(\delta)$، وابسته به δ ولی مستقل از s یا a، هست بطوری که

به‌ازای $1-\delta \le \sigma \le 2$ و $|t| \ge 1$، $|\zeta(s,a) - a^{-s}| \le A(\delta)|t|^{\delta}$: (۳۰)

به‌ازای $-\delta \le \sigma \le \delta$ و $|t| \ge 1$، $|\zeta(s,a) - a^{-s}| \le A(\delta)|t|^{1+\delta}$: (۳۱)

به‌ازای $-m-\delta \le \sigma \le -m+\delta$، که $m = 1, 2, 3, \ldots$، و $|t| \ge 1$، (۳۲)

$$|\zeta(s,a)| \le A(\delta)|t|^{m+1+\delta}.$$

برهان. برای قسمت (آ)، با استفاده از سری معرف $\zeta(s, a)$ بدست می‌آوریم

$$|\zeta(s, a) - a^{-s}| \le \sum_{n=1}^{\infty} \frac{1}{(n+a)^{\sigma}} \le \sum_{n=1}^{\infty} \frac{1}{n^{1+\delta}} = \zeta(1+\delta),$$

که (۲۹) را ایجاب می‌کند.

برای قسمت (ب)، با استفاده از نمایش (۲۵) وقتی $1 - \delta \le \sigma \le 2$ خواهیم داشت

$$|\zeta(s, a) - a^{-s}| \le \sum_{n=1}^{N} \frac{1}{(n+a)^{\sigma}} + \frac{(N+a)^{1-\sigma}}{|s-1|} + |s| \int_N^{\infty} \frac{dx}{(x+a)^{\sigma+1}}$$
$$< 1 + \int_1^N \frac{dx}{(x+a)^{\sigma}} + \frac{(N+a)^{1-\sigma}}{|s-1|} + \frac{|s|}{\sigma}(N+a)^{-\sigma}.$$

چون $\sigma \ge 1 - \delta > 0$، داریم $(x+a)^{\sigma} \ge (x+a)^{1-\delta} > x^{1-\delta}$؛ درنتیجه،

$$\int_1^N \frac{dx}{(x+a)^{\sigma}} \le \int_1^N \frac{dx}{x^{1-\delta}} < \frac{N^{\delta}}{\delta}.$$

همچنین، از اینکه $|s-1| = |\sigma - 1 + it| \ge |t| \ge 1$، داریم

$$\frac{(N+a)^{1-\sigma}}{|s-1|} \le (N+a)^{\delta} \le (N+1)^{\delta}.$$

بالاخره، چون $|s| \le |\sigma| + |t| \le 2 + |t|$، معلوم می‌شود که

$$\frac{|s|}{\sigma}(N+a)^{-\sigma} < \frac{2+|t|}{1-\delta}(N+a)^{\delta-1} < \frac{2+|t|}{1-\delta}\frac{1}{N^{1-\delta}}.$$

این نتیجه می‌دهد که

$$|\zeta(s, a) - a^{-s}| < 1 + \frac{N^{\delta}}{\delta} + (N+1)^{\delta} + \frac{2+|t|}{1-\delta}\frac{N^{\delta}}{N}.$$

حال $N = 1 + [|t|]$ را اختیار می‌کنیم. دراین صورت، سه جملهٔ اخیر $O(|t|^{\delta})$ اند، که ثابت ایجاب شده توسط علامت O فقط به δ بستگی دارد. این (۳۰) را ثابت می‌کند.

برای اثبات (۳۱)، از نمایش (۲۷) استفاده می‌کنیم. این نتیجه می‌دهد که

$$|\zeta(s, a) - a^{-s}| \le \sum_{n=1}^{N} \frac{1}{(n+a)^{\sigma}} + \frac{(N+a)^{1-\sigma}}{|s-1|} + \frac{1}{2}|s|\{|\zeta(s+1), a) - a^{-s-1}|\}$$
$$+ \frac{1}{2}|s| \sum_{n=1}^{N} \frac{1}{(n+a)^{\sigma+1}} + \frac{1}{2}|s||s+1| \sum_{n=N}^{\infty} \frac{1}{(n+a)^{\sigma+2}}.$$

مثل برهان (۳۰)، $N = 1 + [|t|]$ رااختیارمی‌کنیم؛ درنتیجه، $N = O(|t|)$، ونشان

می‌دهیم که هر جملهٔ سمت راست $O(|t|^{1+\delta})$ است، که ثابت حاصل از علامت O فقط به δ بستگی دارد. نامساویهای $-\delta \le \sigma \le \delta$ ایجاب می‌کنندکه $1 - \delta \le 1 - \sigma \le 1 + \delta$؛ درنتیجه،

$$\sum_{n=1}^{N} \frac{1}{(n+a)^{\sigma}} < 1 + \int_{1}^{N} \frac{dx}{(x+a)^{\sigma}} < 1 + \frac{(N+a)^{1-\sigma}}{1-\sigma}$$
$$\le 1 + \frac{(N+1)^{1+\delta}}{1-\delta} = O(|t|^{1+\delta}).$$

چون $|s-1| \ge |t| \ge 1$، جملهٔ دوم نیز $O(|t|^{1+\delta})$ است. درجملهٔ سوم (۳۰) رابکار می‌بریم، توجه می‌کنیم که $1 - \delta \le \sigma + 1 \le 1 + \delta$ و $|s| = O(|t|)$، و درمی‌یابیم که این جمله نیز $O(|t|^{1+\delta})$ است. دیگر آنکه، داریم

$$|s| \sum_{n=1}^{N} \frac{1}{(n+a)^{\sigma+1}} = O\left(|t| \int_{1}^{N} \frac{dx}{(x+a)^{1-\delta}}\right)$$
$$= O(|t|N^{-\delta}) = O(|t|^{1-\delta}) = O(|t|^{1+\delta}).$$

بالاخره،

$$|s||s+1| \sum_{n=N}^{\infty} \frac{1}{(n+a)^{\sigma+2}} = O\left(|t|^{2} \int_{N}^{\infty} \frac{dx}{(x+a)^{\sigma+2}}\right) = O(|t|^{2}N^{-\sigma-1})$$
$$= O(|t|^{2}N^{\delta-1}) = O(|t|^{1+\delta}).$$

این برهان (۳۱) را تمام می‌کند.

برهان (۳۲) مشابه فوق است، جز آنکه از (۲۸) استفاده کرده و توجه می‌کنیم که، وقتی $\sigma < 0$، $a^{-\sigma} = O(1)$.

۱۶.۱۲ نامساویهایی برای $|\zeta(s)|$ و $|L(s, \chi)|$

وقتی $a = 1$، تخمینها در قضیهٔ ۲۳.۱۲ تخمینهای متناظری برای $|\zeta(s)|$ بدست می‌دهند. این تخمینها به کرانهایی برای L ـ سریهای دیریکله منجر می‌شوند. اگر $\sigma \ge 1 + \delta$، که در آن $\delta > 0$؛ هردوی $|\zeta(s)|$ و $|L(s, \chi)|$ تحت تسلط $\zeta(1+\delta)$ هستند؛ درنتیجه، فقط $\sigma \le 1 + \delta$ را درنظر می‌گیریم.

قضیهٔ ۲۴.۱۲. فرض کنیم χ یک مشخص دیریکله به هنگ k بوده، و نیز $0 < \delta < 1$. *دراین صورت، ثابت مثبتی مانند $A(\delta)$، که وابسته به δ ولی مستقل از s یا k است، وجود دارد بطوری که، به‌ازای $s = \sigma + it$ با $|t| \ge 1$،*

اگر $-m - \delta \le \sigma \le -m + \delta$ ، که در آن $m = -1, 0, 1, 2, \ldots$ ،

$$|L(s, \chi)| \le A(\delta)|kt|^{m+1+\delta}. \qquad (۳۳)$$

برهان . رابطهٔ

$$L(s, \chi) = k^{-s}\sum_{r=1}^{k-1} \chi(r)\zeta\left(s, \frac{r}{k}\right)$$

را به‌یاد می‌آوریم . اگر $m = 1, 2, 3, \ldots$ ، با استفاده از (۳۲) بدست می‌آید

$$|L(s, \chi)| \le k^{-\sigma}\sum_{r=1}^{k-1} \left|\zeta\left(s, \frac{r}{k}\right)\right| < k^{m+\delta}kA(\delta)|t|^{m+1+\delta},$$

که (۳۳) را به‌ازای $m \ge 1$ ثابت می‌کند . اگر 0 یا $m = -1$ ، می‌نویسیم

$$L(s, \chi) = \sum_{r=1}^{k-1} \frac{\chi(r)}{r^s} + k^{-s}\sum_{r=1}^{k-1} \chi(r)\left\{\zeta\left(s, \frac{r}{k}\right) - \left(\frac{r}{k}\right)^{-s}\right\}. \qquad (۳۴)$$

چون $-m - \delta \le \sigma \le -m + \delta$ ، می‌توان با استفاده از (۳۰) و (۳۱) بدست آورد که

$$k^{-\sigma}\left|\zeta\left(s, \frac{r}{k}\right) - \left(\frac{r}{k}\right)^{-s}\right| \le k^{m+\delta}A(\delta)|t|^{m+1+\delta};$$

درنتیجه ، مجموع دوم در (۳۴) تحت تسلط $A(\delta)|kt|^{m+1+\delta}$ است . مجموع اول تحت تسلط

$$\sum_{r=1}^{k-1} \frac{1}{r^\sigma} \le \sum_{r=1}^{k-1} r^{m+\delta} < 1 + \int_1^k x^{m+\delta}\, dx = \frac{k^{m+1+\delta}}{m+1+\delta} \le \frac{k^{m+1+\delta}}{\delta}$$

است ، و این مجموع را نیز می‌توان در تخمین $A(\delta)|kt|^{m+1+\delta}$ جذب کرد .

تمرین برای فصل ۱۲

۱ . فرض‌کنید $f(n)$ یک تابع حسابی باشد که متناوب به هنگ k است .

(آ) ثابت‌کنید سری دیریکلهٔ $\sum f(n)n^{-s}$ به‌ازای $\sigma > 1$ به‌طور مطلق همگراست‌و ،

اگر $\sigma > 1$ ، $\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = k^{-s}\sum_{r=1}^{k} f(r)\zeta\left(s, \frac{r}{k}\right)$.

(ب) اگر $\sum_{r=1}^{k} f(r) = 0$ ، ثابت کنید سری دیریکلهٔ $\sum f(n)n^{-s}$ به‌ازای $\sigma > 0$ همگراست ،وتابع تمامی‌مانند $F(s)$ هست‌بطوری‌که به‌ازای $\sigma > 0$ ، $F(s) = \sum f(n)n^{-s}$.

۲ . اگر x حقیقی بوده و $\sigma > 1$ ، $F(x, s)$ را تابع زتای متناوب بگیرید :

$$F(x, s) = \sum_{n=1}^{\infty} \frac{e^{2\pi i n x}}{n^s}.$$

اگر $0 < a < 1$ و $\sigma > 1$ ، ثابت کنید فرمول هرویتس ایجاب می‌کند که

$$F(a, s) = \frac{\Gamma(1-s)}{(2\pi)^{1-s}} \{e^{\pi i(1-s)/2}\zeta(1-s, a) + e^{\pi i(s-1)/2}\zeta(1-s, 1-a)\}.$$

۳ . اگر $0 < a < 1$ ، با استفاده از فرمول تمرین ۲ می‌توان تعریف $F(a, s)$ را روی تمام صفحهٔ s تعمیم‌داد . ثابت‌کنید این $F(a, s)$ تعمیم یافته یک تابع تمام از s است .

۴ . اگر $0 < a < 1$ و $0 < b < 1$ ، قرار دهید

$$\Phi(a, b, s) = \frac{\Gamma(s)}{(2\pi)^s} \{\zeta(s, a)F(b, 1+s) + \zeta(s, 1-a)F(1-b, 1+s)\},$$

که در آن F تابع تمرین ۲ است . ثابت کنید

$$\frac{\Phi(a, b, s)}{\Gamma(s)\Gamma(-s)} = e^{\pi i s/2}\{\zeta(s, a)\zeta(-s, 1-b) + \zeta(s, 1-a)\zeta(-s, b)\}$$
$$+ e^{-\pi i s/2}\{\zeta(-s, 1-b)\zeta(s, 1-a) + \zeta(-s, b)\zeta(s, a)\},$$

و نتیجه‌بگیرید که $\Phi(a, b, s) = \Phi(1-b, a, -s)$. این معادلهٔ تابعی در نظریهٔ‌توابع هنگی بیضوی مفید است .

در تمرینهای ۵ ، ۶ ، و ۷ ، $\xi(s)$ تابع تمام مذکور در بخش ۱۲ . ۸ است :

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

۵ . ثابت کنید که $\xi(s)$ بر خطوط $t = 0$ و $\sigma = 1/2$ حقیقی است ، و $\xi(0) = \xi(1) = 1/2$.

۶ . ثابت کنید که صفرهای $\xi(s)$ (در صورت وجود) همه در نوار $0 \le \sigma \le 1$ قرار داشته و به‌طور متقارن حول خطوط $t = 0$ و $\sigma = 1/2$ واقعند .

۷ . نشان دهید که صفرهای $\xi(s)$ در نوار بحرانی $0 < \sigma < 1$ (درصورت وجود) با صفرهای $\zeta(s)$ دارای یک موضع و یک مرتبهٔ تکرار هستند .

۸ . فرض کنید χ یک مشخص اولیه به هنگ k باشد . تعریف کنید

$$a = a(\chi) = \begin{cases} 0 & \text{اگر } \chi(-1) = 1 \text{ ،} \\ 1 & \text{اگر } \chi(-1) = -1 \text{ ،} \end{cases}$$

(آ) نشان دهید که معادلهٔ تابعی مربوط‌به $L(s, \chi)$ به شکل زیر است :

$L(1-s, \bar{\chi}) = \varepsilon(\chi)2(2\pi)^{-s}k^{s-\frac{1}{2}}\cos\left(\frac{\pi(s-a)}{2}\right)\Gamma(s)L(s, \chi)$ ، که در آن $|\varepsilon(\chi)| = 1$.

(ب) فرض کنید

$$\xi(s, \chi) = \left(\frac{k}{\pi}\right)^{(s+a)/2} \Gamma\left(\frac{s+a}{2}\right) L(s, \chi).$$

نشان دهید که $\xi(1-s, \bar{\chi}) = \varepsilon(\chi)\xi(s, \chi)$.

۹ . به تمرین ۸ بازمی‌گردیم .

(آ) ثابت کنید که اگر $\sigma > 1$ یا $\sigma < 0$ ، $\xi(s, \chi) \neq 0$.

(ب) مواضع صفرهای $L(s, \chi)$ در نیمصفحهٔ $\sigma < 0$ را توصیف کنید .

۱۰ . فرض کنید χ یک مشخص غیر اصلی به هنگ k باشد . مواضع صفرهای $L(s, \chi)$ در نیمصفحهٔ $\sigma < 0$ را توصیف کنید .

۱۱ . ثابت کنید که چندجمله‌ایهای برنولی در روابط زیر صدق می‌کنند :
به‌ازای هر $n \geq 0$ ، $B_n(1-x) = (-1)^n B_n(x)$ و $B_{2n+1}(\frac{1}{2}) = 0$.

۱۲ . فرض کنید B_n عدد برنولی n م باشد . توجه کنید که

$$B_2 = \tfrac{1}{6} = 1 - \tfrac{1}{2} - \tfrac{1}{3}, \qquad B_4 = \tfrac{-1}{30} = 1 - \tfrac{1}{2} - \tfrac{1}{3} - \tfrac{1}{5},$$
$$B_6 = \tfrac{1}{42} = 1 - \tfrac{1}{2} - \tfrac{1}{3} - \tfrac{1}{7}$$

این فرمولها مبین قضیه‌ای هستند که در ۱۸۴۰ به‌وسیلهٔ فون اشتات [1] و کلاسن [2] (مستقل از هم) کشف شده است . اگر $n \geq 1$ ، داریم

$$B_{2n} = I_n - \sum_{p-1|2n} \frac{1}{p},$$

که در آن I_n عددی صحیح است و مجموع روی تمام اعداد p گرفته می‌شود که $p-1$ ، $2n$ را عاد می‌کند . این تمرین برهانی منسوب به لوکاس [3] را مختصرا" شرح می‌دهد .

(آ) ثابت کنید که

$$B_n = \sum_{k=0}^{n} \frac{1}{k+1} \sum_{r=0}^{k} (-1)^r \binom{k}{r} r^n.$$

[**راهنمایی .** بنویسید $x = \log\{1 + (e^x - 1)\}$ و از سری توانی مربوط به $x/(e^x - 1)$ استفاده کنید .]

(ب) ثابت کنید

---

1. von Staudt
2. Clausen
3. Lucas

$$B_n = \sum_{k=0}^{n} \frac{k!}{k+1} c(n, k),$$

که در آن $c(n, k)$ عددی صحیح است.

(پ) اگر a, b صحیح بوده و داشته باشیم $a \geq 2$ ، $b \geq 2$ ، و $ab > 4$ ، ثابت کنید $ab|(ab-1)!$. این نشان می‌دهد که، در مجموع قسمت (ب) ، هر جمله با $k+1$ مرکب، که $k > 3$ ، یک عدد صحیح است.

(ت) هرگاه p اول باشد، ثابت کنید

$$\sum_{r=0}^{p-1} (-1)^r \binom{p-1}{r} r^n \equiv \begin{cases} -1 \pmod p & \text{اگر } p-1|n \text{ و } n > 0 \text{ ،} \\ 0 \pmod p & \text{اگر } p-1 \nmid n \text{ ،} \end{cases}$$

(ث) با استفاده از نتایج فوق یا روشی دیگر، قضیهٔ فون اشتات ـ کلاسن را ثابت کنید.

۱۳ . ثابت کنید که اگر $n \geq 2$ ، مشتق چندجمله‌ای برنولی $B_n(x)$ مساوی $nB_{n-1}(x)$ است.

۱۴ . ثابت کنید چندجمله‌ایهای برنولی در فرمول جمع

$$B_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} B_k(x) y^{n-k}$$

صدق می‌کنند.

۱۵ . ثابت کنید چندجمله‌ایهای برنولی در فرمول ضرب

$$B_p(mx) = m^{p-1} \sum_{k=0}^{m-1} B_p\left(x + \frac{k}{m}\right)$$

صدق می‌کنند.

۱۶ . ثابت کنید که اگر $r \geq 1$ ، اعداد برنولی در رابطهٔ

$$\sum_{k=0}^{r} \frac{2^{2k} B_{2k}}{(2k)!(2r+1-2k)!} = \frac{1}{(2r)!}$$

صدق می‌کنند.

۱۷ . انتگرال $\int_0^1 x B_p(x)\, dx$ را به دو راه حساب کرده، و فرمول زیر را نتیجه بگیرید:

$$\sum_{r=0}^{p} \binom{p}{r} \frac{B_r}{p+2-r} = \frac{B_{p+1}}{p+1}.$$

۱۸ . (آ) اتحاد زیر را ثابت کنید:

$$\frac{uv}{(e^u-1)(e^v-1)} \frac{e^{u+v}-1}{u+v} = \frac{uv}{u+v}\left(1 + \frac{1}{e^u-1} + \frac{1}{e^v-1}\right)$$

$$= 1 + \sum_{n=2}^{\infty} \frac{uv}{n!}\left(\frac{u^{n-1} + v^{n-1}}{u+v}\right)B_n.$$

(ب) فرض‌کنید $J = \int_0^1 B_p(x)B_q(x)\,dx$. نشان دهید که J ضریب $p!q!u^pv^q$ دربسط قسمت (آ) است. با استفاده از این، نتیجه بگیرید که

$$\int_0^1 B_p(x)B_q(x)\,dx = \begin{cases} (-1)^{p+1}\dfrac{p!q!}{(p+q)!}B_{p+q} & \text{اگر } p \ge 1, q \ge 1 \text{ ،} \\ 1 & \text{اگر } p = q = 0 \text{ ،} \\ 0 & \text{اگر } p \ge 1, q = 0 \text{ ، یا } p = 0, q \ge 1 \text{ ،} \end{cases}$$

۱۹ . (آ) با استفاده از روشی شبیه روش تمرین ۱۸ ، اتحاد زیر را نتیجه بگیرید :

$$(u+v)\sum_{m=0}^{\infty}\sum_{n=0}^{\infty} B_m(x)B_n(x)\frac{u^mv^n}{m!n!} = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} B_{m+n}(x)\frac{u^mv^n}{m!n!}\sum_{r=0}^{\infty}\frac{B_{2r}}{(2r)!}(u^{2r}v + uv^{2r}).$$

(ب) ضرایب قسمت (آ) را مقایسه کرده و، با انتگرالگیری از نتیجه، فرمول زیر را به‌ازای $m \ge 1, n \ge 1$ بدست آورید :

$$B_m(x)B_n(x) = \sum_r \left\{\binom{m}{2r}n + \binom{n}{2r}m\right\}\frac{B_{2r}B_{m+n-2r}(x)}{m+n-2r} + (-1)^{m+1}\frac{m!n!}{(m+n)!}B_{m+n}.$$

برد اندیس r را نشان دهید.

۲۰ . نشان دهید که اگر $m \ge 1$ ، $n \ge 1$ ، و $p \ge 1$ ، داریم

$$\int_0^1 B_m(x)B_n(x)B_p(x)\,dx$$
$$= (-1)^{p+1}p!\sum_r \left\{\binom{m}{2r}n + \binom{n}{2r}m\right\}\frac{(m+n-2r-1)!}{(m+n+p-2r)!}B_{2r}B_{m+n+p-2r}.$$

در حالت خاص، $\int_0^1 B_2{}^3(x)\,dx$ را از این فرمول حساب کنید.

۲۱ . فرض‌کنید $f(n)$ یک تابع حسابی باشد که متناوب به هنگ k است، و

$$g(n) = \frac{1}{k}\sum_{m \bmod k} f(m)e^{-2\pi imn/k}$$

ضرایب فوریه متناهی f باشند. اگر

$$F(s) = k^{-s}\sum_{r=1}^{k} f(r)\zeta\left(s, \frac{r}{k}\right),$$

ثابت کنید

$$F(1-s) = \frac{\Gamma(s)}{(2\pi)^s}\left\{e^{\pi is/2}\sum_{r=1}^{k} g(r)\zeta\left(s, \frac{r}{k}\right) + e^{-\pi is/2}\sum_{r=1}^{k} g(-r)\zeta\left(s, \frac{r}{k}\right)\right\}.$$

۲۲ . فرض کنید χ یک مشخص غیر اصلی به هنگ k بوده ، و $S(x) = \sum_{n \le x} \chi(n)$.

(آ) اگر $N \ge 1$ و $\sigma > 0$ ، ثابت کنید

$$L(s, \chi) = \sum_{n=1}^{N} \frac{\chi(n)}{n^s} + s \int_N^{\infty} \frac{S(x) - S(N)}{x^{s+1}}\, dx.$$

(ب) اگر $s = \sigma + it$ ، $\sigma \ge \delta > 0$ ، و $|t| \ge 0$ ، با استفاده از قسمت (آ) نشان دهید که ثابتی مانند $A(\delta)$ هست بطوری که

$$|L(s, \chi)| \le A(\delta) B(k) (|t| + 1)^{1-\delta}$$

که در آن $B(k)$ یک کران بالایی برای $|S(x)|$ است . در قضیهٔ ۱۵۰۱۳ نشان دادیم که $B(k) = O(\sqrt{k} \log k)$.

(پ) ثابت کنید ، به‌ازای ثابتی چون $A > 0$ ،

$$|L(s, \chi)| \le A \log k$$ ، $0 \le |t| \le 2$ و $\sigma \ge 1 - \frac{1}{\log k}$ اگر

[راهنمایی . در قسمت (آ) $N = k$ را اختیار کنید .]

۱۳ برهان تحلیلی قضیهٔ اعداد اول

۱۰۱۳ طرح برهان

قضیهٔ اعداد اول معادل حکم زیر است:

$$\psi(x) \sim x \text{ ، } x \to \infty \text{ وقتی } \text{ ،} \qquad (۱)$$

که در آن $\psi(x)$ تابع چبیشف است:

$$\psi(x) = \sum_{n \le x} \Lambda(n).$$

در این فصل یک برهان تحلیلی برای (۱) مبتنی بر خواص تابع زتای ریمان ارائه می‌دهیم. برهان تحلیلی از برهـان مقدماتی مذکور در فصل ۴ کوتاهتر است، و ایده‌های اصلی‌اش آسانتر فهمیده می‌شوند. در این بخش نکات اصلی این برهان را به اختصار شرح می‌دهیم.

تابع ψ یک تابع پلـه‌ای است، و راحتتر اسـت که انتگرال آن را، که با ψ_1 نشان می‌دهیم، در نظر بگیریم. لذا، انتگرال

$$\psi_1(x) = \int_1^x \psi(t)\, dt$$

را درنظر مـی‌گیریم. انتگـرال ψ_1 یک تابع خطی قطعه قطعه پیوسته است. ابتدا نشان می‌دهیم که رابطهٔ مجانبی

$$\psi_1(x) \sim \frac{1}{2}x^2 \text{ ، } x \to \infty \text{ وقتی} \qquad (۲)$$

(۱) را ایجاب می‌کند، وسپس (۲) را ثابت می‌کنیم. برای این‌کار، $\psi_1(x)/x^2$ را برحسب تابع زتای ریمان و به‌وسیلهٔ یک انتگرال کنتوری بیان می‌کنیم:

$$\frac{\psi_1(x)}{x^2} = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} \frac{x^{s-1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right) ds \text{ ، که در آن } c > 1 \text{ .}$$

خارج قسمت $-\zeta'(s)/\zeta(s)$ دارای قطب مرتبهٔ اول در $s = 1$ با ماندهٔ 1 است. اگر این قطب را جدا کنیم، فرمول زیر بدست خواهد آمد:

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2}\left(1 - \frac{1}{x}\right)^2 = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} \frac{x^{s-1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}\right) ds \text{ ، } c > 1 \text{ به‌ازای}$$

قرار می‌دهیم

$$h(s) = \frac{1}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}\right)$$

و معادلهٔ اخیر را به‌شکل زیر می‌نویسیم:

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2}\left(1 - \frac{1}{x}\right)^2 = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} x^{s-1} h(s)\, ds \tag{۳}$$
$$= \frac{x^{c-1}}{2\pi}\int_{-\infty}^{+\infty} h(c+it)e^{it\log x}\, dt.$$

برای اتمام برهان، باید نشان داد که

$$\lim_{x\to\infty} \frac{x^{c-1}}{2\pi}\int_{-\infty}^{+\infty} h(c+it)e^{it\log x}\, dt = 0. \tag{۴}$$

اما لم ریمان ــ لبگ در نظریهٔ سریهای فوریه می‌گوید که اگر انتگرال $\int_{-\infty}^{+\infty} |f(t)|\, dt$ همگرا باشد،

$$\lim_{x\to\infty}\int_{-\infty}^{+\infty} f(t)e^{itx}\, dt = 0$$

انتگرال (۴) از این‌نوع‌است، که در آن x با $\log x$ عوض شده است، ومی‌توان‌به‌آسانی نشان داد که انتگرال $\int_{-\infty}^{+\infty} |h(c+it)|\, dt$ در صورت $c > 1$ همگراست؛ درنتیجه، انتگرال

(۴)، وقتی $x \to \infty$، به 0 میل می‌کند. اما، عامل x^{c-1} خارج انتگرال، وقتی $c > 1$، به ∞ میل می‌کند؛ درنتیجه، با صورت مبهم $0 \cdot \infty$ روبروهستیم. معادلهٔ (۳) به‌ازای هر $c > 1$ برقرار است. اگر می‌شد در (۳) بگذاریم $c = 1$، عامل مشکل‌زای x^{c-1} ناپدید می‌شود. اما، دراین صورت، $h(c+it)$ می‌شود $h(1+it)$ و انتگرالده‌مستلزم $\zeta'(s)/\zeta(s)$ بر خط $\sigma = 1$ می‌باشد. درایــن حالت، اثبات همگرایی انتگرال $\int_{-\infty}^{+\infty} |h(1+it)|\, dt$ مشکلتر

است، نکته‌ای کــه قبل از اعمال لم ریمان ــ لبگ باید تحقیق شود. آخرین و مشکلترین بخش برهان نشــان دادن این است که می‌توان در (۳) c را با 1 عوض کرد و انتگرال $\int_{-\infty}^{+\infty} |h(1+it)|\, dt$ همگرا می‌بــاشد. این امر به بررسی مشروحتری از تابع زتای ریمان در

مجاورت خط $\sigma = 1$ نیاز دارد .

حال بــه برنامه‌ای کــه خطوطش در بالا ترسیم شد می‌پردازیم . بحث را با چند لم آغاز می‌کنیم .

۲۰۱۳ چند لم

لم ۱ . به‌ازای هر تابع حسابی $a(n)$ ، قرار می‌دهیم

$$A(x) = \sum_{n \le x} a(n),$$

که در آن اگر $x < 1$ ، $A(x) = 0$. **در این صورت ،**

$$\sum_{n \le x} (x - n)a(n) = \int_1^x A(t)\, dt. \tag{۵}$$

برهان . اتحاد آبـل (قضیهٔ ۲۰۴) را بکار می‌بریم ، که می‌گوید اگر f بر $[1, x]$ مشتق پیوسته داشته باشد ،

$$\sum_{n \le x} a(n) f(n) = A(x) f(x) - \int_1^x A(t) f'(t)\, dt \quad . \tag{۶}$$

با فرض $f(t) = t$ ، داریم

$$A(x)f(x) = x \sum_{n \le x} a(n) \quad \text{و} \quad \sum_{n \le x} a(n) f(n) = \sum_{n \le x} n a(n)$$

درنتیجه، (۶) به (۵) تحویل خواهد شد .

لم بعدی شکل قاعدهٔ هوپیتال[1] برای توابع قطعه قطعه خطی صعودی است .

لم ۲ . فرض‌کنیم $A(x) = \sum_{n \le x} a(n)$ **و** $A_1(x) = \int_1^x A(t)\, dt$. **همچنین ، به‌ازای هر** n ، $a(n) \ge 0$. **هرگاه فرمول مجانبی زیر را به‌ازای** $c > 0$ **ای و** $L > 0$ **ی داشته باشیم**

$$\text{وقتی } x \to \infty \text{ ، } A_1(x) \sim Lx^c \text{ ،} \tag{۷}$$

آنگاه نیز خواهیم داشت

---

1. L'Hôspital

وقتی $x \to \infty$ ، $A(x) \sim cLx^{c-1}$ ·

(۸)

به عبارت دیگر، مشتقگیری صوری از (۷) نتیجهٔ صحیح می‌دهد.

برهان. تابع $A(x)$ صعودی است، زیرا $a(n)$ نامنفی است. $\beta > 1$ ای اختیار کرده و تفاضل $A_1(\beta x) - A_1(x)$ را درنظر می‌گیریم. داریم

$$A_1(\beta x) - A_1(x) = \int_x^{\beta x} A(u)\,du \geq \int_x^{\beta x} A(x)\,du = A(x)(\beta x - x)$$
$$= x(\beta - 1)A(x).$$

این نتیجه می‌دهد که

$$xA(x) \leq \frac{1}{\beta - 1}\{A_1(\beta x) - A_1(x)\}$$

یا

$$\frac{A(x)}{x^{c-1}} \leq \frac{1}{\beta - 1}\left\{\frac{A_1(\beta x)}{(\beta x)^c}\beta^c - \frac{A_1(x)}{x^c}\right\}.$$

β را ثابت گرفته و در این نامساوی فرض می‌کنیم $x \to \infty$. درمی‌یابیم که

$$\limsup_{x\to\infty} \frac{A(x)}{x^{c-1}} \leq \frac{1}{\beta - 1}(L\beta^c - L) = L\frac{\beta^c - 1}{\beta - 1}.$$

حال فرض کنیم $\beta \to 1+$. خارج قسمت سمت راست خارج قسمت تفاضلی برای مشتق x^c در $x = 1$ است و دارای حد c می‌باشد. بنابراین،

$$\limsup_{x\to\infty} \frac{A(x)}{x^{c-1}} \leq cL. \tag{۹}$$

حال α ی دلخواهی که $0 < \alpha < 1$ درنظر گرفته و تفاضل $A_1(x) - A_1(\alpha x)$ را تشکیل می‌دهیم. استدلالی مشابه فوق نشان می‌دهد که

$$\liminf_{x\to\infty} \frac{A(x)}{x^{c-1}} \geq L\frac{1 - \alpha^c}{1 - \alpha}.$$

وقتی $\alpha \to 1-$، طرف راست به cL میل می‌کند. این، همراه با (۹)، نشان می‌دهد که، وقتی $x \to \infty$ ، $A(x)/x^{c-1}$ به حد cL میل خواهد کرد.

وقتی $a(n) = \Lambda(n)$، داریم $A(x) = \psi(x)$ ، $A_1(x) = \psi_1(x)$ ، و $a(n) \geq 0$. لذا، می‌توان لمهای ۱ و ۲ را بکار برده و فورا" قضیهٔ زیر را بدست آورد.

قضیهٔ ۱۰۱۳ . داریم

$$\psi_1(x) = \sum_{n \le x} (x-n)\Lambda(n). \qquad (۱۰)$$

همچنین، رابطهٔ مجانبی $\psi_1(x) \sim x^2/2$ ایجاب می‌کند که، وقتی $x \to \infty$ ، $\psi(x) \sim x$.

کار بعدی ما بیان $\psi_1(x)/x^2$ به صورت یک انتگرال کنتوری شامل تابع زتاست . برای این کار، به‌حالات خاص $k = 1$ و $k = 2$ لم زیر در باب انتگرالهای کنتوری نیاز داریم . (با لم ۴ در فصل ۱۱ قیاس کنید .)

لم ۳ . ***هرگاه $c > 0$ و $u > 0$ ، آنگاه، به‌ازای هر عدد صحیح $k \ge 1$ ،***

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} \frac{u^{-z}}{z(z+1)\cdots(z+k)}\,dz = \begin{cases} \frac{1}{k!}(1-u)^k & \text{اگر } 0 < u \le 1 \\ 0 & \text{اگر } u > 1 \end{cases}$$

انتگرال به‌طور مطلق همگراست .

برهان . ابتدا توجه می‌کنیم که انتگرالده مساوی $u^{-z}\Gamma(z)/\Gamma(z+k+1)$ است . این امر از استفادهٔ مکرر معادلهٔ تابعی $\Gamma(z+1) = z\Gamma(z)$ نتیجه می‌شود . برای اثبات لم ، قضیهٔ ماندهٔ کشی را بر انتگرال

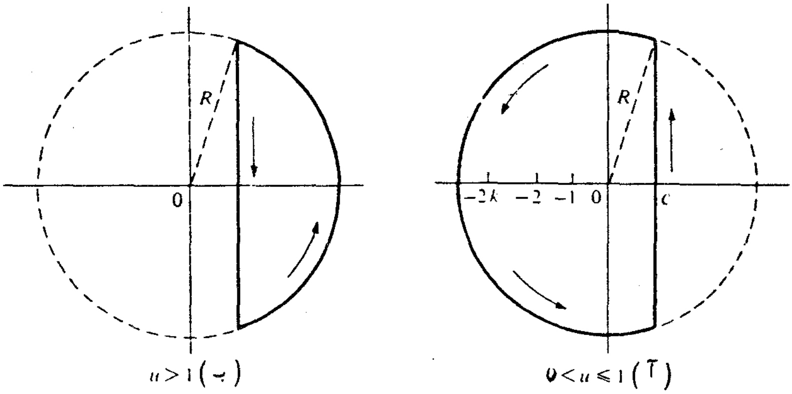
$$\frac{1}{2\pi i}\int_{C(R)} \frac{u^{-z}\Gamma(z)}{\Gamma(z+k+1)}\,dz$$

اعمال می‌کنیم ، که در آن $C(R)$ کنتور شکل ۱۰۱۳ (آ) است اگر $0 < u \le 1$ ، و کنتور شکل ۱۰۱۳ (ب) است اگر $u > 1$. شعاع R دایره بزرگتر از $2k + c$ است ؛ درنتیجه، همهٔ قطبها در $z = 0, -1, \ldots, -k$ داخل دایره قرار دارند .

حال نشان می‌دهیم که، وقتی $R \to \infty$ انتگرال در امتداد هر قوس مستدیر به 0 میل می‌کند . اگر $z = x + iy$ و $|z| = R$ ، انتگرالده تحت تسلط

$$\left|\frac{u^{-z}}{z(z+1)\cdots(z+k)}\right| = \frac{u^{-x}}{|z||z+1|\cdots|z+k|} \le \frac{u^{-c}}{R|z+1|\cdots|z+k|}$$

است . نامساوی $u^{-x} \le u^{-c}$ ازاین‌امرکه u^{-x} یک‌تابع صعودی‌از x است‌اگر $0 < u \le 1$ ویک تابع نزولی است اگر $u > 1$ نتیجه می‌شود . حال اگر $1 \le n \le k$ ، داریم



شکل ۱۰۱۳

$$|z+n| \geq |z| - n = R - n \geq R - k \geq R/2$$

زیرا $R > 2k$. لذا ، انتگرال در امتداد هر قوس مستدیر تحت تسلط

$$\frac{2\pi R u^{-c}}{R(\frac{1}{2}R)^k} = O(R^{-k})$$

است ، و چون $k \geq 1$ ، این ، وقتی $R \to \infty$ ، به 0 میل خواهد کرد .

اگر $u > 1$ ، انتگرالده داخل $C(R)$ تحلیلی است ؛ درنتیجه ، $\int_{C(R)} = 0$. با فرض $R \to \infty$ ، درمی‌یابیم که لم دراین حالت ثابت شده است .

اگر $0 < u \leq 1$ ، انتگرال‌رابه‌وسیلهٔ‌قضیهٔ‌ماندهٔ‌کشی حول $C(R)$ حساب می‌کنیم . انتگرالده در اعداد صحیح $n = 0, -1, \ldots, -k$ دارای قطب است ؛ درنتیجه ،

$$\begin{aligned}\frac{1}{2\pi i}\int_{C(R)} \frac{u^{-z}\Gamma(z)}{\Gamma(z+k+1)}\,dz &= \sum_{n=0}^{k} \operatorname*{Res}_{z=-n} \frac{u^{-z}\Gamma(z)}{\Gamma(z+k+1)} \\ &= \sum_{n=0}^{k} \frac{u^n}{\Gamma(k+1-n)} \operatorname*{Res}_{z=-n} \Gamma(z) = \sum_{n=0}^{k} \frac{u^n(-1)^n}{(k-n)!\,n!} \\ &= \frac{1}{k!}\sum_{n=0}^{k}\binom{k}{n}(-u)^n = \frac{(1-u)^k}{k!}.\end{aligned}$$

با فرض $R \to \infty$ ، لم بدست خواهد آمد .

۳.۱۳ نمایش انتگرال کنتوری برای $\psi_1(x)/x^2$

قضیهٔ ۲.۱۳ . *اگر $c > 1$ و $x \geq 1$ ، داریم*

$$\frac{\psi_1(x)}{x^2} = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} \frac{x^{s-1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right) ds. \tag{۱۱}$$

برهان. از معادلهٔ (۱۰) داریم $\psi_1(x)/x = \sum_{n\le x}(1-n/x)\Lambda(n)$. حال لم ۳ را به ازای $k=1$ و $u=n/x$ بکار می‌بریم . اگر $n \le x$ ، بدست می‌آید که

$$1-\frac{n}{x} = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{(x/n)^s}{s(s+1)}\,ds.$$

با ضرب این رابطه در $\Lambda(n)$ و جمعبندی روی همهٔ $n \le x$ های ، معلوم می‌شود که

$$\frac{\psi_1(x)}{x} = \sum_{n\le x}\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{\Lambda(n)(x/n)^s}{s(s+1)}\,ds = \sum_{n=1}^{\infty}\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{\Lambda(n)(x/n)^s}{s(s+1)}\,ds$$

زیرا انتگرال به‌ازای $n > x$ صفر می‌شود . این را می‌توان به صورت زیر نوشت :

$$\frac{\psi_1(x)}{x} = \sum_{n=1}^{\infty}\int_{c-\infty i}^{c+\infty i} f_n(s)\,ds, \tag{۱۲}$$

که در آن $2\pi i f_n(x) = \Lambda(n)(x/n)^s/(s^2+s)$. حال می‌خواهیم مجموع و انتگرال را در (۱۲) عوض کنیم . برای این کار ، کافی است ثابت شود که سری

$$\sum_{n=1}^{\infty}\int_{c-\infty i}^{c+\infty i}|f_n(s)|\,ds \tag{۱۳}$$

همگراست . (ر.ک. قضیهٔ ۱۰.۲۶ در [۲] .) مجموعهای جزئی این سری در نامساوی زیر صدق می‌کنند :

$$\sum_{n=1}^{N}\int_{c-\infty i}^{c+\infty i}\frac{\Lambda(n)(x/n)^c}{|s||s+1|}\,ds = \sum_{n=1}^{N}\frac{\Lambda(n)}{n^c}\int_{c-\infty i}^{c+\infty i}\frac{x^c}{|s||s+1|}\,ds \le A\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^c},$$

که در آن A ثابت است ؛ درنتیجه ، (۱۳) همگرا می‌باشد . لذا ، می‌توان مجموع و انتگرال در (۱۲) را با هم عوض کرد و بدست آورد که

$$\frac{\psi_1(x)}{x} = \int_{c-\infty i}^{c+\infty i}\sum_{n=1}^{\infty} f_n(s)\,ds = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{x^s}{s(s+1)}\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}\,ds$$

$$= \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{x^s}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right) ds.$$

حال با تقسیم بر x (۱۱) بدست خواهد آمد .

قضیهٔ ۳.۱۳ . *اگر* $c > 1$ *و* $x \ge 1$ *، داریم*

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2}\left(1 - \frac{1}{x}\right)^2 = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} x^{s-1} h(s)\, ds, \tag{۱۴}$$

که درآن

$$h(s) = \frac{1}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}\right). \tag{۱۵}$$

برهان. این بار، با استفاده از لم ۳ بهازای $k = 2$ ، بدست میآوریم

$$\frac{1}{2}\left(1 - \frac{1}{x}\right)^2 = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} \frac{x^s}{s(s+1)(s+2)}\, ds,$$

که درآن $c > 0$. از تعویض s با $s - 1$ در انتگرال (با فرض $c > 1$)و تفریق حاصل از (۱۱) ، قضیهٔ ۳۰۱۳ بدست خواهد آمد.

اگر مسیر انتگرالگیری را با نوشتن $s = c + it$ پارامتریزه کنیم ، درمییابیم که $x^{s-1} = x^{c-1}x^{it} = x^{c-1}e^{it\log x}$ و معادلهٔ (۱۴) خواهد شد

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2}\left(1 - \frac{1}{x}\right)^2 = \frac{x^{c-1}}{2}\int_{c-\infty i}^{c+\infty i} h(c+it)e^{it\log x}\, dt. \tag{۱۶}$$

کار بعدی ما نشان دادن این است که طرف راست (۱۶) ، وقتی $x \to \infty$ ، به 0 میل میکند. همانطور که قبلاً ذکرشد، ابتدا نشان میدهیم که میتوان در (۱۶) $c = 1$ قرار داد. برای اینکار، کافی است $\zeta(s)$ را در همسایگی خط $\sigma = 1$ بررسی کنیم.

۴۰۱۳ کرانهای بالایی برای $|\zeta(s)|$ و $|\zeta'(s)|$ نزدیک خط $\sigma = 1$

برای بررسی $\zeta(s)$ در نزدیکیخط $\sigma = 1$ ، از نمایش حاصل ازقضیهٔ ۲۱۰۱۲ ، که بهازای $\sigma > 0$ معتبر است، استفادهمیکنیم:

$$\zeta(s) = \sum_{n=1}^{N}\frac{1}{n^s} - s\int_N^\infty \frac{x - [x]}{x^{s+1}}\, dx + \frac{N^{1-s}}{s-1}. \tag{۱۷}$$

همچنین، از فرمول مربوط به $\zeta'(s)$ که از مشتقگیری طرفین (۱۷) بدست میآید، استفاده میکنیم:

$$\zeta'(s) = -\sum_{n=1}^{N}\frac{\log n}{n^s} + s\int_N^\infty \frac{(x-[x])\log x}{x^{s+1}}\, dx - \int_N^\infty \frac{x-[x]}{x^{s+1}}\, dx - \frac{N^{1-s}\log N}{s-1} - \frac{N^{1-s}}{(s-1)^2}. \tag{۱۸}$$

در قضیهٔ زیر از این روابط برای بدست آوردن کرانهای بالایی برای $|\zeta(s)|$ و $|\zeta'(s)|$ استفاده می‌کنیم .

قضیهٔ ۴.۱۳ . به‌ازای هر $A > 0$ ، ثابتی مانند M (وابستهٔ به A) وجود دارد بطوری که

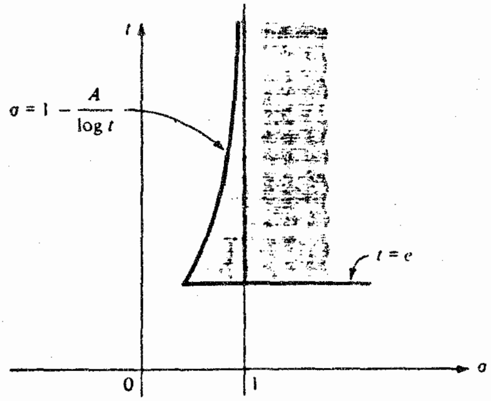
$$|\zeta(s)| \le M \log t \quad \text{و} \quad |\zeta'(s)| \le M \log^2 t \tag{۱۹}$$

و اینها به‌ازای هر s با $\sigma \ge 1/2$ و صادق در

$$t \ge e \quad \text{و} \quad \sigma > 1 - \frac{A}{\log t} \tag{۲۰}$$

برقرارند .

تذکر. نامساویهای (۲۰) ناحیه‌ای از نوع نموده در شکل ۲.۱۳ را توصیف می‌کنند .



شکل ۲.۱۳

برهان. اگر $\sigma \ge 2$ ، داریم $|\zeta(s)| \le \zeta(2)$ و $|\zeta'(s)| \le |\zeta'(2)|$ ونامساویهای (۱۹) بداهتاً برقرارند . لذا ، می‌توان فرض کرد $\sigma < 2$ و $t \ge e$. دراین صورت ، داریم

$$|s| \le \sigma + t \le 2 + t < 2t \quad \text{و} \quad |s - 1| \ge t \text{ ؛}$$

درنتیجه ، $1/|s-1| \le 1/t$. اگر $|\zeta(s)|$ را بااستفاده از (۱۷) تخمین بزنیم ، درمی‌یابیم که

$$|\zeta(s)| \le \sum_{n=1}^{N} \frac{1}{n^\sigma} + 2t \int_N^\infty \frac{1}{x^{\sigma+1}}\,dx + \frac{N^{1-\sigma}}{t} = \sum_{n=1}^{N} \frac{1}{n^\sigma} + \frac{2t}{\sigma N^\sigma} + \frac{N^{1-\sigma}}{t}.$$

حال، با اختیار $N = [t]$، N را به t وابسته می‌کنیم. پس $N \le t < N + 1$ و، اگر $n \le N$، $\log n \le \log t$. نامساوی (۲۰) ایجاب می‌کند که $1 - \sigma < A/\log t$؛ درنتیجه،

$$\frac{1}{n^{\sigma}} = \frac{n^{1-\sigma}}{n} = \frac{1}{n} e^{(1-\sigma)\log n} < \frac{1}{n} e^{A \log n/\log t} \le \frac{1}{n} e^{A} = O\left(\frac{1}{n}\right).$$

لذا،

$$\frac{2t}{\sigma N^{\sigma}} < \frac{N+1}{N} = O(1) \quad \text{و} \quad \frac{N^{1-\sigma}}{t} = \frac{N}{t}\frac{1}{N^{\sigma}} = O\left(\frac{1}{N}\right) = O(1)\text{؛}$$

درنتیجه،

$$|\zeta(s)| = O\left(\sum_{n=1}^{N} \frac{1}{n}\right) + O(1) = O(\log N) + O(1) = O(\log t).$$

این نامساوی مربوط به $|\zeta(s)|$ در (۱۹) را ثابت می‌کند. برای بدست آوردن نامساوی مربوط به $|\zeta'(s)|$، همین نوع استدلال را درمورد (۱۸) بکار می‌بریم. تنها فرق اساسی این است که عامل اضافی $\log N$ سمت راست ظاهر می‌شود. اما $\log N = O(\log t)$؛ در نتیجه، در ناحیهٔ مشخص شده خواهیم داشت $|\zeta'(s)| = O(\log^2 t)$.

۵.۱۳ صفر نشدن $\zeta(s)$ بر خط $\sigma = 1$

در این بخش ثابت می‌کنیم به‌ازای هر t حقیقی، $\zeta(1 + it) \ne 0$. برهان بر نامساویی استوار است که در بخش بعد نیز لازم می‌شود.

قضیهٔ ۵.۱۳. *اگر $\sigma > 1$، داریم*

$$\zeta^3(\sigma)|\zeta(\sigma + it)|^4|\zeta(\sigma + 2it)| \ge 1. \tag{۲۱}$$

برهان. اتحاد $\zeta(s) = e^{G(s)}$ را که در بخش ۹.۱۱، مثال ۱، ثابت شد به‌یاد می‌آوریم، که در آن

$$G(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} n^{-s} = \sum_{p} \sum_{m=1}^{\infty} \frac{1}{mp^{ms}} \qquad (\sigma > 1).$$

این را می‌توان به صورت زیر نوشت:

$$\zeta(s) = \exp\left\{\sum_{p} \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}\right\} = \exp\left\{\sum_{p} \sum_{m=1}^{\infty} \frac{e^{-imt\log p}}{mp^{m\sigma}}\right\},$$

که از آن معلوم می‌شود که

$$|\zeta(s)| = \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{\cos(mt \log p)}{mp^{m\sigma}}\right\}.$$

این فرمول را چندبار به‌ازای $s = \sigma$ ، $s = \sigma + it$ ، و $s = \sigma + 2it$ بکار برده، وبدست می‌آوریم

$$\zeta^3(\sigma)|\zeta(\sigma + it)|^4|\zeta(\sigma + 2it)| = \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{3 + 4\cos(mt \log p) + \cos(2mt \log p)}{mp^{m\sigma}}\right\}.$$

اما نامساوی مثلثاتی زیر را داریم :

$$3 + 4\cos\theta + \cos 2\theta \geq 0,$$

که از اتحاد زیر نتیجه می‌شود :

$$3 + 4\cos\theta + \cos 2\theta = 3 + 4\cos\theta + 2\cos^2\theta - 1 = 2(1 + \cos\theta)^2.$$

لذا ، هرجمله در سری نامتناهی اخیر نامنفی است ؛ درنتیجه ، (۲۱) بدست خواهدآمد .

قضیهٔ ۶.۱۳ . به‌ازای هر t حقیقی ، داریم $\zeta(1 + it) \neq 0$.

برهان. کافی است $t \neq 0$ را درنظر بگیریم . (۲۱) را به شکل زیر می‌نویسیم

$$\{(\sigma - 1)\zeta(\sigma)\}^3 \left|\frac{\zeta(\sigma + it)}{\sigma - 1}\right|^4 |\zeta(\sigma + 2it)| \geq \frac{1}{\sigma - 1}. \qquad (۲۲)$$

این درصورتی که $\sigma > 1$ معتبر است . حال فرض کنیم در (۲۲) $\sigma \to 1+$. عامل اول به 1 نزدیک می‌شود ، زیرا $\zeta(s)$ درقطب $s = 1$ ماندهٔ 1 دارد . عامل سوم به $|\zeta(1 + 2it)|$ میل می‌کند . اگر $\zeta(1 + it)$ مساوی 0 می‌بود ، عامل وسط را می‌شد به‌صورت زیر نوشت :

وقتی $\sigma \to 1+$ ، $\left|\frac{\zeta(\sigma + it) - \zeta(1 + it)}{\sigma - 1}\right|^4 \to |\zeta'(1 + it)|^4$.

لذا ، اگر به‌ازای $t \neq 0$ ای می‌داشتیم $\zeta(1 + it) = 0$ ، طرف‌چپ (۲۲) ، وقتی $\sigma \to 1+$ ، به حد $|\zeta'(1 + it)|^4|\zeta(1 + 2it)|$ نزدیک مـی‌شد . امـا طرف راست ، وقتی $\sigma \to 1+$ ، به ∞ میل می‌کند ، و این تناقضی بدست خواهد داد .

۶.۱۳ نامساویهایی برای $|1/\zeta(s)|$ و $|\zeta'(s)/\zeta(s)|$

حال قضیهٔ ۵.۱۳ را بـار دیگر بکار برده ، نامساویهای زیر را برای $|1/\zeta(s)|$ و $|\zeta'(s)/\zeta(s)|$ بدست می‌آوریم .

قضیهٔ ۷.۱۳ . ثابتی مانند $M > 0$ هست بطوری که هر وقت $\sigma \geq 1$ و $t \geq e$ ،

$$\left|\frac{1}{\zeta(s)}\right| < M \log^7 t \quad \text{و} \quad \left|\frac{\zeta'(s)}{\zeta(s)}\right| < M \log^9 t \, .$$

برهان. بهازای $\sigma \geq 2$ ، داریم

$$\left|\frac{1}{\zeta(s)}\right| = \left|\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right| \leq \sum_{n=1}^{\infty} \frac{1}{n^2} \leq \zeta(2)$$

و

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leq \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^2} ;$$

درنتیجه ،اگر $\sigma \geq 2$ ، نامساویها بداهتا "برقرارند . پس فرض کنیم $1 \leq \sigma \leq 2$ و $t \geq e$. نامساوی (۲۱) را بهصورت زیر مینویسیم :

$$\frac{1}{|\zeta(\sigma + it)|} \leq \zeta(\sigma)^{3/4} |\zeta(\sigma + 2it)|^{1/4}.$$

اما $(\sigma - 1)\zeta(\sigma)$ در بازهٔ $1 \leq \sigma \leq 2$ کراندار است ؛ مثلا " $(\sigma - 1)\zeta(\sigma) \leq M$ ، که در آن M یک ثابت مطلق است . دراین صورت ،

اگر $1 < \sigma \leq 2$ ، $\zeta(\sigma) \leq \dfrac{M}{\sigma - 1}$.

همچنین ، اگر $1 < \sigma \leq 2$ ، $\zeta(\sigma + 2it) = O(\log t)$ (قضیهٔ ۴.۱۳) ؛ درنتیجه ، اگر $1 \leq \sigma \leq 2$ ، داریم

$$\frac{1}{|\zeta(\sigma + it)|} \leq \frac{M^{3/4}(\log t)^{1/4}}{(\sigma - 1)^{3/4}} = \frac{A(\log t)^{1/4}}{(\sigma - 1)^{3/4}},$$

که در آن A یک ثابت مطلق است . لذا ، بهازای ثابتی چون $B > 0$ ،

اگر $1 < \sigma \leq 2$ و $t \geq e$ ، $|\zeta(\sigma + it)| > \dfrac{B(\sigma - 1)^{3/4}}{(\log t)^{1/4}}$. (۲۳)

این بهازای $\sigma = 1$ نیز بداهتا " برقرار است . فرض کنیم α عدد دلخواهی صادق در $1 < \alpha < 2$ باشد . دراین صورت ، اگر $t \geq e$ ،$1 \leq \sigma \leq \alpha$ ، با استفاده از قضیهٔ ۴.۱۳ میتوان نوشت

$$|\zeta(\sigma + it) - \zeta(\alpha + it)| \leq \int_{\sigma}^{\alpha} |\zeta'(u + it)| \, du \leq (\alpha - \sigma) M \log^2 t$$
$$\leq (\alpha - 1) M \log^2 t.$$

از اینرو، طبق نامساوی مثلثی،

$$|\zeta(\sigma + it)| \geq |\zeta(\alpha + it)| - |\zeta(\sigma + it) - \zeta(\alpha + it)|$$
$$\geq |\zeta(\alpha + it)| - (\alpha - 1)M \log^2 t \geq \frac{B(\alpha - 1)^{3/4}}{(\log t)^{1/4}} - (\alpha - 1)M \log^2 t.$$

این درصورت $1 \leq \sigma \leq 2$ برقرار است و، بنابر (۲۳)، به‌ازای $\alpha \leq \sigma \leq 2$ نیز برقرار است، زیرا $(\sigma - 1)^{3/4} \geq (\alpha - 1)^{3/4}$. به‌عبارت دیگر، اگر $1 \leq \sigma \leq \alpha$ و $t \geq e$، به‌ازای هر α صادق در $1 < \alpha < 2$ نامساوی زیر راداریم:

$$|\zeta(\sigma + it)| \geq \frac{B(\alpha - 1)^{3/4}}{(\log t)^{1/4}} - (\alpha - 1)M \log^2 t \, .$$

حال α را به t وابسته کرده و آن را طوری می‌گیریم که جملهٔ اول سمت راست دوبرابر جملهٔ دوم باشد. برای این لازم است

$$\alpha = 1 + \left(\frac{B}{2M}\right)^4 \frac{1}{(\log t)^9} \, .$$

واضح‌است‌که $\alpha > 1$ و، اگربه‌ازای t_0 ی $t \geq t_0$، $\alpha < 2$. لذا، اگر $t \geq t_0$ و $1 \leq \sigma \leq 2$، خواهیم داشت

$$|\zeta(\sigma + it)| \geq (\alpha - 1)M \log^2 t = \frac{C}{(\log t)^7} \, .$$

اگر $e \leq t \leq t_0$، نامساوی نیز (شاید) با C ای متفاوت برقرار است. این ثابت می‌کندکه به‌ازای هر $\sigma \geq 1, t \geq e$، $|\zeta(s)| \geq C \log^{-7} t$، که به ما کران بالایی متناظری برای $|1/\zeta(s)|$ می‌دهد. برای بدست آوردن نامساوی برای $|\zeta'(s)/\zeta(s)|$، قضیهٔ ۴.۱۳ را بکار برده و عامل اضافی $\log^2 t$ را بدست می‌آوریم.

۷.۱۳ اتمام برهان قضیهٔ اعداد اول

حال تقریبا" آماده‌ایم که برهان قضیهٔ اعداد اول را تمام کنیم. به یک مطلب دیگر از نظریهٔ توابع مختلط نیاز داریم، که آن را به‌صورت لم بیان می‌کنیم.

لم ۴. *هرگاه $f(s)$ در $s = \alpha$ قطبی از مرتبهٔ k داشته باشد، آنگاه خارج قسمت $f'(s)/f(s)$ قطبی از مرتبهٔ اول در $s = \alpha$ با ماندهٔ $-k$ دارد.*

برهان. داریم $f(s) = g(s)/(s - \alpha)^k$، که در آن g در α تحلیلی بوده و $g(\alpha) \neq 0$.

از اینرو، به‌ازای هر s در همسایگی α ، داریم

$$f'(s) = \frac{g'(s)}{(s-\alpha)^k} - \frac{kg(s)}{(s-\alpha)^{k+1}} = \frac{g(s)}{(s-\alpha)^k}\left\{\frac{-k}{s-\alpha} + \frac{g'(s)}{g(s)}\right\}.$$

لذا،

$$\frac{f'(s)}{f(s)} = \frac{-k}{s-\alpha} + \frac{g'(s)}{g(s)}.$$

این لم را ثابت می‌کند، زیرا $g'(s)/g(s)$ در α تحلیلی است.

قضیهٔ ۸.۱۳ . *تابع*

$$F(s) = -\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$$

در $s = 1$ تحلیلی است.

برهان. بنابــر لم ۴، $-\zeta'(s)/\zeta(s)$ در 1 یک قطب مرتبهٔ اول با ماندهٔ 1 دارد، همین طور است $1/(s-1)$. از اینرو، تفاضل آنها در $s = 1$ تحلیلی است.

قضیهٔ ۹.۱۳ . *به‌ازای $x \geq 1$ ، داریم*

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2}\left(1-\frac{1}{x}\right)^2 = \frac{1}{2\pi}\int_{-\infty}^{\infty} h(1+it)e^{it\log x}\,dt,$$

که در آن انتگرال $\int_{-\infty}^{\infty} |h(1+it)|\,dt$ *همگراست. لذا، طبق لم ریمان ــ لبگ، داریم*

$$\psi_1(x) \sim x^2/2\,; \tag{۲۴}$$

و درنتیجه،

وقتی $x \to \infty$ ، $\psi(x) \sim x$.

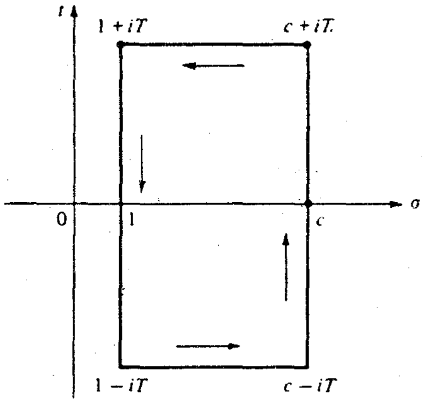
برهان. در قضیهٔ ۳.۱۳ ثابت شد که اگر $c > 1$ و $x \geq 1$ ، داریم

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2}\left(1-\frac{1}{x}\right)^2 = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} x^{s-1}h(s)\,ds,$$

که در آن

$$h(s) = \frac{1}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}\right).$$

اولین کار ما نشان دادن این است که می‌توان مسیر انتگرالگیری را به خط $\sigma = 1$ حرکت داد. برای این کار، قضیهٔ کشی را بر مستطیل R شکل ۳۰۱۳ اعمال می‌کنیم. انتگرال



شکل ۳۰۱۳

$x^{s-1}h(s)$ حول R مساوی 0 است، زیرا انتگرالده داخل و بر R تحلیلی است. حال‌نشان می‌دهیم که، وقتی $T \to \infty$، انتگرالها در امتداد پاره خطهای افقی به 0 میل می‌کنند. چون انتگرالده درنقاط مزدوج یک قدر مطلق دارد، کافی است فقط پاره خط بالایی، یعنی $t = T$، را درنظر بگیریم. براین پاره خط تخمینهای زیر را داریم:

$$\left|\frac{1}{s(s+1)}\right| \leq \frac{1}{T^2} \quad \text{و} \quad \left|\frac{1}{s(s+1)(s-1)}\right| \leq \frac{1}{T^3} \leq \frac{1}{T^2}.$$

همچنین، ثابتی مانند M هست بطوری‌که‌اگر $\sigma \geq 1$ و $t \geq e$، $|\zeta'(s)/\zeta(s)| \leq M \log^9 t$. از اینرو، اگر $T \geq e$، داریم

$$|h(s)| \leq \frac{M \log^9 T}{T^2};$$

درنتیجه،

$$\left|\int_1^c x^{s-1}h(s)\,ds\right| \leq \int_1^c x^{c-1}\frac{M \log^9 T}{T^2}\,d\sigma = Mx^{c-1}\frac{\log^9 T}{T^2}(c-1).$$

لذا، اگر $T \to \infty$، انتگرالهادرامتداد پاره خطهای افقی به 0 میل می‌کنند؛ ودرنتیجه، خواهیم داشت

$$\int_{c-\infty i}^{c+\infty i} x^{s-1}h(s)\,ds = \int_{1-\infty i}^{1+\infty i} x^{s-1}h(s)\,ds.$$

بر خط $\sigma = 1$ می‌نویسیم $s = 1 + it$ ، خواهیم داشت

$$\frac{1}{2\pi i}\int_{1-\infty i}^{1+\infty i} x^{s-1}h(s)\,ds = \frac{1}{2\pi}\int_{-\infty}^{\infty} h(i+it)e^{it\log x}\,dt.$$

حال توجه می‌کنیم که

$$\int_{-\infty}^{\infty}|h(1+it)|\,dt = \int_{-e}^{e} + \int_{e}^{\infty} + \int_{-\infty}^{-e}.$$

در انتگرال از e تا ∞ ، داریم

$$|h(1+it)| \le \frac{M\log^9 t}{t^2}\ ;$$

درنتیجه ، $\int_e^\infty |h(1+it)|\,dt$ همگراست . بهمین نحو ، $\int_{-\infty}^{-e}$ همگراست ؛ درنتیجه ، $\int_{-\infty}^{\infty} |h(1+it)|\,dt$ همگرامی‌باشد . لذا ، می‌توان لم ریمان ـ لبگ را بکار برده بدست‌آورد که $\psi_1(x) \sim x^2/2$. این ، بنابرقضیهٔ ۱۰۱۳ ، ایجاب می‌کندکه‌وقتی $x \to \infty$ ، $\psi(x) \sim x$ ، و این برهان قضیهٔ اعداد اول را تمام خواهد کرد .

۸۰۱۳ نواحی فارغ از صفر برای $\zeta(s)$

نامساوی $|1/\zeta(s)| < M\log^7 t$ ، که در قضیهٔ ۷۰۱۳ به‌ازای $\sigma \ge 1$ و $t \ge e$ ثابت شد ، را می‌توان به‌طرف چپ خط $\sigma = 1$ تعمیم داد . تخمین در یک نوار قائم بدست نیامده‌است ، بلکه در نـاحیه‌ای بدست آمده که بنوعی شبیه ناحیهٔ شکل ۲۰۱۳ است ، که در آن کرانهٔ چپ منحنی ، وقتی $t \to \infty$ ، به‌طور مجانبی به خط $\sigma = 1$ نزدیک می‌شود . نامساوی‌صفر نشدن $\zeta(s)$ را دراین ناحیه ایجاب می‌کند . به‌طور دقیقتر ،

قضیهٔ ۱۰۰۱۳ . فرض‌کنیم $\sigma \ge 1/2$. دراین‌صورت ، ثابتهایی‌مانند $A > 0$ و $C > 0$ هستند بطوری که

$$|\zeta(\sigma+it)| > \frac{C}{\log^7 t}$$

هر وقت

$$1 - \frac{A}{\log^9 t} < \sigma \le 1 \quad \text{و} \quad t \ge e \tag{۲۵}$$

برقرار است . این ایجـاب می‌کند که اگر σ و t در (۲۵) صدق کنند ، $\zeta(\sigma+it) \ne 0$.

برهان. نامساوی مثلثی، همراه‌با قضیهٔ ۷۰۱۳، نتیجه می‌دهد که، به‌ازای $B > 0$ ای،

$$|\zeta(\sigma + it)| \geq |\zeta(1 + it)| - |\zeta(1 + it) - \zeta(\sigma + it)| \tag{۲۶}$$
$$> \frac{B}{\log^7 t} - |\zeta(1 + it) - \zeta(\sigma + it)|.$$

برای تخمین آخرین جمله، می‌نویسیم

$$|\zeta(1 + it) - \zeta(\sigma + it)| = \left|\int_\sigma^1 \zeta'(u + it)\, du\right| \leq \int_\sigma^1 |\zeta'(u + it)|\, du.$$

چون $t \geq e$، داریم $\log^9 t \geq \log t$؛ درنتیجه، $1 - (A/\log^9 t) \geq 1 - (A/\log t)$.
لذا، اگر σ به‌ازای هر $A > 0$ در (۲۵) صدق کند، می‌توان قضیهٔ ۴۰۱۳ را برای تخمین $|\zeta'(u - it)|$ بکار برد، که نتیجه می‌دهد

$$|\zeta(1 + it) - \zeta(\sigma + it)| \leq M(1 - \sigma)\log^2 t < M \log^2 t \frac{A}{\log^9 t} = \frac{MA}{\log^7 t}.$$

با استفاده از این در (۲۶)، معلوم می‌شود که

$$|\zeta(\sigma + it)| > \frac{B - MA}{\log^7 t}.$$

این نامساوی به‌ازای $B > 0$، هر $A > 0$، و $M > 0$ ی وابسته‌به A برقرار است. یک مقدار از M که به‌ازای A ای بکار رود، برای هر A ی کوچکتر نیز کارساز است. لذا، A را می‌توان آنقدر کوچک گرفت که $B - MA > 0$. اگر قرار دهیم $C = B - MA$، آخرین‌نامساوی‌خواهدشد $|\zeta(\sigma + it)| > C \log^{-7} t$، که قضیه را به‌ازای هر σ و t صادق در

$$t \geq e \quad \text{و} \quad 1 - \frac{A}{\log^9 t} < \sigma < 1$$

ثابت می‌کند. امااین‌نتیجه، طبق قضیهٔ ۷۰۱۳، برای $\sigma = 1$ نیز برقرار است؛ درنتیجه، برهان تمام خواهد بود.

می‌دانیم که اگر $\sigma \geq 1$، $\zeta(s) \neq 0$، و معادلهٔ تابعی

$$\zeta(s) = 2(2\pi)^{1-s}\Gamma(1 - s)\sin\left(\frac{\pi s}{2}\right)\zeta(1 - s)$$

نشان می‌دهد که‌اگر $\sigma \leq 0$، جز به‌ازای صفرها در $s = -2, -4, -6, \ldots$ که از صفر شدن $\sin(\pi s/2)$ ناشی می‌شوند، $\zeta(s) \neq 0$. اینها را صفرهای "بدیهی" $\zeta(s)$ می‌نامند.

قضیهٔ زیر نشان می‌دهد که، صرف نظر از صفرهای بدیهی، $\zeta(s)$ صفر دیگری بر محور حقیقی ندارد.

قضیهٔ ۱۱.۱۳. *اگر* $\sigma > 0$*، داریم*

$$(1 - 2^{1-s})\zeta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}. \qquad (۲۷)$$

این ایجاب می‌کند که اگر s *حقیقی بوده و* $0 < s < 1$*،* $\zeta(s) < 0$.

برهان. ابتدا فرض می‌کنیم $\sigma > 1$. دراین صورت، داریم

$$\begin{aligned}(1 - 2^{1-s})\zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} - 2\sum_{n=1}^{\infty} \frac{1}{(2n)^s}\\ &= (1 + 2^{-s} + 3^{-s} + \cdots) - 2(2^{-s} + 4^{-s} + 6^{-s} + \cdots)\\ &= 1 - 2^{-s} + 3^{-s} - 4^{-s} + 5^{-s} - 6^{-s} + \cdots,\end{aligned}$$

که (۲۷) را به‌ازای $\sigma > 1$ ثابت می‌کند. اما، اگر $\sigma > 0$، سری سمت راست همگراست؛ درنتیجه، (۲۷)، طبق ادامهٔ تحلیلی، به‌ازای $\sigma > 0$ نیز برقرار می‌باشد.

وقتی s حقیقی باشد، سری (۲۷) یک سری متناوب با مجموع مثبت است. اگر $0 < s < 1$، عامل $(1 - 2^{1-s})$ منفی است، درنتیجه، $\zeta(s)$ نیز منفی می‌باشد.

۹.۱۳ فرض ریمان

ریمان[۵۸] دریادداشت ۸ صفحه‌ای مشهورش در ۱۸۵۹ درباب $\pi(x)$ می‌گوید که احتمالاً "صفرهای نابدیهی $\zeta(s)$ همه بر خط $\sigma = 1/2$ قرار دارند، اگر چه وی نتوانست آن را ثابت کند. اکنون این حکم که همهٔ صفرهای نابدیهی جزء حقیقی $1/2$ دارند را **فرض ریمان** می‌نامند. در سال ۱۹۰۰، هیلبرت[1] مسئلهٔ اثبات یارد فرض ریمان را به‌عنوان یکی از مهمترین مسائل برای ریاضیدانان قرن بیستم ذکر کرد. این مسئله تا امروز لاینحل مانده است.

فرض ریمان نظر بسیاری از ریاضیدانان معروف را بخود جلب کرد، و مطالب زیادی درباب توزیع صفرهای $\zeta(s)$ کشف شده است. معادلهٔ تابعی نشان می‌دهد که تمام صفرهای نابدیهی (درصورت وجود) باید در نوار $0 < \sigma < 1$، به نام "نوار بحرانی" قرارداشته باشند. به‌آسانی معلوم می‌شود که صفرها به‌طور متقارن حول محور حقیقی و حول "خط

---

1. Hilbert

بحرانی" $\sigma = 1/2$ واقع اند.

درسال ۱۹۱۵، هاردی ثابت کرد که بی‌نهایت صفر بر خط بحرانی وجود دارند. درسال ۱۹۲۱، هاردی و لیتلوود نشان دادند که، اگر T به قدر کافی بزرگ باشد، تعداد صفرهای واقع برپاره‌خط بین $1/2$ و $(1/2) + iT$، به‌ازای‌ثابتی چون A، دست کم‌مساوی AT است. در سال ۱۹۴۲، سلبرگ این مطلب را با نشان دادن اینکه این عدد، به‌ازای $A > 0$ ای، دست کم مساوی $AT \log T$ است، اصلاح کرد. همچنین، معلوم شده است‌که این‌عدددرنوار بحرانی که در آن $0 < t < T$، وقتی $T \to \infty$، با $T \log T/2\pi$ مجانب است؛ لذا، نتیجهٔ سلبرگ‌نشان‌می‌دهد که کسر مثبتی از صفرها بر خط‌بحرانی قراردارند. اخیرا" (۱۹۷۴) لوینسون[1] نشان داد که این کسر دست کم $7/10$ است. یعنی، ثابت قضیهٔ سلبرگ در $A \geq 7/20\pi$ صدق می‌کند.

محاسبات گسترده توسط گرام[2]، بکلوند[3]، لمر، هیزل‌گرو[4]، روسر[5]، یوهه[6]، شونفلد[7]، و دیگران نشان داده است که سه میلیون و نیم صفراول بالای‌محورحقیقی‌برخط بحرانی قرار دارند. با وجود همهٔ این شواهد در جهت فرض ریمان، محاسبات نیز چند پدیده را آشکارکرده‌اندکه‌ممکن است مثالهای‌نقضی برای فرض ریمان وجود داشته باشند. برای خواندن داستان‌جالبی‌ازمحاسبات به مقیاس بزرگ در باب $\zeta(s)$، خواننده‌می‌تواند به [۱۷] مراجعه کند.

۱۳. ۱۰ کاربرد در مورد تابع مقسوم علیهی

گاهی قضیهٔ اعداداول رامی‌توان‌برای تخمین مرتبهٔ بزرگی توابع حسابی ضربی بکاربرد. در این بخش، از آن برای بدست‌آوردن نامساویهایی برای $d(n)$، یعنی تعداد مقسوم علیه‌های n، استفاده می‌کنیم.

درفصل ۳ ثابت شد که مرتبهٔ متوسط $d(n)$ مساوی $\log n$ است. وقتی n اول باشد، داریم $d(n) = 2$، درنتیجه، رشد $d(n)$ وقتی بیشترین نمودرا دارد که n مقسوم علیه‌های زیادی داشته باشد. فرض‌کنیم n حاصل ضرب‌همهٔ‌اعداداول نابیشتر از x باشد؛ مثلا"،

$$n = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p_{\pi(x)}. \qquad (۲۸)$$

چون $d(n)$ ضربی است، داریم

$$d(n) = d(2)d(3) \cdots d(p_{\pi(x)}) = 2^{\pi(x)}.$$

---

1. Levinson 2. Gram 3. Backlund 4. Haselgrove
5. Rosser 6. Yohe 7. Schoenfeld

به‌ازای x بزرگ، $\pi(x)$ تقریبا" مساوی $x/\log x$ است و (۲۸) ایجاب می‌کند که

$$\log n = \sum_{p \le x} \log p = \vartheta(x) \sim x\,;$$

درنتیجه، $2^{\pi(x)}$ تقریبا" مساوی $2^{\log n/\log\log n}$ است. اما

$$2^{a\log n} = e^{a\log n\log 2} = n^{a\log 2}\,;$$

درنتیجه، $2^{\log n/\log\log n} = n^{\log 2/\log\log n}$. به‌عبارت‌دیگر، وقتی n به شکل (۲۸) باشد، $d(n)$ تقریبا" مساوی $2^{\log n/\log\log n} = n^{\log 2/\log\log n}$ است.

اگر این ایده را باکمی‌دقت تعقیب کنیم، نامساویهای زیر برای $d(n)$ بدست‌می‌آیند.

قضیهٔ ۱۲.۱۳ . فرض‌کنیم $\varepsilon > 0$ داده شده باشد. در این صورت،

(آ) عدد صحیحی مانند $N(\varepsilon)$ هست بطوری که $n \ge N(\varepsilon)$ ایجاب می‌کند که

$$d(n) < 2^{(1+\varepsilon)\log n/\log\log n} = n^{(1+\varepsilon)\log 2/\log\log n}.$$

(ب) به‌ازای بی‌نهایت n، داریم

$$d(n) > 2^{(1-\varepsilon)\log n/\log\log n} = n^{(1-\varepsilon)\log 2/\log\log n}.$$

تذکر. این نامساویها معادل رابطهٔ

$$\limsup_{n\to\infty} \frac{\log d(n)\log\log n}{\log n} = \log 2$$

می‌باشند.

برهان. می‌نویسیم $n = p_1^{a_1}\cdots p_k^{a_k}$؛ درنتیجه، $d(n) = \prod_{i=1}^{k}(a_i+1)$. حاصلضرب را به‌دو قسمت تجزیه‌می‌کنیم به این ترتیب که آن مقسوم علیه‌های اول کوچکتر از $f(n)$ را ازآن مقسوم علیه‌های اول ناکمتر از $f(n)$ جدا می‌کنیم، که $f(n)$ بعدا" معین خواهد شد. پس $d(n) = P_1(n)P_2(n)$، که در آن

$$P_1(n) = \prod_{p_i < f(n)} (a_i+1) \quad \text{و} \quad P_2(n) = \prod_{p_i \ge f(n)} (a_i+1).$$

در حاصل ضرب $P_2(n)$، از نامساوی $(a+1) \le 2^a$ استفاده کرده بدست می‌آوریم $P_2(n) \le 2^{S(n)}$، که در آن

$$S(n) = \sum_{\substack{i=1 \\ p_i \ge f(n)}}^{k} a_i.$$

اما

$$n = \prod_{i=1}^{k} p_i^{a_i} \geq \prod_{p_i \geq f(n)} p_i^{a_i} \geq \prod_{p_i \geq f(n)} f(n)^{a_i} = f(n)^{S(n)};$$

درنتیجه،

$$\log n \geq S(n)\log f(n) \quad \text{یا} \quad S(n) \leq \frac{\log n}{\log f(n)}.$$

این نتیجه می‌دهد که

$$P_2(n) \leq 2^{\log n/\log f(n)}. \qquad (۲۹)$$

برای تخمین $P_1(n)$، می‌نویسیم

$$P_1(n) = \exp\left\{\sum_{p_i < f(n)} \log(a_i + 1)\right\}$$

و نشان‌می‌دهیم‌که اگر n به قدر کافی بزرگ باشد، $\log(a_i + 1) < 2\log\log n$. درواقع، داریم

$$n \geq p_i^{a_i} \geq 2^{a_i};$$

درنتیجه،

$$\log n \geq a_i \log 2 \quad \text{یا} \quad a_i \leq \log n/\log 2.$$

از اینرو، به‌ازای n_1 ی،

$$\text{اگر } n \geq n_1 \text{،} \quad 1 + a_i \leq 1 + \frac{\log n}{\log 2} < (\log n)^2.$$

لذا، $n \geq n_1$ ایجاب می‌کند که $\log(1 + a_i) < \log(\log n)^2 = 2\log\log n$. این نتیجه می‌دهد که

$$P_1(n) < \exp\left\{2\log\log n \sum_{p_i < f(n)} 1\right\} \leq \exp\{2\log\log n\, \pi(f(n))\}.$$

با استفاده از نامساوی $\pi(x) < 6x/\log x$ (ر.ک. قضیهٔ ۶.۴)، بدست می‌آوریم

$$P_1(n) < \exp\left\{\frac{12f(n)\log\log n}{\log f(n)}\right\} = 2^{cf(n)\log\log n/\log f(n)}, \qquad (۳۰)$$

که درآن $c = 12/\log 2$. از تلفیق (۲۹) با (۳۰)، بدست می‌آوریم $d(n) = P_1(n)P_2(n) < 2^{g(n)}$، که درآن

$$g(n) = \frac{\log n + cf(n)\log\log n}{\log f(n)} = \frac{\log n}{\log\log n}\,\frac{1 + c\dfrac{f(n)\log\log n}{\log n}}{\dfrac{\log f(n)}{\log\log n}}.$$

حال $f(n)$ را طوری می‌گیریم که[۸] وقتی $n \to \infty$ ، $f(n)\log\log n/\log n \to 0$ و نیز $\log f(n)/\log\log n \to 1$. برای این‌کار ، کافی است

$$f(n) = \frac{\log n}{(\log\log n)^2}$$

را اختیار کنیم . دراین صورت ، اگر به‌ازای $N(\varepsilon)$ ی $n \geq N(\varepsilon)$ ،

$$g(n) = \frac{\log n}{\log\log n}\frac{1+o(1)}{1+o(1)} = \frac{\log n}{\log\log n}(1+o(1)) < (1+\varepsilon)\frac{\log n}{\log\log n} \cdot$$

این قسمت (آ) را ثابت می‌کند .

برای اثبات قسمت (ب) ، مجموعه‌ای از اعداد صحیح n دارای تعداد زیادی عامل اول اختیارمی‌کنیم . درواقع ، n را حاصل ضرب همهٔ اعداد اول نابیشتر از x می‌گیریم . دراین صورت ، $n \to x$ اگر و فقط اگر $x \to \infty$. طبق قضیهٔ اعداد اول ، به‌ازای چنین n ، داریم

$$d(n) = 2^{\pi(x)} = 2^{(1+o(1))x/\log x}.$$

همچنین ، به‌ازای چنین n ، خواهیم داشت

$$\log n = \sum_{p\leq x}\log p = \vartheta(x) = x(1+o(1));$$

درنتیجه ،

$$x = \frac{\log n}{1+o(1)} = (1+o(1))\log n \cdot$$

لذا ،

$$\log x = \log\log n + \log(1+o(1)) = \log\log n\left(1 + \frac{\log(1+o(1))}{\log\log n}\right)$$
$$= (1+o(1))\log\log n.$$

از اینرو ، به‌ازای چنین n ، $x/\log x = (1+o(1))\log n/\log\log n$ ، و

$$d(n) = 2^{(1+o(1))\log n/\log\log n} \text{ .}$$

اما ، اگر بــه‌ازای $N(\varepsilon)$ ی $n \geq N(\varepsilon)$ ، $1+o(1) > 1-\varepsilon$ ، و این (ب) را ثابت خواهد کــرد .

تذکر. به‌عنوان نتیجه‌ای از قضیهٔ ۱۲۰۱۳ ، رابطهٔ

$$d(n) = o(n^{\delta}) \qquad (۳۱)$$

به‌ازای هر $\delta > 0$ بدست می‌آید. این نتیجه را می‌توان بدون استفاده از قضیهٔ اعداد اول نیز بدست آورد. (ر.ک. تمرین ۱۳۰۱۲.)

۱۱۰۱۳ کاربرد در مورد کامل اویلر

نوع استدلال بکار رفته در بخش پیش را می‌توان برای بدست آوردن نامساویهایی برای $\varphi(n)$ بکار برد. وقتی n اول باشد، داریم $\varphi(n) = n - 1$. وقتی n تعداد زیادی عامل اول داشته باشد، $\varphi(n)$ خیلی کوچکتر خواهد بود. در واقع، اگر n حاصل ضرب تمام اعداد اول نابیشتر از x باشد، داریم

$$\varphi(n) = n\prod_{p\le x}\left(1 - \frac{1}{p}\right).$$

قضیهٔ زیر رفتار مجانبی این حاصل ضرب را به‌ازای x های بزرگ بدست می‌دهد.

قضیهٔ ۱۳۰۱۳. *ثابت مثبتی مانند c هست بطوری که، به‌ازای $x \ge 2$،*

$$\prod_{p\le x}\left(1 - \frac{1}{p}\right) = \frac{c}{\log x} + O\left(\frac{1}{\log^2 x}\right). \tag{۳۲}$$

تذکر. می‌توان نشان داد که $c = e^{-C}$، که در آن C ثابت اویلر است. (ر.ک. [۳۱].)

برهان. فرض کنیم $P(x)$ حاصل ضرب (۳۲) باشد. دراین صورت، $\log P(x) = \sum_{p\le x}\log(1 - 1/p)$. برای تخمین این مجموع، از بسط به‌صورت سری توانی

$$-\log(1 - t) = t + \frac{t^2}{2} + \frac{t^3}{3} + \cdots + \frac{t^n}{n} + \cdots \quad (|t| < 1)$$

به‌ازای $t = 1/p$ استفاده می‌کنیم. با انتقال یک جمله به طرف اول، به‌ازای $a_p = -\log(1 - 1/p) - 1/p$، داریم

$$0 < a_p = \frac{1}{2p^2} + \frac{1}{3p^3} + \cdots < \frac{1}{2}\left(\frac{1}{p^2} + \frac{1}{p^3} + \cdots\right) = \frac{1}{2p(p-1)}.$$

این نامساوی نشان می‌دهد که سری نامتناهی

$$\sum_p a_p = \sum_p \left\{-\log\left(1 - \frac{1}{p}\right) - \frac{1}{p}\right\} \tag{۳۳}$$

همگراست، زیرا تحت تسلط $\sum_{n=2}^{\infty} 1/n(n-1)$ می‌باشد. اگر B مجموع سری (۳۳) باشد، داریم

$$0 < B - \sum_{p \le x} a_p = \sum_{p > x} a_p \le \sum_{n \ge x} \frac{1}{n(n-1)} = -\sum_{n \ge x}\left(\frac{1}{n} - \frac{1}{n-1}\right) = O\left(\frac{1}{x}\right).$$

ازاینرو،

$$\sum_{p \le x} a_p = B + O\left(\frac{1}{x}\right),$$

یا

$$-\log P(x) = \sum_{p \le x} \frac{1}{p} + B + O\left(\frac{1}{x}\right).$$

اما، طبق قضیهٔ ۱۲۰۴، مجموع طرف راست مساوی $\log\log x + A + O(1/\log x)$ است؛ درنتیجه،

$$\log P(x) = -\log\log x - B - A + O\left(\frac{1}{\log x}\right).$$

بنابراین،

$$P(x) = \exp\{\log P(x)\} = e^{-B-A} e^{-\log\log x} e^{O(1/\log x)}.$$

حال‌فرض‌کنیم $c = e^{-B-A}$ و، با استفاده از نامساوی $e^u = 1 + O(u)$ به‌ازای $0 < u < 1$، بدست می‌آوریم

$$P(x) = \frac{c}{\log x}\left\{1 + O\left(\frac{1}{\log x}\right)\right\} = \frac{c}{\log x} + O\left(\frac{1}{\log^2 x}\right).$$

این برهان را تمام خواهد کرد.

قضیهٔ ۱۴۰۱۳ . فرض‌کنیم c ثابت قضیهٔ ۱۳۰۱۳ بوده، و $\varepsilon > 0$ داده شده باشد.
(آ) $N(\varepsilon)$ی وجود دارد بطوری‌که

$$\text{به‌ازای هر } n \ge N(\varepsilon)، \quad \varphi(n) \ge (1-\varepsilon)\frac{cn}{\log\log n}؛$$

(ب) به‌ازای بی‌نهایت n داریم

$$\varphi(n) \le (1+\varepsilon)\frac{cn}{\log\log n}.$$

به عبارت دیگر،

$$\liminf_{n \to \infty} \frac{\varphi(n)\log\log n}{n} = c.$$

برهان. ابتدا قسمت (ب) را ثابت می‌کنیم. $n = \prod_{p \le x} p$ را اختیار می‌کنیم. دراین صورت،

$$\frac{\varphi(n)}{n} = \prod_{p \le x}\left(1 - \frac{1}{p}\right) = \frac{c}{\log x} + O\left(\frac{1}{\log^2 x}\right).$$

اما $\log n = \vartheta(x) = (1 + o(1))x$ ؛ درنتیجه، $\log\log n = (1 + o(1))\log x$. از اینرو، اگر به‌ازای $N(\varepsilon)$ ی $n \ge N(\varepsilon)$،

$$\frac{\varphi(n)}{n} = \frac{c(1 + o(1))}{\log\log n} + O\left(\frac{1}{(\log\log n)^2}\right) = \frac{c(1 + o(1))}{\log\log n} \le (1 + \varepsilon)\frac{c}{\log\log n}.$$

این (ب) را ثابت می‌کند.

برای اثبات (آ)، $n > 1$ را اختیار کرده و می‌نویسیم

$$\frac{\varphi(n)}{n} = \prod_{p|n}\left(1 - \frac{1}{p}\right) = P_1(n)P_2(n),$$

که در آن

$$P_2(n) = \prod_{\substack{p|n \\ p > \log n}}\left(1 - \frac{1}{p}\right) \quad \text{و} \quad P_1(n) = \prod_{\substack{p|n \\ p \le \log n}}\left(1 - \frac{1}{p}\right).$$

دراین صورت،

$$P_2(n) > \prod_{\substack{p|n \\ p > \log n}}\left(1 - \frac{1}{\log n}\right) = \left(1 - \frac{1}{\log n}\right)^{f(n)}, \tag{۳۴}$$

که در آن $f(n)$ تعداد اعداد اولی است که n را عاد می‌کنند و از $\log n$ متجاوزند. چون

$$n \ge \prod_{p|n} p > \prod_{\substack{p|n \\ p > \log n}} p \ge (\log n)^{f(n)},$$

معلوم می‌شود که $\log n > f(n)\log\log n$ ؛ درنتیجه، $f(n) < \log n/\log\log n$. چون $1 - (1/\log n) < 1$، نامساوی (۳۴) نتیجه می‌دهد که

$$P_2(n) > \left(1 - \frac{1}{\log n}\right)^{\log n/\log\log n} = \left\{\left(1 - \frac{1}{\log n}\right)^{\log n}\right\}^{1/\log\log n} \tag{۳۵}$$

اما، وقتی $u \to \infty$، $(1 - (1/u))^u \to e^{-1}$ ؛ درنتیجه، آخرین طرف در (۳۵)، وقتی $n \to \infty$، به 1 میل خواهد کرد. از اینرو، (۳۵) نتیجه می‌دهد که،

وقتی $n \to \infty$، $P_2(n) > 1 + o(1)$.

لذا، اگر $n \ge N(\varepsilon)$،

$$\frac{\varphi(n)}{n} = P_1(n)P_2(n) > (1+o(1)) \prod_{\substack{p|n \\ p\le \log n}} \left(1-\frac{1}{p}\right) \ge (1+o(1)) \prod_{p\le \log n}\left(1-\frac{1}{p}\right)$$

$$= (1+o(1))\frac{c}{\log\log n}(1+o(1)) \ge (1-\varepsilon)\frac{c}{\log\log n}\,.$$

این قسمت (آ) را ثابت می‌کند.

۱۲۰۱۳ تعمیم نامساوی پولیا برای مجموعهای مشخص

این فصل را با تعمیم نامساوی پولیا (قضیهٔ ۲۱۰۸) به مشخصهای غیر اصلی دلخواه خاتمه می‌دهیم. در اثبات آن از تخمین

$$d(n) = O(n^\delta)$$

برای تابع مقسوم علیه که در (۳۱) بدست آمد استفاده می‌کنیم.

قضیهٔ ۱۵۰۱۳ . *هرگاه χ یک مشخص غیر اصلی به هنگ k باشد، به‌ازای هر $x \ge 2$ داریم*

$$\sum_{m\le x}\chi(m) = O(\sqrt{k}\log k).$$

برهان. اگر χ اولیه باشد، قضیهٔ ۲۱۰۸ نشان می‌دهد که

$$\sum_{m\le x}\chi(m) < \sqrt{k}\log k.$$

حال مشخص غیر اصلی χ به هنگ k را در نظر گرفته، و فرض کنیم c هادی χ باشد. دراین صورت، $c|k$ ، $c<k$ ، و می‌توان نوشت

$$\chi(m) = \psi(m)\chi_1(m)\ ,$$

که در آن χ_1 مشخص اصلی به‌هنگ k بوده‌و ψ یک مشخص‌اولیه به هنگ c باشد. دراین صورت،

$$\sum_{m\le x}\chi(m) = \sum_{\substack{m\le x\\(m,k)=1}}\psi(m) = \sum_{m\le x}\psi(m)\sum_{d|(m,k)}\mu(d) = \sum_{m\le x}\sum_{\substack{d|k\\d|m}}\mu(d)\psi(m)$$

$$= \sum_{d|k}\mu(d)\sum_{q\le x/d}\psi(qd) = \sum_{d|k}\mu(d)\psi(d)\sum_{q\le x/d}\psi(q).$$

از اینرو،

$$\left|\sum_{m \le x} \chi(m)\right| \le \sum_{d|k} |\mu(d)\psi(d)| \left|\sum_{q \le x/d} \psi(q)\right| < \sqrt{c} \log c \sum_{d|k} |\mu(d)\psi(d)|, \qquad (۳۶)$$

زیرا ψ اولیه به هنگ c است. درمجموع‌اخیر، هر عامل $|\mu(d)\psi(d)|$ مساوی 0 یا 1 است. اگر $|\mu(d)\psi(d)| = 1$، $|\mu(d)| = 1$؛ درنتیجه، d یک مقسوم علیه فارغ از مربع k است؛ مثلاً،

$$d = p_1 p_2 \cdots p_r.$$

همچنین، $|\psi(d)| = 1$؛ درنتیجه، $(d, c) = 1$، بدین معنی که هیچ عامل اول p_i، c را عاد نمی‌کند. از اینرو، هر p_i، k/c را عاد می‌کند؛ درنتیجه، d، k/c را عاد خواهد کرد. به عبارت دیگر، به‌ازای هر $\delta > 0$،

$$\sum_{d|k} |\mu(d)\psi(d)| \le \sum_{d|k/c} 1 = d\left(\frac{k}{c}\right) = O\left(\left(\frac{k}{c}\right)^{\delta}\right).$$

بالاخص، $d(k/c) = O(\sqrt{k/c})$؛ درنتیجه، (۳۶) ایجاب می‌کند که

$$\sum_{m \le x} \chi(m) = O\left(\sqrt{\frac{k}{c}} \sqrt{c} \log c\right) = O(\sqrt{k} \log c) = O(\sqrt{k} \log k).$$

تمرین برای فصل ۱۳

۱. چبیشف ثابت کرد که اگر $\psi(x)/x$، وقتی $x \to \infty$، به‌حدی میل کند، این حدمساوی 1 است. در تمرین ۲۶.۴ برهانی به اختصار ذکر شد. دراین تمرین برهان دیگری مبتنی بر اتحاد

$$-\frac{\zeta'(s)}{\zeta(s)} = s \int_1^{\infty} \frac{\psi(x)}{x^{s+1}}\, dx, \qquad (\sigma > 1) \qquad (۳۷)$$

که در تمرین ۱۱.۱ (ت) داده شد ذکر خواهد شد.

(آ) ثابت کنید وقتی $s \to 1$، $(1 - s)\zeta'(s)/\zeta(s) \to 1$.

(ب) فرض کنید $\delta = \limsup_{x \to \infty}(\psi(x)/x)$. به‌ازای $\varepsilon > 0$، $N = N(\varepsilon)$ را طوری بگیرید که $x \ge N$ ایجاب کند که $\psi(x) \le (\delta + \varepsilon)x$. s را حقیقی گرفته، $1 < s \le 2$، انتگرال (۳۷) رابه دو قسمت تجزیه کنید: $\int_1^N + \int_N^\infty$، و با تخمین هر قسمت نامساوی زیر را بدست آورید:

$$-\frac{\zeta'(s)}{\zeta(s)} \le C(\varepsilon) + \frac{s(\delta + \varepsilon)}{s - 1},$$

که درآن $C(\varepsilon)$ ثابتی مستقل از x است. با استفاده از (آ)، نتیجه بگیرید که $\delta \geq 1$.

(پ) فرض کنید $\gamma = \liminf_{x\to\infty}(\psi(x)/x)$ و، بااستفاده از استدلالی مشابه، نتیجه‌بگیرید که $\gamma \leq 1$. لذا، هرگاه $\psi(x)/x$، وقتی $x \to \infty$، به حدی میل کند، آنگاه $\gamma = \delta = 1$.

۲. فرض کنید $A(x) = \sum_{n\leq x} a(n)$، که در آن

$$a(n) = \begin{cases} 0 & \text{اگر } n \neq \text{ توان اولی باشد}، \\ \dfrac{1}{k} & \text{اگر } n = p^k، \end{cases}$$

ثابت کنید که $A(x) = \pi(x) + O(\sqrt{x}\log\log x)$.

۳. (آ) هرگاه $c > 1$ و عددی صحیح $x \neq$، ثابت کنید که اگر $x > 1$،

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} \log\zeta(s)\frac{x^s}{s}\,ds = \pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \cdots$$

(ب) نشان دهید که قضیهٔ اعداد اول معادل رابطهٔ مجانبی زیر است:

$$\text{وقتی } x\to\infty،\quad \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} \log\zeta(s)\frac{x^s}{s}\,ds \sim \frac{x}{\log x}.$$

برهانی از قضیهٔ اعداد اول که مبتنی بر این رابطه است به وسیلهٔ لاندو در۱۹۰۳ داده شده است.

۴. فرض کنید $M(x) = \sum_{n\leq x}\mu(n)$. مرتبهٔ بزرگی دقیق $M(x)$ به‌ازای x های بزرگ معلوم نیست. در فصل ۴ نشان داده شد که قضیهٔ اعدا اول معادل رابطهٔ "وقتی $x\to\infty$، $M(x) = o(x)$" است. این تمرین مرتبهٔ بزرگی $M(x)$ را با فرض ریمان پیوند می‌دهد. فرض کنید ثابت مثبتی مانند θ باشد بطوری که

$$\text{به‌ازای } x \geq 1،\quad M(x) = O(x^\theta).$$

ثابت کنید فرمول

$$\frac{1}{\zeta(s)} = s\int_1^\infty \frac{M(x)}{x^{s+1}}\,dx,$$

که‌به‌ازای $\sigma > 1$ برقراراست (ر.ک. تمرین ۱۰۱۱ (پ))، به‌ازای $\sigma > \theta$ نیز معتبر است. نتیجه بگیرید که به‌ازای $\sigma > \theta$، $\zeta(s) \neq 0$. بالاخص، این نشان می‌دهد که رابطهٔ $M(x) = O(x^{1/2+\varepsilon})$ به‌ازای‌هر $\varepsilon > 0$ فرض ریمان را ایجاب می‌کند. همچنین،

می‌توان نشان داد که فرض ریمان ایجاب می‌کند که به‌ازای هر $\varepsilon > 0$ ، $M(x) = O(x^{1/2+\varepsilon})$.
(ر.ک. تیچمارش[1] [۶۹] ، ص ۳۱۵) .

۵ . لم زیر، که شبیه لم ۲ است، را ثابت کنید.
فرض کنید

$$A_1(x) = \int_1^x \frac{A(u)}{u}\,du,$$

که در آن $A(u)$ یک تابع صعودی نامنفی به‌ازای $u \geq 1$ است. اگر فرمول مجانبی
وقتی $x \to \infty$ ، $A_1(x) \sim Lx^c$
را به‌ازای $c > 0$ ای و $L > 0$ ی داشته باشیم، نیز خواهیم داشت:
وقتی $x \to \infty$ ، $A(x) \sim cLx^c$.

۶ . ثابت کنید که

$$\text{اگر } 0 < y < 1 \text{ ، } \frac{1}{2\pi i}\int_{2-\infty i}^{2+\infty i} \frac{y^s}{s^2}\,ds = 0 .$$

اگر $y \geq 1$ ، مقدار این انتگرال چیست؟

۷ .
$$\frac{1}{2\pi i}\int_{2-\infty i}^{2+\infty i} \frac{x^s}{s^2}\left(-\frac{\zeta'(s)}{\zeta(s)}\right) ds$$

را به‌صورت یک مجموع متناهی شامل $\Lambda(n)$ بیان کنید.

۸ . فرض کنید χ یک مشخص دیریکله به هنگ k و با مشخص اصلی χ_1 باشد. تعریف کنید

$$F(\sigma, t) = 3\,\frac{L'}{L}(\sigma, \chi_1) + 4\,\frac{L'}{L}(\sigma + it, \chi) + \frac{L'}{L}(\sigma + 2it, \chi^2).$$

اگر $\sigma > 1$ ، ثابت کنید $F(\sigma, t)$ دارای جزء حقیقی مساوی

$$-\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma}\,\mathrm{Re}\{3\chi_1(n) + 4\chi(n)n^{-it} + \chi^2(n)n^{-2it}\}$$

است، و نتیجه بگیرید که $\mathrm{Re}\ F(\sigma, t) \leq 0$.

۹ . فرض کنید $L(s, \chi)$ صفری از مرتبهٔ $m \geq 1$ در $s = 1 + it$ داشته باشد. ثابت کنید به‌ازای این t داریم

(آ) وقتی $\sigma \to 1+$ ، $\frac{L'}{L}(\sigma + it, \chi) = \frac{m}{\sigma - 1} + O(1)$ ؛

---

1. Titchmarsh

و

(ب) عدد صحیحی مانند $r \geq 0$ هست بطوری که

$$\frac{L'}{L}(\sigma + 2it, \chi^2) = \frac{r}{\sigma - 1} + O(1) \quad \text{،} \sigma \to 1+ \text{ وقتی}$$

جز وقتی $\chi^2 = \chi_1$ و $t = 0$.

۱۰ . با استفاده از تمرینهای ۸ و ۹ ، ثابت کنید

بەازای هر t حقیقی ، اگر $\chi^2 \neq \chi_1$ ، $L(1 + it, \chi) \neq 0$ ،

و

بەازای هر $t \neq 0$ حقیقی ، اگر $\chi^2 = \chi_1$ ، $L(1 + it, \chi) \neq 0$.

[**راهنمایی .** $F(\sigma, t)$ را ، وقتی $\sigma \to 1+$ ، درنظر بگیرید .]

۱۱ . ثابت کنید احکام زیر بەازای هر تابع حسابی $f(n)$ معادلند :

(آ) بەازای هر $\varepsilon > 0$ و هر $n \geq n_1$ ، $f(n) = O(n^\varepsilon)$ ؛

(ب) بەازای هر $\delta > 0$ ، وقتی $n \to \infty$ ، $f(n) = o(n^\delta)$.

۱۲ . فرض کنید $f(n)$ یک تابع ضربی باشد بطوری که اگر p اول باشد ،

وقتی $p^m \to \infty$ ، $f(p^m) \to 0$.

یعنی ، بەازای هر $\varepsilon > 0$ ، $N(\varepsilon)$ ی هست بطوری که هروقت $p^m > N(\varepsilon)$ ، $|f(p^m)| < \varepsilon$.

ثابت کنید وقتی $n \to \infty$ ، $f(n) \to 0$.

[**راهنمایی .** ثابتی مانند $A > 0$ هست بطوری که بەازای هر p اول و هر $m \geq 0$ ، $|f(p^m)| < A$ ، وثابتی مانند $B > 0$ هست بطوری که هروقت $p^m > B$ ، $|f(p^m)| < 1$.]

۱۳ . بەازای $\alpha \geq 0$ ، قرار دهید $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$. ثابت کنید بەازای هر $\delta > 0$ ،

وقتی $n \to \infty$ ، $\sigma_\alpha(n) = o(n^{\alpha + \delta})$.

[**راهنمایی .** از تمرین ۱۲ استفاده کنید .]

۱۴ افزارها

۱.۱۴ مقدمه

تا اینجا عمدتاً به *نظریهٔ ضربی اعداد* پرداخته‌ایم؛ یعنی، بررسی توابع حسابی مربوط به تجزیهٔ اعداد صحیح به اعداد اول. حال به شاخهٔ دیگری از نظریهٔ اعداد، به‌نام *نظریهٔ جمعی اعداد*، می‌پردازیم. یک مسئلهٔ اساسی درآن بیان یک عدد صحیح مثبت n به صورت مجموعی از اعداد صحیح از مجموعه‌ای مانند A، مثلاً

$$A = \{a_1, a_2, \ldots\},$$

است‌که‌درآن a_i ها اعدادخاصی ازقبیل اعداد اول، مربعی، مکعبی، مثلثی، و غیره‌اند. هر نمایش n به صورت مجموعی از عناصر A یک *افراز* n نام دارد، و ما به تابع حسابی $A(n)$ که تعداد افرازهای n به جمعوندهای گرفته شده از A را می‌شمارد علاقه‌مندیم.

این مطلب را با چند مثال معروف توضیح می‌دهیم.

حدس گلدباخ. **هر عدد زوج $n > 4$ مجموع دو عدد *اول* فرد *است*.**

دراین مثال، $A(n)$ تعداد جوابهای معادلهٔ

$$n = p_1 + p_2 \tag{1}$$

است، که درآن p_i ها اعداد اول فردی می‌باشند. حکم گلدباخ این است که به‌ازای $n > 4$ زوج، $A(n) \geq 1$. قدمت این حدس به ۱۷۴۲ باز می‌گردد و تا این تاریخ‌قطعیت نیافته است. در سال ۱۹۳۷، ریاضیدان روسی وینوگرادف، ثابت کرد که هر عدد فرد به‌قدرکافی بزرگ مجموع سه عدد اول فرد است. در ۱۹۶۶، ریاضیدان چینی، چن‌جینگ رون، ثابت‌کرد هر عدد زوج به‌قدر کافی بزرگ مجموع یک عدد اول و عددی دیگراست

که تعداد عاملهای اول آن از دو بیشتر نیست .(ر.ک. [۱۰] .)

نمایش با مربعها. **بهازای هر عدد صحیح $k \geq 2$ ، *تابع افراز* $r_k(n)$ را درنظر میگیریم که تعداد جوابهای معادلهٔ**

$$n = x_1^2 + \cdots + x_k^2 \tag{۲}$$

را میشمارد ، که در آن x_i مثبت ، منفی ، *یا* صفر است ، و مرتبهٔ جمعوندها بهحساب میآیند .

ژاکوبی [۳۴] ، بهازای $k = 2, 4, 6, 8$ ، $r_k(n)$ را برحسب توابع مقسوم علیهی بیان کرد . مثلا" ، ثابت کرد

$$r_2(n) = 4\{d_1(n) - d_3(n)\},$$

که در آن $d_1(n)$ و $d_3(n)$ تعداد مقسوم علیههای n اند که بترتیب همنهشت 1 و 3 به هنگ 4 میباشند. مثلا" ، $r_2(5) = 8$ ،زیراهردو مقسوم علیه، یعنی 1 و 5 ، همنهشت 1 به هنگ 4 میباشند . در واقع ، چهار نمایش زیر وجود دارند :

$$5 = 2^2 + 1^2 = (-2)^2 + 1^2 = (-2)^2 + (-1)^2 = 2^2 + (-1)^2,$$

و چهار نمایش دیگر که در آنها ترتیب جمعوندها عکس شده است .

ژاکوبی ، بهازای $k = 4$ ، ثابت کرد که

$$r_4(n) = \sum_{d|n} d = 8\sigma(n) \quad \text{اگر } n \text{ فرد باشد ،}$$

$$= 24 \sum_{\substack{d|n \\ d \text{ فرد}}} d \quad \text{اگر } n \text{ زوج باشد ،}$$

فرمولهای مربوط به $r_6(n)$ و $r_8(n)$ کمی پیچیدهترولی از یک نوع کلی اند . (ر.ک. [۱۴] .)

فرمولهای دقیق مربوط به $r_k(n)$ بهازای $k = 3, 5, 7$ نیزبدست آمدهاند ؛ این فرمولها شامل تعمیم ژاکوبی علامت لژاندر برای ماندههای مربعی اند . مثلا" ، اگر n فرد باشد ، معلوم شده است که

$$r_3(n) = 24 \sum_{m \leq n/4} (m|n) \quad \text{اگر } n \equiv 1 \pmod 4 \text{ ،}$$

$$= 8 \sum_{m \leq n/2} (m|n) \quad \text{اگر } n \equiv 3 \pmod 4 \text{ ،}$$

که در آن اعداد x_1, x_2, x_3 در (۲) نسبت بهم اول گرفته شدهاند .

تحلیل $r_k(n)$ بهازای مقادیربزرگ k خیلی مشکلتر است . دراین باب مطالب زیادی

به وسیلـهٔ مردل[1] ، هاردی ، لیتلوود ، رامـانوجان ، و بسیـاری دیگر نوشته شده است .
به‌ازای $k \geq 5$ ، می‌دانیم که $r_k(n)$ را می‌توان با یک فرمول مجانبی به شکل

$$r_k(n) = \rho_k(n) + R_k(n) \tag{۳}$$

بیان کرد ، که در آن $\rho_k(n)$ جملهٔ اصلی است که با سری نامتناهی زیر داده می‌شود :

$$\rho_k(n) = \frac{\pi^{k/2} n^{k/2-1}}{\Gamma\left(\frac{k}{2}\right)} \sum_{q=1}^{\infty} \sum_{\substack{h=1 \\ (h,q)=1}}^{q} \left(\frac{G(h:q)}{q}\right)^k e^{-2\pi i n h/q},$$

و $R_k(n)$ جملهٔ مـانده با مرتبهٔ کوچکتر است . این سری مربوط به $\rho_k(n)$ **سری منفرد** نام دارد ، و اعداد $G(h:q)$ مجموعهای گاوس مربعی می‌باشند :

$$G(h:q) = \sum_{r=1}^{q} e^{2\pi i h r^2/q}.$$

در سال ۱۹۱۷ ، مـردل اظهار داشت که $r_k(n)$ ضریب x^n در بسط به صورت سری توانی توان k ام سری

$$\vartheta = 1 + 2\sum_{n=1}^{\infty} x^{n^2}$$

است . تابع ϑ به توابع هنگی بیضوی کـه در اثبات فرمول (۳) نقش مهمی دارند مربوط اسـت .

مسئلهٔ ویرینگ[2] . ***تعیین اینکه بـه‌ازای عدد صحیح مثبت k ، عدد صحیحی مانند s (فقط تابع k) وجود دارد که معادلهٔ***

$$n = x_1^k + x_2^k + \cdots + x_s^k \tag{۴}$$

به‌ازای هر $n \geq 1$ جواب داشته باشد .

این مسئله بـه‌نام ریاضیدان انگلیسی ، ای. ویرینگ ، نامگذاری شده است ، که در ۱۷۷۰ وی (بدون اثبات و با گواه‌عددی محدود) گفت که هر n مجموع 4 مربع ، یا 9 مکعب ، یا 19 توان چهارم ، و غیره است . دراین مثال ، تابع افراز $A(n)$ تعداد جوابهای (۴) است ، و مسئله تعیین وجود s ی است که به‌ازای هر n ، $A(n) \geq 1$.
هرگاه s به‌ازای k مفروض وجود داشته باشد ، کوچکترین مقدار s وجود دارد و با

---

1. Mordell
2. Waring

$g(k)$ نموده می‌شود . لاگرانژوجود $g(2)$ را در ۱۷۷۰ ثابت‌کرد و ، در طول ۱۳۹ سال‌بعدی ، وجود $g(k)$ به‌ازای $k = 3, 4, 5, 6, 7, 8, 10$ نشان‌داده شد . در سال ۱۹۰۹ ، هیلبرت ، به استقرا ، وجود $g(k)$ را به‌ازای‌هر k ثابت‌کرداما مقدار عددی آن را به‌ازای k دلخواه معین نکرد . اکنون مقدار دقیق $g(k)$ به‌ازای هر k ، جز $k = 4$ ، معلوم شده است . هاردی و لیتلوود یک فرمول مجانبی برای جوابهای (۴) برحسب یک سری دادند که شبیه (۳) است . برای تاریخچهٔ مسئلهٔ ویرینگ ، ر.ک. دبلیو . جی . الیسون[1] [۱۸] .

افرازهای نامحدود

از اساسی‌ترین‌مسائل درنظریهٔ جمعی اعداد مسئلهٔ افرازهای نامحدوداست . مجموعهٔ جمعوندها مرکب است از تمام اعداد صحیح مثبت ، و تابع افراز مورد بررسی تعداد طرقی است که می‌توان n رابه‌صورت مجموعی ازاعداد صحیح مثبت نابیشتر از n نوشت ؛ یعنی ، تعداد جوابهای

$$n = a_{i_1} + a_{i_2} + \cdots \tag{۵}$$

تعدادجمعوندها نامحدوداست ، مجازند تکرار شوند ، و ترتیب جمعوندها اهمیتی ندارد . تابع افراز نظیر با $p(n)$ نموده و ***تابع افراز نامحدود*** ، یا فقط ***تابع افراز*** ، نامیده می‌شود . جمعوندها ***فرازها*** نامیده می‌شوند . مثلاً ، دقیقاً پنج افراز از 4 وجود دارند :

$$4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1;$$

درنتیجه ، $p(4) = 5$. به‌همین‌نحو ، $p(5) = 7$ ؛ افرازهای 5 عبارتند از

$$5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1$$
$$= 1 + 1 + 1 + 1 + 1.$$

بقیهٔ این فصل به بررسی $p(n)$ و توابع مربوط به آن اختصاص دارد .

۲.۱۴ نمایش هندسی افرازها

برای نمایش هندسی افرازها راه ساده‌ای وجود دارد ، وآن نمایشی از نقاط مشبکه به نام ***نمودار*** است . مثلاً ، افراز 15 به صورت

$$6 + 3 + 3 + 2 + 1$$

را می‌توان با 15 نقطهٔ مشبکه که در پنج سطر آرایش یافته‌اند نمایش‌داد :

---

1. W. J. Ellison

. . . . . .
. . .
. . .
. .
.

اگر این نمودار را عمودی بخوانیم ، افراز دیگری از 15 بدست می‌آوریم :

$$5 + 4 + 3 + 1 + 1 + 1.$$

دو افراز بــه‌این صورت را **مزدوج** می‌نامیم . توجه کنید که **بزرگترین** فراز در هریک از این افرازها مساوی **تعداد** فرازها در دیگری است . لذا ، قضیهٔ زیر را داریم .

قضیهٔ ۱۰۱۴ . ***تعداد افرازهای n به m فرازمساوی تعداد افرازهای n به فرازهایی‌است که بزرگترین آنها m است .***

با استدلالهای ترکیباتی ساده‌ای در نمودارها ، می‌توان قضایایی را ثابت کرد ، و ما بعداً "به توصیف زیبایی ازاین روش بازمی‌گردیم . با اینحال ، عمیقترین نتایج در نظریهٔ افرازها نیاز به بحث تحلیلی‌تری دارد که اینک به‌آن می‌پردازیم .

۳۰۱۴ توابع مولد برای افرازها

تابع $F(s)$ تعریف شده با سری دیریکلهٔ $F(s) = \sum f(n)n^{-s}$ را یک **تابع مولد** ضرایب $f(n)$ می‌نامیم . سریهای دیریکله ، بخاطر رابطهٔ

$$n^{-s}m^{-s} = (nm)^{-s},$$

توابع مــولد مفیدی در نظریهٔ ضربی اعداد هستند . در نظـریهٔ جمعی اعداد ، بخاطر $x^n x^m = x^{n+m}$ ، مناسبتر آن است که از توابع مولد نموده شده با سریهای توانی

$$F(x) = \sum f(n)x^n$$

استفاده شود . قضیهٔ زیر تابع مولدی برای تابع افراز $p(n)$ نشان می‌دهد .

قضیهٔ ۲۰۱۴ (اویلر) . ***به‌ازای $|x| < 1$ ، داریم***

$$\prod_{m=1}^{\infty} \frac{1}{1 - x^m} = \sum_{n=0}^{\infty} p(n)x^n,$$

که در آن $p(0) = 1$.

برهان. ابتدا، صرف نظر از مسائل همگرایی، برهان صوری این اتحاد را می‌آوریم؛ سپس، برهان دقیقتر آن را خواهیم داد.

اگر هر عامل در این حاصل ضرب به سری توانی داده شود (سری هندسی)، بدست می‌آوریم

$$\prod_{n=1}^{\infty} \frac{1}{1-x^n} = (1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^3 + x^6 + \cdots)\cdots$$

حال سریهای سمت راست را در هم ضرب می‌کنیم، به این نحو که گویی چند جمله‌ای‌اند، و توانهای همانند x را دسته بندی کرده، سریی توانی به شکل

$$1 + \sum_{k=1}^{\infty} a(k)x^k$$

بدست می‌آوریم. می‌خواهیم نشان دهیم که $a(k) = p(k)$. فرض کنید جملهٔ x^{k_1} را از سری اول، جملهٔ x^{2k_2} را از سری دوم، جملهٔ x^{3k_3} را از سری سوم، . . .، و جملهٔ x^{mk_m} را از سری m م گرفته باشیم، که هر $k_i \geq 0$. حاصل ضرب آنها، مثلاً، مساوی است با

$$x^{k_1}x^{2k_2}x^{3k_3}\cdots x^{mk_m} = x^k,$$

که در آن

$$k = k_1 + 2k_2 + 3k_3 + \cdots + mk_m.$$

این را می‌توان به صورت زیر نیز نوشت:

$$k = (1 + 1 + \cdots + 1) + (2 + 2 + \cdots + 2) + \cdots + (m + m + \cdots + m),$$

که در آن پرانتز اول شامل k_1 یک، پرانتز دوم شامل k_2 دو، و غیره است. این یک افراز از k به جمعوندهای مثبت است. لذا، هر افراز k یک چنین جملهٔ x^k تولید می‌کند و، بعکس، هر جملهٔ x^k از یک افراز نظیر از k می‌آید. بنابراین، $a(k)$، یعنی ضریب x^k، مساوی $p(k)$، یعنی تعداد افرازهای k، است.

استدلال فوق یک برهان دقیق نیست، زیرا مسائل همگرایی را نادیده گرفته‌ایم و نیز بی‌نهایت سری هندسی را در هم ضرب کرده‌ایم، طوری که گویی چند جمله‌ای‌اند. با اینحال، تبدیل ایده‌های فوق به یک برهان دقیق مشکل نیست.

برای این‌کار، x را به بازهٔ $0 \leq x < 1$ مقید کرده، و دو تابع

$$F(x) = \prod_{k=1}^{\infty} \frac{1}{1-x^k} = \lim_{m\to\infty} F_m(x) \quad \text{و} \quad F_m(x) = \prod_{k=1}^{m} \frac{1}{1-x^k}$$

را معرفی می‌کنیم. حاصل ضرب معرف $F(x)$ به‌ازای $0 \leq x < 1$ به‌طور مطلق همگراست، زیرا متقابل آن $\prod(1 - x^k)$ به‌طور مطلق همگراست (چون سری $\sum x^k$ به‌طور مطلق همگراست).

همچنین، توجه کنید که دنباله‌ٔ $\{F_m(x)\}$ به‌ازای هر x ثابت صعودی است، زیرا

$$F_{m+1}(x) = \frac{1}{1 - x^{m+1}} F_m(x) \geq F_m(x).$$

از اینـرو، به‌ازای هر x ثابت، که $0 \leq x < 1$، و هر m، $F_m(x) \leq F(x)$. اما $F_m(x)$ حاصل ضرب تعدادی متناهی سری به‌طور مطلق همگراست. لذا، این نیز یک سری به‌طور مطلق همگراست که می‌توان آن را به‌صورت زیر نوشت:

$$F_m(x) = 1 + \sum_{k=1}^{\infty} p_m(k)x^k \quad .$$

در اینجا $p_m(k)$ تعداد جوابهای معادله‌ٔ

$$k = k_1 + 2k_2 + \cdots + mk_m$$

است. به‌عبارت دیگر، $p_m(k)$ تعداد افرازهای k به‌فرازهایی‌است که از m متجاوزنیست. هرگاه $k \geq m$، آنگاه $p_m(k) = p(k)$. لذا، همواره داریم

$$p_m(k) \leq p(k),$$

که در آن تساوی وقتی است که $m \geq k$. به عبارت دیگر، داریم

$$\lim_{m \to \infty} p_m(k) = p(k).$$

حال سری مربوط‌به $F_m(x)$ را به‌دو قسمت تجزیه می‌کنیم:

$$F_m(x) = \sum_{k=0}^{m} p_m(k)x^k + \sum_{k=m+1}^{\infty} p_m(k)x^k$$
$$= \sum_{k=0}^{m} p(k)x^k + \sum_{k=m+1}^{\infty} p_m(k)x^k.$$

چون $x \geq 0$، داریم

$$\sum_{k=0}^{m} p(k)x^k \leq F_m(x) \leq F(x).$$

این نشان می‌دهد که سری $\sum_{k=0}^{\infty} p(k)x^k$ همگراست. بعلاوه، چون $p_m(k) \leq p(k)$، داریم

$$\sum_{k=0}^{\infty} p_m(k)x^k \leq \sum_{k=0}^{\infty} p(k)x^k \leq F(x);$$

درنتیجه، به‌ازای هر x ثابت، سری $\sum p_m(k)x^k$ نسبت به m به‌طور یکنواخت همگراست. با فرض $m \to \infty$، بدست می‌آید

$$F(x) = \lim_{m \to \infty} F_m(x) = \lim_{m \to \infty} \sum_{k=0}^{\infty} p_m(k)x^k = \sum_{k=0}^{\infty} \lim_{m \to \infty} p_m(x)x^k = \sum_{k=0}^{\infty} p(k)x^k,$$

که اتحاد اویلر را به‌ازای $0 \le x < 1$ ثابت می‌کند. این اتحاد را با ادامهٔ تحلیلی به قرص یکهٔ $|x| < 1$ تعمیم می‌دهیم.

جدول ۱۰۱۴ توابع مولد

توابع مولد	تعدادافرازهای n به فرازهایی که
$\prod_{m=1}^{\infty} \frac{1}{1-x^{2m-1}}$	فردند
$\prod_{m=1}^{\infty} \frac{1}{1-x^{2m}}$	زوجند
$\prod_{m=1}^{\infty} \frac{1}{1-x^{m^2}}$	مربعی‌اند
$\prod_{p} \frac{1}{1-x^{p}}$	اولند
$\prod_{m=1}^{\infty} (1+x^{m})$	نامساوی‌اند
$\prod_{m=1}^{\infty} (1+x^{2m-1})$	فرد و نامساوی‌اند
$\prod_{m=1}^{\infty} (1+x^{2m})$	زوج و نامساوی‌اند
$\prod_{m=1}^{\infty} (1+x^{m^2})$	مربعی و متمایزند
$\prod_{p} (1+x^{p})$	اول و متمایزند

بااستدلالاتی مشابه، می‌توان توابع مولد توابع افراز بسیار دیگر را فوراً بدست آورد. چند مثال در جدول ۱۰۱۴ ذکر شده‌اند.

۴۰۱۴ قضیهٔ اعداد مخمسی اویلر

حال تابع افرازی را درنظر می‌گیریم که با حاصل ضرب $\prod(1-x^m)$ تولید می‌شود؛ یعنی،

متقابل تابع مولد $p(n)$ ، و می‌نویسیم

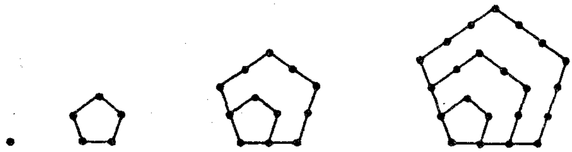
$$\prod_{m=1}^{\infty}(1-x^m)=1+\sum_{n=1}^{\infty}a(n)x^n.$$

برای بیان $a(n)$ به صورت یک تابع افراز، توجه می‌کنیم که هر افراز n به دو فراز نامساوی جمله‌ای مانند x^n درسمت راست‌تولید می‌کند با ضریب $+1$ یا -1 . اگر x^n حاصل ضرب تعداد زوجی جمله باشد، این ضریب $+1$ است و، درغیر این‌صورت، -1 می‌باشد. بنابراین،

$$a(n)=p_e(n)-p_o(n),$$

که‌درآن $p_e(n)$ تعدادافرازهای n به تعدادی فراز زوج و نامساوی، و $p_o(n)$ تعداد افرازها به تعدادی فراز فرد و نامساوی است. اویلر ثابت کرد که به‌ازای هر n ، جز آنهایی که تعلق به مجموعهٔ خاصی به نام مجموعهٔ اعداد مخمسی دارند، $p_e(n)=p_o(n)$.

اعداد مخمسی $1, 5, 12, 22, \ldots$ در مقدمهٔ تاریخی ذکر شدند. ارتباط این اعداد به پنج ضلعیها در شکل ۱۰۱۴ نموده شده است.



1    $1+4=5$ $1+4+7=12$ $1+4+7+10=22$

شکل ۱۰۱۴

این اعداد مجموعهای جزئی جملات تصاعد حسابی زیر می‌باشند:

$$1, 4, 7, 10, 13, \ldots, 3n+1, \ldots$$

اگر $\omega(n)$ مجموع n جملهٔ اول دراین تصاعد باشد،

$$\omega(n)=\sum_{k=0}^{n-1}(3k+1)=\frac{3n(n-1)}{2}+n=\frac{3n^2-n}{2}.$$

اعداد $\omega(n)$ و $\omega(-n)=(3n^2+n)/2$ *اعداد* مخمسی نامیده می‌شوند.

قضیهٔ ۳۰۱۴ . قضیهٔ اعداد مخمسی اویلر. *اگر* $|x|<1$ *، داریم*

$$\prod_{m=1}^{\infty}(1-x^m)=1-x-x^2+x^5+x^7-x^{12}-x^{15}+\cdots$$

$$=1+\sum_{n=1}^{\infty}(-1)^n\{x^{\omega(n)}+x^{\omega(-n)}\}=\sum_{n=-\infty}^{\infty}(-1)^n x^{\omega(n)}.$$

برهان. ابتدا قضیه را به‌ازای $0 \le x < 1$ ثابت می‌کنیم و، سپس، با ادامهٔ تحلیلی، آن‌را به فرض $|x| < 1$ تعمیم می‌دهیم. تعریف می‌کنیم $P_0 = S_0 = 1$ و، به‌ازای $n \ge 1$، قرار می‌دهیم

$$S_n = 1 + \sum_{r=1}^{n}(-1)^r\{x^{\omega(r)} + x^{\omega(-r)}\} \quad \text{و} \quad P_n = \prod_{r=1}^{n}(1 - x^r).$$

حاصل ضرب نامتناهی $\prod(1 - x^m)$ همگراست؛ درنتیجه، وقتی $n \to \infty$، $P_n \to \prod(1 - x^m)$. ثابت می‌کنیم (با استفاده از روش شانکس[1] [۶۳]) که

$$|S_n - P_n| \le nx^{n+1}. \tag{۶}$$

چون‌وقتی $n \to \infty$، $nx^{n+1} \to 0$، این اتحاد اویلر را به‌ازای $0 \le x < 1$ ثابت می‌کند.

برای اثبات (۶)، قرار می‌دهیم $g(r) = r(r + 1)/2$ و مجموعهای

$$F_n = \sum_{r=0}^{n}(-1)^r \frac{P_n}{P_r} x^{rn + g(r)}$$

را معرفی می‌کنیم.

ابتدا نشان می‌دهیم که F_n شکل دیگری از S_n است. به‌آسانی معلوم می‌شود که $F_1 = S_1 = 1 - x - x^2$. لذا، اگر نشان دهیم

$$F_n - F_{n-1} = S_n - S_{n-1} \quad \text{یا} \quad F_n - S_n = F_{n-1} - S_{n-1},$$

این ثابت می‌کند که به‌ازای هر $n \ge 1$، $F_n = S_n$. اما

$$F_n - F_{n-1} = \sum_{r=0}^{n}(-1)^r \frac{P_n}{P_r} x^{rn+g(r)} - \sum_{r=0}^{n-1}(-1)^r \frac{P_{n-1}}{P_r} x^{r(n-1)+g(r)}.$$

در مجموع اول می‌نویسیم $P_n = (1 - x^n)P_{n-1}$، و جملهٔ با $r = n$ را جدا می‌کنیم. سپس، با پخش تفاضل $1 - x^n$، بدست می‌آوریم

$$F_n - F_{n-1} = (-1)^n x^{n^2+g(n)} + \sum_{r=0}^{n-1}(-1)^r \frac{P_{n-1}}{P_r} x^{rn+g(r)}$$
$$- \sum_{r=0}^{n-1}(-1)^r \frac{P_{n-1}}{P_r} x^{(r+1)n+g(r)} - \sum_{r=0}^{n-1}(-1)^r \frac{P_{n-1}}{P_r} x^{r(n-1)+g(r)}.$$

حال مجموعهای اول‌و سوم را تلفیق کرده و توجه می‌کنیم که جمله با $r = 0$ حذف می‌شود. در مجموع دوم اندیس را انتقال داده و بدست می‌آوریم

---

1. Shanks

$$F_n - F_{n-1} = (-1)^n x^{n^2+g(n)} + \sum_{r=1}^{n-1}(-1)^r \frac{P_{n-1}}{P_r} x^{r(n-1)+g(r)}(x^r - 1)$$
$$- \sum_{r=1}^{n}(-1)^{r-1} \frac{P_{n-1}}{P_{r-1}} x^{rn+g(r-1)}.$$

اما $(x^r - 1)/P_r = -1/P_{r-1}$ و $r(n-1) + g(r) = rn + g(r-1)$؛ درنتیجه، دو مجموع اخیر جمله به جمله حذف می‌شوند جز جمله با $r = n$ در مجموع دوم. لذا، داریم

$$F_n - F_{n-1} = (-1)^n x^{n^2+g(n)} + (-1)^n x^{n^2+g(n-1)}.$$

اما

$$n^2 + g(n) = n^2 + \frac{n(n+1)}{2} = \omega(-n) \quad \text{و} \quad n^2 + g(n-1) = \omega(n);$$

درنتیجه،

$$F_n - F_{n-1} = (-1)^n\{x^{\omega(n)} + x^{\omega(-n)}\} = S_n - S_{n-1};$$

و لـــذا، بـــه‌ازای هـــر $n \geq 1$، $F_n = S_n$. در مجموع معرف F_n اولین جمله P_n است؛ درنتیجه،

$$F_n = P_n + \sum_{r=1}^{n}(-1)^r \frac{P_n}{P_r} x^{rn+g(r)}. \tag{۷}$$

توجه‌کنیدکه $0 < P_n/P_r \leq 1$، زیرا $0 \leq x < 1$. همچنین، هر عامل $x^{rn+g(r)}$ از x^{n+1} نابیشتر است؛ درنتیجه، مجموع‌سمت راست (۷) از بالا به وسیلهٔ nx^{n+1} کراندار است. بنابـــراین، $|F_n - P_n| \leq nx^{n+1}$ و، چون $F_n = S_n$، این (۶) را ثابت و برهان اتحاد اویلر را تمام می‌کند.

۵.۱۴ برهان ترکیباتی قضیهٔ اعداد مخمسی اویلر

اویلر قضیهٔ اعـــداد مخمسی خـــودرا در ۱۷۵۰ به استقرا ثابت کرد. بعدها برهانهایی به وسیلهٔ لـــژاندر در ۱۸۳۰ و ژاکـــوبی در ۱۸۴۶ بدست آمدند. دراین بخش، برهان ترکیباتی جالبی که اف. فرانکلین[1] [۲۲] در ۱۸۸۱ داده توصیف می‌شود.

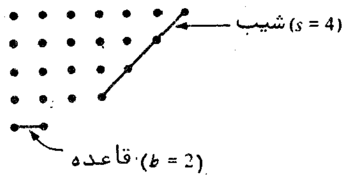
قبلا" گفتیم

$$\prod_{m=1}^{\infty}(1 - x^m) = 1 + \sum_{n=1}^{\infty}\{p_e(n) - p_o(n)\}x^n,$$

1. F. Franklin

کــه درآن $p_e(n)$ تعداد افــرازهای n به تعــدادی فراز زوج و نامساوی، و $p_o(n)$ تعداد افرازها بــه‌تعدادی فراز فرد و نامساوی است. فرانکلین، با استفاده از نمایش افرازها به وسیلهٔ نقاط مشبکه، وجود تناظر یک به یکی بین افرازهای n به فرازهایی نامساوی و فرد یا زوج بطوری‌که، جز وقتی n یک عدد مــخــمسی است، $p_e(n) = p_o(n)$، را نشان‌داد.

نمودار یک افراز n به فرازهای نــامساوی را درنظر می‌گیریم. گوییم این نمودار به **شکل متعارف** است اگر، همــانطور که شکل ۲.۱۴ نشان می‌دهد، فرازها به ترتیب نزولی



شکل ۲.۱۴

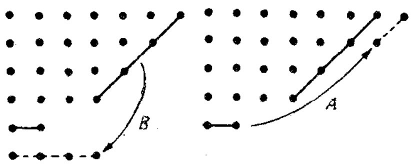
آرایش یــافته باشند. طویلترین پاره خط واصل بین نقاط در آخرین سطر **قاعدهٔ** نمودار نام دارد، و تعــداد نقاط‌مشبکهٔ واقع بر قاعده را با b نشان می‌دهیم. لذا، $b \geq 1$. طویلترین پاره خط $45°$ واصل بین آخرین نقطه در سطر اول و نقاط دیگر در نمودار **شیب** نام دارد، و تعــداد نقاط مشبکهٔ واقع بر شیب با s نموده می‌شود. لذا، $s \geq 1$. در شکل ۲.۱۴ داریم $b = 2$ و $s = 4$.

حال برای این نمودار دو عمل A و B را تعریف می‌کنیم. همانطور که شکل ۳.۱۴ (آ) نشان داده، عمل A نقاط قاعده‌را طوری‌حرکت‌می‌دهدکه برخطی‌موازی‌شیب قرار‌می‌گیرند. عمل B، همانطور که شکل ۳.۱۴ (ب) نشان داده، نقاط شیب را طوری‌حرکت می‌دهد که بر خطی موازی قاعده قرار گیرند. گوییم عمل **مجاز** است اگر شکل متعارف نمودار را حفظ کند؛ یعنی، اگر نمودار جدید مجددا" فرازهایی نامساوی به ترتیب نزولی داشته باشد.

اگر A مجاز بــاشد، افراز جدیدی از n به فرازهای نامساوی بدست می‌آید، ولی تعدادفرازهایکی ازقبل کمتر است. اگر B مجاز باشد، افراز جدیدی به فرازهای نامساوی بدست می‌آید، ولی تعداد فرازها یکی از قبل بیشتر است. لذا، اگر به‌ازای هر افراز n درست یکــی از A و B مجاز بــاشد، تناظر یک به یکی بین افرازهای n به تعدادی فراز نامساوی فرد و زوج وجوددارد؛ درنتیجه، به‌ازای هرچنین n، $p_e(n) = p_o(n)$.

برای تعییــن مجــاز بــودن A یا B سه حالت درنظر می‌گیریم: (۱) $b < s$؛ (۲) $b = s$؛ (۳) $b > s$.

حالت ۱. هرگاه $b < s$، آنگاه $b \leq s - 1$؛ درنتیجه، A مجاز است ولی B نیست، زیرا B شکل متعارف را خراب می‌کند. (ر.ک. شکل ۳.۱۴.)



(ب) عمل B (آ) عمل A

شکل ۳۰۱۴

حالت ۲. هرگاه $b = s$ ، عمل B مجاز نیست، زیرا نمودار جدیدی بدست می‌دهد که به‌شکل‌متعارف نیست. عمل A مجاز است جز، همانطور که شکل ۴۰۱۴ (آ) نشان داده، وقتی قاعده و شیب متقاطع باشند، که در این حالت نمودار به شکل متعارف نیست.

حالت ۳. هرگاه $b > s$ ، عمل A مجاز نیست، ولی B ، جز وقتی $b = s + 1$ ، مجاز است‌و، همانطور که شکل ۴۰۱۴ (ب) نشان داده، قاعده و شیب متقاطع می‌باشند. دراین حالت، نمودار جدید شامل دو قسمت مساوی است.

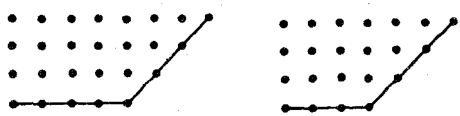
از اینـــرو، درست یکی از A و B مجاز است، با دو استثنای مذکور در بالا. حالت استثنایی اول، نموده شده در شکل ۴۰۱۴ (آ)، را درنظر می‌گیریم، و فرض می‌کنیم در نمودار k سطروجود داشته باشند. پس نیز داریم $b = k$ ؛ درنتیجه، عدد n از رابطهٔ زیر بدست می‌آید:

$$n = k + (k + 1) + \cdots + (2k - 1) = \frac{3k^2 - k}{2} = \omega(k).$$

برای این افراز n افرازی اضافی به فرازهای زوج داریم اگر k زوج باشد، و افرازی اضافی به فرازهای فرد داریم اگر k فرد باشد؛ درنتیجه،

$$p_e(n) - p_o(n) = (-1)^k.$$

در حالت‌استثنایی دیگر، که در شکل ۴۰۱۴ (ب) نموده شده، در هر سطر نقطهٔ مشبکهٔ



$b = s + 1$ (ب) $b = s$ (آ)

شکل ۴۰۱۴ هیچیک از A و B مجاز نیست.

اضافی وجود دارد؛ درنتیجه،

$$n = \frac{3k^2 - k}{2} + k = \frac{3k^2 + k}{2} = \omega(-k)$$

و مجددا" $p_e(n) - p_o(n) = (-1)^k$. این برهان فرانکلین اتحاد اویلر را تمام می‌کند .

۶۰۱۴ فرمول بازگشتی اویلر برای $p(n)$

قضیهٔ ۴۰۱۴ . فرض کنیم $p(0) = 1$ و ، اگر $n < 0$ ، $p(n)$ را 0 تعریف می‌کنیم . در این صورت ، به‌ازای $n \geq 1$ داریم

$$p(n) - p(n-1) - p(n-2) + p(n-5) + p(n-7) + \cdots = 0, \tag{۸}$$

یا ، به صورت معادل ،

$$p(n) = \sum_{k=1}^{\infty} (-1)^{k+1}\{p(n-\omega(k)) + p(n-\omega(-k))\}.$$

برهان . قضایای ۲۰۱۴ و ۳۰۱۴ اتحاد زیر را بدست می‌دهند :

$$\left(1 + \sum_{k=1}^{\infty} (-1)^k \{x^{\omega(k)} + x^{\omega(-k)}\}\right)\left(\sum_{m=0}^{\infty} p(m)x^m\right) = 1.$$

اگر $n \geq 1$ ، ضریب x^n سمت راست 0 است ؛ درنتیجه ، با متحد گرفتن ضرایب ، (۸) فورا" بدست می‌آید .

مک ماهون[1] ، با استفاده از این فرمول بازگشتی ، $p(n)$ را تا $n = 200$ حساب کرد . در اینجا چند مقدار نمونه از جدول وی را ذکر می‌کنیم :

$$\begin{aligned}
p(1) &= 1\\
p(5) &= 7\\
p(10) &= 42\\
p(15) &= 176\\
p(20) &= 627\\
p(25) &= 1{,}958\\
p(30) &= 5{,}604\\
p(40) &= 37{,}338\\
p(50) &= 204{,}226\\
p(100) &= 190{,}569{,}292\\
p(200) &= 3{,}972{,}999{,}029{,}388
\end{aligned}$$

---

1. MacMahon

این مثالها نشان می‌دهند که $p(n)$ بسرعت با n رشد می‌کند. بزرگترین مقدار $p(n)$ ی که تا بحال حساب شده است $p(14,031)$، یعنی عددی با 127 رقم، است. دی. اچ. لمر [۴۲] این عدد را برای اثبات حدس رامانوجان حساب کرد، که می‌گوید $p(14,031) \equiv 0 \pmod{11^4}$. این حدس درست بود. واضح است که فرمول بازگشتی (۸) برای محاسبهٔ این مقدار از $p(n)$ بکار نرفته بود. در عوض، لمر از فرمول مجانبی رادماخر[1] [۵۴] استفاده کرد، که ایجاب می‌کند که

$$\text{وقتی } n \to \infty \text{ ،} \quad p(n) \sim \frac{e^{K\sqrt{n}}}{4n\sqrt{3}} \text{ ،}$$

که در آن $K = \pi(2/3)^{1/2}$. به‌ازای $n = 200$ ، کمیت سمت‌راست تقریبا " 4×10^{12} است، که خیلی نزدیک به مقدار واقعی آن $p(200)$ است که در جدول مک ماهون آمده است.

تا آخراین‌جلد بدست آوردن فرمول مجانبی رادماخر برای $p(n)$ را نشان می‌دهیم. در این برهان به‌آمادگی زیادی در نظریهٔ توابع هنگی بیضوی نیاز داریم. در بخش بعد کران بالایی نادقیقی برای $p(n)$ می‌دهیم که مستلزم نمایی $e^{K\sqrt{n}}$ بوده و با سعی نسبتا" کمی قابل بدست آمدن است.

۷.۱۴ یک کران بالایی برای $p(n)$

قضیهٔ ۵.۱۴. *اگر* $n \geq 1$ ، داریم $p(n) < e^{K\sqrt{n}}$ ، که در آن $K = \pi(2/3)^{1/2}$.

برهان. فرض کنیم

$$F(x) = \prod_{n=1}^{\infty}(1 - x^n)^{-1} = 1 + \sum_{k=1}^{\infty} p(k)x^k,$$

و x را به بازهٔ $0 < x < 1$ محدود می‌کنیم. پس داریم $p(n)x^n < F(x)$ ، که از آن خواهیم داشت $\log p(n) + n \log x < \log F(x)$ ، یا

$$\log p(n) < \log F(x) + n \log \frac{1}{x}. \tag{۹}$$

جملات $\log F(x)$ و $n \log(1/x)$ را جدا تخمین می‌زنیم. ابتدا می‌نویسیم

$$\log F(x) = -\log \prod_{n=1}^{\infty}(1 - x^n) = -\sum_{n=1}^{\infty}\log(1 - x^n) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{x^{mn}}{m}$$

---

1. Rademacher

$$= \sum_{m=1}^{\infty} \frac{1}{m} \sum_{n=1}^{\infty} (x^m)^n = \sum_{m=1}^{\infty} \frac{1}{m} \frac{x^m}{1-x^m}.$$

چون داریم

$$\frac{1-x^m}{1-x} = 1 + x + x^2 + \cdots + x^{m-1},$$

و چون $0 < x < 1$ ، می‌توان نوشت

$$mx^{m-1} < \frac{1-x^m}{1-x} < m;$$

و درنتیجه،

$$\frac{m(1-x)}{x} < \frac{1-x^m}{x^m} < \frac{m(1-x)}{x^m}.$$

با عکس کردن و تقسیم بر m ، بدست می‌آوریم

$$\frac{1}{m^2} \frac{x^m}{1-x} \le \frac{1}{m} \frac{x^m}{1-x^m} \le \frac{1}{m^2} \frac{x}{1-x}.$$

با جمعبندی روی m ، خواهیم داشت

$$\log F(x) = \sum_{m=1}^{\infty} \frac{1}{m} \frac{x^m}{1-x^m} \le \frac{x}{1-x} \sum_{m=1}^{\infty} \frac{1}{m^2} = \frac{\pi^2}{6} \frac{x}{1-x} = \frac{\pi^2}{6t},$$

که درآن

$$t = \frac{1-x}{x}.$$

توجه کنید که t ، وقتی x از 0 تا 1 تغییر کند، مقادیر مثبت از ∞ تا 0 را می‌گیرد. حال جملهٔ $n \log(1/x)$ راتخمین می‌زنیم. به‌ازای $t > 0$ ، داریم $\log(1+t) < t$. امـــا

$$1 + t = 1 + \frac{1-x}{x} = \frac{1}{x} \text{ ؛ درنتیجه، } \log \frac{1}{x} < t.$$

اما

$$\log p(n) < \log F(x) + n \log \frac{1}{x} < \frac{\pi^2}{6t} + nt. \qquad (۱۰)$$

مینیمم $(\pi^2/6t) + nt$ وقتی رخ می‌دهدکه دو جمله مساوی باشند؛ یعنی، وقتی $\pi^2/(6t) = nt$ یا $t = \pi/\sqrt{6n}$. به‌ازای این مقدار t ، داریم

$$\log p(n) < 2nt = 2n\pi/\sqrt{6n} = K\sqrt{n}\,;$$

درنتیجه ، همانطور که حکم شده ، $p(n) < e^{K\sqrt{n}}$.

تذکر. ج . اچ. وان لینت[1] [۴۸] با کمـــی سعـــی بیشتر نشان داده است که می‌توان نامساوی اصلاح شده‌ای بدست آورد :

$$\text{به‌ازای } n > 1 ،\quad p(n) < \frac{\pi e^{K\sqrt{n}}}{\sqrt{6(n-1)}} \;.\qquad (۱۱)$$

چون اگر $k \geq n$ ، $p(k) \geq p(n)$ ، به‌ازای $n > 1$ ، داریم

$$F(x) > \sum_{k=n}^{\infty} p(k)x^k \geq p(n)\sum_{k=n}^{\infty} x^k = \frac{p(n)x^n}{1-x}.$$

با لگاریتم گرفتن ، به‌جای (۹) نامساوی زیر را داریم

$$\log p(n) < \log F(x) + n\log\frac{1}{x} + \log(1-x).$$

چون $1 - x = tx$ ، داریـــم $\log(1-x) = \log t - \log(1/x)$ ؛ درنتیجـــه ، (۱۰) را می‌توان با

$$\log p(n) < \frac{\pi^2}{6t} + (n-1)t + \log t \qquad (۱۲)$$

جایگزین کرد . محاسبهٔ ساده‌ای با مشتقات نشان می‌دهد که تابع

$$f(t) = \frac{\pi^2}{6t} + (n-1)t + \log t$$

مینیمم خود را در

$$t = \frac{-1 + \sqrt{1 + [4(n-1)\pi^2/6]}}{2(n-1)}$$

دارد . بـــا استفاده از ایـــن مقـــدار در (۱۲) و حذف جملات نامربوط، (۱۱) بدست خواهد آمد .

۸.۱۴ اتحاد حاصل ضرب سه‌گانهٔ ژاکوبی

دراین بخش اتحـــاد معروفی از ژاکوبی از نظریهٔ توابع تتا توصیف می‌شود . قضیهٔ اعداد

---

1. J. H. van Lint

مخمسی اویلر و اتحادهای افرازی بسیار دیگر حالات خاصی از فرمول ژاکوبی می‌باشند.

قضیهٔ ۶.۱۴ . اتحاد حاصل ضرب سه‌گانهٔ ژاکوبی. *به‌ازای اعداد مختلط* x و z که $|x| < 1$ و $z \neq 0$، داریم

$$\prod_{n=1}^{\infty}(1 - x^{2n})(1 + x^{2n-1}z^2)(1 + x^{2n-1}z^{-2}) = \sum_{m=-\infty}^{\infty} x^{m^2}z^{2m}. \qquad (۱۳)$$

برهان. قید $|x| < 1$ همگرایی مطلق هریک از حاصل ضربهای $\prod(1 - x^{2n}),\ \prod(1 + x^{2n-1}z^2),\ \prod(1 + x^{2n-1}z^{-2})$، وسری (۱۳) را تضمین می‌کند. بعلاوه، به‌ازای هر x ثابت که $|x| < 1$، سری و حاصل ضربها بر زیر مجموعه‌های فشردهٔ صفحهٔ z غیرشامل $z = 0$ به‌طوریکنواخت همگرایند؛ درنتیجه، هر طرف (۱۳) به‌ازای $z \neq 0$ یک تابع تحلیلی است. به‌ازای $z \neq 0$ ثابت، سری و حاصل ضربها نیز به‌ازای $|x| \leq r < 1$ به‌طور یکنواخت همگرایند؛ لذا، نمایش توابعی تحلیلی از x در قرص $|x| < 1$ خواهند بود.

برای اثبات (۱۳)، x را ثابت گرفته و $F(z)$ را به‌ازای $z \neq 0$ با معادلهٔ زیر تعریف می‌کنیم:

$$F(z) = \prod_{n=1}^{\infty}(1 + x^{2n-1}z^2)(1 + x^{2n-1}z^{-2}). \qquad (۱۴)$$

ابتدا نشان می‌دهیم که F در معادلهٔ تابعی

$$xz^2F(xz) = F(z) \qquad (۱۵)$$

صدق می‌کند. از (۱۴) معلوم می‌شود که

$$F(xz) = \prod_{n=1}^{\infty}(1 + x^{2n+1}z^2)(1 + x^{2n-3}z^{-2})$$
$$= \prod_{m=2}^{\infty}(1 + x^{2m-1}z^2) \prod_{r=0}^{\infty}(1 + x^{2r-1}z^{-2}).$$

چون $xz^2 = (1 + xz^2)/(1 + x^{-1}z^{-2})$، ضرب آخرین معادله در xz^2 رابطهٔ (۱۵) را نتیجه می‌دهد.

حال فرض کنیم $G(z)$ طرف چپ (۱۳) باشد؛ درنتیجه،

$$G(z) = F(z)\prod_{n=1}^{\infty}(1 - x^{2n}). \qquad (۱۶)$$

دراین صورت ، $G(z)$ در معادلهٔ تابعی (۱۵) نیز صدق می‌کند . بعلاوه ، $G(z)$ یک تابع زوج از z است کـه به‌ازای هر $z \neq 0$ تحلیلی بوده ؛ درنتیجه ، بسط‌لوران[1] به شکل زیر دارد :

$$G(z) = \sum_{m=-\infty}^{\infty} a_m z^{2m} \tag{۱۷}$$

که درآن $a_{-m} = a_m$ زیرا $G(z) = G(z^{-1})$. (ضرایب a_m به x وابسته‌اند .) با استفاده از معادلهٔ تابعی (۱۵) در (۱۷) ، معلوم می‌شود که ضرایب در فرمول بازگشتی

$$a_m = x^{2m-1} a_{m-1}$$

صدق می‌کند ، که وقتی تکرار شود ، نتیجه می‌دهد که

$$a_m = a_0 x^{m^2} \quad \text{، } m \geq 0 \text{ به‌ازای هر}$$

زیرا $1 + 3 + \cdots + (2m-1) = m^2$. ایـن رابطه به‌ازای $m < 0$ نیز برقرار است . از اینرو ، (۱۷) خواهد شد

$$G_x(z) = a_0(x) \sum_{m=-\infty}^{\infty} x^{m^2} z^{2m}, \tag{۱۸}$$

که درآن $G_x(z)$ را به‌جای $G(z)$ و $a_0(x)$ را به‌جای a_0 نوشته‌ایم تا بستگی به x را نشان دهیم . توجـه کنید که (۱۸) ایجاب می‌کند که وقتی $x \to 0$ ، $a_0(x) \to 1$. برای اتمام برهان ، باید نشان داد که به‌ازای هر x ، $a_0(x) = 1$.

با فرض $z = e^{\pi i/4}$ در (۱۸) ، معلوم می‌شود که

$$\frac{G_x(e^{\pi i/4})}{a_0(x)} = \sum_{m=-\infty}^{\infty} x^{m^2} i^m = \sum_{n=-\infty}^{\infty} (-1)^n x^{(2n)^2} \tag{۱۹}$$

زیراکه‌اگر m فرد باشد ، $i^m = -i^{-m}$. از (۱۸) دیده می‌شود که سری سمت راست (۱۹) مساوی $G_{x^4}(i)/a_0(x^4)$ است ؛ درنتیجه ، اتحاد زیر را داریم :

$$\frac{G_x(e^{\pi i/4})}{a_0(x)} = \frac{G_{x^4}(i)}{a_0(x^4)}. \tag{۲۰}$$

حال نشان مـی‌دهیم که $G_x(e^{\pi i/4}) = G_{x^4}(i)$. درواقع ، (۱۴) و (۱۶) نتیجه می‌دهند که

$$G_x(e^{\pi i/4}) = \prod_{n=1}^{\infty} (1 - x^{2n})(1 + x^{4n-2}).$$

چون هر عدد زوج به شکل $4n$ یا $4n-2$ است ، داریم

---

1. Laurent

$$\prod_{n=1}^{\infty}(1-x^{2n})=\prod_{n=1}^{\infty}(1-x^{4n})(1-x^{4n-2})\;;$$

درنتیجه،

$$G_x(e^{\pi i/4})=\prod_{n=1}^{\infty}(1-x^{4n})(1-x^{4n-2})(1+x^{4n-2})=\prod_{n=1}^{\infty}(1-x^{4n})(1-x^{8n-4})$$

$$=\prod_{n=1}^{\infty}(1-x^{8n})(1-x^{8n-4})(1-x^{8n-4})=G_{x^4}(i).$$

ازاینرو، (۲۰) ایجاب می‌کندکه $a_0(x)=a_0(x^4)$. از تعویض x با $x^4, x^{4^2},\ldots$ ، معلوم می‌شود که

به‌ازای $k=1,2,\ldots$ ، $a_0(x)=a_0(x^{4^k})$.

اما، وقتی $k\to\infty$ ، $x^{4^k}\to 0$ و، وقتی $x\to 0$ ، $a_0(x)\to 1$ ؛ درنتیجه، به‌ازای هر x ، $a_0(x)=1$. این برهان را تمام می‌کند.

۹.۱۴ نتایج اتحاد ژاکوبی

اگر در اتحاد ژاکوبی x را با x^a و z^2 را با x^b عوض کنیم، معلوم می‌شود که

$$\prod_{n=1}^{\infty}(1-x^{2na})(1+x^{2na-a+b})(1+x^{2na-a-b})=\sum_{m=-\infty}^{\infty}x^{am^2+bm}.$$

بهمین نحو، اگر $z^2=-x^b$ ، درمی‌یابیم که

$$\prod_{n=1}^{\infty}(1-x^{2na})(1-x^{2na-a+b})(1-x^{2na-a-b})=\sum_{m=-\infty}^{\infty}(-1)^m x^{am^2+bm}.$$

برای بدست‌آوردن قضیهٔ اعداد مخمسی اویلر، کافی است در اتحاد اخیر اختیار کنیم $a=3/2$ و $b=1/2$.

فرمول ژاکوبی به فرمول مهم دیگری برای مکعب حاصل ضرب اویلر منجر می‌شود.

قضیهٔ ۷.۱۴ . *اگر* $|x|<1$ *، داریم*

$$\prod_{n=1}^{\infty}(1-x^n)^3=\sum_{m=-\infty}^{\infty}(-1)^m m x^{(m^2+m)/2}$$

$$=\sum_{m=0}^{\infty}(-1)^m(2m+1)x^{(m^2+m)/2}. \qquad (۲۱)$$

برهان. از تعویض z^2 با $-xz$ در اتحاد ژاکوبی، بدست می‌آید

$$\prod_{n=1}^{\infty}(1-x^{2n})(1-x^{2n}z)(1-x^{2\cancel{n}-2}z^{-1}) = \sum_{m=0}^{\infty}(-1)^m x^{m^2+m}(z^m - z^{-m-1}).$$

حال، با استفاده از روابط

$$\prod_{n=1}^{\infty}(1-x^{2n-2}z^{-1}) = (1-z^{-1})\prod_{n=1}^{\infty}(1-x^{2n}z^{-1})$$

و

$$z^m - z^{-m-1} = (1-z^{-1})(1+z^{-1}+z^{-2}+\cdots+z^{-2m})z^m,$$

جملات طرفین را تغییر آرایش می‌دهیم. با حذف عامل $1 - z^{-1}$، خواهیم داشت

$$\prod_{n=1}^{\infty}(1-x^{2n})(1-x^{2n}z)(1-x^{2n}z^{-1})$$
$$= \sum_{m=0}^{\infty}(-1)^m x^{m^2+m}z^m(1+z^{-1}+z^{-2}+\cdots+z^{-2m}).$$

با فرض $z = 1$ و تعویض x با $x^{1/2}$، (۲۱) بدست خواهد آمد.

۱۰.۱۴ مشتقگیری لگاریتمی از توابع مولد

قضیهٔ ۴.۱۴ یک فرمول بازگشتی برای $p(n)$ بدست می‌دهد. انواع دیگر فرمولهای بازگشتی برای توابع حسابی وجود دارند که می‌توان آنها را با مشتقگیری لگاریتمی از توابع مولد نتیجه گرفت. روش کار را در محدودهٔ زیر توضیح می‌دهیم.

فرض کنیم A مجموعه‌ای از اعداد صحیح مثبت بوده، و $f(n)$ تابع حسابی مفروضی باشد. همچنین، حاصل ضرب

$$F_A(x) = \prod_{n\in A}(1-x^n)^{-f(n)/n}$$

و سری

$$G_A(x) = \sum_{n\in A}\frac{f(n)}{n}x^n$$

به‌ازای $|x| < 1$ به‌طور مطلق همگرا بوده و در قرص یکهٔ $|x| < 1$ توابعی تحلیلی نمایش دهید. لگاریتم حاصل ضرب مساوی است با

$$\log F_A(x) = -\sum_{n\in A}\frac{f(n)}{n}\log(1-x^n) = \sum_{n\in A}\frac{f(n)}{n}\sum_{m=1}^{\infty}\frac{x^{mn}}{m} = \sum_{m=1}^{\infty}\frac{1}{m}G_A(x^m).$$

با مشتقگیری و ضرب در x، بدست می‌آوریم

$$x\frac{F'_A(x)}{F_A(x)} = \sum_{m=1}^{\infty} G'_A(x^m)x^m = \sum_{m=1}^{\infty} \sum_{n\in A} f(n)x^{mn} = \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \chi_A(n)f(n)x^{mn},$$

که در آن χ_A تابع مشخص مجموعهٔ A است :

$$\chi_A(n) = \begin{cases} 1 & \text{اگر } n\in A \\ 0 & \text{اگر } n\notin A \end{cases}$$

اگر جملات با $mn = k$ را دسته بندی کنیم ، درمی‌یابیم که

$$\sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \chi_A(n)f(n)x^{mn} = \sum_{k=1}^{\infty} f_A(k)x^k,$$

که در آن

$$f_A(k) = \sum_{d|k} \chi_A(d)f(d) = \sum_{\substack{d|k \\ d\in A}} f(d).$$

لذا ، اتحاد زیر را داریم :

$$xF'_A(x) = F_A(x)\sum_{k=1}^{\infty} f_A(k)x^k. \qquad (۲۲)$$

حال حاصل ضرب $F_A(x)$ را به‌صورت سری توانی می‌نویسیم : $F_A(x) = \sum_{n=0}^{\infty} p_{A,f}(n)x^n$

که در آن $p_{A,f}(0) = 1$ و ، با متحد گرفتن ضرایب x^n در (۲۲) ، فرمول بازگشتی (۲۴) در قضیهٔ زیر بدست می‌آید .

قضیهٔ ۸۰۱۴ . به‌ازای مجموعهٔ A و تابع حسابی f ، اعداد $p_{A,f}(n)$ تعریف شده با معادلهٔ

$$\prod_{n\in A}(1-x^n)^{-f(n)/n} = 1 + \sum_{n=1}^{\infty} p_{A,f}(n)x^n \qquad (۲۳)$$

در فرمول بازگشتی زیر صدق می‌کنند :

$$np_{A,f}(n) = \sum_{k=1}^{n} f_A(k)p_{A,f}(n-k), \qquad (۲۴)$$

که در آن $p_{A,f}(0) = 1$ و

$$f_A(k) = \sum_{\substack{d|k \\ d\in A}} f(d).$$

مثال ۱. فرض‌کنیم A مجموعهٔ تمام اعداد صحیح مثبت باشد. هرگاه $f(n) = n$ ، آنگاه $p_{A,f}(n) = p(n)$ ، یعنی مساوی تابع افراز نامحدود، و $f_A(k) = \sigma(k)$ ، یعنی مساوی مجموع مقسوم علیه‌های k است. معادلهٔ (۲۴) خواهد شد

$$np(n) = \sum_{k=1}^{n} \sigma(k)p(n-k),$$

رابطهٔ جالبی که یک تابع نظریهٔ ضربی اعداد را به یک تابع نظریهٔ جمعی اعداد مربوط می‌سازد.

مثال ۲. A ی مثال ۱ را گرفته، ولی فرض می‌کنیم $f(n) = -n$. دراین صورت، ضرایب (۲۳) به‌وسیلهٔ قضیهٔ اعداد مخمسی اویلر معین می‌شود و فرمول بازگشتی (۲۴) خواهد شد

$$np_{A,f}(n) = -\sum_{k=1}^{n} \sigma(k)p_{A,f}(n-k) = -\sigma(n) - \sum_{k=1}^{n-1} p_{A,f}(k)\sigma(n-k), \qquad (۲۵)$$

که در آن

$$p_{A,f}(n) = \begin{cases} (-1)^m & \text{اگر } n \text{ یک عدد مخمسی } \omega(m) \text{ یا } \omega(-m) \text{ باشد،} \\ 0 & \text{اگر } n \text{ یک عدد مخمسی نباشد،} \end{cases}$$

معادلهٔ (۲۵) را می‌توان به صورت زیر نوشت:

$$\sigma(n) - \sigma(n-1) - \sigma(n-2) + \sigma(n-5) + \sigma(n-7) - \cdots$$
$$= \begin{cases} (-1)^{m-1}\omega(m) & \text{اگر } n = \omega(m) \text{ ،} \\ (-1)^{m-1}\omega(-m) & \text{اگر } n = \omega(-m) \text{ ،} \\ 0 & \text{درغیر این‌صورت ،} \end{cases}$$

مجموع سمت چپ وقتی ختم می‌شود که جملهٔ $\sigma(k)$ دارای $k \le 1$ باشد. در توضیح این مطلب گوییم که، وقتی $n = 6$ و $n = 7$ ، اینها روابط زیر را نتیجه می‌دهند:

$$\sigma(6) = \sigma(5) + \sigma(4) - \sigma(1),$$
$$\sigma(7) = \sigma(6) + \sigma(5) - \sigma(2) - 7.$$

۱۱.۱۴ اتحادهای افرازی رامانوجان

بررسی جدول مک‌ماهون تابع افراز، رامانوجان را به کشف چند خاصیت بخشپذیری جالب $p(n)$ هدایت کرد. مثلاً، وی ثابت کرد که

$$p(5m+4) \equiv 0 \pmod{5}, \qquad (۲۶)$$

$$p(7m+5) \equiv 0 \pmod 7, \tag{۲۷}$$

$$p(11m+6) \equiv 0 \pmod{11}. \tag{۲۸}$$

او در رابطه با این کشفها دو اتحاد جالب را نیز بدون برهان ذکر نمود :

$$\sum_{m=0}^{\infty} p(5m+4)x^m = 5\frac{\varphi(x^5)^5}{\varphi(x)^6}, \tag{۲۹}$$

و

$$\sum_{m=0}^{\infty} p(7m+5)x^m = 7\frac{\varphi(x^7)^3}{\varphi(x)^4} + 49x\frac{\varphi(x^7)^7}{\varphi(x)^8}, \tag{۳۰}$$

که در آن

$$\varphi(x) = \prod_{n=1}^{\infty}(1-x^n).$$

چون توابع سمت راست (۲۹) و (۳۰) دارای بسط به‌صورت سری توانی با ضرایب صحیح‌اند، اتحادهای رامانوجان فورا" همنهشتیهای (۲۶) و (۲۷) را ایجاب می‌کنند.

برهانهایی از (۲۹) و (۳۰)، که بر نظریهٔ توابع هنگی استوارند، به وسیلهٔ دارلینگ[1]، مردل، رادماخر، سوکرمن[2]، و دیگران بدست آمده‌اند. برهانهایی دیگر، مستقل از نظریهٔ توابع هنگی، توسط کروزویج[3] [۳۶] و بعدا" به وسیلهٔ کولبرگ[4] داده شد. روش کولبرگ نه فقط اتحادهای رامانوجان بلکه اتحادهای جدید زیادی را نیز بدست داد. برهان کروزویج (۲۹) در تمرینهای ۱۱ تا ۱۵ مختصرا" شرح داده شده است.

تمرین برای فصل ۱۴

۱. فرض کنید A مجموعه‌ای ناتهی از اعداد صحیح مثبت باشد.

(آ) ثابت کنید حاصل ضرب

$$\prod_{m\in A}(1-x^m)^{-1}$$

تابع مولد تعداد افرازهای n به فرازهای متعلق به مجموعهٔ A است.

(ب) تابع افراز تولید شده به وسیلهٔ حاصل ضرب

$$\prod_{m\in A}(1+x^m)$$

را توصیف کنید. بالاخص، تابع افراز تولید شده به‌وسیلهٔ حاصل ضرب متناهی

---

1. Darling 2. Zuckerman 3. Kruyswijk 4. Kolberg

$\prod_{m=1}^{k}(1+x^m)$ را توصیف نمایید .

۲ . اگر $|x|<1$ ، ثابت کنید

$$\prod_{m=1}^{\infty}(1+x^m)=\prod_{m=1}^{\infty}(1-x^{2m-1})^{-1},$$

و نتیجه بگیرید کــه تعدادافرازهای n به فرازهای نامساوی مساوی تعداد افرازهای n به فرازهای فرد است .

۳ . به ازای x و z مختلط‌که $|x|<1$ ، قرار دهید

$$f(x,z)=\prod_{m=1}^{\infty}(1-x^m z).$$

(آ) ثابت کنیــد این حاصل ضرب به‌ازای هر z ثابت یک تابع تحلیلی از x در قرص $|x|<1$ است و ، بــه‌ازای هر x ثابت که $|x|<1$ ، حاصل ضرب یک تابع تمام از z است .

(ب) اعداد $a_n(x)$ را با معادلهٔ

$$f(x,z)=\sum_{n=0}^{\infty}a_n(x)z^n$$

تعریف کنید . نشان دهید که $f(x,z)=(1-xz)f(x,zx)$ و ، با استفاده از این ،ثابت کنید که ضرایب در فرمول بازگشتی

$$a_n(x)=a_n(x)x^n-a_{n-1}(x)x^n$$

صدق می‌کنند .

(پ) از قسمت (ب) نتیجه بگیرید که $a_n(x)=(-1)^n x^{n(n+1)/2}/P_n(x)$ ، که در آن

$$P_n(x)=\prod_{r=1}^{n}(1-x^r).$$

این اتحاد زیر را به‌ازای $|x|<1$ و z دلخواه ثابت می‌کند :

$$\prod_{m=1}^{\infty}(1-x^m z)=\sum_{n=0}^{\infty}\frac{(-1)^n}{P_n(x)}x^{n(n+1)/2}z^n.$$

۴ . با استفــاده از روشی شبیــه روش تمــرین ۳ ، ثابت کنید که اگر $|x|<1$ و $|z|<1$ ، داریــم

$$\prod_{m=1}^{\infty}(1-x^m z)^{-1}=\sum_{n=0}^{\infty}\frac{z^n}{P_n(x)},$$

که در آن $P_n(x)=\prod_{r=1}^{n}(1-x^r)$.

۵ . اگر $x \neq 1$ ، قرار دهید $Q_0(x) = 1$ و، به‌ازای $n \geq 1$ ، تعریف کنید

$$Q_n(x) = \prod_{r=1}^{n} \frac{1 - x^{2r}}{1 - x^{2r-1}}.$$

(آ) اتحادهای متناهی زیر از شانکس را نتیجه بگیرید :

$$\sum_{m=1}^{2n} x^{m(m-1)/2} = \sum_{s=0}^{n-1} \frac{Q_n(x)}{Q_s(x)} x^{s(2n+1)},$$
$$\sum_{m=1}^{2n+1} x^{m(m-1)/2} = \sum_{s=0}^{n} \frac{Q_n(x)}{Q_s(x)} x^{s(2n+1)}.$$

(ب) با استفاده‌ازاتحادهای شانکس، قضیهٔ اعداد مثلثی گاوس را نتیجه بگیرید :

به‌ازای $|x| < 1$ ، $\sum_{m=1}^{\infty} x^{m(m-1)/2} = \prod_{n=1}^{\infty} \frac{1 - x^{2n}}{1 - x^{2n-1}}$.

۶ . اتحاد زیر به‌ازای $|x| < 1$ معتبر است :

$$\sum_{m=-\infty}^{\infty} x^{m(m+1)/2} = \prod_{n=1}^{\infty}(1 + x^{n-1})(1 - x^{2n}).$$

(آ) این اتحاد را از اتحادهای تمرینهای ۲ تا ۵ (ب) نتیجه بگیرید .

(ب) این اتحاد را از اتحاد حاصل ضرب سه‌گانهٔ ژاکوبی نتیجه بگیرید .

۷ . ثابت کنید اتحادهای زیر، که به‌ازای $|x| < 1$ معتبرند، نتایج اتحاد حاصل ضرب سه‌گانهٔ ژاکوبی‌اند :

(آ) $\sum_{m=-\infty}^{\infty} (-1)^m x^{m(5m-3)/2} = \prod_{n=1}^{\infty}(1 - x^{5n})(1 - x^{5n-1})(1 - x^{5n-4})$ ؛

(ب) $\sum_{m=-\infty}^{\infty} (-1)^m x^{m(5m+1)/2} = \prod_{n=1}^{\infty}(1 - x^{5n})(1 - x^{5n-2})(1 - x^{5n-3})$.

۸ . ثابت کنید فرمول بازگشتی

$$np(n) = \sum_{k=1}^{n} \sigma(k)p(n-k),$$

که در بخش ۱۴.۱۰ بدست آمد، را می‌توان به شکل زیر نوشت :

$$np(n) = \sum_{m=1}^{n} \sum_{k \leq n/m} mp(n-km).$$

۹ . فرض کنید هر عدد صحیح مثبت k به $g(k)$ رنگ مختلف نوشته شده باشد، که درآن $g(k)$ یک عدد صحیح مثبت است . همچنین، $p_g(n)$ تعداد افرازهای n باشد که درآنها

هر فراز k حداکثردر $g(k)$ رنگ‌مختلف‌ظاهرمی‌شود . وقتی به‌ازای هر k ، $g(k)=1$ ، این‌تابع افراز نامحدود $p(n)$ است . حاصل ضربی‌نامتناهی بیابید که $p_g(n)$ را تولیدکند ، و ثابت کنید یک تابع حسابی مانند f (وابسته به g) هست بطوری که

$$np_g(n)=\sum_{k=1}^{n} f(k)p_g(n-k).$$

۱۰ . برای نمـادها به بخش ۱۴ . ۱۰ رجوع کنید . با حل معادلهٔ دیفرانسیل مرتبهٔ اول در (۲۲) ، ثابت کنید که اگر $|x|<1$ ، داریم

$$\prod_{n\in A}(1-x^n)^{-f(n)/n}=\exp\left\{\int_0^x \frac{H(t)}{t}\,dt\right\},$$

که در آن

$$H(x)=\sum_{k=1}^{\infty} f_A(k)x^k \quad \text{و} \quad f_A(k)=\sum_{\substack{d|k\\ d\in A}} f(d) \cdot$$

نتیجه بگیرید که

$$\text{به‌ازای } |x|<1 \text{ ،} \quad \prod_{n=1}^{\infty}(1-x^n)^{\mu(n)/n}=e^{-x} \text{ ،}$$

که در آن $\mu(n)$ تابع موبیوس است .

تمرینهای زیر برهان مختصری از اتحاد افرازی رامانوجان

$$\sum_{m=0}^{\infty} p(5m+4)x^m=5\,\frac{\varphi(x^5)^5}{\varphi(x)^6} \text{ ، که در آن } \varphi(x)=\prod_{n=1}^{\infty}(1-x^n)$$

را به‌روش کروزویج که به نظریهٔ توابع هنگی نیازی ندارد توضیح می‌دهد .

۱۱ . (آ) فرض کنید $\varepsilon=e^{2\pi i/k}$ که در آن $k\geq 1$ ، و نشان دهید که به‌ازای هر x ، داریم

$$\prod_{h=1}^{k}(1-x\varepsilon^h)=1-x^k.$$

(ب) بطور کلی ، اگر $(n,k)=d$ ، ثابت کنید

$$\prod_{h=1}^{k}(1-x\varepsilon^{nh})=(1-x^{k/d})^d.$$

و نتیجه بگیرید که

$$\prod_{h=1}^{k}(1-x^n e^{2\pi i n h/k})=\begin{cases}1-x^{nk} & \text{اگر } (n,k)=1 \text{ ،}\\ (1-x^n)^k & \text{اگر } k|n\end{cases}$$

۱۲ . (آ) با استفاده از تمرین ۱۱ (ب) ، ثابت کنید به‌ازای q اول و $|x|<1$ ، داریم

$$\prod_{n=1}^{\infty}\prod_{h=1}^{q}(1-x^n e^{2\pi inh/q})=\frac{\varphi(x^q)^{q+1}}{\varphi(x^{q^2})}.$$

(ب) اتحاد

$$\sum_{m=0}^{\infty}p(m)x^m=\frac{\varphi(x^{25})}{\varphi(x^5)^6}\prod_{h=1}^{4}\prod_{n=1}^{\infty}(1-x^n e^{2\pi inh/5})$$

را نتیجه بگیرید

۱۳. اگر q اول بوده و $0 \le r < q$ ، گوییم سری توانی به شکل

$$\sum_{n=0}^{\infty}a(n)x^{qn+r}$$

از نوع r به هنگ q است.

(آ) با استفاده از قضیهٔ اعداد مخمسی ، نشان دهید که $\varphi(x)$ مجموع سه سری توانی است:

$$\varphi(x)=\prod_{n=1}^{\infty}(1-x^n)=I_0+I_1+I_2,$$

که در آن I_k یک سری توانی از نوع k به هنگ 5 است.

(ب) فرض کنید $\alpha=e^{2\pi i/5}$ ، و نشان دهید که

$$\prod_{h=1}^{4}\prod_{n=1}^{\infty}(1-x^n\alpha^{nh})=\prod_{h=1}^{4}(I_0+I_1\alpha^h+I_2\alpha^{2h}).$$

(پ) با استفاده از تمرین ۱۲ (ب) ، نشان دهید

$$\sum_{m=0}^{\infty}p(5m+4)x^{5m+4}=V_4\frac{\varphi(x^{25})}{\varphi(x^5)^6},$$

که در آن V_4 سری توانی از نوع 4 به هنگ 5 است که از حاصل ضرب قسمت (ب) بدست می‌آید.

۱۴. (آ) با استفاده از قضیهٔ ۷.۱۴ ، نشان دهید که مکعب حاصل ضرب اویلرمجموع سه سری توانی است:

$$\varphi(x)^3=W_0+W_1+W_3,$$

که در آن W_k یک سری توانی از نوع k به هنگ 5 است.

(ب) با استفاده از اتحاد $W_0+W_1+W_3=(I_0+I_1+I_2)^3$ ، نشان دهید که‌سری توانی تمرین ۱۳ (آ) در رابطهٔ

$$I_0I_2=-I_1{}^2$$

صدق می‌کند.

(پ) ثابت کنید که $I_1 = -x\varphi(x^{25})$.

۱۵ . توجه کنید که حاصل ضرب $\prod_{h=1}^{4}(I_0 + I_1\alpha^h + I_2\alpha^{2h})$ یک چندجمله‌ای همگن نسبت به I_0, I_1, I_2 از درجهٔ 4 است ؛ درنتیجه ، جمــلات بکار رفته در سری از نوع 4 به هنگ 5 از جملات $I_1{}^4$ ، $I_0 I_1{}^2 I_2$ ، و $I_0{}^2 I_2{}^2$ می‌آیند .

(آ) با استفاده از تمرین ۱۴ (پ) ، نشان دهید که ثابتی چون c هست بطوری کــه

$$V_4 = cI_1{}^4,$$

که در آن V_4 سری توانی تمرین ۱۳ (پ) است ، و نتیجه بگیرید که

$$\sum_{m=0}^{\infty} p(5m + 4)x^{5m+4} = cx^4 \frac{\varphi(x^{25})^5}{\varphi(x^5)^6}.$$

(ب) ثابت کنید $c = 5$ ، و اتحاد رامانوجان را نتیجه بگیرید :

$$\sum_{m=0}^{\infty} p(5m + 4)x^m = 5\frac{\varphi(x^5)^5}{\varphi(x)^6}.$$

کتابنامه

MR denotes reference to *Mathematical Reviews*.

1. Apostol, Tom M. (1970) Euler's φ-function and separable Gauss sums. *Proc. Amer. Math. Soc.*, *24*: 482–485; *MR* 41, #1661.
2. Apostol, Tom M. (1974) *Mathematical Analysis*, 2nd ed. Reading, Mass.: Addison–Wesley Publishing Co.
3. Ayoub, Raymond G. (1963) *An Introduction to the Analytic Theory of Numbers.* Mathematical Surveys, No. 10. Providence, R. I.: American Mathematical Society.
4. Bell, E. T. (1915) An arithmetical theory of certain numerical functions. *University of Washington Publ. in Math. and Phys. Sci., No. 1, Vol. 1*: 1–44.
5. Borozdkin, K. G. (1956) K voprosu o postoyanni I. M. Vinogradova. *Trudy tretego vsesoľuznogo matematičeskogo siezda, Vol. I*, Moskva [Russian].
6. Buhštab, A. A. (1965) New results in the investigation of the Goldbach–Euler problem and the problem of prime pairs. [Russian]. *Dokl. Akad. Nauk SSSR*, *162*: 735–738; *MR* 31, #2226. [English translation: (1965) *Soviet Math. Dokl. 6*: 729–732.]
7. Chandrasekharan, Komaravolu (1968) *Introduction to Analytic Number Theory.* Die Grundlehren der Mathematischen Wissenschaften, Band 148. New York: Springer–Verlag.
8. Chandrasekharan, Komaravolu (1970) *Arithmetical Functions.* Die Grundlehren der Mathematischen Wissenschaften, Band 167. New York. Springer–Verlag.
9. Chebyshev, P. L. Sur la fonction qui détermine la totalité des nombres premiers inferieurs à une limite donèe. (a) (1851) *Mem. Ac. Sc. St. Pétersbourg*, *6*: 141–157. (b) (1852) *Jour. de Math* (1) *17*: 341–365. [*Oeuvres, 1*: 27–48.]
10. Chen, Jing-run (1966) On the representation of a large even integer as the sum of a prime and the product of at most two primes. *Kexue Tongbao* (Foreign Lang. Ed.), *17*: 385–386; *MR* 34, #7483.
11. Clarkson, James A. (1966) On the series of prime reciprocals. *Proc. Amer. Math. Soc.*, *17*: 541; *MR* 32, #5573.
12. Davenport, Harold (1967) *Multiplicative Number Theory.* Lectures in Advanced Mathematics, No. 1. Chicago: Markham Publishing Co.

13. Dickson, Leonard Eugene (1919) *History of the Theory of Numbers.* (3 volumes). Washington, D. C.: Carnegie Institution of Washington. Reprinted by Chelsea Publishing Co., New York, 1966.

14. Dickson, Leonard Eugene (1930) *Studies in the Theory of Numbers.* Chicago: The University of Chicago Press.

15. Dirichlet, P. G. Lejeune (1837) Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftichen Factor sind, unendliche viele Primzahlen enthält. *Abhand. Ak. Wiss. Berlin*: 45–81. [*Werke, 1*: 315–342.]

16. Dirichlet, P. G. Lejeune (1840) Ueber eine Eigenschaft der quadratischen Formen. *Bericht Ak. Wiss. Berlin*: 49–52. [*Werke, 1*: 497–502.]

17. Edwards, H. M. (1974) *Riemann's Zeta Function.* New York and London: Academic Press.

18. Ellison, W. J. (1971) Waring's problem. *Amer. Math. Monthly, 78*: 10–36.

19. Erdös, Paul (1949) On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. *Proc. Nat. Acad. Sci. U.S.A., 35*: 374–384; *MR* 10, 595.

20. Euler, Leonhard (1737) Variae observationes circa series infinitas. *Commentarii Academiae Scientiarum Imperialis Petropolitanae, 9*: 160–188. [*Opera Omnia* (1), *14*: 216–244.]

21. Euler, Leonhard (1748) *Introductio in Analysin Infinitorum,* Vol. 1. Lausanne: Bousquet. [*Opera Omnia* (1), *8*.]

22. Franklin, F. (1881) Sur le développement du produit infini $(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots$. *Comptes Rendus Acad. Sci. (Paris), 92*: 448–450.

23. Gauss, C. F. (1801) *Disquisitiones Arithmeticae.* Lipsiae. [English translation: Arthur A. Clarke (1966) New Haven: Yale University Press.

24. Gauss, C. F. (1849) Letter to Encke, dated 24 December. [*Werke*, Vol. II, 444–447.]

25. Gerstenhaber, Murray (1963) The 152nd proof of the law of quadratic reciprocity. *Amer. Math. Monthly, 70*: 397–398; *MR* 27, #100.

26. Goldbach, C. (1742) Letter to Euler, dated 7 June.

27. Grosswald, Emil (1966) *Topics from the Theory of Numbers.* New York: The Macmillan Co.

28. Hadamard, J. (1896) Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. *Bull. Soc. Math. France, 24*: 199–220.

29. Hagis, Peter, Jr. (1973) A lower bound for the set of odd perfect numbers. *Math. Comp., 27*: 951–953; *MR* 48, #3854.

30. Hardy, G. H. (1940) *Ramanujan. Twelve Lectures on Subjects Suggested by His Life and Work*. Cambridge: The University Press.

31. Hardy, G. H. and Wright, E. M. (1960) *An Introduction to the Theory of Numbers,* 4th ed. Oxford: Clarendon Press.

32. Hemer, Ove (1954) Notes on the Diophantine equation $y^2 - k = x^3$. *Ark. Mat.,* 3: 67–77; *MR* 15, 776.

33. Ingham, A. E. (1932) *The Distribution of Prime Numbers.* Cambridge Tracts in Mathematics and Mathematical Physics, No. 30. Cambridge: The University Press.

34. Jacobi, C. G. J. (1829) *Fundamenta Nova Theoriae Functionum Ellipticarum.* [*Gesammelte Werke*, Band I, 49–239.]

35. Kolesnik, G. A. (1969) An improvement of the remainder term in the divisor prob-

lem. (Russian). *Mat. Zametki, 6*: 545–554; *MR* 41, #1659. [English translation (1969), *Math. Notes*, 6: 784–791.]

36. Kruyswijk, D. (1950) On some well-known properties of the partition function $p(n)$ and Euler's infinite product. *Nieuw Arch. Wisk.*, (2) *23*: 97–107; *MR* 11, 715.
37. Landau, E. (1909) *Handbuch der Lehre von der Verteilung der Primzahlen*. Leipzig: Teubner. Reprinted by Chelsea, 1953.
38. Landau, E. (1927) *Vorlesungen über Zahlentheorie* (3 volumes). Leipzig: Hirzel. Reprinted by Chelsea, 1947.
39. Leech, J. (1957) Note on the distribution of prime numbers. *J. London Math. Soc.*, *32*: 56–58; *MR* 18, 642.
40. Legendre, A. M. (1798) *Essai sur la Theorie des Nombres*. Paris: Duprat.
41. Lehmer, D. H. (1959) On the exact number of primes less than a given limit. *Illinois J. Math.*, *3*: 381–388; *MR* 21, #5613.
42. Lehmer, D. H. (1936) On a conjecture of Ramanujan. *J. London Math. Soc.*, *11*: 114–118.
43. Lehmer, D. N. (1914) List of prime numbers from 1 to 10, 006, 721. Washington, D.C.: Carnegie Institution of Washington, Publ. No. 165.
44. LeVeque, W. J. (1956) *Topics in Number Theory* (2 volumes). Reading, Mass.: Addison-Wesley Publishing Co.
45. LeVeque, W. J. (1974) *Reviews in Number Theory* (6 volumes). Providence, RI: American Mathematical Society.
46. Levinson, N. (1969) A motivated account of an elementary proof of the prime number theorem. *Amer. Math. Monthly*, *76*: 225–245; *MR* 39, #2712.
47. Levinson, Norman (1974) More than one third of zeros of Riemann's zeta-function are on $\sigma = 1/2$. *Advances Math.*, *13*: 383–436.
48. van Lint, Jacobus Hendricus (1974) *Combinatorial Theory Seminar*. (Eindhoven University of Technology), Lecture Notes in Mathematics 382. Springer Verlag. Chapter 4.
49. Littlewood, J. E. (1914) Sur la distribution des nombres premiers. *Comptes Rendus Acad. Sci. (Paris)*, *158*: 1869–1872.
50. Mills, W. H. (1947) A prime-representing function. *Bull. Amer. Math. Soc.*, *53*: 604; *MR* 8, 567.
51. Nevanlinna, V. (1962) Über den elementaren Beweis des Primzahlsatzes. *Soc. Sci. Fenn. Comment. Phys.-Math.*, *27 No. 3*, 8 pp.; *MR* 26, #2416.
52. Niven, I. and Zuckerman, H. S. (1972) *An Introduction to the Theory of Numbers*, 3rd ed. New York: John Wiley and Sons, Inc.
53. Prachar, Karl (1957) *Primzahlverteilung*. Die Grundlehren der Mathematischen Wissenschaften, Band 91. Berlin–Göttingen–Heidelberg: Springer Verlag.
54. Rademacher, Hans (1937) On the partition function $p(n)$. *Proc. London Math. Soc.*, *43*: 241–254.
55. Rademacher, Hans (1964) *Lectures on Elementary Number Theory*. New York: Blaisdell Publishing Co.
56. Rademacher, Hans (1973) *Topics in Analytic Number Theory*. Die Grundlehren der Mathematischen Wissenschaften, Band 169 New York–Heidelberg–Berlin: Springer Verlag.
57. Rènyi, A. (1948) On the representation of an even number as the sum of a single prime and a single almost-prime number. (Russian). *Izv. Akad. Nauk SSSR Ser.*

Mat., *12*: 57–78; *MR* 9, 413. [English translation: (1962) *Amer. Math. Soc. Transl.* *19* (2): 299–321.]

58. Riemann, B. (1859) Über die Anzahl der Primzahlen unter einer gegebener Grösse. *Monatsber. Akad. Berlin*, 671–680.
59. Robinson, R. M. (1958) A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers. *Proc. Amer. Math. Soc.*, *9*: 673–681; *MR* 20, #3097.
60. Rosser, J. Barkley, and Schoenfeld, Lowell (1962) Approximate formulas for some functions of prime number theory. *Illinois J. Math.*, *6*: 69–94; *MR* 25, #1139.
61. Schnirelmann, L. (1930) On additive properties of numbers. (Russian). *Izv. Donskowo Politechn. Inst. (Nowotscherkask)*, 14 (2–3): 3–28.
62. Selberg, Atle (1949) An elementary proof of the prime number theorem. *Ann. of Math.*, *50*: 305–313; *MR* 10, 595.
63. Shanks, Daniel (1951) A short proof of an identity of Euler. *Proc. Amer. Math. Soc.*, *2*: 747–749; *MR* 13, 321.
64. Shapiro, Harold N. (1950) On the number of primes less than or equal x. *Proc. Amer. Math. Soc.*, *1*: 346–348; *MR* 12, 80.
65. Shapiro, Harold N. (1952) On primes in arithmetic progression II. *Ann. of Math.* *52*: 231–243: *MR* 12, 81.
66. Shen, Mok-Kong (1964) On checking the Goldbach conjecture. *Nordisk Tidskr. Informations-Behandling*, *4*: 243–245; *MR* 30, #3051.
67. Sierpiński, Waclaw (1964) *Elementary Theory of Numbers*. Translated from Polish by A. Hulanicki. Monografie Matematyczne, Tom 42. Warsaw: Państwowe Wzdawnictwo Naukowe.
68. Tatuzawa, Tikao, and Iseki Kaneshiro (1951) On Selberg's elementary proof of the prime number theorem. *Proc. Japan Acad.*, *27*: 340–342; *MR* 13, 725.
69. Titchmarsh, E. C. (1951) *The Theory of the Riemann Zeta Function*. Oxford: Clarendon Press.
70. Uspensky, J. V., and Heaslett, M. A. (1939) *Elementary Number Theory*. New York: McGraw-Hill Book Co.
71. Vallée Poussin, Ch. de la (1896) Recherches analytiques sur la théorie des nombres premiers. *Ann. Soc. Sci. Bruxelles*, 20_2: 183–256, 281–297.
72. Vinogradov, A. I. (1965) The density hypothesis for Dirichlet *L*-series. (Russian). *Izv. Akad. Nauk SSSR, Ser. Math. 29*: 903–934; *MR* 33, #5579. [Correction: (1966) *ibid.*, *30*: 719–720; *MR* 33, #2607.]
73. Vinogradov, I. M. (1937) The representation of an odd number as the sum of three primes. (Russian.) *Dokl. Akad. Nauk SSSR*, 16: 139–142.
74. Vinogradov, I. M. (1954) *Elements of Number Theory*. Translated by S. Kravetz. New York: Dover Publications.
75. Walfisz, A. (1963) *Weylsche Exponentialsummen in der neueren Zahlentheorie*. Mathematische Forschungsberichte, XV, V E B Deutscher Verlag der Wissenschaften, Berlin.
76. Williams, H. C., and Zarnke, C. R. (1972) Some prime numbers of the form $2A3^n + 1$ and $2A3^n - 1$. *Math. Comp.* *26*: 995–998; *MR* 47, #3299.
77. Wrathall, Claude P. (1964) New factors of Fermat numbers. *Math. Comp.*, *18*: 324–325; *MR* 29, #1167.

78. Yin, Wen-lin (1956) Note on the representation of large integers as sums of primes. *Bull. Acad. Polon. Sci. Cl. III*, 4: 793–795; *MR 19*, 16.

واژه‌نامه فارسی به انگلیسی

identity	اتحاد
analytic	تحلیلی
continuation	ادامهٔ
induction	استقرا
principle of	اصل
cross - classification principle	اصل رده‌بندی چلیپایی
primes	اعداد اول
twin	دوقلو
partition	افراز
L-function	L ـ تابع
algorithm	الگوریتم
euclidean	اقلیدسی
division	تقسیم
integral	انتگرال
logarithmic	لگاریتمی
index	اندیس
divisibility	بخشپذیری
greatest common divisor	بزرگترین مقسوم علیه مشترک
expansion	بسط
finite	متناهی

convolution	پیچش
function	تابع
partition	افراز
arithmetical	حسابی
multiplicative	ضربی
totient	کامل
completely multiplicative	کاملا" ضربی
divisor	مقسوم علیهی
generating	مولد
number - theoretic	نظریهٔ اعداد
identity	همانی
equality	تساوی
asymptotic	مجانبی
constant	ثابت
product	حاصل ضرب
conjecture	حدس
arithmetic	حساب
ring	حلقه
property	خاصیت
decomposition	تجزیه
line	خط
critical	بحرانی
residue system	دستگاه مانده‌ای
complete	تام
reduced	تحویل یافته

رابطه	relation
تعامدی	orthogonality
رده	class
مانده‌ای	residue
ریشه	root
اولیه	primitive
زیر گروه	subgroup
سری	series
توانی صوری	formal power
سه‌تایی	triple
فیثاغوری	pythagorean
صفر	zero
بدیهی	trivial
ضرب	multiplication
ضریب	coefficient
طول	abscissa
همگرایی	of convergence
عامل	factor
عدد اول	prime
علامت	symbol
بزرگترین عدد صحیح	greatest integer
عنصر	element
همانی	identity

فارغ از مربع	squarefree
فرض	hypothesis
فرمول	formula
انعکاس	inversion
جمعبندی	summation
درونیابی	interpolation
مجانبی	asymptotic
قانون	law
تقابل مربعی	of quadratic reciprocity
کامل	totient
کسر	fraction
تحویل یافته	reduced
کوچکترین مضرب مشترک	least common multiple
گروه	group
آبلی	abelian
تعویضپذیر	commutative
دوری	cyclic
مشخص	character
مانده	residue
مربعی	quadratic
متوسط	average
مجموع	sum
جدایی پذیر	separable
هندسی	geometric
محک	criterion
مربعی	quadratic

همنهشتی	congruence
مرتبهٔ	order
متوسط	average
یک گروه	of a group
مشتق	derivative
مشخص	character
اصلی	principal
اولیه	primitive
معادله	equation
تابعی	functional
دیوفانتینی	diophantine
معکوس	inverse
مقسوم علیه	divisor
مشترک	common
ناحیه	region
فارغ از صفر	zero-free
نامانده	nonresidue
نامساوی	inequality
نسبت بهم اول	relatively prime
نظریهٔ اعداد	number theory
جمعی	additive
ضربی	multiplicative
نقطه	point
مشبکه	lattice
نما	exponent
نوار	strip
بحرانی	critical
نیمصفحه	half-plane
همگرایی	of convergence

هادی	conductor
یک مشخص	of a character
همنهشتی	congruence
چندجمله‌ای	polynomial
خطی	linear
دوجمله‌ای	binomial
نمایی	exponential
هنگ	modulus
القایی	induced

واژه‌نامه انگلیسی به فارسی

abelian	آبلی
abscissa	طول
of absolute convergence	همگرایی مطلق
of convergence	همگرایی
additive	جمعی
number theory	نظریهٔ . . . اعداد
algorithm	الگوریتم
division	تقسیم
euclidean	اقلیدسی
analytic	تحلیلی
continuation	ادامهٔ
arithmetic	حساب
fundamental theorem of	قضیهٔ اساسی
arithmetical	حسابی
function	تابع
asymptotic	مجانبی
equality	تساوی
average (arithmetic mean)	متوسط (میانگین حسابی)
order	مرتبهٔ
binomial	دوجمله‌ای

congruence	همنهشتی
character	مشخص
primitive	اولیه
principal	اصلی
class	رده
of residue	مانده‌ای
common	مشترک
divisor	مقسوم‌علیه
commutative	تعویضپذیر
group	گروه
complete	تام
residue system	دستگاه مانده‌ای
completely	کاملا"
multiplicative	ضربی
conductor	هادی
of a character	یک مشخص
congruence	همنهشتی
convolution	پیچش
generalized	تعمیم یافته
critical	بحرانی
line	خط
strip	نوار
cross-classification	رده بندی چلیپایی
principle	اصل
cyclic	دوری
group	گروه
decomposition	ترکیب
derivative	مشتق

divisibility	بخشپذیری
division	تقسیم
algorithm	الگوریتم
divisor	مقسوم علیه
function	تابع
euclidean	اقلیدسی
algorithm	الگوریتم
exponent	نما
of a modulo m	به هنگ m
exponential	نمایی
congruence	همنهشتی
factor	عامل
finite	متناهی
fourier expansion	بسط فوریه‌ء
formal	صوری
power series	سری توانی
function	تابع
arithmetical	حسابی
completely multiplicative	کاملا" ضربی
divisor	مقسوم علیهی
functional	تابعی
equation	معادله‌ء
fundamental	اساسی
theorem of arithmetic	قضیه‌ء . . . حساب
gamma	گاما
function	تابع
generating	مولد

function	تابع
geometric	هندسی
sum	مجموع
greatest	بزرگترین
common divisor	مقسوم علیه مشترک
integer symbol	علامت . . . عدد صحیح
group	گروه
abelian	آبلی
cyclic	دوری
character	مشخص
half-plane	نیمصفحه
of absolute convergence	همگرایی مطلق
of convergence	همگرایی
identity	همانی
element	عنصر
function	تابع
index	اندیس(ها)
calculus	حساب
induced	تحویل یافته
modulus	هنگ
induction	استقرا
principle of	اصل
inequality	نامساوی
infinitude	نامتناهی بودن
of primes	اعداد اول
inverse	معکوس
inversion	انعکاس
furmula	فرمول

lattice	مشبکه
point	نقطهٔ
law	قانون
least	کوچکترین
common multiple	مضرب مشترک
L-function	L- تابع
linear	خطی
congruence	همنهشتی
logarithmic	لگاریتمی
integral	انتگرال
mean value	مقدار میانگین
multiplication	ضرب
multipicative	ضربی
function	تابع
number theory	نظریهٔ . . . اعداد
nonresidue	نامانده
number-theoretic	نظریهٔ اعداد
function	تابع
order	مرتبه
of a group	یک گروه
orthogonality	تعامد(ی)
relation	رابطهٔ
partition	افراز
function	تابع
pentagonal	مخمسی
number	عدد

perfect	تام
number	عدد
periodic	متناوب
polygonal	چند ضلعی
number	عدد
polynomial	چند جمله‌ای
congruence	همنهشتی
prime	عدد اول
primitive	اولیه
character	مشخص
root	ریشهٔ
principal	اصلی
character	مشخص
product	حاصل ضرب
pythagorean	فیثاغوری
triple	سه‌تایی
quadratic	مربعی
congruence	همنهشتی
reciprocity	تقابل
law	قانون
reduced	تحویل یافته
fraction	کسر
relatively prime	نسبت بهم اول
residue	مانده (ای)
class	ردهٔ
quadratic	مربعی
system	دستگاه
ring	حلقه

of formal power series	سریهای توانی صوری
separable	جدایی پذیر
squarefree	فارغ از مربع
subgroup	زیر گروه
summation	جمعبندی
formula	فرمول
symbol	علامت
system	دستگاه
of residues	مانده‌ها
totient	کامل
function	تابع
triangular	مثلثی
number	عدد
trivial	بدیهی
zero	صفر
twin	دوقلو
primes	اعداد اول
unique factorization	یکتایی تجزیه
theorem	قضیهٔ
visibility	قابل رویت
of lattice point	نقطهٔ مشبکهٔ
zero	صفر
free region	ناحیهٔ فارغ از

فهرست راهنما

فهرست علامات خاص