دانشگاه فردوسی مشهد
انتشارات دانشگاه
شماره ۴۹۲

تألیف: جان استیلول

اصول نظریه اعداد

ترجمه: دکتر مجید میرزا وزیری
دانشیار گروه ریاضی دانشگاه فردوسی مشهد

بسم الله الرحمن الرحیم

دانشگاه فردوسی مشهد

انتشارات، شمارهٔ ۴۹۳

اصول نظریه اعداد

تألیف:

جان استیلول

ترجمه:

دکتر مجید میرزاوزیری

دانشیار گروه ریاضی دانشگاه فردوسی

۱–

مقدمهٔ مترجم

روزی یکی از اشراف از **اقلیدس** پرسید که آیا راهی کوتاه‌تر از خواندن کتاب **اصول** برای آشنایی با هندسه وجود دارد. **اقلیدس** در پاسخ گفت: هیچ جادهٔ ملوکانه‌ای به سمت هندسه کشیده نشده است.

کتاب حاضر ترجمه‌ای از Elements of Number Theory تألیف John Stillwell است. نام کتاب شاید چندان بی‌ارتباط به نام کتاب معروف اقلیدس نباشد. آنچه این کتاب را از متون مشابه، متمایز می‌سازد خودآموز بودن آن است. شیوهٔ بیان مباحث، آن قدر ساده است که حتی برای مبتدیان نیز به خوبی قابل فهم است. تمرینهای مناسبی که در فواصل بخشها آمده است این امکان را برای خواننده فراهم می‌آورد تا دانشی را که در هر بخش کسب کرده است محک بزنند. تمرینها توسط شماره مشخص شده‌اند ولی تعاریف و احکام ارائه شده فاقد شماره هستند. شاید در نظر اول این تفاوتِ مشهود با کتابهای متعارف، غیر طبیعی جلوه کند اما این کار باعث می‌گردد که خواننده انسی بیشتر با کتاب

برقرار کند. مثلاً به جای آن که برای ارجاع به قضیه‌ای از شماره‌ای شبیه **۳.۴.۵** استفاده شود، نام آن قضیه – که گاهی اوقات به افتخار اثبات کنندهٔ آن نامگذاری گردیده است – آمده است. بدین ترتیب احکام ارائه شده، پیشینهٔ تاریخی خود را نیز به نمایش می‌گذارند و مثلاً صورت بی‌جان **قضیهٔ ۳.۴.۵** به شکل **قضیهٔ لاگرانژ** در می‌آید که دلپذیرتر است.

علاوه بر آن، در هر فصل از کتاب بخشی به نام **بحث** وجود دارد که جنبه‌های تاریخی مباحث مطرح شده در آن فصل را مورد بررسی قرار می‌دهد. این امر نیز بر زیبایی کتاب افزوده است.

تأکید مناسبی که بر مسألهٔ رمزنگاری و دستگاه RSA (به عنوان فصلی مجزا) در کتاب شده است، باعث می‌گردد تا جنبه‌های کاربردی نظریه اعداد نیز حفظ و معرفی گردد.

از ویراستار علمی کتاب **آقای دکتر محمد صال مصلحیان** که با نگاهی دقیق به ویراستاری علمی این کتاب همت گماشتند و از **آقای دکتر اندیشه قدیریان** که ویراستاری ادبی این اثر را عهده‌دار بودند سپاسگزارم. همچنین از **خانم نوشین میرزاده** و **خانم لیلا کشفی** که نسخهٔ دستنویس را خوانده و در بازنگری متن تایپ شده همراهی‌ام کردند تشکر می‌کنم.

مشکلاتی که در ریاضی-فارسی نویسی داریم باعث می‌گردد که هر ترجمه‌ای (در کمال دقت و با حفظ امانت و پایبندی به متن اصلی) از روح نوشته و نویسنده فاصله بگیرد. برای جلوگیری از تعلیق در جملات مجبوریم آنها را به یکی دو جملهٔ کوتاه‌تر تبدیل کنیم و همین باعث می‌گردد تا زیبایی پنهان شده در واژه‌ها، کمرنگ‌تر جلوه کند. عباراتی که به صورت جملهٔ معترضه در زبان انگلیسی معمولاً بین دو علامت "،" قرار می‌گیرند، به اجبار در ترجمهٔ فارسی یا باید به جملهٔ بعد موکول گردند یا به شیوهٔ نازیبای درج در بین دو علامت "(" و ")" جلوه‌گر شوند. از این رو در ترجمه، روانی گفتار از بین می‌رود و بی‌تردید این امر باعث می‌شود بخش مهم نوشته که انتقال احساس نویسنده به خواننده است ضعیف گردد. امیدوارم کوششی که در انتقال حس

نویسنده داشته‌ام نافرجام نمانده باشد چرا که معتقدم مهم‌ترین وظیفه‌ای که هر خواننده در قبال آنچه می‌خواند دارد این است که احساس نویسنده را درک کند و طعمی را که در ضمیر واژه‌هایش پنهان ساخته است بچشد.

بی‌تردید معتقدم که ترجمهٔ حاضر خالی از نقص نیست و موجب امتنان است اگر نظرات اصلاحی خود را از طریق نشانی mirzavaziri@math.um.ac.ir به اطلاع برسانید.

دانشگاه فردوسی مشهد
مجید میرزاوزیری
بهار ۱۳۸۶

مقدمهٔ مؤلف

این کتاب به منظور تکمیل کتاب دیگرم، اصول جبر نوشته شده است و انگیزهٔ نگارش آن، مسألهٔ حل معادله‌های چندجمله‌ای می‌باشد. با این حال این کتاب، مستقل از کتاب جبر و احتمالاً ساده‌تر از آن است. در اصول جبر، در پی حل به وسیلهٔ رادیکالها بودیم که ما را به مفاهیم میدان و گروه، و مرتبط شدن آنها با یکدیگر در نظریهٔ ارزشمند گالوا[۱] رهنمون گرداند. در کتاب حاضر در پی جوابهای صحیح هستیم و این ما را به مفاهیم حلقه و ایده‌آل رهنمون می‌سازد. این دو مفهوم، در نظریهٔ ایده‌آلها[۲] که به همان میزان ارزشمند است و منسوب به کومر[۳] و ددکیند[۴] می‌باشد به هم می‌پیوندند.

حل معادلات در اعداد صحیح، مسألهٔ اصلی نظریه اعداد است. لذا این کتاب، واقعاً یک کتاب نظریه اعداد است که اکثر احکام آن را می‌توان در هر درس متعارفی از نظریه اعداد دید. اما اعداد با ساختار جبری‌شان بهتر درک می‌گردند و مفاهیم جبری لازم - حلقه و ایده‌آل - برای ارائه شدن، هیچ انگیزه‌ای بهتر از نظریه اعداد ندارند.

---

[۱] Galois
[۲] theory of ideals
[۳] Kummer
[۴] Dedekind

اولین مثال غیر بدیهی از یک حلقه در نظریه اعدادِ اویلر[۵] و گاوس[۶] ظاهر می‌گردد. مفهوم ایده‌آل – که امروزه به اندازهٔ مفهوم زیرگروههای نرمال در نظریهٔ گروهها عادی شده است – نیز به گونه‌ای کاملاً قهرمانانه از نظریه اعداد نشأت گرفته است. کومر، هنگامی که در علم حساب برای تعمیمی خاص از اعداد صحیح در مورد یکتایی تجزیه به اعداد اول با شکست مواجه شد، در حدود سال ۱۸۴۰ نوع جدیدی از اعداد را برای غلبه بر این مشکل خلق کرد. او این اعداد را اعداد ایده‌آلی[۷] نامید زیرا نمی‌دانست که آنها دقیقاً چه هستند، گرچه آشنا بود که چگونه رفتار می‌کنند. ددکیند در سال ۱۸۷۱ دریافت که این اعداد ایده‌آلی را می‌توان توسط مجموعه‌هایی از اعداد واقعی شناسایی کرد و چنین مجموعه‌هایی را ایده‌آل نامید.

ددکیند دریافت که ایده‌آلها را می‌توان کاملاً ساده‌تر تعریف کرد؛ آن قدر ساده که برای دانشجویی که امروزه با آن برخورد می‌کند ممکن است این همه هیاهو در مورد آن تعجب‌آور باشد. تنها در ایفای نقش ایده‌آلها به عنوان اعداد ایده‌آلی است که می‌توان قدر ایدهٔ بی‌شائبهٔ ایده‌آلها را دانست؛ چیزی که بر رؤیای ناممکن کومر، جامهٔ تحقق پوشانید.

لذا حل معادله‌ها در اعداد صحیح – شبیه حل به وسیلهٔ رادیکالها – اریکه‌ای باوقار است که می‌توان به نیکی، جبر را بر آن نهاد. این جایگاهی است که به حق می‌توان حلقه‌ها و ایده‌آلها را معرفی نمود و برای اولین بار آنها را به کار برد. این امر حتی موقعیتی را برای معرفی برخی حلقه‌های مرموز همانند چهارگانها[۸] مهیا می‌سازد که با استفاده از آن می‌توان قضیهٔ لاگرانژ[۹] را اثبات کرد؛ قضیه‌ای که بیان می‌دارد هر عدد طبیعی، مجموع چهار مجذور است.

این کتاب مبتنی بر دو درس کوتاه (هر کدام شامل ۲۰ درسنامه) است که در

---

[۵] Euler
[۶] Gauss
[۷] ideal numbers
[۸] quaternions
[۹] Lagrange's theorem

سالهای اخیر در دانشگاه مُناش[۱۰] ارائه شده‌اند؛ یکی در مورد نظریه اعداد مقدماتی و دیگری در مورد نظریهٔ حلقه‌ها با کاربردهایی در نظریه جبری اعداد. لذا آنچه در اینجا آمده است برای یک درس یک ترمی مناسب است که می‌توان برخی تغییرات لازم را در حذف بخشهای ستاره‌دار اختیاری اعمال کرد. برای درسی با حجم کمتر می‌توان در انتهای فصل ۹ متوقف شد؛ تا آنجا اکثر نتایج متعارف، از قضیهٔ اقلیدس در مورد نامتناهی بودن اعداد اول گرفته تا قانون تقابل مربعی، پوشش داده شده است.

با این حال باید خاطر نشان کرد که این بدان معنی نیست که کتاب حاضر، درس متعارفی در نظریه اعداد است. سعی کرده‌ام از برهانهایی که به منظور بدنام کردن نظریه اعداد ارائه شده‌اند اجتناب کنم تا ایده‌هایی را که در بسیاری از موقعیتها کار می‌کنند وحدت بخشم. این ایده‌ها شامل ساختارهای جبری هستند اما ایده‌هایی از نظریهٔ مقدماتی اعداد مانند الگوریتم اقلیدسی و یکتایی تجزیه به اعداد اول نیز آمده‌اند. به ویژه، الگوریتم اقلیدسی را به عنوان پلی به سمت نظریهٔ تصویری کانوِی[۱۱] برای صورتهای مربعی به کار برده‌ام که نگرش جدیدی برای معادلهٔ پِل[۱۲] است.

در انتهای اکثر بخشها تمرینهایی آمده است که در نتیجه، هر ایده یا برهان جدید، با حل آن تمرینها بلادرنگ تقویت می‌گردد. برخی از آنها بر ایده‌هایی خاص تمرکز دارند در حالی که بقیهٔ آنها خط کلی استدلال را (در گامهایی آسان) تکرار می‌کنند تا حکمی مشابه اثبات گردد. هدف هر تمرین باید از تفسیرهای همراه آن روشن باشد. لذا اساتید و خوانندگانی که به طور مستقل کتاب را مطالعه می‌کنند به یک میزان قادر خواهند بود مسیری لذت بخش را در خلال کتاب بیابند.

تشکر خاص خود را به دانشجویان دانشگاه مُناش (که این کتاب بر مبنای درسهایی که آنها گذرانده‌اند نوشته شده است) تقدیم می‌دارم. عکس‌العمل آنها

---

[۱۰] Monash
[۱۱] Conway
[۱۲] Pell

به شیوه‌هایی گوناگون، مرا در بهبود آنچه عرضه گردیده است یاری داد. به ویژه از لی ویلسون[۱۳] که نشان داد می‌توان با مطالعه‌ای مستقل بر مباحث این کتاب تسلط یافت سپاسگزارم.

تشکرات مخصوص خود را به همسرم الاین[۱۴] (که غلط‌گیری نسخهٔ اولیهٔ کتاب را انجام داد[۱۵]) و جان میلر[۱۶] و ایب شنیتزر[۱۷] (که با دقت بسیار نسخهٔ بازنگری شده را خواندند و مرا از بسیاری لغزشهای ریاضی و ادبی بر حذر داشتند) تقدیم می‌دارم.

جان استیلول
ملبورن جنوبی، جولای ۲۰۰۲

---

[۱۳] Ley Wilson
[۱۴] Elaine
[۱۵] لازم به ذکر است که مؤلف، کتاب را به همسرش تقدیم کرده است.
[۱۶] John Miller
[۱۷] Abe Shenitzer

فهرست

۱

اعداد طبیعی و صحیح

پیش‌نگاه

ناگفته پیداست که شمارش، مبدأ تفکر ریاضی است و بی‌شک بازشناسیِ خاستگاه مسائل ریاضی دشوار می‌باشد. پال اردوش[۱] به عنوان مسأله حل کن بزرگ مجارستانی، همیشه می‌گفت که اگر بتوانید در مورد مسألهٔ حل ناشده‌ای که بیش از ۲۰۰ سال قدمت دارد فکر کنید، این مسأله احتمالاً مسأله‌ای در حوزهٔ نظریه اعداد است.

در دهه‌های اخیر، مسائل مشکل در نظریهٔ اعداد حقیقتاً مورد توجه واقع شده‌اند. رمزنگاریِ کلید عمومی[۲] که امنیت آن وابسته به سختی تجزیهٔ اعداد بزرگ است یکی از عمومی‌ترین کاربردهای ریاضیات در زندگی روزمره می‌باشد.

به هر حال، مسائل شریانهای حیاتی نظریهٔ اعداد هستند و این مبحث با پایه‌ریزی نظریه‌ها برای قابل فهم ساختن آنها پیشرفت می‌کند. در فصل حاضر برخی مسائل نه چندان سختی را که نقش مهمی در توسعهٔ نظریهٔ اعداد ایفا

---

[۱] Paul Erdös

[۲] public key encryption

می‌کنند معرفی می‌کنیم؛ چرا که به روشها و مفاهیم اساسی منجر می‌شوند.

- شمارش موجب به وجود آمدن استقراء[۳] می‌شود که کلید همهٔ حقایق در مورد اعداد، از پیش پا افتاده‌ترین موضوعات از قبیل $a+b=b+a$ تا نتیجهٔ حیرت‌آور اقلیدس[۴] در باب نامتناهی بودن تعداد اعداد اول است.

- تقسیم (با باقیمانده) کلیدی محاسباتی در برهان اقلیدس و موضوعات دیگر مربوط به مطالعهٔ اعداد اول است.

- نماد دودویی که از تقسیم با باقیمانده نتیجه می‌شود به روشی برای به توان رساندن سریع که در رمزنگاری کلید عمومی به کار می‌رود منجر می‌گردد.

- معادلهٔ فیثاغورسی[۵]

$$x^{۲}+y^{۲}=z^{۲}$$

در هندسه، در نظریهٔ اعداد نیز به همان میزان اهمیت دارد چرا که دارای جوابهای صحیح است.

در این فصل به نشان دادن این ایده‌ها در کار با چند مورد جالب ولی به ظاهر اتفاقی بسنده می‌کنیم. در فصلهای بعدی این ایده‌ها با عمق بیشتری توسعه می‌یابند تا نشان دهند که چگونه این مفاهیم وحدت می‌یابند تا خواص حیرت‌انگیز دیگری از اعداد را توصیف کنند.

---

[۳] induction
[۴] Euclid
[۵] Pythagorean equation

۱.۱ اعداد طبیعی

نظریهٔ اعداد با اعداد طبیعی[۶]، یعنی

$$۱, ۲, ۳, ۴, ۵, ۶, ۷, ۸, ۹, \ldots$$

که توسط ۱ و افزودن متوالی ۱ تولید می‌شود آغاز می‌گردد. مجموعهٔ اعداد طبیعی را با $\mathbb{N}$ نمایش می‌دهیم. روی $\mathbb{N}$ اعمال $+$ و $\times$ را داریم که به خودی خود ساده هستند اما به مفاهیم جالبی منجر می‌گردند.

مثلاً می‌گوییم عدد a عدد n را عاد می‌کند[۷] اگر برای عددی طبیعی مانند b داشته باشیم $n = ab$. یک عدد طبیعی مانند p اول[۸] نامیده می‌شود اگر تنها اعداد طبیعی که p را عاد می‌کنند ۱ و خود p باشند.

عادپذیری و اعداد اول در ورای بسیاری از مسائل جالب ریاضیات قرار دارند و نیز زمینهٔ کاربردهای اخیر نظریهٔ اعداد (در رمزنگاری، امنیت اینترنت، انتقال پول الکترونیکی و غیره) می‌باشند.

دنبالهٔ اعداد اول با

$$۲, ۳, ۵, ۷, ۱۱, ۱۳, ۱۷, ۱۹, ۲۳, ۲۹, ۳۱, ۳۷, \ldots$$

آغاز می‌شود و به روشی به ظاهر اتفاقی ادامه می‌یابد. الگوی بسیار کوچکی در این دنباله وجود دارد که حتی نمی‌توان به وضوح دید که این الگو همواره ادامه پیدا می‌کند یا نه. اما اقلیدس (در حدود ۳۰۰ سال قبل از میلاد) اساساً به شکل زیر اثبات کرد که تعدادی نامتناهی عدد اول وجود دارد.

نامتناهی بودن اعداد اول. برای هر تعداد عدد اول داده شده مانند $p_۱$، $p_۲$، $p_۳$، ...، p_k همواره می‌توانیم عدد اول دیگری مانند p بیابیم.

---

[۶] natural numbers

[۷] divides

[۸] prime

برهان. عدد

$$N = p_1 p_2 p_3 \cdots p_k + 1$$

را تشکیل می‌دهیم. در این صورت هیچ یک از اعداد اول داده شدهٔ p_1، p_2، p_3، …، p_k عدد N را عاد نمی‌کند زیرا تقسیم N بر هر یک از این اعداد دارای باقیماندهٔ ۱ است. از طرف دیگر عددی اول مانند p عدد N را عاد می‌کند. زیرا اگر خود N اول باشد می‌توانیم قرار دهیم $p = N$ و در غیر این صورت برای اعداد کوچک‌تری مانند a و b داریم $N = ab$. به طور مشابه، اگر a یا b اول باشند p را برابر همان عدد قرار می‌دهیم و اگر چنین نباشد a و b را به عوامل کوچک‌تر می‌شکنیم و به همین ترتیب[9]. نهایتاً باید به عددی اول مانند p که N را عاد می‌کند برسیم زیرا اعداد طبیعی نمی‌توانند تا ابد اکیداً کاهش یابند[10]. □

تمرینها

نه تنها دنبالهٔ اعداد اول الگوی واضحی ندارد، بلکه حتی فرمول ساده‌ای که فقط عدد اول تولید کند نیز وجود ندارد. با این حال برخی کم‌خطاهای جالب وجود دارند.

۱.۱.۱ بررسی کنید که تابع درجهٔ دوم $n^2 + n + 41$ برای همهٔ مقادیر کوچک n (مثلاً برای n های کوچک‌تر از ۳۰) اول است.

۲.۱.۱ علی رغم این نشان دهید که $n^2 + n + 41$ برای مقادیر مشخصی از n اول نیست.

---

[9] شاید بهتر باشد از یک استقرای ساده برای اثبات این امر استفاده کنیم. اما استقراء موضوعی است که در بخش بعد بدان می‌پردازیم. (م)

[10] این مطلب به اصل نزول نامتناهی فرما موسوم است. به بیان دقیق‌تر این اصل، که از صورتهای معادل اصل استقراء است، بیان می‌کند که هیچ دنبالهٔ اکیداً نزولی از اعداد طبیعی وجود ندارد. (م)

۳.۱.۱ کوچک‌ترین n ممکن چند است؟

۲.۱ استقراء

روشی که هم اکنون برای یافتن مقسوم‌علیه‌های اول N به کار رفت معمولاً نزول[۱۱] نامیده می‌شود و نمونه‌ای از روشی کلی است که استقراء نام دارد.

سبک نزول از استدلال استقرایی متکی بر این حقیقت است که هر فرآیند تولید اعداد طبیعیِ کوچک‌تر و کوچک‌تر باید سرانجام متوقف گردد. فرآیند کاستن مکرر ۱ از هر عدد طبیعی مانند n در تعدادی متناهی گام به پایان می‌رسد. از این رو فقط تعدادی متناهی گام رو به عقب با شروع از n وجود دارد. همچنین سبک صعود[۱۲] از استقراء نیز وجود دارد که از فرآیند ساختن خود اعداد طبیعی (با شروع از ۱ و افزودن تکراری ۱) پیروی می‌کند.

یک برهان استقرایی صعودی در دو گام به انجام می‌رسد: گام پایه (شروع) و گام استقراء (رفتن از n به $n+۱$). در اینجا این کار را برای یک مثال انجام می‌دهیم. اثبات می‌کنیم که هر عدد به صورت $k^۳+۲k$ توسط ۳ عاد می‌شود.

گام پایه. ادعا برای $k=۱$ درست است چون $۳ = ۱ \times ۲ + ۱^۳$ که مسلماً توسط ۳ عاد می‌شود.

گام استقراء. فرض کنیم که ادعا برای $k=n$ درست باشد یعنی ۳ عدد $n^۳+۲n$ را عاد کند. می‌خواهیم نتیجه بگیریم که برای $k=n+۱$ نیز این ادعا درست است یعنی ۳ عدد $(n+۱)^۳+۲(n+۱)$ را نیز عاد می‌کند. داریم

$$\begin{aligned} &(n+۱)^۳+۲(n+۱) \\ &= n^۳+۳n^۲+۳n+۱+۲n+۲ \\ &= n^۳+۲n+۳n^۲+۳n+۳ \end{aligned}$$

---

۱۱ descent

۱۲ ascent

$$= (n^3 + 2n) + 3(n^2 + n + 1)$$

و سمت راست، مجموع $n^3 + 2n$ (که بنابر فرض مضرب ۳ است) با $3(n^2 + n + 1)$ می‌باشد که به طور بدیهی مضرب ۳ است. بنابراین همان طور که انتظار داشتیم $(n+1)^3 + 2(n+1)$ توسط ۳ عاد می‌شود. □

استقراء نه تنها برای اثبات قضایای مربوط به $\mathbb{N}$ بلکه برای تعریف توابع مقدماتی روی $\mathbb{N}$ نیز اساسی است. فقط لازم است که یک تابع یعنی تابع تالی[13] $s(n) = n + 1$ را در نظر بگیریم؛ پس از آن می‌توان + و × را به استقراء تعریف کرد. در این کتاب سعی نداریم که هر چیزی را از پایه بنا بنهیم. لذا تعریف + و × و خواص اساسی آنها را فرض می‌گیریم اما اشاره‌ای به تعریف استقرایی آنها به دلیل ساده بودنشان ارزشمند است.

برای هر عدد طبیعی مانند m عدد $m + 1$ را توسط

$$m + 1 = s(m)$$

تعریف می‌کنیم. سپس با داشتن تعریف $m + n$، برای هر عدد m عدد $m + s(n)$ را به صورت

$$m + s(n) = s(m + n)$$

تعریف می‌کنیم. در این صورت به استقراء روی n نتیجه می‌شود که $m + n$ برای هر دو عدد طبیعی m و n تعریف شده است. تعریف $m \times n$ به طور مشابه بر مبنای تابع تالی و تابع + (که هم اکنون تعریف شد) می‌باشد:

$$\begin{aligned} m \times 1 &= m \\ m \times s(n) &= m \times n + m. \end{aligned}$$

از این تعاریف استقرایی می‌توان برهانهای استقرایی خواص اساسی + و ×، از جمله $m + n = n + m$ و $\ell(m + n) = \ell m + \ell n$ را به دست داد. چنین برهانهایی در ابتدا توسط گراسمان[14] (۱۸۶۱) (در کتابی برای دانش‌آموزان

---

[13] successor function

[14] Grassmaan

دبیرستانی!) ارائه گردید اما مورد اقبال واقع نشد. این مطلب همراه با آنالیزی از خود تابع تالی توسط ددکیند[۱۵] (۱۸۸۸) مجدداً کشف شد. برای اطلاعاتی در این زمینه استیلول[۱۶] (۱۹۹۸) فصل ۱ را ببینید.

تمرینها

فرآیند جالبی از نزول را می‌توان در الگوریتمی موسوم به کسرهای مصری[۱۷] که توسط فیبوناچی[۱۸] (۱۲۰۲) معرفی گردید مشاهده کرد. هدف این الگوریتم نشان دادن هر کسر مانند $\frac{a}{b}$ (که $0 < b < a$) به صورت مجموعی از جملات متمایز به صورت $\frac{1}{n}$ که کسرهای یکه[۱۹] نامیده می‌شوند می‌باشد. (مصریان قدیم کسرها را به این روش نمایش می‌دادند.)

الگوریتم فیبوناچی در نگاهی اجمالی کم کردن تکراریِ بزرگ‌ترین کسر یکهٔ ممکن می‌باشد. مثلاً با به کار بردن این الگوریتم روی کسر $\frac{11}{12}$،

کم کردن بزرگ‌ترین کسر یکهٔ کوچک‌تر از $\frac{11}{12}$ یعنی $\frac{1}{2}$، $\frac{11}{12} - \frac{1}{2} = \frac{5}{12}$

کم کردن بزرگ‌ترین کسر یکهٔ کوچک‌تر از $\frac{5}{12}$ یعنی $\frac{1}{3}$، $\frac{5}{12} - \frac{1}{3} = \frac{1}{12}$

را به دست می‌آوریم. از این رو $\frac{11}{12} = \frac{1}{2} + \frac{1}{3} + \frac{1}{12}$.

کسرهای تولید شده توسط کم کردن متوالی، همواره دنباله‌ای نزولی از صورت کسرها (در مثال ما دنبالهٔ ۱۱، ۵، ۱) را به دست می‌دهد. از این رو لزوماً به عدد ۱ ختم خواهد شد.

۱.۲.۱ از الگوریتم فیبوناچی برای یافتن نمایش مصری کسر $\frac{9}{11}$ استفاده کنید.

---

[۱۵] Dedekind
[۱۶] Stillwell
[۱۷] Egyptian fractions
[۱۸] Fibonacci
[۱۹] unit fractions

۲.۲.۱ اگر a، b و q اعدادی طبیعی با شرط $\frac{1}{q+1} < \frac{b}{a} < \frac{1}{q}$ باشند، نشان دهید که
$$\frac{b}{a} - \frac{1}{q+1} = \frac{b'}{a(q+1)},$$
که در آن $0 < b' < b$. بدین ترتیب نتیجه بگیرید که الگوریتم فیبوناچی همواره درست کار می‌کند.

۳.۱ اعداد صحیح

بنا به دلایل متعدد، متداول است که مجموعهٔ $\mathbb{N}$ از اعداد طبیعی را به گروه[۲۰] $\mathbb{Z}$ از اعداد صحیح[۲۱] با افزودن عنصر همانی[۲۲] ۰ و قرینهٔ[۲۳] $-n$ برای هر عدد طبیعی مانند n توسیع دهیم. یک دلیل برای این کار این است که مطمئن شویم تفاضل $m - n$ متشکل از هر دو عدد صحیح معنی دارد. لذا $\mathbb{Z}$ مجموعه‌ای است که روی آن سه عمل $+$، $-$ و $\times$ تعریف شده است. (نماد $\mathbb{Z}$ از کلمهٔ آلمانی Zahlen به معنای اعداد آمده است.)

$\mathbb{Z}$ گروهی آبلی[۲۴] تحت عمل $+$ است زیرا سه خاصیت گروه را دارد:

شرکت پذیری[۲۵]: $a + (b + c) = (a + b) + c$.

وجود عضو همانی: $a + 0 = a$.

وجود معکوس برای هر عضو: $a + (-a) = 0$.

و نیز خاصیت آبلی بودن: $a + b = b + a$.

$\mathbb{Z}$ قدیمی‌تر از مفهوم گروه آبلی است. این مفهوم تنها پس از ظهور مثالهای دیگر، مخصوصاً گروههای آبلی متناهی، توانست متصور گردد. با برخی از این

[۲۰] group
[۲۱] integer numbers
[۲۲] identity
[۲۳] inverse
[۲۴] Abelian group
[۲۵] associativity

مثالها در فصل ۳ برخورد خواهیم کرد.

$\mathbb{Z}$ تحت اعمال + و × یک حلقه[۲۶] است: تحت عمل + یک گروه آبلی است و عمل × به عمل + توسط خاصیت زیر مرتبط می‌گردد:

توزیع پذیری[۲۷]: $a(b+c) = ab + ac$.

مفهوم حلقه نیز خیلی دیرتر از $\mathbb{Z}$ پدیدار شد. این مفهوم در پی تلاشهایی در قرن هجدهم و نوزدهم برای تعمیم مفهوم اعداد صحیح رشد کرد. یکی از این تعمیمها را در بخش ۸.۱ خواهیم دید و مفهوم کلی حلقه را در فصل ۱۰ مورد توجه قرار خواهیم داد.

خواص حلقه نشان می‌دهد که $\mathbb{Z}$ ساختاری بیشتر از $\mathbb{N}$ دارد، گرچه باید قانع شویم که این مطلب هیچ چیزی را ساده‌تر نمی‌کند. حضور اعداد صحیح منفی یعنی ۱−، ۲−، ۳−، ... در $\mathbb{Z}$ مفهوم اعداد اول را اندکی پیچیده‌تر می‌کند. چون هر عدد صحیح مانند n توسط ۱، ۱−، n و $-n$ عاد می‌شود باید عدد اول را در $\mathbb{Z}$ به عنوان عددی صحیح مانند p که فقط توسط ۱ ± (موسوم به یکه‌های[۲۸] $\mathbb{Z}$) و $\pm p$ عاد می‌شود تعریف کنیم.

اما در حالت کلی کار کردن با اعداد صحیح در مقایسه با اعداد طبیعی آسان‌تر است. برای روشن شدن این تفاوت مسأله‌ای را مورد بررسی قرار می‌دهیم.

مسأله. اعداد به صورت $۴m + ۷n$ را توصیف کنید

۱. که در آن m و n اعدادی طبیعی هستند،

۲. که در آن m و n اعدادی صحیح هستند.

در حالت اول این اعداد عبارتند از **۱۱، ۱۵، ۱۸، ۱۹، ۲۲، ۲۳، ۲۵، ۲۶، ۲۷** و همهٔ اعداد بزرگ‌تر یا مساوی **۲۹**. اعداد کوچک‌تر از **۲۹** را می‌توان با آزمایش تحقیق کرد (می‌پذیریم که طاقت‌فرساست). برای آن که ببینیم همهٔ اعداد بزرگ‌تر یا مساوی **۲۹** به صورت $۴m + ۷n$ هستند در ابتدا این مطلب را

---

[۲۶] ring
[۲۷] distributivity
[۲۸] units

برای ۲۹، ۳۰، ۳۱ و ۳۲ تحقیق می‌کنیم؛ یعنی

$$۲۹ = ۲ \times ۴ + ۳ \times ۷$$
$$۳۰ = ۴ \times ۴ + ۲ \times ۷$$
$$۳۱ = ٦ \times ۴ + ۱ \times ۷$$
$$۳۲ = ۱ \times ۴ + ۴ \times ۷.$$

سپس می‌توانیم چهار عدد طبیعی بعدی را با افزودن یک ۴ به هر یک از اینها و چهار عدد بعدی را با افزودن دو ۴، و به همین ترتیب، به دست آوریم (این در حقیقت برهانی استقرایی است).

در حالت دوم همهٔ اعداد صحیح به دست می‌آید. اثبات این امر بسیار آسان است. چون $۷ - ۴ \times ۲ = ۱$، در نتیجه $n = ۲n \times ۴ - ۷n$ برای هر عدد صحیح مانند n.

این نوع مسأله به کمک ب.م.م. (بزرگ‌ترین مقسوم علیه مشترک[۲۹]) یا gcd که در فصل بعد مطالعه می‌کنیم آسان‌تر درک می‌شود. اما در ابتدا لازم است از نزدیک‌تر به تقسیم، بالاخص تقسیم با باقیمانده که موضوع بخش بعد است، نظری بیفکنیم.

تمرینها

یک مسألهٔ عینی، مشابه توصیف $۴m + ۷n$، مسألهٔ خرید کردن است: فرض کنیم می‌توانیم با کمیتهای ٦، ۹ یا ۲۰ خرید کنیم. چه مقادیری را می‌توان خرید؟ این مسأله توصیف اعداد به صورت $٦i + ۹j + ۲۰k$ برای اعداد طبیعی یا صفر i، j و k است[۳۰].

---

[۲۹] greatest common divisor

[۳۰] البته ظاهراً فرض بر آن است که می‌خواهیم فقط با پرداخت کردن این کمیتها، مقداری خرید کنیم. اگر قرار باشد که هم پرداخت کنیم و هم دریافت کنیم آنگاه با توصیف همین اعداد

در می‌یابیم که اعداد ممکن شامل همهٔ اعداد بزرگ‌تر یا مساوی ۴۴ و مجموعه‌ای نامنظم از اعداد کوچک‌تر از ۴۳ است.

۱.۳.۱ شرح دهید که چرا ۴۳ قابل حصول نیست.

۲.۳.۱ نشان دهید که چگونه هر یک از اعداد ۴۴، ۴۵، ۴۶، ۴۷، ۴۸ و ۴۹ حاصل می‌شوند.

۳.۳.۱ از تمرین ۲.۳.۱ نتیجه بگیرید که هر عدد بزرگ‌تر از ۴۳ قابل حصول است. اما اگر مقادیر ۶-، ۹- و ۲۰- مجاز باشند (مثلاً با پس گرفتن پول)، آنگاه هر عدد صحیح قابل حصول است.

۴.۳.۱ نشان دهید که در حقیقت برای اعداد صحیحی مانند m و n داریم $۱ = ۹m + ۲۰n$.

۵.۳.۱ از تمرین ۴.۳.۱ نتیجه بگیرید که هر عدد صحیح برای اعداد صحیحی مانند m و n به صورت $۹m + ۲۰n$ قابل بیان است.

۶.۳.۱ آیا هر عدد صحیح به صورت $۶m + ۹n$ قابل بیان است؟ نتایج تمرینهای ۴.۳.۱ و ۵.۳.۱ برای حالتی که دو عدد داده شده دارای مقسوم‌علیه مشترک باشند چگونه باید بیان شود؟

۴.۱ تقسیم با باقیمانده

همان طور که در بخش ۱.۱ متذکر شدیم، می‌گوییم یک عدد طبیعی مانند b عدد n را عاد می‌کند هرگاه برای عددی طبیعی مانند c داشته باشیم $n = bc$. نیز می‌گوییم که b مقسوم‌علیهی[۳۱] از n است و n مضربی[۳۲] از b. همین تعاریف در هر حالتی که مفهومی از ضرب در میان باشد (مانند $\mathbb{Z}$) به کار می‌رود.

برای حالتی که i، j و k صحیح هستند مواجه می‌شویم. (م)

[۳۱] divisor

[۳۲] multiple

در $\mathbb{N}$ یا $\mathbb{Z}$ به راحتی ممکن است اتفاق بیفتد که b عدد a را عاد نکند. مثلاً ۴ عدد ۲۳ را عاد نمی‌کند. در این حالت با خارج قسمت[۳۳] q و باقیمانده[۳۴] r در تقسیم a بر b مواجه می‌شویم. خارج قسمت، بزرگ‌ترین عدد مانند q است که qb کوچک‌تر یا مساوی a باشد و باقیمانده برابر است با $a - qb$. مثلاً

$$۲۳ = ۵ \times ۴ + ۳.$$

لذا وقتی ۲۳ را بر ۴ تقسیم می‌کنیم خارج قسمت ۵ و باقیماندهٔ ۳ داریم.

باقیماندهٔ $r = a - qb$ را می‌توان با تکرار کم کردن b از a به دست آورد. این کار، اعداد طبیعی[۳۵] a، $a - b$، $a - ۲b$، ... که کاهش می‌یابند (و لذا بنابر نزول شامل کوچک‌ترین عضوی چون $r = a - qb \geq ۰$ هستند) را به دست می‌دهد. باقیماندهٔ r کوچک‌تر از b است. شکل ۱.۱ به طور بدیهی نشان می‌دهد که a بین مضارب متوالی b قرار دارد و از این رو لزوماً در فاصلهٔ کمتر از b از نزدیک‌ترین مضرب b (یعنی qb) می‌باشد.

شکل ۱.۱: تقسیم با باقیمانده

مهم. هدف اصلی تقسیم با باقیمانده یافتن باقیمانده است که به ما می‌گوید b عدد a را عاد می‌کند یا نه.

تشکیل کسر $\frac{a}{b}$ برای تعیین این که b عدد a را عاد می‌کند یا نه کمکی نخواهد کرد (و ممکن است گیج کننده باشد) چون ما را به دانستن این موضوع نزدیک نخواهد کرد. مثلاً کسر

$$\frac{۴۳۵۶۰۰۲۹}{۷۷۷۷۷}$$

[۳۳] quotient
[۳۴] remainder
[۳۵] بهتر است بگوییم صحیح ناصفر. (م)

به ما نمی‌گوید که ۷۷۷۷۷ عدد ۴۳۵۶۰۰۲۹ را عاد می‌کند یا نه. برای فهمیدن این موضوع باید بدانیم باقیمانده ۰ است یا نه. می‌توانستیم تقسیم کامل با باقیمانده را انجام دهیم:

$$۴۳۵۶۰۰۲۹ = ۵۶۰ \times ۷۷۷۷۷ + ۴۹۰۹$$

که می‌گوید باقیمانده دقیقاً برابر ۴۹۰۹ است. یا این که می‌توانستیم کسر را به طور عددی محاسبه کنیم

$$\frac{۴۳۵۶۰۰۲۹}{۷۷۷۷۷} = ۵۶۰/۰۶۳۱\ldots$$

که برای فهمیدن ۰ نبودن باقیمانده کافی است. (و می‌توانیم خارج قسمت $q = ۵۶۰$ را که در قسمت قبل از اعشار آمده است بخوانیم و بدین ترتیب دریابیم که باقیمانده برابر $۴۳۵۶۰۰۲۹ - ۵۶۰ \times ۷۷۷۷۷ = ۴۹۰۹$ است.)

تمرینها

۱.۴.۱ با استفاده از ماشین حساب یا رایانه روش بالا را به کار برید تا باقیماندهٔ تقسیم ۱۲۳۴۵۶۷۸ را بر ۳۳۳۳ بیابید.

۲.۴.۱ مضارب ۳۳۳۳ در دو طرف ۱۲۳۴۵۶۷۸ را محاسبه کنید.

۵.۱ نماد دودویی

تقسیم با باقیمانده روشی طبیعی برای یافتن نمایش دودویی[۳۶] یک عدد طبیعی دلخواه مانند n است. ارقام نمایش، با تقسیم n بر ۲، نوشتن باقیمانده و

[۳۶] binary numeral

تکرار این فرآیند تا رسیدن به خارج قسمت ۰ تعیین می‌گردند. سپس دنبالهٔ باقیمانده‌ها، که به ترتیب عکس نوشته شود، همان نمایش دودویی است.

مثال. نمایش دودویی برای ۲۰۰۱.

$$\begin{aligned}
۲۰۰۱ &= ۱۰۰۰ \times ۲ + ۱\\
۱۰۰۰ &= ۵۰۰ \times ۲ + ۰\\
۵۰۰ &= ۲۵۰ \times ۲ + ۰\\
۲۵۰ &= ۱۲۵ \times ۲ + ۰\\
۱۲۵ &= ۶۲ \times ۲ + ۱\\
۶۲ &= ۳۱ \times ۲ + ۰\\
۳۱ &= ۱۵ \times ۲ + ۱\\
۱۵ &= ۷ \times ۲ + ۱\\
۷ &= ۳ \times ۲ + ۱\\
۳ &= ۱ \times ۲ + ۱\\
۱ &= ۰ \times ۲ + ۱.
\end{aligned}$$

از این رو نمایش دودویی برای ۲۰۰۱ عبارت است از ۱۱۱۱۱۰۱۰۰۰۱.

یک نمایش دودویی کلی مانند $a_k a_{k-۱} \cdots a_۱ a_۰$ که در آن هر a_i برابر ۰ یا ۱ است به جای عدد

$$n = a_k ۲^k + a_{k-۱} ۲^{k-۱} + \cdots + a_۱ ۲ + a_۰$$

می‌نشیند، چون تکرار تقسیم این عدد بر ۲ باقیمانده‌های متوالی $a_۰$، $a_۱$، ...، $a_{k-۱}$، a_k را به دست می‌دهد. لذا می‌توان n را از ارقام دودویی آن با ضرب کردن آنها در توانهای مناسب ۲ و جمع نمودن، مجدداً ساخت.

با این حال کارآیی بیشتری دارد که $a_k a_{k-۱} \cdots a_۱ a_۰$ را به صورت کدی برای ساختن n از عدد ۰ با دنباله‌ای از مضاعف کردنها (ضرب کردن در ۲) و افزودن ۱، یعنی عکس همان دنباله از اعمال که به وسیلهٔ آن نمایش دودویی از روی n محاسبه شد، تلقی کنیم. با حرکت از چپ به راست مضاعف می‌کنیم و مقدار a_i را (اگر صفر نباشد) به حاصل می‌افزاییم.

شکل ۲.۱ روشی برای محاسبهٔ ۲۰۰۱ که آن را از روی نمایش دودویی ۱۱۱۱۱۰۱۰۰۰۱ بازسازی کند نشان می‌دهد.

1	1	1	1	1	0	1	0	0	0	1		
+1											=	1
×2											=	2
	+1										=	3
	×2										=	6
		+1									=	7
		×2									=	14
			+1								=	15
			×2								=	30
				+1							=	31
				×2							=	62
					+0						=	62
					×2						=	124
						+1					=	125
						×2					=	250
							+0				=	250
							×2				=	500
								+0			=	500
								×2			=	1000
									+0		=	1000
									×2		=	2000
										+1	=	2001

شکل ۲.۱: بازسازی یک عدد از روی نمایش دودویی آن

تعداد اعمال

تعداد مضاعف کردنها در این فرآیند، یکی کمتر از تعداد ارقام نمایش دودویی برای n است و از این رو یکی کمتر از $\log_{۲} n$ می‌باشد، چون بزرگ‌ترین عدد k رقمی (که نمایش دودویی آن شامل k تا ۱ می‌باشد) برابر $۲^k - ۱$ است و لذا لگاریتم آن در پایهٔ ۲ کوچک‌تر از $k = \log_{۲}(۲^k)$ می‌باشد.

به طور مشابه، تعداد جمع کردنها کمتر از $\log_{۲} n$ می‌باشد. لذا تعداد کل اعمال، اعم از مضاعف کردن یا افزودن ۱، که برای تولید n لازم است کمتر از $۲ \log_{۲} n$ است.

این مشاهده روش بسیار کارآمدی برای محاسبهٔ توانها را مبتنی بر تکرار مربع کردن[۳۷] به دست می‌دهد. برای تشکیل m^n با $m = m^{۱}$ شروع می‌کنیم و به طور تکراری توان را (با مربع کردن) مضاعف می‌کنیم یا به آن ۱ می‌افزاییم (با ضرب کردن در m). می‌توانیم با مضاعف کردن یا افزودن ۱، با کمتر از $۲ \log_{۲} n$ بار عمل کردن، به توان n ام برسیم. پس می‌توانیم m^n را با مربع کردن یا ضرب کردن در m با کمتر از $۲ \log_{۲} n$ عمل تشکیل دهیم. یعنی برای تشکیل m^n کمتر از $۲ \log_{۲} n$ عمل ضرب لازم است.

لذا تعداد اعمال، متناسب با طول n (تعداد ارقام دودویی یا اعشاری آن) می‌باشد. مسائل کمی از نظریهٔ اعداد را می‌توان با چنین گام اندکی حل کرد و این پاسخ سریع برای این مسألهٔ خاص در رمزنگاری مدرن و دستگاه‌های امنیتی الکترونیکی حائز اهمیت است (فصل ۴ را ببینید).

---

[۳۷] repeated squaring

تمرینها

نماد دودویی اغلب بیشتر از انسان توسط رایانه استفاده می‌شود چون ما ۱۰ انگشت داریم و از این رو متداول است که مبنای ۱۰ را به جای مبنای ۲ استفاده کنیم. با این حال، برخی اعداد مهم به صورت دودویی راحت‌تر نوشته می‌شوند.اعداد مرسن[۳۸] (که اعداد اولی به صورت $۲^p - ۱$ برای p یی اول می‌باشند) مثالهایی از این دست هستند.

۱.۵.۱ نشان دهید که نمایش دودویی برای $۲^p - ۱$ برابر ۱۱۱...۱ (p رقم) می‌باشد. همچنین نشان دهید که اولین چهار عدد مرسن اول نمایش دودویی ۱۱، ۱۱۱، ۱۱۱۱۱ و ۱۱۱۱۱۱۱ دارند.

۲.۵.۱ اما چنین نیست که هر عدد اول مانند p یک عدد اول $۲^p - ۱$ را به دست دهد: عدد $۲^{۱۱} - ۱$ را تجزیه کنید.

۳.۵.۱ همچنین نشان دهید که $۲^n - ۱$ هرگز اول نیست اگر n اول نباشد. (راهنمایی: فرض کنید $n = pq$ و $x = ۲^p$. نشان دهید که $x - ۱$ عدد $x^q - ۱$ را عاد می‌کند.)

اعداد اول مرسن پس از مارین مرسن[۳۹] (۱۵۸۸-۱۶۴۸)، اولین کسی است که توجهی به مسألهٔ یافتن آنها داشت، این نام را به خود گرفته‌اند. این اعداد (گرچه نه تحت این نام) در قضیهٔ معروفی از اقلیدس در مورد اعداد تام[۴۰] ظاهر می‌شوند. یک عدد، تام نامیده می‌شود هرگاه برابر مجموع مقسوم‌علیه‌های سرهٔ خود (مقسوم‌علیه‌های کمتر از خود) باشد. مثلاً ٦ تام است چون مقسوم‌علیه‌های سرهٔ آن ۱، ۲ و ۳ هستند و $۱ + ۲ + ۳ = ٦$. قضیهٔ اقلیدس بیان می‌دارد که اگر $۲^p - ۱$ اول باشد آنگاه $۲^{p-۱}(۲^p - ۱)$ تام است. در فصل ۲، هنگامی که برخی نظریه‌های تقسیم‌پذیری را توسعه دادیم، در مورد

[۳۸] Mersenne primes
[۳۹] Marin Mersenne
[۴۰] perfect numbers

این قضیه بحث می‌کنیم. در حال حاضر مشاهده می‌کنیم که اعداد تام اقلیدس نیز نمایش دودویی ساده‌ای دارند.

۴.۵.۱ نشان دهید که اولین چهار عدد تام به دست آمده از اعداد اول مرسن نمایش دودویی ۱۱۰، ۱۱۱۰۰، ۱۱۱۱۱۰۰۰۰ و ۱۱۱۱۱۱۱۰۰۰۰۰۰ دارند.

۵.۵.۱ نمایش دودویی $(۲^p - ۱)۲^{p-۱}$ چیست؟

۶.۱ معادله‌های دیوفانتی

حل معادلات، هدفی سنتی در جبر است و بخشهای خاص جبر برای تجزیه و تحلیل روشهای ویژهٔ حل معادله توسیع یافته‌اند. حل به وسیلهٔ رادیکالها[۴۱] یک شاخه از این سنت است که توسط فرمول قدیمی

$$x = \frac{-b \pm \sqrt{b^۲ - ۴ac}}{۲a}$$

برای حل معادلهٔ درجهٔ دوم کلی $ax^۲ + bx + c = ۰$ و فرمولهای پیچیده‌تر (شامل ریشهٔ سوم همانند ریشهٔ دوم) برای حل معادلات درجهٔ سوم و چهارم نمایان می‌شود. این روش حل با مفاهیم میدان[۴۲] و گروه تجزیه و تحلیل می‌شوند که منجر به نظریهٔ گالوا[۴۳] می‌گردد. نتیجهٔ اصلی آن را می‌توان در کتاب مکملی بر این کتاب، یعنی استیلول (۱۹۹۴)، یافت.

شاخه‌های مهم دیگر این سنت، یافتن جواب صحیح است که هدف اصلی کتاب حاضر می‌باشد. این مبحث منجر به مفاهیم حلقه و نظریهٔ ایده‌آلها[۴۴]

---

[۴۱] solution by radicals
[۴۲] field
[۴۳] Galois Theory
[۴۴] ideal theory

می‌گردد. معادله‌هایی که جواب صحیح آنها مورد توجه باشد دیوفانتی[۴۵] نامیده می‌شوند، گرچه واقعاً این معادله‌ها نیستند که دیوفانتی می‌باشند بلکه جوابهای آنها چنین است. علی رغم این، معادله‌های خاصی وجود دارند که دیوفانتی تلقی می‌شوند چون پاسخهای آنها مورد علاقه‌ای ویژه است.

- معادلهٔ فیثاغورسی $x^2 + y^2 = z^2$ که جوابهای طبیعی (x, y, z) برای آن به عنوان سه‌تایی‌های فیثاغورسی[۴۶] معروف هستند.
- معادلهٔ پِل[۴۷] $x^2 - ny^2 = 1$ برای عدد طبیعی نامربع دلخواهی مانند n.
- معادلهٔ باشه[۴۸] $y^3 = x^2 + n$ برای عدد طبیعی دلخواهی مانند n.
- معادلهٔ فرما[۴۹] $x^n + y^n = z^n$ برای $n > 2$.

معادلهٔ فیثاغورسی موضوع یک کتیبهٔ رُسی بابِلی است و از حدود ۱۸۰۰ قبل از میلاد با عنوان پلیمپتن ۳۲۲[۵۰] (نامش برگرفته از عدد کاتالوگ موزهٔ آن می‌باشد) با این نام شناخته می‌شده است. این معادله قدیمی‌ترین مسألهٔ شناخته شده در ریاضیات است. این لوح شامل دو ستون اعداد طبیعیِ y و z نشان داده شده در شکل ۳.۱ است.

بخش سمت چپ کتیبه، مفقود شده است اما مطمئناً ستونی از مقادیر است زیرا هر مقدار $y^2 - z^2$ مربع صحیحی مانند x^2 است و لذا این جدول، اساساً فهرستی‌از سه‌تایی‌های فیثاغورسی می‌باشد.

این بدان مفهوم است که سه‌تایی‌های فیثاغورسی مدتها قبل از خود فیثاغورس (که در حدود ۵۰۰ قبل از میلاد زندگی می‌کرده است) شناخته شده بودند و بابِلیها آشکارا روش ماهرانهٔ تولید آنها را می‌دانسته‌اند. توجه کنید

[۴۵] Diophantine
[۴۶] Pythagorean triples
[۴۷] Pell equation
[۴۸] Bachet equation
[۴۹] Fermat equation
[۵۰] Plimpton 322

که پلیمپتن ۳۲۲ شامل هیچ سه‌تایی فیثاغورسی معروفی مانند (۳,۴,۵)، (۵,۱۲,۱۳) یا (۸,۱۵,۱۸) نیست اما شامل سه‌تایی‌های به دست آمده از آنها که اغلب به روشهایی غیر بدیهی حاصل می‌شوند می‌باشد.

y	z
119	169
3367	4825
4601	6649
12709	18541
65	97
319	481
2291	3541
799	1249
481	769
4961	8161
45	75
1679	2929
161	289
1771	3229
56	106

شکل ۱.۳: پلیمپتن ۳۲۲

در حدود ۳۰۰ قبل از میلاد، اقلیدس نشان داد که همهٔ جوابهای طبیعی $x^۲ + y^۲ = z^۲$ را می‌توان توسط فرمولهای

$$x = (u^۲ - v^۲)w, \qquad y = ۲uvw, \qquad z = (u^۲ + v^۲)w,$$

با فرض آن که u، v و w اعدادی طبیعی هستند، تولید کرد. (همچنین با همین فرمولها که جای x و y عوض شده باشد.)

به سادگی می‌توان بررسی کرد که این فرمولها

$$x^۲ + y^۲ = z^۲$$

را به دست می‌دهند، اما به آسانی دیده نمی‌شود که هر جواب باید به این صورت باشد. رهیافت دیگری به این مسأله، با استفاده از اعداد گویا، توسط

دیوفانتوس[۵۱] در حدود ۲۰۰ پس از میلاد یافت شد. دیوفانتوس در حل معادلات در اعداد گویا متخصص بود و لذا جوابهای وی به مفهوم ما دقیقاً دیوفانتی نیستند ولی در این حالت جوابهای گویا و صحیح اساساً معادلند.

تمرینها

۱.۶.۱ (ترجیحاً به کمک رایانه) بررسی کنید که $z^۲ - y^۲$ برای هر یک از جفتهای (y, z) مذکور در پلیمپتن ۳۲۲، مربع کامل است.

۲.۶.۱ همچنین بررسی کنید که x عددی سرراست به مفهوم بابِلی است؛ بدین معنی که توسط ۶۰ یا حداقل مقسوم‌علیهی از ۶۰ عاد می‌شود. (دستگاه عددنویسی بابِلی مبنای ۶۰ داشته است.)

۳.۶.۱ تحقیق کنید که اگر

$$x = (u^۲ - v^۲)w, \qquad y = ۲uvw, \qquad z = (u^۲ + v^۲)w,$$

آنگاه $x^۲ + y^۲ = z^۲$.

۴.۶.۱ مقادیر u و v (با شرط $w = ۱$) را بیابید که به وسیلهٔ فرمولهای اقلیدس، سه‌تایی‌های فیثاغورسی $(۳, ۴, ۵)$، $(۵, ۱۲, ۱۳)$، $(۷, ۲۴, ۲۵)$ و $(۸, ۱۵, ۱۷)$ را به دست دهند.

---

[۵۱] Diophantus

۷.۱ روش وتر دیوفانتوس

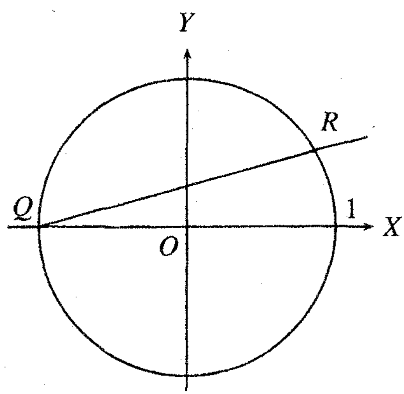
یک جواب صحیح مانند $(x, y, z) = (a, b, c)$ برای $x^۲ + y^۲ = z^۲$ ایجاب می‌کند که

$$(\frac{a}{c})^۲ + (\frac{b}{c})^۲ = ۱.$$

لذا $X = \frac{a}{c}$ و $Y = \frac{b}{c}$ یک جواب گویا برای معادلهٔ

$$X^۲ + Y^۲ = ۱$$

است؛ به بیان دیگر، یک نقطهٔ گویا روی دایرهٔ واحد. (توافقاً، هر مضرب این سه‌تایی مانند (ma, mb, mc) متناظر با همان نقطه است اما همین که a، b و c را به وسیلهٔ X و Y به دست آوردیم به سادگی می‌توانیم مضرب را درج کنیم.)



شکل ۴.۱: روش وتر برای نقاط گویا

دیوفانتوس نقاط گویا روی $X^۲ + Y^۲ = ۱$ را به روشی جبری یافت که تعبیر هندسی آن در شکل ۴.۱ نشان داده شده است.

اگر وتر واصل بین نقطهٔ گویای دلخواهی مانند R و نقطهٔ $Q = (-۱, ۰)$ را رسم کنیم، خطی با شیب گویا به دست می‌آید چون مختصات R و Q گویا هستند. اگر این شیب را t بنامیم آنگاه معادلهٔ این خط عبارت است از

$$Y = t(X + ۱).$$

بالعکس هر خط از این نوع، با شیب گویای t، دایره را در نقطه‌ای گویا چون R قطع می‌کند. این مطلب را می‌توان با محاسبهٔ مختصات R مشاهده کرد. این کار را با قرار دادن $Y = t(X + ۱)$ و $X^۲ + Y^۲ = ۱$ و رسیدن به

$$X^۲ + t^۲(X + ۱)^۲ = ۱$$

انجام می‌دهیم تا معادلهٔ درجهٔ دوم

$$X^۲(۱ + t^۲) + ۲t^۲X + t^۲ - ۱ = ۰$$

بر حسب X به دست آید. فرمول حل معادلهٔ درجهٔ دوم، جواب

$$X = -۱, \frac{۱ - t^۲}{۱ + t^۲}$$

را به دست می‌دهد. جواب $X = -۱$ متناظر با نقطهٔ Q است و لذا مختص X در R برابر $\frac{۱-t^۲}{۱+t^۲}$ می‌باشد. از این رو مختص Y آن نیز عبارت است از

$$Y = t(\frac{۱ - t^۲}{۱ + t^۲} + ۱) = \frac{۲t}{۱ + t^۲}.$$

خلاصه آن که: یک نقطهٔ گویای دلخواه روی دایرهٔ واحد $X^۲ + Y^۲ = ۱$ دارای مختصات

$$(\frac{۱ - t^۲}{۱ + t^۲}, \frac{۲t}{۱ + t^۲}),$$

برای t یی گویا و دلخواه، می‌باشد.

حال می‌توانیم فرمول اقلیدس را بازسازی کنیم.

یک عدد گویای دلخواه مانند t می‌تواند به صورت $t = \frac{v}{u}$، که $u, v \in \mathbb{Z}$، نوشته شود. در این صورت نقطهٔ گویای R به صورت

$$(\frac{۱ - \frac{v^۲}{u^۲}}{۱ + \frac{v^۲}{u^۲}}, \frac{۲\frac{v}{u}}{۱ + \frac{v^۲}{u^۲}}) = (\frac{u^۲ - v^۲}{u^۲ + v^۲}, \frac{۲uv}{u^۲ + v^۲})$$

در می‌آید. لذا اگر این نقطه به صورت

$$(\frac{x}{z}, \frac{y}{z})$$

برای x و y و z ی در $\mathbb{Z}$ باشد آنگاه باید داشته باشیم

$$\frac{x}{z} = \frac{u^۲ - v^۲}{u^۲ + v^۲}, \qquad \frac{y}{z} = \frac{۲uv}{u^۲ + v^۲}$$

برای u و v یی در $\mathbb{Z}$.

فرمول اقلیدس برای x و y و z نیز همین فرمولها را برای $\frac{x}{z}$ و $\frac{y}{z}$ به دست می‌دهد. لذا نتیجهٔ اقلیدس و دیوفانتوس اساساً یکی است.

تفاوتی که بین جوابهای گویا و صحیح معادلهٔ $x^۲ + y^۲ = z^۲$ وجود دارد اندک است زیرا این معادله بر حسب x و y و z همگن[۵۲] می‌باشد. از این رو هر جواب گویا را می‌توان در عددی ضرب کرد تا جوابی صحیح به دست آید. این وضعیت کاملاً متفاوت با معادله‌های ناهمگن از قبیل $y^۲ = x^۳ - ۲$ است که در آن یافتن جوابهای صحیح ممکن است بسیار سخت‌تر باشد.

روش دیوفانتوس برای جوابهای گویا را می‌توان به معادله‌های مکعبی تعمیم داد که نتیجهٔ موفقیت‌آمیزی به همراه دارد؛ مثلاً سیلورمن[۵۳] و تیت[۵۴] (۱۹۹۲) را ببینید. با این حال، این روش جوابهای صحیح را، مگر در مواردی اندک که معادله همگن باشد، به دست نمی‌دهد و از این رو جدا از مسیری است که در این کتاب در پی آن هستیم. در حقیقت، اغلب این حالت پیش می‌آید که معادلهٔ مکعبی، تعدادی نامتناهی جواب گویا و فقط تعدادی متناهی جواب صحیح دارد (مثل معادله‌های باشه). از آنجایی که می‌خواهیم جوابهای صحیح را مورد مطالعه قرار دهیم ساختار وتری را کنار می‌گذاریم و در بخش بعد به روش جبری یافتن سه‌تایی‌های فیثاغورسی می‌پردازیم: استفاده از اعداد صحیح تعمیم‌یافته[۵۵].

[۵۲] homogeneous
[۵۳] Silverman
[۵۴] Tate
[۵۵] generalized integers

تمرینها

خود دیوفانتوس روش خود را به معادله‌هایی به صورت

$$y^{۲} = \quad \text{تابعی مکعبی بر حسب } x$$

که در آن همهٔ ضرایب، گویا هستند تعمیم داد. در اینجا ارتباط بین هندسه و جبر این است که خط راستی که از دو نقطهٔ گویا می‌گذرد منحنی را در نقطهٔ گویای سومی قطع می‌کند. پس وقتی فقط یک نقطهٔ گویای بدیهی روی منحنی وجود دارد، می‌توان از مماس گذرنده از این نقطه به جای وتر استفاده کرد چون وقتی مماس به صورت جبری نگریسته شود منحنی را در دو نقطه قطع می‌کند.

معادلهٔ $y^{۲} = x^{۳} - ۲$، به همان میزان که محاسبات دشواری را منجر می‌شود، نمونهٔ خوبی برای روشن ساختن روش مماس می‌باشد. (توجه کنید که این معادله یک معادلهٔ باشه است: در اینجا جای x و y را عوض کرده‌ایم تا مطابق با نماد معمولی ما برای منحنیهای مکعبی باشد.)

۱.۷.۱ نشان دهید که مماس بر $y^{۲} = x^{۳} - ۲$ در نقطهٔ گویای بدیهی $(۳, ۵)$ به صورت $y = \frac{۲۷}{۱۰}x - \frac{۳۱}{۱۰}$ است.

۲.۷.۱ با قرار دادن $y = \frac{۲۷}{۱۰}x - \frac{۳۱}{۱۰}$ در معادلهٔ منحنی نشان دهید که مماس، منحنی را هنگامی قطع می‌کند که

$$۱۰۰x^{۳} - ۷۲۹x^{۲} + ۱۶۷۴x - ۱۱۶۱ = ۰.$$

۳.۷.۱ با دو بار تقسیم کردن $۱۰۰x^{۳} - ۷۲۹x^{۲} + ۱۶۷۴x - ۱۱۶۱$ بر $x - ۳$ یا به روشی دیگر، نشان دهید که مماس، منحنی را دو بار در $x = ۳$ و یک بار در $x = \frac{۱۲۹}{۱۰۰}$ قطع می‌کند.

۴.۷.۱ بدین ترتیب نقطهٔ گویایی روی منحنی $y^۲ = x^۳ - ۲$ غیر از $(۳, \pm ۵)$ بیابید.

در حقیقت تعدادی نامتناهی نقطهٔ گویا روی منحنی $y^۲ = x^۳ - ۲$ وجود دارد (گرچه تا سال ۱۹۳۰ این مطلب را نمی‌دانستند؛ مُردل[۵۶] (۱۹٦۹) فصل ۲٦ را ببینید)، اما بعداً نشان خواهیم داد که تنها نقاط صحیح آن $(۳, \pm ۵)$ هستند.

۸.۱ اعداد صحیح گاوسی

هنگامی که از اعداد مختلط برای تجزیهٔ مجموع دو مربع استفاده کنیم معادلهٔ فیثاغورسی در پرتویی جدید ظاهر می‌گردد:

$$x^۲ + y^۲ = (x - y\mathrm{i})(x + y\mathrm{i}),$$

که در آن $\mathrm{i} = \sqrt{-۱}$. برای اعداد صحیح دادهٔ شدهٔ x و y، عوامل $x - y\mathrm{i}$ و $x + y\mathrm{i}$ را می‌توان به عنوان اعداد صحیح مختلط[۵۷] تلقی کرد. مجموعهٔ چنین اعداد صحیحی را با

$$\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} : \ a, b \in \mathbb{Z}\}$$

نمایش می‌دهیم و آن را پس از گاوس[۵۸]، اولین کسی که فهمید $\mathbb{Z}[\mathrm{i}]$ خواص مشترک زیادی با $\mathbb{Z}$ دارد، اعداد صحیح گاوسی[۵۹] می‌نامیم.

برای شروع واضح است که جمع، تفاضل و حاصل ضرب اعداد $\mathbb{Z}[\mathrm{i}]$ نیز در $\mathbb{Z}[\mathrm{i}]$ هستند. از این رو می‌توانیم آزادانه +، − و × را به کار بریم و با همان

---

[۵۶] Mordell

[۵۷] complex integers

[۵۸] Gauss

[۵۹] Gaussian integers

قواعد $\mathbb{Z}$ محاسبه کنیم. این مطلب قبل از هر چیز، نتایج زیبایی در مورد جمع مربعها و سه‌تایی‌های فیثاغورسی به دست می‌دهد.

اتحاد دو مجذور. مجموع دو مجذور ضربدر مجموع دو مجذور، خود مجموع دو مجذور است، یعنی

$$(a_1^2+b_1^2)(a_2^2+b_2^2)=(a_1a_2-b_1b_2)^2+(a_1b_2+b_1a_2)^2.$$

برهان. مجموع دو مجذور را همانند بالا تجزیه می‌کنیم. سپس مجدداً دو عاملِ با علامت منفی و دو عاملِ با علامت مثبت را در هم ضرب می‌کنیم:

$$\begin{aligned}(a_1^2+b_1^2)(a_2^2+b_2^2) &= (a_1-b_1\mathrm{i})(a_1+b_1\mathrm{i})(a_2-b_2\mathrm{i})(a_2+b_2\mathrm{i})\\ &= (a_1-b_1\mathrm{i})(a_2-b_2\mathrm{i})(a_1+b_1\mathrm{i})(a_2+b_2\mathrm{i})\\ &= [a_1a_2-b_1b_2-(a_1b_2+b_1a_2)\mathrm{i}]\\ &\quad\times[a_1a_2-b_1b_2+(a_1b_2+b_1a_2)\mathrm{i}]\\ &= (a_1a_2-b_1b_2)^2+(a_1b_2+b_1a_2)^2.\ \square\end{aligned}$$

نتیجه. اگر سه‌تایی‌های (a_1,b_1,c_1) و (a_2,b_2,c_2) فیثاغورسی باشند آنگاه سه‌تایی $(a_1a_2-b_1b_2,a_1b_2+b_1a_2,c_1c_2)$ نیز چنین است.

برهان. اگر (a_1,b_1,c_1) و (a_2,b_2,c_2) سه‌تایی‌های فیثاغورسی باشند آنگاه

$$a_1^2+b_1^2=c_1^2,\qquad a_2^2+b_2^2=c_2^2.$$

بنابراین از اتحاد دو مجذور نتیجه می‌شود که

$$\begin{aligned}(c_1c_2)^2 &= c_1^2c_2^2\\ &= (a_1^2+b_1^2)(a_2^2+b_2^2)\\ &= (a_1a_2-b_1b_2)^2+(a_1b_2+b_1a_2)^2.\end{aligned}$$

و این بیان می‌دارد که $(a_1a_2 - b_1b_2, a_1b_2 + b_1a_2, c_1c_2)$ یک سه‌تایی فیثاغورسی است. □

البته اتحاد دو مجذور را می‌توان بدون استفاده از $\sqrt{-1}$ با ضرب کردن دو طرف و مقایسهٔ نتیجه اثبات کرد و احتمالاً اولین بار به این روش کشف گردیده است چون مدتها قبل از معرفی اعداد مختلط شناخته شده بوده است. گرچه این اتحاد اولین بار صریحاً توسط الخازن[60] در حدود 950 بعد از میلاد ارائه شده است، با این حال به نظر می‌رسد که برای دیوفانتوس و شاید حتی برای بابِلیها آشنا بوده است، چون بسیاری از سه‌تایی‌هایی را که در پلیمپتن ۳۲۲ ذکر شده‌اند می‌توان از سه‌تایی‌های کوچک‌تر توسط این نتیجه‌گیری به دست آورد (تمرینها را ببینید.)

با این حال، اتحاد دو مجذور در دنیای $\mathbb{C}$، یعنی اعداد مختلط، طبیعی‌تر است زیرا یکی از خواص اساسی آن را بیان می‌دارد؛ خاصیت ضربی نرم. اگر $z = a + bi$، آنگاه تعریف می‌کنیم

$$\text{نرم}\,(z) = |a + bi|^2 = a^2 + b^2.$$

و از اتحاد دو مجذور نتیجه می‌شود که

$$\text{نرم}\,(z_1)\ \text{نرم}\,(z_2) = \text{نرم}\,(z_1z_2) \qquad (*)$$

زیرا $z_1 = a_1 + b_1i$ و $z_2 = a_2 + b_2i$ ایجاب می‌کند

$$z_1z_2 = a_1a_2 - b_1b_2 + (a_1b_2 + b_1a_2)i.$$

در جبر و آنالیز مختلط متداول‌تر است که خاصیت ضربی $(*)$ را بر حسب قدر مطلق[61] که به صورت $|z| = \sqrt{a^2 + b^2}$ تعریف می‌شود بیان کنیم، یعنی

$$|z_1|\,|z_2| = |z_1z_2| \qquad (**)$$

[60] al-Khazin
[61] absolute value

(*) و (**) به طور بدیهی معادلند اما نرم مفهومی مفیدتر در $\mathbb{Z}[\mathrm{i}]$ است چون یک عدد صحیح معمولی است و خواص مشخصی از $\mathbb{Z}[\mathrm{i}]$ را که باید از خواص $\mathbb{Z}$ نتیجه شود ممکن می‌سازد.

همچنین است برای خواص مقدماتی اعداد صحیح گاوسی. $\mathbb{Z}[\mathrm{i}]$ نیز خواص عمیق مشترکی با $\mathbb{Z}$ دارد که دربارهٔ مقسوم‌علیه‌ها و اعداد اول می‌باشد. این خواص برای $\mathbb{Z}$ در فصل بعد و برای $\mathbb{Z}[\mathrm{i}]$ در فصل ٦ اثبات خواهد شد.

با این حال می‌توانیم با این رویا که $\mathbb{Z}[\mathrm{i}]$ رموزی از معادلهٔ فیثاغورسی یعنی

$$z^2 = x^2 + y^2 = (x - y\mathrm{i})(x + y\mathrm{i})$$

را حفظ می‌کند، اندکی بیشتر به جلو سفر کنیم. اگر اعداد صحیح x و y مقسوم‌علیه مشترک اولی نداشته باشند آنگاه به نظر می‌رسد که $x - y\mathrm{i}$ و $x + y\mathrm{i}$ نیز مقسوم‌علیه اول مشترکی نخواهند داشت؛ بسته به این که اول چه مفهومی در $\mathbb{Z}[\mathrm{i}]$ داشته باشد. اگر چنین باشد آنگاه به نظر خواهد رسید که عوامل $x - y\mathrm{i}$ و $x + y\mathrm{i}$ از z^2 که مربع کامل است، خود باید مربعهایی در $\mathbb{Z}[\mathrm{i}]$ باشند. بالاخص برای u و v یی در $\mathbb{Z}$ داریم

$$x - y\mathrm{i} = (u - v\mathrm{i})^2.$$

اما در این حالت

$$x - y\mathrm{i} = u^2 - v^2 - 2uv\mathrm{i}.$$

و با مساوی قرار دادن قسمتهای حقیقی و موهومی داریم $x = u^2 - v^2$ و $y = 2uv$ و از این رو $z = u^2 + v^2$.

لذا مجدداً به فرمول اقلیدس برای سه‌تایی‌های فیثاغورسی رسیدیم! (یا به بیان دقیق‌تر، فرمول سه‌تایی فیثاغورسی اولیه[62] که از آنها همهٔ سه‌تایی‌های

---
[62] primitive

دیگر با ضرب کردن در عددی ثابت به دست می‌آید نتیجه می‌شود. سه‌تایی‌های اولیه، آنهایی هستند که x، y و z مقسوم‌علیه اول مشترکی ندارند.)

این ایده که عوامل یک مربع که مقسوم‌علیه اول مشترکی ندارند باید خود مربع باشند اساساً در $\mathbb{Z}[i]$ درست است اما برای آن که دلیل آن را ببینیم باید ابتدا بفهمیم که چرا در $\mathbb{N}$ این مطلب درست است. این موضوع در فصل بعد توضیح داده خواهد شد.

تمرینها

قاعدهٔ ما برای تولید سه‌تایی‌های فیثاغورسی جدید از روی قبلیها، نتایج جالبی به دست می‌دهد.

۱.۸.۱ سه‌تایی‌هایی فیثاغورسی را بیابید که از موارد زیر به دست می‌آیند.

- $(۴, ۳, ۵)$ و خودش،
- $(۱۲, ۵, ۱۳)$ و خودش،
- $(۱۵, ۸, ۱۷)$ و خودش.

۲.۸.۱ آیا این نتایج چیزی در مورد هر یک از درایه‌های پلیمپتن ۳۲۲ می‌گوید؟

۳.۸.۱ سعی کنید که درایه‌های دیگر پلیمپتن ۳۲۲ را توسط سه‌تایی‌های کوچک‌تر تولید کنید.

بدیهی است که می‌توانیم بی‌نهایت سه‌تایی فیثاغورسی مانند (x, y, z) تولید کنیم، اما (حتی از فرمولهای اقلیدس) روشن نیست که آیا قید قابل توجهی

روی عناصر x و y و z آن وجود دارد. مثلاً آیا امکان دارد که x و y فرد و z زوج باشد؟ به این سؤال می‌توان با در نظر گرفتن باقیمانده‌های تقسیم بر ۴ پاسخ داد.

۴.۸.۱ نشان دهید که مربع یک عدد فرد مانند $2n+1$ در تقسیم بر ۴ باقیماندهٔ ۱ دارد.

۵.۸.۱ باقیماندهٔ تقسیم یک عدد زوج بر ۴ چیست؟

۶.۸.۱ از تمرینهای ۴.۸.۱ و ۵.۸.۱ نتیجه بگیرید که مجموع دو مربع فرد هرگز مربع نیست.

۹.۱ بحث

کشف سه تایی‌های فیثاغورسی که در آن مجموع x^2+y^2 خود یک مربع است منجر به سؤالی کلی‌تر می‌شود: هنگامی که x و y در $\mathbb{Z}$ تغییر می‌کنند چه مقادیری توسط x^2+y^2 اختیار می‌شود؟ تمرینهای فوق ایجاب می‌کنند که x^2+y^2 نمی‌تواند مقداری به صورت $4n+3$ را اختیار کند (چرا؟). و مسألهٔ اصلی در توصیف مقادیر ممکن این است که همهٔ اعداد اول به صورت x^2+y^2 را بیابیم.

چنین سؤالهایی اولین بار توسط فرما در حدود سال ۱۶۴۰ هنگامی که با خواندن کارهای دیوفانتوس بارقه‌ای در ذهن وی زده شد، مورد مطالعه واقع گردید. وی قادر بود به آن سؤالها و نیز سؤالهای متناظر در مورد x^2+2y^2 و x^2+3y^2 پاسخ دهد. در قرن هجدهم این موضوع توسط اویلر[63]، لاگرانژ[64]، لژاندر[65] و گاوس به مطالعهٔ صورتهای مربعیِ[66] کلی $ax^2+bxy+cy^2$ منجر

[63] Euler
[64] Legrange
[65] Legendre
[66] quadratic forms

گردید. نقطهٔ پایانی این تحقیقات رسالات حسابی[۶۷] گاوس (۱۸۰۱) است؛ کتابی با چنان عمق و پیچیدگی که بهترین نظریه اعداد دانهای قرن نوزدهم - دیریکله[۶۸]، کومر[۶۹]، کرونکر[۷۰] و ددکیند - دریافتند مجبورند آن را به گونه‌ای بازنویسی کنند تا خوانندگان معمولی قادر به درک نتایج گاوس باشند.

دلیل آن که رسالات آن قدر پیچیده بود این است که وقتی گاوس آن را می‌نوشت جبر مجرد[۷۱] وجود نداشت. بدون مفاهیم جبری جدید، خواصِ ساختاریِ عمیقِ صورتهای مربعیِ کشف شده توسط گاوس را نمی‌توان به وضوح بیان کرد و لذا ممکن است توسط خوانندگانی که فاقد قدرت فنی گاوس هستند به راحتی کنار گذاشته شود. ایده‌های گاوس با ظرافت در هم می‌آمیزد و منجر به حقایقی می‌شود که باعث گردید کومر، کرونکر و ددکیند مفاهیم حلقه‌ها، ایده‌آلها و گروههای آبلی را معرفی کنند.

یک گام میانی در تکامل تدریجی نظریهٔ حلقه‌ها، خلق نظریهٔ جبری اعداد[۷۲] بود: نظریه‌ای که در آن اعداد جبری نظیر $\sqrt{۲}$ و i برای روشن ساختن خواص اعداد طبیعی و صحیح به کار می‌روند. در حدود ۱۷۷۰، اویلر و لاگرانژ قبلاً اعداد جبری را برای مطالعهٔ معادله‌های دیوفانتی خاصی به کار برده بودند. مثلاً اویلر به طور کامیابانه‌ای همهٔ جوابهای صحیح $y^۳ = x^۲ + ۲$ را با تجزیهٔ عبارت سمت راست به صورت $(x + \sqrt{-۲})(x - \sqrt{-۲})$ یافت. وی فرض کرد که وقتی a و b اعدادی صحیح باشند، اعداد به صورت $a + b\sqrt{-۲}$ شبیه اعداد صحیح رفتار می کنند (بخش ۱.۷ را ببینید). همین فرض ما را قادر می‌سازد که همهٔ اعداد اول به صورت $x^۲ + ۲y^۲$ را بیابیم.

چنین استدلالی توسط گاوس در رسالات رد شده بود زیرا مفهوم این که اعداد جبری شبیه اعداد صحیح رفتار می کنند چندان روشن نبود. در سال

[۶۷] Disquisitiones Arithmeticae
[۶۸] Dirichlet
[۶۹] Kummer
[۷۰] Kronecker
[۷۱] abstract algebra
[۷۲] algebraic number theory

۱۸۰۱ گاوس احتمالاً دستگاه‌هایی از اعداد جبری را که شبیه اعداد صحیح رفتار نمی‌کنند از قبل می‌شناخت. بنابراین وی مستقیماً با صورتهای مربعی و ضرایب صحیح آنها، که با مهارت محیرالعقول خود در جبر سنتی آنها را مهار ساخته بود، کار می‌کرد. با این حال گاوس (۱۸۳۲) با اثبات این که اعداد صحیح گاوسی، یعنی $\mathbb{Z}[\mathrm{i}]$، به ویژه نسبت به تجزیه به اعداد اول واقعاً شبیه اعداد صحیح معمولی، یعنی $\mathbb{Z}$، رفتار می‌کنند اولین گام خود را به سمت نظریهٔ مجرد اعداد صحیح جبری برداشت. همان طور که در فصل ٦ خواهیم دید، این روش در میان چیزهای دیگر، راهی زیبا برای رفتار کردن با صورتهای مربعی $x^۲ + y^۲$ را به دست می‌دهد.

پیروزی عظیم کومر و ددکیند، مهار کردن دستگاه‌هایی از اعداد جبری بود که شبیه $\mathbb{Z}$ رفتار نمی‌کردند. ایشان این کار را به وسیلهٔ الحاق کردن اعدادی جدید به انجام رساندند. اعداد ایده‌آلی[۷۳] کومر و رمزگشایی ددکیند برای آنها در سال ۱۸۷۱ در زمرهٔ مهیج‌ترین اکتشافات ریاضی می‌باشند. اعداد ایده‌آلی نیز به طور طبیعی به وسیلهٔ نظریهٔ صورتهای مربعی، بالاخص به وسیلهٔ صورت $x^۲ + ۵y^۲$ پدیدار شدند. بدین ترتیب، در سراسر این کتاب، صورتهای مربعی را به عنوان یک سرنخ تعقیب می‌کنیم. صورتهای مربعی نه تنها زمینهٔ تاریخی مناسبی برای اکثر مفاهیمی که به طور معمول توسط نظریهٔ حلقه‌ها پوشش داده می‌شوند می‌باشند بلکه ساده‌ترین و روشن‌ترین مثالها را نیز مهیا می‌سازند.

---
[۷۳] ideal numbers

۲

الگوریتم اقلیدسی

پیش‌نگاه

اعداد اول را می‌توان به عنوان بلوکهای ساختمانی اعداد طبیعی تلقی کرد زیرا هر عدد طبیعی حاصل ضربی از اعداد اول است. (ضمناً، این نکته توضیح می‌دهد که چرا ۱ اول تلقی نمی‌گردد چرا که با ضرب کردن ۱ هیچ چیزی جز خود ۱ ساخته نمی‌شود[1].) اما حتی اگر اعداد اول بلوکهای ساختمانی باشند، به دست آوردن آنها به طور مستقیم کار ساده‌ای نیست. هیچ روش ساده‌ای برای این که آزمایش کنیم عدد طبیعی داده شده‌ای اول است یا نه وجود ندارد و حتی نمی‌توان کوچک‌ترین مقسوم علیه اول یک عدد داده شده را در حالت کلی به سادگی پیدا کرد.

به جای مطالعهٔ مقسوم‌علیه‌های یک عدد، بهتر است مقسوم‌علیه‌های مشترک جفت عدد a و b را مورد مطالعه قرار دهیم. الگوریتم قدیمی اقلیدسی به صورتی قابل توجه روشی کارآمد برای یافتن بزرگ‌ترین مقسوم علیه مشترک

[1] البته بهتر است گفته شود که هر عدد طبیعی غیر از ۱ حاصل ضرب منحصر به فردی از اعداد اول است. بنابراین اگر ۱ را اول تلقی می‌کردیم منحصر به فرد بودن تجزیه به اعداد اول را از دست می‌دادیم. (م)

(ب.م.م. یا gcd) اعداد طبیعی داده شدهٔ a و b است و پرتویی غیر منتظره بر اعداد اول و تجزیه به اعداد اول می‌افکند.

این الگوریتم با نمایش $\gcd(a,b)$ به عنوان ترکیبی خطی مانند $ma+nb$ که در آن m و n صحیح هستند، این تأثیر شگرف را دارد و نیز به درکی روشن از مسألهٔ حل معادله‌های خطی در اعداد صحیح منجر می‌شود.

۱.۲ ب.م.م. به وسیلهٔ کم کردن

اگر اعداد طبیعی a و b دارای مقسوم‌علیه مشترک d باشند آنگاه برای a' و b' ی طبیعی داریم

$$a = a'd, \qquad b = b'd.$$

از این مطلب نتیجه می‌شود که d عدد $a-b$ را عاد می‌کند چون

$$a - b = a'd - b'd = (a' - b')d.$$

به بیان دیگر هر مقسوم علیه مشترک a و b مقسوم‌علیهی از $a-b$ می‌باشد.

اقلیدس این حقیقت را برای یافتن بزرگ‌ترین مقسوم‌علیه مشترک a و b، یعنی $\gcd(a,b)$ با کم کردن تکراری عدد کوچک‌تر از عدد بزرگ‌تر به کار برد. به بیان دقیق، الگوریتم وی چنین پیش می‌رود.

فرض کنیم $a > b$ و نیز

$$a_1 = a, \qquad b_1 = b.$$

در این صورتِ برای هر زوج (a_i, b_i) زوج (a_{i+1}, b_{i+1}) را به صورت

$$a_{i+1} = \max(b_i, a_i - b_i), \qquad b_{i+1} = \min(b_i, a_i - b_i)$$

تشکیل می‌دهیم. چون این فرآیند، اعداد طبیعی کوچک‌تر و کوچک‌تر تولید می‌کند، باید (بنابر نزول) متوقف شود. نهایتاً داریم

$$a_k = b_k$$

که در این حالت نتیجه می‌گیریم که $\gcd(a, b) = a_k = b_k$.

دلیل آن که این الگوریتم کار می‌کند این است که

$$\gcd(a_۱, b_۱) = \gcd(a_۲, b_۲) = \ldots = \gcd(a_k, b_k).$$

چون هر مقسوم‌علیه مشترک زوج $(a_۱, b_۱)$ مقسوم علیهی از زوجهای $(a_۲, b_۲)$، $(a_۳, b_۳)$، ...، (a_k, b_k) (که توسط کم کردنهای متوالی تولید شده‌اند) نیز می‌باشد.

مثال. $a = ۳۴$، $b = ۱۹$.

الگوریتم، زوجهای زیر را می‌دهد:

$$\begin{aligned}
(a_۱, b_۱) &= (۳۴, ۱۹) \\
(a_۲, b_۲) &= (۱۹, ۳۴ - ۱۹) = (۱۹, ۱۵) \\
(a_۳, b_۳) &= (۱۵, ۱۹ - ۱۵) = (۱۵, ۴) \\
(a_۴, b_۴) &= (۱۵ - ۴, ۴) = (۱۱, ۴) \\
(a_۵, b_۵) &= (۱۱ - ۴, ۴) = (۷, ۴) \\
(a_۶, b_۶) &= (۴, ۷ - ۴) = (۴, ۳) \\
(a_۷, b_۷) &= (۳, ۴ - ۳) = (۳, ۱) \\
(a_۸, b_۸) &= (۳ - ۱, ۱) = (۲, ۱) \\
(a_۹, b_۹) &= (۲ - ۱, ۱) = (۱, ۱)
\end{aligned}$$

و در نتیجه $\gcd(۳۴, ۱۹) = \gcd(۱, ۱) = ۱$.

جفت عدد صحیح a و b که $\gcd(a,b) = ۱$ نسبت به هم اول[۲] نامیده می‌شوند. لذا الگوریتم اقلیدسی وسیلهٔ ساده‌ای برای تصمیم‌گیری در مورد نسبت به هم اول بودن دو عدد صحیح به دست می‌دهد. در بخش بعد می‌بینیم که این الگوریتم (در یک شکل اندکی تعمیم یافته) بسیار کارآمد است: $\gcd(a,b)$ را در تعداد گامی متناسب با تعداد کل ارقام a و b ارائه می‌دهد. تشخیص این که یک عدد صحیح مانند n اول است سخت‌تر می‌باشد: روشی که در ابتدا به ذهن می‌رسد مستلزم تعداد گامی متناسب با اندازهٔ n است که به طور نمایی بزرگ می‌باشد (در حدود ۲^k که k تعداد ارقام دودویی n است).

تمرینها

شروع از یک زوج عدد طبیعی و حرکت در الگوریتم کم کردن در جهت عکس (یعنی افزودن تکراری دو عددی که آخر تولید شده‌اند) چیزی به دست می‌دهد که دنبالهٔ لوکا[۳] نامیده می‌شود. معروف‌ترین آنها دنبالهٔ فیبوناچی یعنی ۱، ۱، ۲، ۳، ۵، ۸، ۱۳، ... می‌باشد که با شروع از $(۱, ۱)$ به دست می‌آید.

۱.۱.۲ توضیح دهید که چرا ب.م.م. هر دو جملهٔ متوالی در دنبالهٔ فیبوناچی برابر ۱ است.

۲.۱.۲ دنبالهٔ لوکا را که با ۱، ۳، ۴، ۷، ۱۱، ۱۸، ۲۹، ... شروع می‌شود در نظر بگیرید. ب.م.م. هر دو جملهٔ متوالی چند است؟

بررسی این که عددی صحیح مانند n اول است یا نه می‌تواند به طور نمایی سخت باشد. این مطلب در روش معروف آزمون تقسیم بر کوچک‌تر یا مساوی $\sqrt{n}$ مشهود است.

---
[۲] relatively prime
[۳] Lucas sequence

۳.۱.۲ اگر n در نمایش دودویی دارای k رقم باشد، آنگاه نشان دهید که حداکثر $2^{\frac{k}{2}}$ عدد کوچک‌تر یا مساوی $\sqrt{n}$ وجود دارد. آیا امکان دارد که دقیقاً $2^{\frac{k}{2}}$ عدد موجود باشد؟

این حقیقت اساسی در مورد مقسوم‌علیه‌های مشترک، یعنی این که اگر d اعداد a و b را عاد کند آنگاه $a \pm b$ را نیز عاد خواهد کرد، پرتویی بر سه‌تایی‌های فیثاغورسی اولیه می‌افکند.

۴.۱.۲ اگر $x = 2uv$، $y = u^2 - v^2$ و $z = u^2 + v^2$، آنگاه نشان دهید که (x, y, z) یک سه‌تایی فیثاغورسی اولیه است فقط و فقط وقتی که $\gcd(u, v) = 1$.

۲.۲ ب.م.م. به وسیله تقسیم با باقیمانده

شکل اقلیدسی الگوریتم اقلیدس معمولاً توسط تقسیم با باقیمانده، به جای کم کردن تکراری، سرعت می‌گیرد. برای زوج (a_i, b_i) داده شده با شرط $a_i > b_i$، زوج بعدی توسط قاعدهٔ

$$a_{i+1} = b_i, \qquad b_{i+1} = b_i \text{ باقیمانده تقسیم } a_i \text{ بر }$$

تولید می‌شود. این روش هنگامی که a_i بسیار بزرگ‌تر از b_i باشد کارآمدتر است که در این حالت بسیاری از کم کردنها توسط فقط یک تقسیم کردن جایگزین می‌گردد. اما الگوریتم، اساساً همان است - تقسیم کردن صرفاً نوعی کم کردن تکراری است - لذا همچنان این مطلب درست است که

$$\gcd(a_1, b_1) = \gcd(a_2, b_2) = \dots$$

تنها تفاوت این است که اکنون، توقف هنگامی اتفاق می‌افتد که b_k عدد a_k را عاد کند، که در این حالت نتیجه می‌گیریم که $\gcd(a, b) = \gcd(a_k, b_k) = b_k$.

مثال. مجدداً $a = ۳۴$، $b = ۱۹$.

الگوریتم با تقسیم، زوجهای زیر را می‌دهد:

$$\begin{aligned}
(a_۱, b_۱) &= (۳۴, ۱۹) \\
(a_۲, b_۲) &= (۱۹, ۳۴ - ۱۹) = (۱۹, ۱۵) \\
(a_۳, b_۳) &= (۱۵, ۱۹ - ۱۵) = (۱۵, ۴) \\
(a_۴, b_۴) &= (۴, ۱۵ - ۳ \times ۴) = (۴, ۳) \\
(a_۵, b_۵) &= (۳, ۴ - ۳) = (۳, ۱).
\end{aligned}$$

از این رو $\gcd(۳۴, ۱۹) = ۱$ چون ۱ عدد ۳ را عاد می‌کند.

در این شکل الگوریتم، به سادگی دیده می‌شود که تعداد تقسیم کردنها قابل مقایسه با تعداد کل ارقام a و b است. در حقیقت، اگر a و b به صورت دودویی نوشته شوند آنگاه هر عمل تقسیم، تعداد کل ارقام را یکی کاهش می‌دهد. اگر تعداد ارقام a بیشتر از b باشد این مطلب واضح است: زوج جدید عبارت است از b همراه با باقیماندهٔ تقسیم بر b که تعداد ارقام آن از b بیشتر نیست. اگر a و b تعداد ارقام یکسانی داشته باشند آنگاه چون a و b لزوماً با رقم ۱ شروع می‌شوند، به سادگی دیده می‌شود که باقیمانده برابر $a - b$ است که تعداد ارقام کمتری نسبت به b دارد.

شکل تقسیم کردنی الگوریتم اقلیدس نه تنها کارآمدتر است بلکه قابلیت کاربرد وسیع‌تری نیز دارد. مثلاً در $\mathbb{Z}[\mathrm{i}]$ می‌توانیم ۱۷ را بر $۴+\mathrm{i}$ (دقیقاً) تقسیم کنیم و خارج قسمت $۴-\mathrm{i}$ داشته باشیم، اما کم کردن $۴+\mathrm{i}$ از ۱۷ به تعداد $۴-\mathrm{i}$ مرتبه، بی‌معنی است. هر نوعی از الگوریتم اقلیدسی در $\mathbb{Z}[\mathrm{i}]$ (که یکی از آنها را در بخش ۴.۶ می‌بینیم) لزوماً از تقسیم با باقیمانده استفاده می‌کند.

تمرینها

شکل تقسیم کردنی الگوریتم اقلیدس در مورد (a,b) با شرط $a>b$ هنگامی اتفاق می‌افتد که بخواهند چیزی را که کسر مسلسل[۴] نامیده می‌شود بیابند. ایدهٔ این کار این است که اگر $a=bq+r$، که در آن $۰ \leq r < b$، آنگاه

$$\frac{a}{b}=\frac{bq+r}{b}=q+\frac{r}{b}=q+\frac{۱}{\frac{b}{r}},$$

و سپس این فرآیند را می‌توان برای کسر $\frac{b}{r}$ تکرار کرد چون بنابر ساختار ما $b>r$. اما زوج (b,r) کوچک‌تر از زوج اولیهٔ (a,b) است[۵] و لذا این فرآیند خاتمه می‌یابد. نتیجهٔ این کار، کسر مسلسل برای $\frac{a}{b}$ نامیده می‌شود.

۱.۲.۲ با شروع از

$$\frac{۳۴}{۱۹}=۱+\frac{۱۵}{۱۹}=۱+\frac{۱}{\frac{۱۹}{۱۵}}=۱+\frac{۱}{۱+\frac{۴}{۱۵}}$$

نشان دهید که کسر مسلسل برای $\frac{۳۴}{۱۹}$ عبارت است از

$$۱+\frac{۱}{۱+\frac{۱}{۳+\frac{۱}{۱+\frac{۱}{۳}}}}.$$

۲.۲.۲ به طور مشابه نشان دهید که

$$\frac{۴۳}{۳۰}=۱+\frac{۱}{۲+\frac{۱}{۳+\frac{۱}{۴}}}.$$

---

[۴] continued fraction

[۵] چون کوچک‌تر بودن بین دو زوج مرتب معنای مشخصی ندارد، بهتر است گفته شود که ماکزیمم زوج (b,r) کوچک‌تر از ماکزیمم زوج (a,b) است. (م)

۳.۲.۲ در حالت کلی نشان دهید که

$$\frac{a}{b} = q_۱ + \cfrac{۱}{q_۲ + \cfrac{۱}{q_۳ + \cfrac{۱}{\ddots}}},$$

که در آن $q_۱$، $q_۲$، $q_۳$، ... خارج‌قسمتهای متوالیاً ظاهر شده در به کار بردن الگوریتم با تقسیم اقلیدسی برای (a, b) می‌باشند.

در قرن هجدهم، اویلر دید الگوریتم اقلیدسی را می‌توان توسط کسرهای مسلسل اجرا کرد که روشی مورد اقبال برای توصیف این الگوریتم در حدود یک قرن یا بیشتر بود. مثلاً گاوس از ذکر نام اقلیدس چشم‌پوشی کرد و منحصراً به الگوریتم کسرهای مسلسل در کتاب رسالات خود ارجاع داد. الگوریتم اقلیدسی به شکلی که ما می‌شناسیم توسط درسهایی در نظریه اعداد دیریکله[۶] (۱۸۶۳) به شکل کنونی تبدیل شد.

۳.۲ نمایش خطی ب.م.م.

احتمالاً بهترین نتیجهٔ الگوریتم اقلیدسی این است که برای اعداد صحیحی مانند m و n می‌توان نوشت

$$\gcd(a, b) = ma + nb.$$

در حقیقت، این مطلب درست است که اعداد a_i و b_i تولید شده توسط الگوریتم اقلیدسی، همگی به صورت $ma + nb$ برای اعداد صحیحی مانند m و n هستند، و البته b_i یی هست که $\gcd(a, b) = b_i$.

این گزاره را در مورد a_i و b_i به وسیلهٔ صورت صعودی استقراء اثبات می‌کنیم. برای شروع، مطمئناً داریم

$$a_۱ = ۱ \times a + ۰ \times b, \qquad b_۱ = ۰ \times a + ۱ \times b.$$

[۶] Dirichlet's Vorlesungen über Zahlentheorie

لذا گزارهٔ فوق‌الذکر برای ۱ $= i$ درست است. و اگر a_i و b_i هر دو به صورت $ma + nb$ باشند آنگاه همین مطلب برای تفاضل آنها، و در نتیجه برای a_{i+1} و b_{i+1}، نیز درست است. لذا، همان گونه که انتظار داشتیم، همهٔ اعداد تولید شده توسط زوج (a, b) در الگوریتم اقلیدسی به صورت $ma + nb$ هستند. □

همچنین این برهان، روشی جهت یافتن m و n برای a و b ی داده شده را پیشنهاد می‌کند و رد پای ضرایب m و n را برای هر a_i و b_i یی که توسط الگوریتم اقلیدسی تولید می‌شوند تعقیب می‌کند.

یک روش عملی برای انجام این کار در مثال زیر نشان داده شده است که در آن محاسبات عددی روی ۳۴ و ۱۹ به موازات محاسبات نمادی روی حروف a و b صورت پذیرفته است. هرگاه که مضربی از عدد دوم را از عدد اول کم می‌کنیم دقیقاً همان کار را روی حروف متناظر آنها نیز انجام می‌دهیم. از این رو ترکیب خطی نهایی حروف a و b برابر ب.م.م. دو عدد است.

مثال. $\gcd(۳۴, ۱۹) = \gcd(a, b)$ به صورت $ma + nb$. برای کارآمد شدن، تقسیم با باقیمانده را به کار می‌بریم و مضرب مناسب عدد دوم را از عدد اول کم می‌کنیم تا باقیمانده را در هر گام به دست آوریم.

$$\begin{aligned}
& (۳۴, ۱۹) = (a, b) \\
\Rightarrow\ & (۱۹, ۱۵) = (b, a - b) \\
\Rightarrow\ & (۱۵, ۴) = (a - b, b - (a - b)) = (a - b, -a + ۲b) \\
\Rightarrow\ & (۴, ۳) = (-a + ۲b, a - b - ۳(-a + ۲b)) = (-a + ۲b, ۴a - ۷b) \\
\Rightarrow\ & (۳, ۱) = (۴a - ۷b, -a + ۲b - (۴a - ۷b)) \\
& = (۴a - ۷b, -۵a + ۹b).
\end{aligned}$$

از سطر آخر ب.م.م. را می‌خوانیم،

$$۱ = -۵a + ۹b.$$

تساوی اخیر درست است چون

$$-۵ \times ۳۴ + ۹ \times ۱۹ = -۱۷۰ + ۱۷۱ = ۱.$$

الگوریتم اقلیدسی شدیداً هم در عمل و هم به طور نظری مهم است. در عمل مفید است چون به طور غیر منتظره‌ای سریع می‌باشد (ب.م.م. دو عدد k رقمی را در حدود k گام می‌دهد) و بسیار سریع‌تر از هر نوع الگوریتم شناخته شده برای پیدا کردن مقسوم‌علیه‌های یک عدد k رقمی است.

و ب.م.م. نه تنها در عمل، بلکه از لحاظ نظری نیز مهم است. نظریهٔ اساسی مقسوم‌علیه‌ها و اعداد اول، همان طور که در بخش ۴.۲ خواهیم دید، مبتنی بر نظریهٔ ب.م.م. است.

الگوریتم اقلیدسی را اغلب برای یافتن $\gcd(a,b)$ و برای پیدا کردن m و n صحیحی که $\gcd(a,b) = ma + nb$ فراخوانی می‌کنیم. بنابراین هم‌اکنون مطمئن شوید که لیاقت عملیِ به کار بردن آن را کسب کرده‌اید!

تمرینها

۱.۳.۲ به کمک الگوریتم اقلیدسی $\gcd(۶۳, ۱۳)$ را تعیین کنید و m و n ی را بیابید که $۶۳m + ۱۳n = ۱$.

۲.۳.۲ m و n ی را بیابید که $۵۵m + ۳۴n = ۱$.

۴.۲ اعداد اول و تجزیه

در بخش ۱.۱ با استفاده از اصل نزول نامتناهی نشان دادیم که اعداد طبیعی خاصی عوامل اول دارند. با اندک تعدیلی در آن استدلال، داریم

وجود تجزیه به اعداد اول. هر عدد طبیعی مانند n را می‌توان به صورت حاصل ضربی از اعداد اول یعنی

$$n = p_۱ p_۲ p_۳ \cdots p_k$$

نوشت.

برهان. اگر n اول باشد چیزی برای اثبات باقی نمی‌ماند. اگر چنین نباشد، برای اعداد طبیعی کوچک‌تری مانند a و b داریم $n = ab$. اگر a یا b اول نباشند آنها را به عوامل کوچک‌تر می‌شکنیم، و به همین ترتیب. چون اعداد طبیعی نمی‌توانند تا ابد کاهش یابند، نهایتاً به تجزیهٔ

$$n = p_۱ p_۲ p_۳ \cdots p_k,$$

که در آن هیچ p_i یی حاصل ضرب اعداد کوچک‌ترش نیست، می‌رسیم. یعنی هر p_i اول است. □

این قضیه از آنچه در بخش ۱.۱ اثبات کردیم مهم‌تر است چون وجود تعدادی نامتناهی عدد اول را ایجاب می‌کند. حتی یکتایی تجزیه به اعداد اول از این هم مهم‌تر است – صرف نظر از این که چگونه n را به اعداد اول بشکنیم، همواره در پایان به اعداد اول یکسانی می‌رسیم.

خاصیت مقسوم‌علیه اول. اگر عددی اول مانند p حاصل ضرب دو عدد طبیعی مانند a و b را عاد کند آنگاه p عدد a یا b را عاد خواهد کرد.

برهان. با فرض آن که p عدد a را عاد نکند باید نشان دهیم که p عدد b را عاد می‌کند.

حال اگر p عدد a را عاد نکند داریم $\gcd(a,p) = ۱$، چون تنها مقسوم‌علیه‌های p خود p و ۱ می‌باشند. لذا، بنابر نتیجهٔ بخش ۳.۲، اعداد صحیحی مانند m و n موجودند که

$$۱ = ma + np$$

با ضرب کردن دو طرف این معادله در b داریم

$$b = mab + npb.$$

حال به سمت راست بنگرید: p عدد ab را بنابر فرض و عدد pb را به طور بدیهی عاد می‌کند. لذا p هر دو جملهٔ سمت راست را عاد می‌کند و از این رو مجموع آنها را عاد می‌کند. یعنی همان طور که می‌خواستیم p عدد b را عاد می‌کند. □

یکتایی تجزیه به اعداد اول. تجزیه به اعداد اول برای هر عدد طبیعی (تا حد ترتیب عوامل) یکتاست.

برهان. به برهان خلف فرض کنیم عددی طبیعی هست که دو تجزیهٔ مختلف دارد. با حذف اعداد اولی که در هر دو تجزیه به طور مشترک آمده‌اند، برابری حاصل ضرب اعداد اول زیر را داریم

$$p_1 p_2 p_3 \cdots p_k = q_1 q_2 q_3 \cdots q_\ell$$

که در آن هیچ p_i و q_j یی برابر نیستند. این مطلب بنابر توضیحات زیر به تناقض می‌انجامد.

چون p_1 عاملی از سمت چپ است پس سمت راست را نیز عاد می‌کند. اما در این صورت با استفادهٔ تکراری از خاصیت مقسوم‌علیه داریم

p_1 عدد $q_1 q_2 q_3 \cdots q_\ell$ را عاد می‌کند

$\Rightarrow$ p_1 عدد q_1 یا $q_2 q_3 \cdots q_\ell$ را عاد می‌کند

$\Rightarrow$ p_1 عدد q_1 یا q_2 یا $q_3 \cdots q_\ell$ را عاد می‌کند

$\vdots$

$\Rightarrow$ p_1 عدد q_1 یا q_2 یا ... یا q_ℓ را عاد می‌کند

$\Rightarrow$ $p_1 = q_1$ یا $p_1 = q_2$ یا ... یا $p_1 = q_\ell$

که با فرض ما در تناقض است. لذا هیچ عدد طبیعی، دو تجزیهٔ متفاوت به اعداد اول ندارد. □

گرچه خاصیت مقسوم‌علیه اول توسط اقلیدس (در حدود ۳۰۰ قبل از میلاد) اثبات شده است، با این حال یکتایی تجزیه به اعداد اول اولین بار توسط گاوس در سال ۱۸۰۱ گفته شد.

تمرینها

گاوس یکتایی تجزیه به اعداد اول را با برهانی بدیع برای خاصیت مقسوم‌علیه اول که در زیر می‌آید به اثبات رساند.

۱.۴.۲ در ابتدا نشان دهید که p نمی‌تواند حاصل ضرب a_1b_1 از اعداد طبیعی a_1 و b_1 که کوچک‌تر از p هستند را عاد کند. یعنی فرض کنید که p عدد a_1b_1 را عاد کند و نشان دهید که p عدد a_1b_2 را نیز عاد می‌کند که در آن

$$b_2 = b_1 \text{ بر } p \text{ باقیمانده تقسیم }$$

و این فرآیند نزول نامتناهی را به دست می‌دهد.

۲.۴.۲ حال از تمرین ۱.۴.۲ استفاده کنید و نشان دهید که اگر p عدد ab را عاد کند ولی a و b را عاد نکند آنگاه p عددی مانند a_1b_1 را، که a_1 و b_1 کوچک‌تر از p هستند، عاد می‌کند. بدین ترتیب خاصیت مقسوم‌علیه اول را نتیجه بگیرید.

۵.۲ نتایج یکتایی تجزیه به اعداد اول

اگر $c = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ که در آن p_1، p_2، ...، p_k اعدادی اول و m_1، m_2، ...، m_k اعدادی طبیعی هستند، آنگاه

$$c^2 = p_1^{2m_1} p_2^{2m_2} \cdots p_k^{2m_k}$$

لذا در تجزیه به اعداد اول برای مربع یک عدد طبیعی، هر عدد اول با توانی زوج ظاهر می‌شود.

و بالعکس اگر

$$d = p_1^{2m_1} p_2^{2m_2} \cdots p_k^{2m_k}$$

آنگاه $d = c^2$. لذا یک عدد طبیعی مربع کامل است فقط و فقط وقتی که هر عدد اول ظاهر شده در تجزیهٔ آن به اعداد اول، با توانی زوج ظاهر شده باشد.

حال فرض کنیم d مربع کامل باشد و $d = ab$، که a و b هیچ مقسوم‌علیه اول مشترکی ندارند (یا همان طور که در بخش ۱.۲ گفتیم، a و b نسبت به هم اول باشند). در این صورت تجزیه‌ای به صورت

$$d = ab = p_1^{2m_1} p_2^{2m_2} \cdots p_k^{2m_k}$$

برای d داریم. چون a و b مقسوم‌علیه اول مشترکی ندارند، هر جمله مانند $p_i^{2m_i}$ باید فقط در تجزیه به اعداد اول یکی از a و b (و نه هر دو) ظاهر شود. به بیان دیگر، در تجزیه به اعداد اول a و b، هر عدد اول با توانی زوج ظاهر می‌شود و از این رو بنابر تبصرهٔ بند قبل، a و b هر دو مربع کامل هستند.

با جمع‌بندی مطالب فوق حکم زیر را داریم

عوامل نسبت به هم اول یک مربع کامل. اگر a و b اعداد طبیعیِ نسبت به هم اولی باشند که حاصل ضرب آنها مربع کامل است، آنگاه a و b هر دو مربع کامل هستند. □

با استفاده از این مطلب که

$$c^3 = p_1^{3m_1} p_2^{3m_2} \cdots p_k^{3m_k}$$

و با برهانی مشابه اثبات می‌شود که یک عدد طبیعی، مکعب کامل است فقط و فقط وقتی که هر عدد اولِ ظاهر شده در تجزیهٔ آن به اعداد اول، با توانی مضرب ۳ آمده باشد، و به علاوه اگر a و b اعداد طبیعیِ نسبت به هم اولی باشند که حاصل ضرب آنها مکعب کامل است، آنگاه a و b هر دو مکعب کامل هستند.

نتیجهٔ مهم دیگری از تجزیه به اعداد اولِ یک مربع کامل، وجود جذرهای اصم است.

جذرهای اصم. اگر N عدد طبیعی غیر مربعی باشد، آنگاه $\sqrt{N}$ اصم است.

برهان. فرض کنیم N عدد طبیعی و $\sqrt{N}$ گویا باشد، یعنی اعدادی طبیعی مانند a و b موجودند باشند که

$$\sqrt{N} = \frac{a}{b}.$$

در این صورت باید نشان دهیم که N مربع کامل است.

با مربع کردن دو طرف داریم

$$N = \frac{a^2}{b^2} = p_1^{2m_1} p_2^{2m_2} \cdots p_k^{2m_k},$$

که p_1، ...، p_k اعدادی اول هستند. هر عدد اول با توانی زوج آمده است چون توان آن دو برابر توان ظاهر شده‌اش در a منهای دو برابر توان ظاهر شده‌اش در b می‌باشد. اما در این صورت N یک مربع کامل است (برای حالتی که برخی از m_i ها منفی باشند نیز همین استدلال را می‌توان به کار برد). □

تجزیه به اعداد اول، ب.م.م. و ک.م.م.

یکتایی تجزیه به اعداد اول ایجاب می‌کند که هر مقسوم‌علیه اول یک عدد طبیعی مانند n واقعاً در تجزیه به اعداد اول آن ظاهر شود. و هر مقسوم‌علیه اول

مشترک a و b در هر دو تجزیهٔ آنها ظاهر خواهد شد. از این رو بزرگ‌ترین مقسوم‌علیه مشترک a و b، حاصل ضرب اعداد اول مشترک در تجزیهٔ آنها به اعداد اول است.

مثال.

$$\begin{aligned} ۶۶۶ &= ۲ \times ۳^۲ \times ۳۷ \\ ۱۰۰۰ &= ۲^۳ \times ۵^۳ \end{aligned}$$

از این رو $\gcd(۶۶۶, ۱۰۰۰) = ۲$.

$$\begin{aligned} ۴۴۴۴ &= ۲^۲ \times ۱۱ \times ۱۰۱ \\ ۹۰۹۰ &= ۲ \times ۳^۲ \times ۵ \times ۱۰۱ \end{aligned}$$

از این رو $\gcd(۴۴۴۴, ۹۰۹۰) = ۲ \times ۱۰۱ = ۲۰۲$.

این روش برای اعدادی که به اندازهٔ کافی کوچک باشند و به راحتی بتوان آنها را به اعداد اول تجزیه کرد کاملاً کارآمد است. اما برای اعداد بزرگ‌تر، الگوریتم اقلیدسی کاملاً برتری دارد. همچنین باید به خاطر داشت که روش تجزیه، به وسیلهٔ یکتایی تجزیه به اعداد اول که به نوبهٔ خود وابسته به نظریهٔ الگوریتم اقلیدسی می‌باشد تأیید می‌گردد.

تجزیه به اعداد اول همچنین کوچک‌ترین مضرب مشترک[۷] (ک.م.م. یا lcm) دو عدد طبیعی را به دست می‌دهد. هر مضرب مشترک a و b باید مضربی از هر توان اول در a و در b باشد. از این رو کوچک‌ترین مضرب مشترک a و b، حاصل ضرب اعداد اول ظاهر شده در تجزیهٔ آنها به اعداد اول، با ماکزیمم توان اتفاق افتاده در a و b می‌باشد.

مثال. با استفاده از تجزیهٔ ۶۶۶، ۱۰۰۰ و ۴۴۴۴، ۹۰۹۰ که در بالا داشتیم، داریم

---

[۷] least common multiple

$$\mathrm{lcm}(۶۶۶, ۱۰۰۰) = ۲^۳ \times ۳^۲ \times ۵^۳ \times ۳۷ = ۳۳۳۰۰۰$$

و

$$\mathrm{lcm}(۴۴۴۴, ۹۰۹۰) = ۲^۲ \times ۳^۲ \times ۵ \times ۱۱ \times ۱۰۱ = ۱۹۹۹۸۰.$$

تمرینها

همان طور که در بخش ۳.۱ تذکر داده شد، مفهوم عدد اول در $\mathbb{Z}$ پیچیده‌تر از $\mathbb{N}$ است زیرا یکهٔ ۱− می‌تواند در تجزیه ظاهر شود. این مطلب، وضعیت مربعها و مکعبهای کامل را در $\mathbb{Z}$ پیچیده می‌سازد، اما تنها اندکی پیچیده.

۱.۵.۲ با مثالی نشان دهید که اگر a و b اعداد صحیح نسبت به هم اولی باشند که حاصل ضرب آنها مربع کامل است، آنگاه لزوماً نمی‌توان نتیجه گرفت که a و b هم مربع کامل هستند. اگر چنین نیست، پس چه می‌توان گفت؟

۲.۵.۲ از طرف دیگر اگر a و b اعداد صحیح نسبت به هم اولی باشند که حاصل ضرب آنها مکعب کامل است، آنگاه a و b مکعب کامل هستند. چرا؟

الگوریتم اقلیدسی بلادرنگ نتیجه می‌دهد که $\gcd(۲۰۰۰, ۲۰۰۱) = ۱$. با این حال باز هم جالب است که واقعاً ببینید ۲۰۰۰ و ۲۰۰۱ هیچ عامل اول مشترکی ندارند.

۳.۵.۲ تجزیه به اعداد اول ۲۰۰۰ و ۲۰۰۱ را بیابید و تأیید کنید که $\gcd(۲۰۰۰, ۲۰۰۱) = ۱$.

همچنین مفید است که فرمولهایی برای $\gcd(a, b)$ و $\mathrm{lcm}(a, b)$ بر حسب تجزیه به اعداد اول داشته باشیم.

۴.۵.۲ فرض کنیم که p_1، p_2، …، p_k همهٔ اعداد اولی باشند که a یا b را عاد می‌کنند و

$$\begin{aligned} a &= p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}, \\ b &= p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}. \end{aligned}$$

نتیجه بگیرید که

$$\begin{aligned} \gcd(a,b) &= p_1^{\min(m_1,n_1)} p_2^{\min(m_2,n_2)} \cdots p_k^{\min(m_k,n_k)}, \\ \operatorname{lcm}(a,b) &= p_1^{\max(m_1,n_1)} p_2^{\max(m_2,n_2)} \cdots p_k^{\max(m_k,n_k)}. \end{aligned}$$

۵.۵.۲ از تمرین ۴.۵.۲ نتیجه بگیرید که $\gcd(a,b)\operatorname{lcm}(a,b) = ab$.

حال که یکتایی تجزیه به اعداد اول را می‌دانیم، می‌توانیم قضیهٔ اویلر در مورد اعداد تام را که در تمرینهای بخش ۵.۱ گفته شد مجدداً مورد بررسی قرار دهیم.

۶.۵.۲ اگر $q = 2^p - 1$ عددی اول باشد، آنگاه نشان دهید که مقسوم‌علیه‌های سرهٔ $2^{p-1}q$ (یعنی آنهایی که کوچک‌تر از این عدد هستند) عبارتند از ۱، ۲، 2^2، …، 2^{p-1} و q، $2q$، 2^2q، …، $2^{p-2}q$.

۷.۵.۲ نشان دهید که

$$1 + 2 + 2^2 + \ldots + 2^{p-2} = 2^{p-1} - 1$$

و نتیجه بگیرید که مجموع مقسوم‌علیه‌های سرهٔ $2^{p-1}q$ برابر $2^{p-1}q$ است. (یعنی $2^{p-1}q$ تام می‌باشد.)

۶.۲ معادله‌های دیوفانتی خطی

ساده‌ترین معادله‌های دیوفانتی غیر بدیهی معادله‌های خطی دو متغیره[۸] یعنی

$$ax + by = c$$

می‌باشند که در آن $a, b, c \in \mathbb{Z}$. چنین معادله‌ای ممکن است بی‌نهایت جواب داشته باشد یا اصلاً جواب نداشته باشد. مثلاً معادلهٔ

$$6x + 15y = 1$$

هیچ جواب صحیحی ندارد. این مطلب بدان جهت است که وقتی x و y صحیح باشند ۳ عدد $6x + 15y$ را عاد می‌کند (چون ۳ هم ٦ و هم ۱۵ را عاد می‌کند)، اما ۳ عدد ۱ را عاد نمی‌کند. این مثال نشان می‌دهد که مقسوم‌علیه‌های مشترک با معادله‌های خطی ارتباط دارند و کلید حل آنها را فاش می‌سازد: نمایش خطی ب.م.م. که در بخش ۳.۲ یافت شد.

محک حل پذیری معادله‌های دیوفانتی خطی. اگر a، b و c اعدادی صحیح باشند، آنگاه معادلهٔ $ax + by = c$ دارای جواب صحیح است فقط و فقط وقتی که $\gcd(a, b)$ عدد c را عاد کند.

برهان. چون $\gcd(a, b)$ اعداد a و b را عاد می‌کند، باید برای هر x و y صحیح $ax + by$ را نیز عاد کند. بنابراین اگر $ax + by = c$ آنگاه $\gcd(a, b)$ عدد c را عاد می‌کند.

بالعکس، با توجه به مطالب بخش ۳.۲، اعداد m و n صحیحی موجودند که $\gcd(a, b) = am + bn$. از این رو اگر $\gcd(a, b)$ عدد c را عاد کند آنگاه عدد صحیحی مانند d موجود است که

$$c = \gcd(a, b)d = (am + bn)d = amd + bnd.$$

بنابراین $x = md$ و $y = nd$ جوابی برای $ax + by = c$ است. □

---

[۸] linear equations in two variables

این برهان همچنین نشان می‌دهد که چگونه جوابی برای $ax + by = c$ (در صورت وجود) بیابیم. یعنی با استفاده از الگوریتم اقلیدسی به صورت نمادین برای یافتن m و n (با به کار بردن حروف، متناظر با اعداد)، $\gcd(a, b)$ را به صورت $am + bn$ می‌نویسیم. سپس m و n را در عدد صحیح d که $c = \gcd(a, b)d$ ضرب می‌کنیم.

اگر یک جواب مانند $x = x_0$ و $y = y_0$ را در دست داشته باشیم، آنگاه بی‌نهایت جواب داریم، چون می‌توانیم هر یک از بی‌نهایت جواب $ax + by = 0$ را به (x_0, y_0) اضافه کنیم.

جواب کلی $ax + by = c$. جواب $ax + by = c$ در $\mathbb{Z}$ عبارت است از $x = x_0 + \frac{bt}{\gcd(a,b)}$ و $y = y_0 - \frac{at}{\gcd(a,b)}$، که در آن $x = x_0$ و $y = y_0$ جواب خاص دلخواهی برای این معادله است و t در $\mathbb{Z}$ تغییر می‌کند.

برهان. چون $x = \frac{bt}{\gcd(a,b)}$ و $y = -\frac{at}{\gcd(a,b)}$ به وضوح جوابی صحیح برای $ax + by = 0$ است، افزودن آن به هر جواب مانند $x = x_0$ و $y = y_0$ از $ax + by = c$ جواب دیگری از $ax + by = c$ را به دست می‌دهد.

بالعکس، اگر x و y جواب دلخواهی برای $ax + by = c$ باشد آنگاه $x' = x - x_0$ و $y' = y - y_0$ در $ax' + by' = 0$ صدق می‌کند. اما هر جواب صحیح $ax' + by' = 0$ جوابی از معادلهٔ

$$a'x' = -b'y'$$

است که ضرایب آن اعداد نسبت به هم اول $a' = \frac{a}{\gcd(a,b)}$ و $b' = \frac{b}{\gcd(a,b)}$ می‌باشند.

چون a' و b' هیچ مقسوم‌علیه مشترکی ندارند، از یکتایی تجزیه نتیجه می‌شود که b' عدد x' را عاد می‌کند. یعنی

برای عدد صحیحی مانند t داریم $x' = b't$ و از این رو $y' = -a't$.

مجدداً با قرار دادن مقادیر x'، y'، a' و b' در معادلهٔ بالا به جواب

$$x = x_\circ + \frac{bt}{\gcd(a,b)}, \qquad y = y_\circ - \frac{at}{\gcd(a,b)}$$

می‌رسیم. □

تمرینها

محک حل پذیری را می‌توان مستقیماً با اثبات نتیجهٔ زیر، بدون به کار بردن الگوریتم اقلیدسی، به دست آورد.

۱.۶.۲ نشان دهید که $\{am + bn : m, n \in \mathbb{Z}\}$ متشکل از همهٔ مضارب صحیح $\gcd(a,b)$ است.

با این حال، الگوریتم اقلیدسی واقعاً برای یافتن جوابهای معادله‌های دیوفانتی خطی ارزشمند است.

۲.۶.۲ جواب صحیحی برای $۳۴x + ۱۹y = ۱$ بیابید.

۳.۶.۲ جواب صحیحی برای $۳۴x + ۱۹y = ۷$ بیابید.

۴.۶.۲ آیا جواب صحیحی برای $۳۴x + ۱۷y = ۱$ وجود دارد؟

۷.۲ * الگوریتم اقلیدسی برداری

در بخش ۳.۲ توسیعی از الگوریتم اقلیدسی را برای محاسبهٔ ب.م.م. دو عدد صحیح a و b به صورت

$$\gcd(a,b) = am + bn,$$

برای m و n ی در $\mathbb{Z}$، به کار بردیم. این توسیع همانند الگوریتم معمولی پیش می‌رود (کم کردن عدد کوچک‌تر از عدد بزرگ‌تر) و هدایت تقلیدی نمادین (که همان اعمال را روی ترکیبهای خطی حروف a و b اجرا می‌کند) را به عهده دارد.

حال می‌خواهیم بخش نمادین الگوریتم را در حالتی که a و b نسبت به هم اول هستند از نزدیک‌تر تجزیه و تحلیل کنیم. برای این کار، به جای هر ترکیب خطی مانند $m_i a + n_i b$، زوج مرتب یا بردار (m_i, n_i) را جایگزین می‌کنیم. برای آن که الگوریتم معمولی را قادر سازیم تا به ساده‌ترین شکل ممکن اجرا شود، قرار می‌دهیم $a > 0$ و $b < 0$ [۹] و عدد مثبت را در مؤلفهٔ اول و عدد دوم را در مؤلفهٔ دوم می‌گذاریم. سپس، هر گام الگوریتم اقلیدسی معمولی در حقیقت یک جمع کردن است: عددِ با قدر مطلق بزرگ‌تر توسط مجموع آن با عدد دیگر جایگزین می‌شود. گامهای متناظر در الگوریتم نمادین جمع کردنهای برداری هستند، لذا فرآیند حاصل را الگوریتم اقلیدسی برداری [۱۰] می‌نامیم.

مثال. شکل ۲.۱ گامهای الگوریتم اقلیدسی برداری را روی $(12, -5)$ با زوجهای عددی در ستون اول، زوجهای نمادین در ستون دوم و زوجهای برداری در ستون سوم نشان می‌دهد. جمعهای واقعی فقط در ستون نمادین نشان داده شده‌اند.

Numbers	Symbolic pairs	Vector pairs
$(12,-5)$	(a,b)	((1,0), (0,1))
$(7,-5)$	$(a+b,b)$	((1,1), (0,1))
$(2,-5)$	$((a+b)+b,b)=(a+2b,b)$	((1,2), (0,1))
$(2,-3)$	$(a+2b,b+(a+2b))=(a+2b,a+3b)$	((1,2), (1,3))
$(2,-1)$	$(a+2b,a+3b+(a+2b))=(a+2b,2a+5b)$	((1,2), (2,5))
$(1,-1)$	$(a+2b+(2a+5b),2a+5b)=(3a+7b,2a+5b)$	((3,7), (2,5))

شکل ۲.۱: خروجی الگوریتمهای اقلیدسی

[۹] توجه کنید که با این فرض $\gcd(a,b)$ تغییری نمی‌کند. (م)

[۱۰] vector Euclidean algorithm

(همانند بخش ۳.۲) از سطر آخر می‌خوانیم که

$$۱ = ۳a + ۷b = ۳ \times ۱۲ - ۷ \times ۵.$$

لذا $(m, n) = (۳, ۷)$ برداری طبیعی است که $۱۲m - ۵n = ۱$.

همچنین جالب است که الگوریتم را یک گام بیشتر اجرا کنیم (در ستون اول عدد ۱ را به ۱− اضافه می‌کنیم تا ۰ حاصل شود)، چون در این صورت ۱۲ و ۵ مجدداً در ستون بردارها ظاهر می‌شوند.

(1,0)	$(3a+7b, 2a+5b+(3a+7b)) = (3a+7b, 5a+12b)$	((3,7), (5,12))

شکل ۲.۲: نتیجهٔ گام اضافی

این مطلب نباید تعجب‌آور باشد چون $۵ \times ۱۲ - ۱۲ \times ۵ = ۰$، گرچه قابل تصور است که می‌شد مضرب بزرگ‌تری از بردار $(۵, ۱۲)$ را به دست آوریم. آنچه جالب است این است که چه قدر ساده به بردار $(۵, ۱۲)$ رسیدیم: یعنی، با بردارهای $\mathbf{i} = (۱, ۰)$ و $\mathbf{j} = (۰, ۱)$ شروع کردیم و دنباله‌ای از گامها را به دست آوردیم که در آن زوج بردار $(v_۱, v_۲)$ با $(v_۱ + v_۲, v_۲)$ یا $(v_۱, v_۱ + v_۲)$ جایگزین می‌شود.

حال این مثال را تعمیم می‌دهیم تا نشان دهیم که:

نسبت به هم اول بودن در الگوریتم اقلیدسی برداری. در اجرای الگوریتم اقلیدسی برداری،

۱. هر بردار تولید شده از $(۱, ۰)$ و $(۰, ۱)$، یک زوج نسبت به هم اول از اعداد طبیعی است. (چنین برداری را اولیه می‌نامیم.)

۲. هر زوج نسبت به هم اول مانند (a, b) از اعداد طبیعی را می‌توان (با شروع الگوریتم اقلیدسی معمولی روی b و $-a$) تولید کرد.

برهان. ۱. بدیهی است که هر بردار تولید شده، زوجی از اعداد طبیعی است چون اولین بردار جدید $(۱, ۱)$ است و جمع کردنهای برداری بعدی نمی‌تواند اعداد ظاهر شده در زوج مرتب را کاهش دهد.

برای آن که ببینیم چرا هر زوج تولید شده نسبت به هم اول است، خاصیت قوی‌تری را اثبات می‌کنیم: اگر $((m_1, n_1), (m_2, n_2))$ یک زوج بردار در گامی دلخواه باشد، آنگاه

$$m_1 n_2 - n_1 m_2 = 1.$$

این مطلب هنگامی که $(m_1, n_1) = (1, 0)$ و $(m_2, n_2) = (0, 1)$، در گام اول درست است. و اگر این مطلب برای زوج بردار $((m_1, n_1), (m_2, n_2))$ درست باشد آنگاه برای زوج بعدی یعنی $((m_1 + m_2, n_1 + n_2), (m_2, n_2))$ یا $((m_1, n_1), (m_1 + m_2, n_1 + n_2))$ نیز درست است زیرا

$$(m_1 + m_2)n_2 - (n_1 + n_2)m_2 = m_1 n_2 - n_1 m_2 = 1$$

و

$$m_1(n_1 + n_2) - n_1(m_1 + m_2) = m_1 n_2 - n_1 m_2 = 1.$$

نتیجه می‌شود که هر بردار (m_1, n_1) تولید شده، یک زوج نسبت به هم اول است چون هر مقسوم‌علیه مشترک از m_1 و n_1 عدد $1 = m_1 n_2 - n_1 m_2$ را نیز عاد می‌کند. به طور مشابه برای هر بردار مانند (m_2, n_2) نیز همین مطلب برقرار است.

۲. اگر a و b دو عدد طبیعی نسبت به هم اول باشند آنگاه الگوریتم اقلیدسی برداری که به وسیلهٔ الگوریتم اقلیدسی معمولی روی b و $-a$ عمل می‌کند، برداری مانند (m, n) تولید می‌کند که $mb - na = 0$ و اعداد m و n بنابر مطالب بخش ۱ نسبت به هم اول هستند.

چون تجزیه به اعداد اول یکتاست، $mb = na$ برای a و b ی نسبت به هم اول و m و n نسبت به هم اول، نتیجه می‌دهد که $m = a$ و $n = b$. از این رو هر زوج نسبت به هم اول مانند (a, b) را می‌توان توسط الگوریتم اقلیدسی برداری تولید کرد. □

تمرینها

برهان نسبت به هم اول بودن در الگوریتم اقلیدسی برداری، چه اعداد b و a– نسبت به هم اول باشند چه نباشند به کار می‌رود.

۱.۷.۲ اگر b و a– نسبت به هم اول نباشند، چه بردار (m,n) ی (که $mb = na$) توسط الگوریتم اقلیدسی برداری تولید می‌شود؟

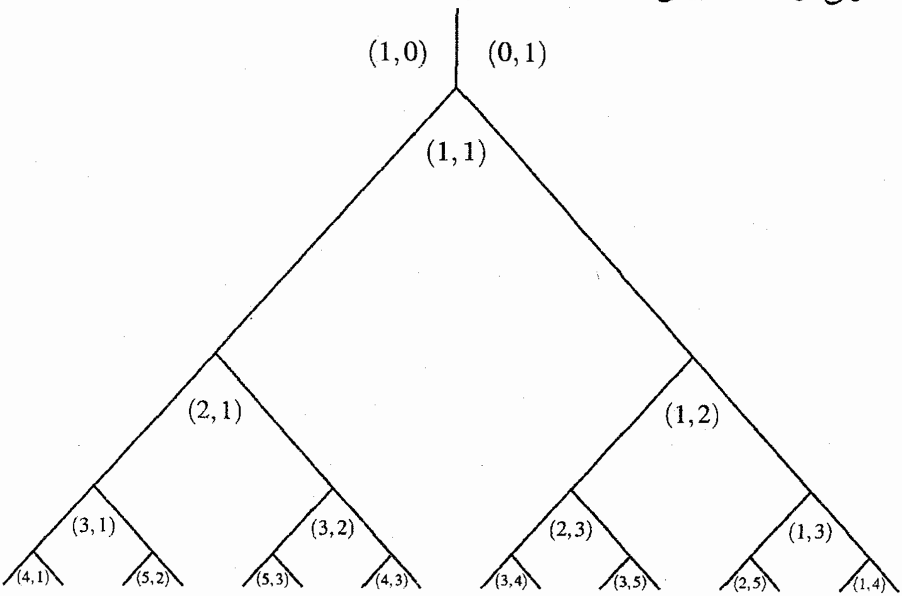
همان طور که در بخش ٦.۲ دیدیم، الگوریتم اقلیدسی نمادین هنگامی که معادله‌های دیوفانتی خطی حل‌می‌شوند به کار می‌رود. تجزیه و تحلیل فوق از الگوریتم برداری، مستقیماً ارتباط آن را با معادله‌های خاصی نشان می‌دهد. فرض کنیم که الگوریتم اقلیدسی معمولی را روی اعداد b و a– تا تولید شدن ۱ و ۱ – اجرا کنیم و فرض کنیم که بردار متناظر، $((m_۱, n_۱), (m_۲, n_۲))$ باشد.

۲.۷.۲ نشان دهید که $(x, y) = (m_۱, n_۱)$ کوچکترین جواب مثبت $bx - ay = ۱$ و نیز $(x, y) = (m_۲, n_۲)$ کوچکترین جواب مثبت $bx - ay = -۱$ است.

۸.۲ * نقشه زوجهای نسبت به هم اول

نتایج بخش قبل به صورت نموداری در شکل ۳.۲ نمایش داده شده است که آن را نقشهٔ زوجهای نسبت به هم اول یا بردارهای اولیه می‌نامیم. این شکل، افرازی از صفحه توسط درختی نامتناهی به ناحیه‌هایی است که توسط زوجهای مرتب صحیح (a, b) برچسب خورده‌اند. دو ناحیهٔ بالایی، $(۱, ۰)$ و $(۰, ۱)$ نامیده می‌شوند و برچسبهای دیگر توسط جمع برداری تولید شده است: اگر ناحیه‌های برچسب خوردهٔ $v_۱$ و $v_۲$ در یک یال مشترک باشند، آنگاه ناحیهٔ زیر نقطهٔ پایینی آن یال، برچسب $v_۱ + v_۲$ می‌گیرد.

از قسمتهای نقشهٔ نشان داده شده در شکل ۳.۲ بر می‌آید که برچسبها متمایزند و هر یک از آنها که مخالف (۰, ۱) و (۱, ۰) باشد زوج نسبت به هم اولی از اعداد طبیعی است.



شکل ۳.۲: ناحیه‌های برچسب خورده توسط زوجهای نسبت به هم اول

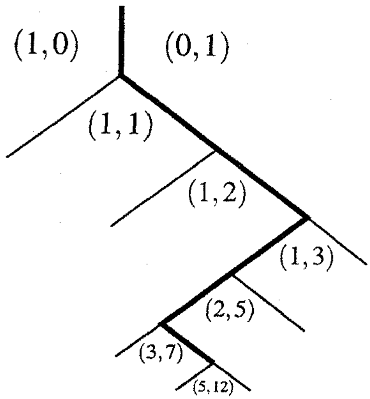
این مطلب را می‌توان توسط ارتباط دادن نقشه با الگوریتم اقلیدسی برداری اثبات کرد: در حقیقت این نقشه چشم‌اندازی از همهٔ خروجیهای الگوریتم است، بدین مفهوم که هر دنباله از زوج بردارهای تولید شده توسط اجرایی از الگوریتم به عنوان دنباله‌ای از زوجهای برچسب کنار یالها (چپ و راست آن) در مسیری متناهی و رو به پایین درخت اتفاق می‌افتد. این مطلب بدان دلیل است که هر دو توسط قاعدهٔ جمع برداری تعیین می‌گردند.

لذا دنبالهٔ

$$((۱,۰),(۰,۱)),((۱,۱),(۰,۱)),\ldots,((۳,۷),(۲,۵))$$

در مثال بخش ۷.۲، دنبالهٔ زوجهای با برچسب چپ/راست برای مسیر نشان

داده شده در شکل ۴.۲ می‌باشد.



شکل ۴.۲: شاخهٔ هدایت کننده به (۵, ۱۲)

بالعکس، هر مسیر رو به پایین درخت که با یال بین (۱, ۰) و (۰, ۱) شروع شود و به بالای ناحیهٔ (a, b) ختم گردد از کنار زوج برچسبهای چپ/راست که همان زوجهای تولید شده توسط الگوریتم اقلیدسی برداری با اعداد ورودی b و $-a$ هستند گذر می‌کند. این مطلب از آن رو درست است که این مسیرها در درخت یکتا هستند. لذا مسیر بالای رأس ناحیهٔ (a, b) باید همان مسیری باشد که متناظر با الگوریتم اقلیدسی برداری اجرا شده روی b و $-a$ است.

این تناظر بین مسیرها و اجراهای الگوریتمهای اقلیدسی برداری به ما امکان می‌دهد تا خواص اساسی نقشه را از خواص الگوریتم، که در بخش قبل اثبات شد، نتیجه بگیریم.

۱. هر ناحیهٔ نقشه، بجز آنهایی که برچسب (۱, ۰) و (۰, ۱) خورده‌اند، توسط یک زوج نسبت به هم اول از اعداد طبیعی برچسب می گیرد. این مطلب از خاصیت ۱ الگوریتم اقلیدسی برداری نتیجه می‌شود.

۲. هر زوج نسبت به هم اول از اعداد طبیعی مانند (a, b) به عنوان یک برچسب اتفاق می‌افتد. این مطلب از خاصیت ۲ الگوریتم اقلیدسی برداری نتیجه می‌شود.

۳. هر برچسب فقط یک بار اتفاق می‌افتد. این مطلب بدین دلیل است که توسط الگوریتم اقلیدسی معمولی که روی b و $a-$ اجرا شده باشد به برچسب (a,b) می‌رسیم و این اجرا، مسیر یکتایی را در درخت معین می‌کند.

تمرینها

نقشهٔ زوجهای نسبت به هم اول در تاریخ ریاضیات، بدون آن که هرگز آن قدر شناخته شده باشد تا نامی رسمی به خود بگیرد، بارها و بارها کشف و مجدداً کشف شده است. شاید بهترین نقش این نقشه در نمایش اعداد گویا باشد چون تناظری یک به یک بین اعداد گویای مثبت و کسرهای تحویل‌یافته[۱۱] مانند $\frac{a}{b}$ وجود دارد که متناظر با زوجهای نسبت به هم اول (a,b) از اعداد طبیعی می‌باشند. این ایده تحت نام کسرهای فَری[۱۲] شناخته می‌شود و بحثی از آن را می‌توان در کانوِی[۱۳] (۱۹۹۷)، ردماخر[۱۴] (۱۹۸۳) و هاردی[۱۵] و رایت[۱۶] (۱۹۷۹) یافت.

ارتباط بین کسرهای تحویل‌یافته و ناحیه‌ها عمیق‌تر از تناظر بدیهی $(a,b) \leftrightarrow \frac{a}{b}$ می‌باشد؛ این تناظر حافظ ترتیب[۱۷] نیز است. یعنی ترتیب کسرها از بزرگ به کوچک، متناظر با ترتیب ناحیه‌ها از چپ به راست می‌باشد.

۱۸.۲ خاصیت $m_۱n_۲ - n_۱m_۲ = ۱$ از بخش ۷.۲ را به کار برید و نشان دهید که اگر ناحیه‌های $(m_۱,n_۱)$ و $(m_۲,n_۲)$ یکدیگر را در یک یال قطع کنند که $(m_۱,n_۱)$ سمت چپ قرار داشته باشد، آنگاه $\frac{m_۲}{n_۲} > \frac{m_۱}{n_۱}$.

---

[۱۱] reduced fractions
[۱۲] Farey fractions
[۱۳] Conway
[۱۴] Rademacher
[۱۵] Hardy
[۱۶] Wright
[۱۷] order preserving

۲۸.۲ نتیجه بگیرید که اگر ناحیهٔ $(m_۱, n_۱)$ هر جایی در سمت چپ $(m_۲, n_۲)$ باشد آنگاه $\frac{m_۱}{n_۱} > \frac{m_۲}{n_۲}$.

۳۸.۲ تمرین ۲.۸.۲ را به منظور ارائهٔ برهانی دیگر برای آن که هر برچسب (a, b) فقط یک بار اتفاق می‌افتد به کار برید.

ساختار درختیِ کسرهای فری با عنوان درخت استرن-بروکت[۱۸] شناخته می‌شود. این ساختار را می‌توان از نقشهٔ ما با انتقال هر برچسب غیر از $(۱, ۰)$ و $(۰, ۱)$ به رأس بالای آن در شکل ۳.۲ به دست آورد. چیزهای بیشتر در مورد درخت استرن-بروکت را می‌توان در گراهام[۱۹] و بقیه (۱۹۹۴) یافت.

ما این شکل را برای نقشه از کانوی (۱۹۹۷) برگرفته‌ایم که از آن برای بیان روشی نموداری و بسیار ساده برای مطالعهٔ صورتهای مربعی استفاده کرده است. برای این منظور، نقشه نسبت به درخت مزیت دارد چون توسیعی طبیعی به نقشه‌ای با ناحیه‌های برچسب خورده توسط همهٔ زوجهای نسبت به هم اول از اعداد صحیح را می‌پذیرد. این ایده را در فصل ۵ به کار می‌بریم.

۹.۲ بحث

نتایج این فصل، پاسخ ما به سؤالی است که در فصل ۱ در مورد $\mathbb{Z}$ و $\mathbb{Z}[i]$ مطرح شد: شبیه اعداد صحیح رفتار می کند چه معنایی دارد؟ به بیان عامیانه، باید اعمال $+$ و $\times$ معنی داشته باشند و دارای خواص حلقه باشند، باید اعداد اول وجود داشته باشند و باید یکتایی تجزیه به اعداد اول (یا به طور معادل، خاصیت مقسوم‌علیه اول) را داشته باشیم.

اهمیت یکتایی تجزیه به اعداد اول اولین بار توسط گاوس (۱۸۰۱) مشخص شد، گرچه همان طور که در بخش ۴.۲ تذکر داده شد، خاصیت

[۱۸] Stern-Brocot tree
[۱۹] Graham

مقسوم‌علیه اول برای اویلر شناخته شده بود. صورت معادل دیگر یکتایی تجزیه به اعداد اول که قابل توجه است توسط اویلر (۱۷۴۸a) کشف شد. این اکتشاف، فرمول ضرب[۲۰] او بود که اکنون تابع زتا، $\zeta(s)$، نامیده می‌شود و توسط دو عبارت زیر تعریف می‌گردد:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\text{اول } p} (1 - \frac{1}{p^{-s}}) \qquad (*)$$

یکی بودن عبارات طرفین تساوی بدیهی نیست و در حقیقت مساوی بودن آنها با یکتایی تجزیه به اعداد اول معادل است! اگر هر یک از پرانتزهای سمت راست را به صورت یک سری هندسی بسط دهیم داریم

$$\frac{1}{1-p^{-s}} = 1 + p^{-s} + p^{-2s} + p^{-3s} + \dots$$

و لذا حاصل ضرب همهٔ عوامل برابر است با حاصل جمع ۱ و جملاتی به صورت

$$p_1^{-m_1 s} p_2^{-m_2 s} \cdots p_k^{-m_k s} = \frac{1}{(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k})^s},$$

که در آن p_1، p_2، ...، p_k اعدادی اول و متمایز و m_1، m_2، ...، m_k اعدادی طبیعی هستند. حال $(*)$ فقط در صورتی برقرار است که هر عدد طبیعی مانند n دقیقاً یک بار به صورت $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ ظاهر شود و این در صورتی درست است که یکتایی تجزیه به اعداد اول را داشته باشیم.

آنچه فرمول ضرب $(*)$ را جذاب‌تر می‌سازد این است که این فرمول نامتناهی بودن اعداد اول را نیز ایجاب می‌کند و لذا این فرمول، دو تا از مهم‌ترین قضایا در مورد اعداد اول را وحدت می‌بخشد. برهان اویلر برای نامتناهی بودن اعداد اول با استفاده از حالت خاص $s = 1$ در فرمول $(*)$ است. اگر فقط تعدادی متناهی عدد اول می‌داشتیم آنگاه سمت راست $(*)$ برای $s = 1$ باید متناهی می‌شد، در حالی که سمت چپ در این حالت برابر

---

[۲۰] product formula

$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots$ است که نامتناهی بودن آن حقیقتی شناخته شده است. لذا یک تناقض داریم و در نتیجه باید تعدادی نامتناهی عدد اول موجود باشد.

الگوریتم اقلیدسی از لحاظ تاریخی برای یکتایی تجزیه به اعداد اول و احراز این خاصیت در $\mathbb{Z}$، $\mathbb{Z}[i]$ و چند حلقهٔ دیگر که بعداً خواهیم دید به کار رفته است. حتی قبل از آن که یکتایی تجزیه به اعداد اول مورد توجه واقع شود، این الگوریتم توسط ریاضیدانان هندی و چینی برای حل معادله‌های دیوفانتی خطی استفاده شده بود. چنین معادله‌هایی در مسائل تقویمی[۲۱] ظاهر می‌شود، مثلاً یک سال $۳۶۵\frac{1}{4}$ روز دارد و یک ماه قمری $۲۹\frac{1}{2}$ روز. یا مثلاً می‌خواهیم چیزهایی را در مورد دفعهٔ بعد که روز اول یک ماه قمری در روز اول سال واقع می‌شود بدانیم.

تاریخ مدرن الگوریتم اقلیدسی با کشف گاوس (۱۸۳۲) آغاز شد که این الگوریتم در $\mathbb{Z}[i]$ نیز به کار رفت. دیریکله این الگوریتم را مبنای کتاب درسی خود[۲۲] در سال ۱۸۶۳ قرار داد و از آن در به دست آوردن نتایجی مقدماتی در مورد $\mathbb{Z}$ به روشی کاملاً شبیه آنچه در اینجا داریم، استفاده کرد. این کتاب درسی چهار ویرایش دارد که پس از مرگ دیریکله با سرمقالهٔ ددکیند تفسیر گردید. وی به شرح کتاب دیریکله با نوشتن مکملهایی برای آن از سال ۱۸۷۱ به بعد پرداخت. ددکیند در نسخه‌های متوالی مکمل X و XI، به وسیلهٔ نظریهٔ ایده‌آلها[۲۳] به تدریج نظریه اعداد را از وابستگی به الگوریتم اقلیدسی رها ساخت. این چیزی است که در چند فصل آخر این کتاب بدان می‌پردازیم.

---
[۲۱] calendar problems
[۲۲] Vorlesungen über Zahlentheorie
[۲۳] ideal theory

۳

حساب همنهشتی

پیش‌نگاه

بسیاری از سؤالات حساب به سؤالاتی در مورد باقیمانده‌ها تحویل می‌شود که می‌توان به روشی دستگاه‌مند به آنها پاسخ داد. برای هر عدد صحیح مانند $n > ۱$، حسابی موسوم به پیمانهٔ n[۱] وجود دارد که بازتابی از حساب معمولی است اما به شکل متناهی، چون فقط با n باقیماندهٔ ۰، ۱، ۲، ...، $n - ۱$ که در تقسیم بر n ظاهر می‌شوند سر و کار دارد. حساب به پیمانهٔ n یا حساب همنهشتی[۲] موضوع فصل حاضر است.

اجازه دهید شما را توسط یکی از مسائل معروف قدیمی به این بحث دعوت کنیم: آزمون تقسیم‌پذیری بر ۹ به وسیلهٔ نُه نُه کنار گذاشتن[۳]. این مطلب توسط حساب $+$، $-$ و $\times$ به پیمانهٔ ۹ شرح داده می‌شود و به طور طبیعی به $+$، $-$ و $\times$ به پیمانهٔ n و مسألهٔ تقسیم کردن به پیمانهٔ n منجر می‌گردد. در می‌یابیم که تقسیم کردن (بر اعداد غیر صفر) به پیمانهٔ n امکان پذیر است فقط و فقط

---

[۱] modulo n

[۲] congruence arithmetic

[۳] casting out nines

وقتی که n اول باشد، و نه در حالت کلی.

تقسیم کردن بر عددی غیر صفر مانند a به پیمانهٔ n به مسألهٔ یافتن معکوس[۴] a به پیمانهٔ n یعنی یافتن b یی که ab در تقسیم بر n دارای باقیماندهٔ ۱ باشد تحویل می‌شود. این مطلب سرنخ ساده‌ای برای فرآیند استفاده شده در فصل ۲ جهت یافتن m و n ی که $ma + nb = \gcd(a, b)$ (با استفاده از الگوریتم اقلیدسی) می‌باشد.

قضایای کلاسیک فرما، اویلر و ویلسون[۵] که در نظریهٔ اعداد و کاربردهای آن مهم هستند مرتبط با مبحث تقسیم کردن می‌باشند. معروف‌ترین کاربرد، یعنی دستگاه رمزنگاری RSA، در فصل بعد مورد بحث قرار می‌گیرد اما در فصل حاضر راه را برای آن هموار می‌کنیم.

همچنین با استفاده از حساب همنهشتی، راه را برای مطالعهٔ صورتهای مربعی $ax^۲ + bxy + cy^۲$ هموار خواهیم ساخت تا نشان دهیم برخی مقادیر مشخص را نمی‌توان به صورتهایی مانند $x^۲ + y^۲$، $x^۲ + ۲y^۲$ و $x^۲ + ۳y^۲$ نوشت.

۱.۳ همنهشتی به پیمانه یک عدد صحیح

نه نه کنار گذاشتن

قاعده‌ای قدیمی برای این که بررسی کنیم عددی طبیعی بر ۹ بخش پذیر است یا نه این است که ببینیم مجموع ارقام آن بر ۹ بخش پذیر است یا نه. مثلاً ۷۷۴ بر ۹ بخش پذیر است چون

$$۷ + ۷ + ۴ = ۱۸$$

چنین است.

---

[۴] inverse
[۵] Wilson

این قاعده که نُه نُه کنار گذاشتن نامیده می‌شود، نه تنها در مورد تقسیم‌پذیری تصمیم می‌گیرد بلکه در حقیقت باقیماندهٔ تقسیم بر ۹ را نیز می‌دهد. مثلاً اگر ارقام ۴۷۶ را جمع کنیم داریم

$$۴ + ۷ + ٦ = ۱۷$$

که در تقسیم بر ۹ باقیماندهٔ ۸ دارد. این عدد همان باقیماندهٔ تقسیم ۴۷۶ بر ۹ است.

البته ۴۷۶ به جای $٦ + ۷ + ۴$ نمی نشیند بلکه به جای

$$۴ \times ۱۰^{۲} + ۷ \times ۱۰ + ٦$$

قرار می‌گیرد. اما از آنجایی که باقیمانده‌ها مد نظر هستند، به طریقی $٦ + ۷ + ۴$ شبیه $٦ + ۱۰ \times ۷ + ۱۰^{۲} \times ۴$ رفتار می‌کند.

برای آن که شرح دهیم چگونه چنین چیزی اتفاق می‌افتد مفهوم همنهشتی را معرفی می‌کنیم.

تعریف. اعداد صحیح a و b را همنهشت به پیمانهٔ n[۶] می‌نامیم و می‌نویسیم

$$a \equiv_n b$$

هرگاه در تقسیم بر n باقیماندهٔ یکسانی داشته باشند. به طور معادل، a با b به پیمانهٔ n همنهشت است هرگاه n عدد $a - b$ را عاد کند.

نیز در این حالت می‌گوییم که a و b متعلق به یک ردهٔ همنهشتی[۷] به پیمانهٔ n هستند.

همنهشتی به پیمانهٔ ۲ آشناترین نوع همنهشتی در زندگی روزمره است[۸] که در آن برای اعداد همنهشت با ۰، همنهشت با ۱ و اعدادی که در یک ردهٔ

---

[۶] congruent mod n

[۷] congruence class

[۸] نمونه‌ای دیگر از همنهشتی در زندگی روزمره، همنهشتی به پیمانهٔ ۱۲ یا ۲۴ است که برای ساعت به کار می‌رود. (م)

همنهشتی قرار دارند به ترتیب، کلمات زوج[۹]، فرد[۱۰] و با زوجیت یکسان[۱۱] را به کار می‌بریم.

همنهشتی به پیمانهٔ ۲ در نماد اعشاری به سادگی درک می‌شود. همچنین در مورد پیمانه‌های ۵ و ۱۰ نیز همین امر صورت می‌پذیرد. مثلاً می‌توانیم بلادرنگ بگوییم که **۱۲۴۴۷۸۸** زوج است، **۱۲۴۴۷۸۵** مضرب ۵ است و **۱۲۴۴۷۸۰** مضرب ۱۰ می‌باشد. این مطلب بدان دلیل است که دو عدد با یکدیگر به پیمانهٔ ۲، ۵ یا ۱۰ همنهشت هستند هرگاه ارقام آخر آنها[۱۲] به ترتیب به پیمانهٔ ۲، ۵ یا ۱۰ همنهشت باشند.

به طور مشابه می‌توانیم با نگاه کردن به دو رقم آخر بگوییم که دو عدد به پیمانهٔ ۴ همنهشت هستند یا نه. و نتایجی مشابه را می‌توان برای همنهشتی به پیمانهٔ حاصل ضربهای دیگر ۲ و ۵ به کار برد.

اما همنهشتی به پیمانهٔ ۹ که مفهومی مرتبط با نُه نُه کنار گذاشتن است به سادگی قابل درک نیست. بدین منظور به حساب همنهشتی احتیاج داریم.

تمرینها

قاعده‌هایی که برای تشخیص همنهشتیهای به پیمانهٔ ۲، ۵ و ۱۰ در بالا ارائه شد به سادگی قابل شرح و تعمیم است.

۱.۱.۳ شرح دهید که چرا باقیماندهٔ تقسیم هر عددی بر ۲ با باقیماندهٔ تقسیم رقم آخر آن بر ۲ یکی است.

۲.۱.۳ چرا همین قاعده را می‌توان برای تقسیم کردن بر ۵ و ۱۰ نیز به کار برد اما برای ۴ نه؟

---

[۹] even

[۱۰] odd

[۱۱] with the same parity

[۱۲] منظور رقم یکان است. (م)

۳.۱.۳ نشان دهید که باقیماندهٔ تقسیم n بر ۴ با باقیماندهٔ تقسیم دو رقم آخر n بر ۴ یکی است.

۴.۱.۳ چند رقم آخر، باقیماندهٔ تقسیم بر ۸ و ۱۶ را تعیین می‌کنند؟

۲.۳ رده‌های همنهشتی و حساب آنها

اعداد صحیحی که دارای باقیماندهٔ a در تقسیم بر n هستند مجموعهٔ

$$\{nk + a : k \in \mathbb{Z}\}$$

را تشکیل می‌دهند که ردهٔ همنهشتی a به پیمانهٔ n نامیده می‌شود و به طور طبیعی آن را با نماد $n\mathbb{Z}+a$ (یا وقتی که $a = ۰$، صرفاً با نماد $n\mathbb{Z}$) نمایش می‌دهیم. مثلاً

$$\begin{aligned} ۲\mathbb{Z} &= \{\text{اعداد زوج}\}, \\ ۲\mathbb{Z}+۱ &= \{\text{اعداد فرد}\}. \end{aligned}$$

هر ردهٔ همنهشتی مجموعه‌ای از نقاط متساوی‌الفاصله در خط اعداد است. مثلاً رده‌های ۳$\mathbb{Z}$، ۳$\mathbb{Z}$+۱ و ۳$\mathbb{Z}$+۲ به ترتیب، نقاط سفید، خاکستری و سیاه شکل ۱.۳ هستند.

شکل ۱.۳: رده‌های همنهشتی به پیمانهٔ ۳

از چنین شکلهایی برداشت می‌شود که اگر هر نقطه از $n\mathbb{Z}+a$ را به هر نقطه از $n\mathbb{Z}+b$ بیفزاییم، نقطه‌ای در $n\mathbb{Z}+(a+b)$ داریم. نیز می‌توانیم این مطلب را به طور جبری ببینیم: هر نقطه از $n\mathbb{Z}+a$ به صورت $nk+a$ و هر نقطه از $n\mathbb{Z}+b$ به

صورت $n\ell + b$ است. لذا جمع آنها، یعنی $n(k+\ell) + (a+b)$، در $n\mathbb{Z}+(a+b)$ می‌باشد.

بنابراین، تعریف جمع رده‌های همنهشتی توسط

$$(n\mathbb{Z} + a) + (n\mathbb{Z} + b) = n\mathbb{Z} + (a + b)$$

معنی دارد، چون هرگاه عنصری از ردهٔ a را با عنصری از ردهٔ b جمع کنیم در ردهٔ $a + b$ خواهیم بود. به طور مشابه، تعریف تفاضل رده‌های همنهشتی توسط

$$(n\mathbb{Z} + a) - (n\mathbb{Z} + b) = n\mathbb{Z} + (a - b)$$

معنی دارد.

نهایتاً حاصل ضرب رده‌های همنهشتی را که توسط

$$(n\mathbb{Z} + a)(n\mathbb{Z} + b) = n\mathbb{Z} + ab$$

تعریف می‌شود داریم، گرچه خیلی بدیهی نیست که هر عضو $n\mathbb{Z}+a$ ضربدر هر عضو $n\mathbb{Z}+b$ عضوی از $n\mathbb{Z}+ab$ می‌باشد. برای این که ببینیم چرا، عضو دلخواه $nk + a$ را از $n\mathbb{Z}+a$ و عضو دلخواه $n\ell + b$ را از $n\mathbb{Z}+b$ اختیار می‌کنیم. حاصل ضرب آنها عبارت است از

$$\begin{aligned}(nk + a)(n\ell + b) &= n^۲k\ell + nkb + n\ell a + ab \\ &= n(nk\ell + kb + \ell a) + ab,\end{aligned}$$

که در حقیقت عضوی از $n\mathbb{Z}+ab$ است.

طریقهٔ دیگری برای رفتار کردن در مورد جمع رده‌های همنهشتی جمع کردن همنهشتیها می‌باشد. اگر همنهشتیهای

$$a_۱ \equiv_n a_۲ \qquad (۱)$$

و

$$b_۱ \equiv_n b_۲ \qquad (۲)$$

را داشته باشیم آنگاه (۱) می‌گوید که $a_۱$ و $a_۲$ در یک ردهٔ همنهشتی، که آن را با $n\mathbb{Z}+a$ نشان می‌دهیم، قرار دارند و (۲) می‌گوید که $b_۱$ و $b_۲$ در یک ردهٔ همنهشتی، که آن را با $n\mathbb{Z}+b$ نشان می‌دهیم، هستند. در این صورت نتیجه می‌شود که مجموعهای $a_۱+b_۱$ و $a_۲+b_۲$ نیز به یک ردهٔ همنهشتی، یعنی $n\mathbb{Z}+(a+b)$ تعلق دارند. از این رو

$$a_۱+b_۱\equiv_n a_۲+b_۲ \qquad (۳)$$

همنهشتی (۳) نتیجهٔ جمع کردن همنهشتیهای (۱) و (۲) است.

به طور مشابه می‌توانیم با کم کردن و ضرب کردن رده‌های همنهشتی نشان دهیم که (۱) و (۲) ایجاب می‌کنند

$$a_۱-b_۱\equiv_n a_۲-b_۲ \qquad (۴)$$

(کم کردن همنهشتیها) و

$$a_۱b_۱\equiv_n a_۲b_۲ \qquad (۵)$$

(ضرب کردن همنهشتیها).

تبصره. دستگاه رده‌های همنهشتی به پیمانهٔ n تحت اعمال $+$ و $\times$ با $\frac{\mathbb{Z}}{n\mathbb{Z}}$ نمایش داده می‌شود. این مطلب با نماد خارج قسمتی برای گروهها تطابق دارد (اصول جبر، بخش ۸.۷ را ببینید)، چون $n\mathbb{Z}$ زیرگروهی از $\mathbb{Z}$ است و رده‌های همنهشتی $n\mathbb{Z}+a$ همرده‌های $n\mathbb{Z}$ در $\mathbb{Z}$ هستند. اما در این کتاب $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ساختار اضافی دیگری دارد که توسط $\times$ ارائه می‌شود.

مجدداً نه نه کنار گذاشتن

با استفاده از حساب به پیمانهٔ ۹ می‌توانیم روش نُه نُه کنار گذاشتن را که در بخش ۱.۳ معرفی شد شرح دهیم.

در ابتدا توجه کنید که

$$10 \equiv_9 1$$

و بنابراین

$$10^2 \equiv_9 1^2 \equiv_9 1$$
$$10^3 \equiv_9 1^3 \equiv_9 1$$

و به همین ترتیب با ضرب کردن همنهشتیها توانهای بعدی ۱۰ نیز به پیمانهٔ ۹ به دست می‌آید.

برای هر عدد صحیح مانند a_i با ضرب کردن همنهشتیها نتیجه می‌شود که

$$a_i 10^i \equiv_9 a_i$$

و نهایتاً با جمع کردن همنهشتیها نتیجه می‌شود که

$$a_k 10^k + \ldots + a_1 10 + a_0 \equiv_9 a_k + \ldots + a_1 + a_0 \qquad (*)$$

اما اگر a_0، a_1، ...، a_k از ۰ تا ۹ (یعنی ارقام اعشاری) باشند آنگاه $a_k 10^k + \ldots + a_1 10 + a_0$ عددی است که نمایش اعشاری آن $a_k \ldots a_1 a_0$ است.

لذا $(*)$ می‌گوید که باقیماندهٔ تقسیم $a_k \ldots a_1 a_0$ بر ۹ با باقیماندهٔ تقسیم $a_k + \ldots + a_1 + a_0$ بر ۹ یکی است. این همان چیزی است که در نه نه کنار گذاشتن انتظارش را داشتیم.

تمرینها

قاعدهٔ دیگری (که می‌توانیم آن را سه سه کنار گذاشتن بنامیم) برای آزمون تقسیم‌پذیری بر ۳ و قاعدهٔ بسیار مشابهی برای آزمون تقسیم‌پذیری بر ۱۱ وجود دارد.

۱.۲.۳ نشان دهید که استدلال فوق را می‌توان برای اثبات

$$a_k 10^k + \ldots + a_1 10 + a_0) \equiv_3 a_k + \ldots + a_1 + a_0$$

به کار برد و از آن نتیجه بگیرید که یک عدد بر ۳ بخش پذیر است فقط و فقط وقتی که مجموع ارقام آن بر ۳ بخش پذیر باشد.

۲.۲.۳ از $10 \equiv_{11} -1$ استفاده کنید تا همنهشتهای 10^2، 10^3، ... را به پیمانهٔ ۱۱ بیابید.

۳.۲.۳ از تمرین ۲.۲.۳ با استفاده از ضرب کردن همنهشتیها نتیجه بگیرید که $a_k a_{k-1} \ldots a_1 a_0$ بر ۱۱ بخش پذیر است فقط و فقط وقتی که مجموع متناوب[13] ارقام آن یعنی $(-1)^k a_k + \ldots + a_2 - a_1 + a_0$ بر ۱۱ بخش پذیر باشد.

۳.۳ معکوس به پیمانه یک عدد اول

در $\mathbb{Z}$ معادلهٔ $ab = 1$ فقط دو جواب دارد: $a, b = 1$ و $a, b = -1$. روش دیگر بیان این مطلب این است که ۱ و ۱− تنها اعداد صحیحی هستند که معکوس دارند. این وضعیت برای حساب به پیمانهٔ p برای p یی اول، جالب‌تر است. در این حالت، اگر $a \not\equiv_p 0$ آنگاه عددی مانند b موجود است که

$$ab \equiv_p 1.$$

و لذا می‌توان گفت که هر $a \not\equiv_p 0$ معکوس ضربی به پیمانهٔ p دارد.

مثال. $p = 5$.

۱ معکوس ۱ دارد، ۲ معکوس ۳ دارد، ۳ معکوس ۲ دارد و ۴ معکوس ۴ دارد.

---

[13] alternating sum

شرط $a \not\equiv_p \circ$ بدین معنی است که p عدد a را عاد نمی‌کند. چون p اول است نتیجه می‌شود که $\gcd(a,p) = ۱$. بنابر بخش ۳.۲ این مطلب نتیجه می‌دهد اعدادی مانند m و n در $\mathbb{Z}$ موجودند که

$$ma + np = ۱.$$

به بیان دیگر،

$$ma \equiv_p ۱.$$

لذا m معکوس a به پیمانهٔ p است. □

لذا می‌توانیم معکوس m برای a را از محاسباتی (مبتنی بر الگوریتم اقلیدسی) که $\gcd(a,b)$ را به صورت $ma + nb$ بیان می‌کند بیابیم. نتیجه می‌شود که محاسبهٔ معکوس به پیمانهٔ p سریع است – حدود n گام برای یک عدد n رقمی به پیمانهٔ p لازم دارد.

گروهها

وجود معکوس برای همهٔ رده‌های همنهشتی غیر صفر به پیمانهٔ p ایجاب می‌کند که این رده‌های همنهشتی یک گروه تشکیل می‌دهند. این مفهومی است که در بخش ۳.۱ به اختصار مورد تذکر واقع شد و اکنون آن را بازنگری می‌کنیم.

یک گروه مانند G، مجموعه‌ای با یک عمل روی آن موسوم به عمل گروه[۱۴] همراه با خواص شرکتپذیری، عضو همانی و معکوس می‌باشد. اگر عمل گروه به صورت ضرب نوشته شود، آنگاه عنصر همانی با نماد ۱ و معکوس $g \in G$ به صورت $g^{-۱}$ نوشته می‌شود و این سه خاصیت عبارتند از:

$$g_۱(g_۲g_۳) = (g_۱g_۲)g_۳ \qquad \text{(شرکتپذیری)}$$

[۱۴] group operation

$$g\text{۱} = \text{۱}g = g \qquad \text{(خاصیت همانی)}$$
$$gg^{-\text{۱}} = g^{-\text{۱}}g = \text{۱} \qquad \text{(خاصیت معکوس)}$$

حال می‌توانیم به طور صوری تأیید کنیم که رده‌های همنهشتی غیر صفر به پیمانهٔ p تحت ضرب یک گروه تشکیل می‌دهند. این گروه را $(\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times}$ می‌نامیم.

خواص گروه $(\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times}$. برای یک عدد اول مانند p، رده‌های همنهشتی غیر صفر به پیمانهٔ p تحت ضرب یک گروه تشکیل می‌دهند.

برهان. ابتدا توجه کنید که ضرب رده‌های همنهشتی، شرکتپذیری را از شرکتپذیری ضرب $\mathbb{Z}$ به صورت زیر به ارث می‌برد:

$$\begin{aligned} & \text{ردهٔ } a \times (\text{ردهٔ } b \times \text{ردهٔ } c) \\ = \; & \text{ردهٔ } a(bc) \\ = \; & \text{ردهٔ } (ab)c \\ = \; & (\text{ردهٔ } a \times \text{ردهٔ } b) \times \text{ردهٔ } c. \end{aligned}$$

نتیجه می‌شود که حاصل ضرب رده‌های همنهشتی غیر صفر به پیمانهٔ p خود غیر صفر است. اگر $ab \equiv_p \circ$ و طرفین را در c که معکوس b است ضرب کنیم، بنابر ضرب همنهشتیها داریم $(ab)c \equiv_p \circ c \equiv_p \circ$. از این رو سمت راست یعنی $\circ$ با سمت چپ یعنی

$$\begin{aligned} (ab)c & \equiv_p a(bc) \\ & \equiv_p a(\text{۱}) \\ & \equiv_p a \end{aligned}$$

همنهشت است. لذا حاصل ضرب تنها هنگامی صفر است که یکی از عاملها صفر باشد، لذا مجموعهٔ رده‌های همنهشتی غیر صفر تحت ضرب به پیمانهٔ p بسته است.

همچنین یک عنصر همانی، یعنی ردهٔ ۱ را داریم و هر عنصر بنابر آنچه گفته شد معکوس دارد. لذا $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ همهٔ خواص یک گروه را دارد. □
$(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ خاصیت اضافی

$$g_۱g_۲ = g_۲g_۱$$

را دارد که مشخص سازندهٔ گروههای آبلی است.

اکثر گروههای این کتاب آبلی هستند، اما اولین قضیه‌ای که استفاده می‌کنیم – قضیهٔ لاگرانژ[۱۵] – به سادگی در حالت کلی اثبات می‌شود. این برهان مبتنی بر مفهوم زیرگروه[۱۶] و همرده[۱۷] می‌باشد.

یک زیرمجموعه مانند H از G که تحت عمل گروه G، خود یک گروه تشکیل دهد زیرگروهی از G نامیده می‌شود و همرده‌های (چپ) H در G مجموعه‌هایی به صورت

$$gH = \{gh : h \in H\}$$

برای هر $g \in G$ می‌باشند. $g_۱$ و $g_۲$ ی متمایز در G لزوماً همرده‌های متمایزی را تولید نمی‌کنند. مثلاً برای $h_\circ \in H$ داریم $h_\circ H = H$ چون به ازای هر $h \in H$ داریم $h_\circ h \in H$ و بالعکس هر $h_۱ \in H$ به صورت $h_\circ h$ است که $h = h_\circ^{-۱}h_۱ \in H$.

در حقیقت برهانی که می‌خواهیم ارائه دهیم نشان می‌دهد که تعداد همرده‌های gH برای زیرگروهی مانند H از گروهی متناهی مانند G دقیقاً برابر $\frac{|G|}{|H|}$ است که در آن $|G|$ و $|H|$ به ترتیب مرتبهٔ[۱۸] (تعداد عناصر) G و H را نشان می‌دهند.

قضیهٔ لاگرانژ. اگر H زیرگروهی از گروه متناهی G باشد، آنگاه $|H|$ عدد $|G|$ را عاد می‌کند.

---

[۱۵] Lagrange's theorem
[۱۶] subgroup
[۱۷] coset
[۱۸] order

برهان. در ابتدا مشاهده می‌شود که مرتبهٔ هر همرده مانند gH با مرتبهٔ H برابر است؛ نگاشت از H به gH که h رابه gh می‌برد یک به یک است. لذا تعداد اعضای همهٔ همرده‌ها برابر است.

سپس، مشاهده می‌کنیم که هر دو همردهٔ با اشتراک ناتهی، با هم برابرند. اگر $g \in g_1H$ و $g \in g_2H$ آنگاه h_1 و h_2 یی در H موجودند که

$$g = g_1h_1, \qquad g = g_2h_2.$$

و بنابراین $g_1h_1 = g_2h_2$. اگر این عبارت را از راست در h_1^{-1} ضرب کنیم در می‌یابیم که $g_1 = g_2h_2h_1^{-1}$ و لذا

$$g_1H = g_2h_2h_1^{-1}H = g_2(h_2h_1^{-1}H).$$

اما $h_2h_1^{-1} \in H$ و لذا بنابر آنچه قبل از برهان گفته شد داریم $h_2h_1^{-1}H = H$. از این رو همان طور که ادعا کردیم $g_1H = g_2H$.

آنچه گفته شد نشان می‌دهد که اعضای G، که تعداد آنها برابر $|G|$ است، به همرده‌های مجزای gH افراز می‌شوند. و چون همهٔ gH ها دارای مرتبهٔ یکسان یعنی برابر $|H|$ هستند، نتیجه می‌گیریم که $|H|$ باید $|G|$ را عاد کند. □

تمرینها

در بخش بعد، از قضیهٔ لاگرانژ برای اثبات قضیه‌ای معروف در مورد همنهشتی به پیمانهٔ p استفاده می‌کنیم. تمرینهای زیر برای خوانندگانی که هنوز با نظریهٔ گروهها کنار نیامده‌اند، راه را جهت ارائهٔ برهانی سرراست‌تر با استفاده از کمترین اطلاعات برای معکوسها هموار می‌سازند. مفاد این تمرینها حالت خاصی از مثال قبل از برهان قضیهٔ لاگرانژ است - که می‌گفت ضرب کردن یک گروه در یکی از عناصرش، مجدداً همان عناصر را تولید می‌کند.

فرض کنیم که $a \not\equiv_p \circ$، یعنی a مضربی از p نباشد. لذا a معکوسی به پیمانهٔ p دارد. از این موضوع بهره ببرید!

۱.۳.۳ نشان دهید که $ia \equiv_p \circ \Rightarrow i \equiv_p \circ$.

۲.۳.۳ نشان دهید که $ia \equiv_p ja \Rightarrow i \equiv_p j$.

۳.۳.۳ از تمرین ۱.۳.۳ و ۲.۳.۳ نتیجه بگیرید که a، $۲a$، $۳a$، ...، $(p-۱)a$ متمایز و ناهمنهشت با ۰ به پیمانهٔ p هستند. از این رو

$$\{a, ۲a, ۳a, \ldots, (p-۱)a\} \equiv_p \{۱, ۲, ۳, \ldots, p-۱\}.$$

۴.۳.۳ نتیجهٔ تمرین ۳.۳.۳ را در حالت $p = ۷$ و $a = ۲$ تحقیق کنید.

۴.۳ قضیه کوچک فرما

اگر توانهای a، $a^۲$، $a^۳$، $a^۴$ ... از عضو دلخواه غیر صفری مانند a به پیمانهٔ p را تشکیل دهیم، آنگاه نهایتاً مقداری تکراری وجود خواهد داشت[۱۹]، مثلاً

$$a^{m+n} \equiv_p a^m.$$

سپس با ضرب کردن طرفین در معکوس a^m به پیمانهٔ p، داریم

$$a^n \equiv_p ۱.$$

لذا در حقیقت این دنباله از توانها همواره شامل ۱ است. مثلاً اگر قرار دهیم $p = ۵$ و $a = ۲$ و به پیمانهٔ ۵ مقادیر ۲، $۲^۲$، $۲^۳$، $۲^۴$، ... را محاسبه کنیم در

[۱۹] در حقیقت در اینجا داریم از اصل لانه کبوتری (pigeonhole principle) استفاده می‌کنیم. (م)

می‌یابیم که $۲^۴ = ۱۶ \equiv_۵ ۱$. دنبالهٔ توانها همان دنبالهٔ متناهی a، $a^۲$، $a^۳$، $a^۴$، ...، $a^{n-۱}$، ۱ را تا ابد تکرار می‌کند و لذا دوری[20] نامیده می‌شود.

از دیدگاه نظریهٔ گروهها، استدلالی که هم‌اکنون ارائه شد نشان می‌دهد که توانهای یک عنصر غیر صفر به پیمانهٔ p زیرگروهی از گروه $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ را تشکیل می‌دهد. (شرکتپذیری و عضو همانی بدیهی هستند و معکوس a^k عبارت است از a^{n-k}). پس قضیهٔ لاگرانژ را می‌توان به کار برد و این قضیه بیان می‌دارد که چگونه مرتبهٔ این زیرگروه (و لذا کوچک‌ترین توان n که برای آن $a^n \equiv_p ۱$) در ارتباط با p است.

قضیهٔ کوچک فرما. اگر p اول باشد و $a \not\equiv_p ۰$، آنگاه

$$a^{p-۱} \equiv_p ۱.$$

برهان. $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ دارای $p - ۱$ عضو است که رده‌های ۱، ۲، ۳، ...، $p - ۱$ می‌باشند. لذا بنابر قضیهٔ لاگرانژ مرتبهٔ هر زیرگروه $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ عدد $p - ۱$ را عاد می‌کند.

به ویژه، اگر $a \not\equiv_p ۰$ و نیز $n > ۱$ کوچک‌ترین توانی باشد که برای آن $a^n \equiv_p ۱$ آنگاه توانهای ردهٔ a گروهی n عضوی تشکیل می‌دهند و لذا n باید $p - ۱$ را عاد کند.

اما اگر

$$a^n \equiv_p ۱$$

و n عدد $p - ۱$ را عاد کند (مثلاً $p - ۱ = mn$) آنگاه

$$a^{p-۱} \equiv_p a^{mn} \equiv_p (a^n)^m \equiv_p ۱^m \equiv_p ۱. \square$$

---

[20] cyclic

کاربرد: فرمولی برای معکوس به پیمانه p

از قضیهٔ کوچک فرما نتیجه می‌شود که برای هر $a \not\equiv_p ۰$،

$$a^{p-۲}a \equiv_p ۱.$$

از این رو $a^{p-۲}$ معکوس a به پیمانهٔ p است. این نه تنها فرمولی صریح برای معکوس به پیمانهٔ p به دست می‌دهد بلکه روشی کارآمد برای محاسبهٔ آن را نیز ایجاب می‌کند که قابل رقابت با روش الگوریتم اقلیدسی بخش قبل است.

از بخش ۵.۱ می‌دانیم که $a^{p-۲}$ را می‌توان با حدوداً $\log p$ عمل ضرب محاسبه کرد و در اینجا اعدادی که باید ضرب شوند کوچک‌تر یا مساوی p می‌باشند چون داریم به پیمانهٔ p کار می‌کنیم. این مطلب را با یافتن معکوس a به روش بخش قبل مقایسه کنید: در آنجا استفاده از الگوریتم اقلیدسی برای بیان $\gcd(a,b) = ۱$ به صورت $ma + nb$ را به کار می‌بردیم که m را به عنوان معکوس a به پیمانهٔ p به دست می‌داد. این کار حدوداً $\log p$ تقسیم با باقیمانده (به علاوهٔ محاسبه‌های دیگری که زمان تحلیل رفتهٔ کمتری دارد) روی اعداد کوچک‌تر یا مساوی p لازم دارد. از آنجایی که تقسیم کردن حدوداً به همان میزانِ ضرب کردن زمان می‌برد، این دو روش سرعت مشابهی دارند.

ریشه‌های اولیه

کوچک‌ترین عدد صحیح مانند n که $a^n \equiv_p ۱$، مرتبهٔ a در $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ نامیده می‌شود. برهان فوق به ما می‌گوید که مرتبهٔ هر عدد غیر صفر مانند a به پیمانهٔ p مقسوم‌علیهی از $p - ۱$ است. همواره a یی از مرتبهٔ دقیقاً $p - ۱$ وجود دارد که ریشهٔ اولیه‌ای[۲۱] به پیمانهٔ p نامیده می‌شود. وجود آن توسط اویلر حدس زده

[۲۱] primitive root

شد و اولین بار توسط گاوس (۱۸۰۱) اثبات شد. ریشه‌های اولیه در این کتاب نقش مهمی ایفا نمی‌کنند، گرچه گاهی اوقات بر نتایج قابل اثبات توسط ابزارهایی دیگر، صحه می‌گذارند. لذا خواص آنها و برهان وجود آنها برای خواندن این کتاب اساسی نیست، اما در بخش ستاره‌دار انتهای این فصل آمده است.

تمرینها

حال برهان قضیهٔ کوچک فرما را که در مجموعه تمرینهای قبلی شروع شده بود کامل می‌کنیم.

۱.۴.۳ از تمرین ۳.۳.۳ نتیجه بگیرید که

$$a^{p-۱} \times ۱ \times ۲ \times ۳ \times \ldots \times (p-۱) \equiv_p ۱ \times ۲ \times ۳ \times \ldots \times (p-۱).$$

۲.۴.۳ تمرین ۳.۴.۱ ایجاب می‌کند که $a^{p-۱} \equiv_p ۱$. چرا؟

حال چند تمرین ساده در مورد ریشه‌های اولیه.

۳.۴.۳ نشان دهید که ۲ ریشهٔ اولیه‌ای برای ۵ است ولی برای ۷ ریشهٔ اولیه نیست.

۴.۴.۳ ریشهٔ اولیه‌ای برای ۷ بیابید.

۵.۴.۳ با فرض وجود ریشهٔ اولیه برای p نشان دهید که هر مقسوم‌علیه $p-۱$ به عنوان مرتبهٔ عنصری از $(\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times}$ ظاهر می‌شود.

۵.۳ قضایای همنهشتی ویلسون و لاگرانژ

قضیهٔ زیر، کاربرد مفید دیگری از معکوس به پیمانهٔ p است که حاصل ضرب $(p-۱)! = ۱ \times ۲ \times ۳ \times \ldots \times (p-۱)$ را (که در برهانی از قضیهٔ کوچک فرما استفاده می‌شود) محاسبه می‌کند. در بخش ۸.۹ دانستن مقدار $(p-۱)!$ به پیمانهٔ p (هنگامی که به قانون تقابل مربعی می‌رسیم) مفید خواهد بود. این قضیه به ویلسون نسبت داده می‌شود (و شاید در حقیقت توسط ابن هیثم[۲۲] در قرن هجدهم میلادی کشف شده باشد)، اما اولین برهان شناخته شده برای آن منسوب به لاگرانژ است.

قضیهٔ ویلسون. اگر p اول باشد آنگاه $(p-۱)! \equiv_p -۱$.

برهان. در این همنهشتی عوامل ۱، ۲، ۳، …، $p-۱$ همگی به پیمانهٔ p معکوس دارند. از این رو هر یک از آنها توسط معکوس خود حذف می‌شود مگر عواملی که خود معکوس خود هستند.

چنین عوامل خودمعکوسی مانند x عبارتند از ۱ و $p-۱ \equiv_p -۱$ و دیگر غیر از این، عنصر خودمعکوس نداریم. زیرا اگر $x^۲ \equiv_p ۱$ آنگاه داریم

$$x^۲ - ۱ \equiv_p (x-۱)(x+۱) \equiv_p ۰.$$

به بیان دیگر p باید $(x-۱)(x+۱)$ را عاد کند. اما در این صورت بنابر خاصیت مقسوم‌علیه اول، p باید $x-۱$ یا $x+۱$ را عاد کند. از این رو همان طور که ادعا شد

$$x \equiv_p ۱ \qquad \text{یا} \qquad x \equiv_p -۱.$$

لذا $(p-۱)!$ همنهشت با -۱ به پیمانهٔ p است. □

این حقیقت که همنهشتی $x^۲ - ۱ \equiv_p ۰$ حداکثر دو جواب دارد تعمیم مهمی منسوب به لاگرانژ دارد.

---
[۲۲] Ibn al-Haytham

قضیهٔ همنهشتی چندجمله‌ای لاگرانژ. اگر $P(x)$ یک چندجمله‌ای از درجهٔ n با ضرایب صحیح و p عددی اول باشد، آنگاه همنهشتی

$$P(x) \equiv_p 0$$

حداکثر n جواب ناهمنهشت به پیمانهٔ p دارد[۲۳].

برهان. اگر هیچ جوابی موجود نباشد کار تمام است. در غیر این صورت فرض کنیم $P(r) \equiv_p 0$ که در آن

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

و $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$. این نتیجه می‌دهد که

$$\begin{aligned} P(x) &\equiv_p P(x) - P(r) \\ &\equiv_p a_n(x^n - r^n) + a_{n-1}(x^{n-1} - r^{n-1}) + \ldots + a_1(x - r) \\ &\equiv_p (x-r)Q(x) \qquad (*) \end{aligned}$$

که در آن $Q(x)$ یک چندجمله‌ای از درجهٔ $n-1$ است. این چندجمله‌ای با حذف کردن $x-r$ از جملات $x^n - r^n$، $x^{n-1} - r^{n-1}$، ...، $x-r$ با استفاده از اتحاد

$$x^k - r^k = (x-r)(x^{k-1} + x^{k-2}r + \ldots + xr^{k-2} + r^{k-1})$$

به دست می‌آید.

از $(*)$، خاصیت مقسوم‌علیه اول و $P(x) \equiv_p 0$ نتیجه می‌شود که

$$x - r \equiv_p 0 \qquad \text{یا} \qquad Q(x) \equiv_p 0.$$

---

[۲۳] توجه کنید که اگر p اول نباشد چنین حکمی در حالت کلی درست نیست. مثلاً $x^3 \equiv_8 0$ دارای چهار جواب دو به دو ناهمنهشت ۰، ۲، ۴ و ۶ به پیمانهٔ ۸ است. (م)

چون $Q(x)$ از درجهٔ $n-۱$ است، می‌توانیم به استقراء فرض کنیم که همنهشتی $Q(x)\equiv_p ۰$ حداکثر $n-۱$ جواب ناهمنهشت دارد. در این صورت همان طور که انتظارش را داشتیم

$$P(x)\equiv_p (x-r)Q(x)\equiv_p ۰$$

حداکثر n جواب ناهمنهشت دارد که یکی $x=r$ است و بقیه از $Q(x)\equiv_p ۰$ به دست می‌آید. □

دو استفادهٔ مهم از این قضیه، اثبات وجود ریشه‌های اولیه برای p (بخش ۹.۳) و اثبات محک اویلر[۲۴] برای مربعهای کامل به پیمانهٔ p می‌باشد.

تمرینها

قضیهٔ ویلسون واقعاً محکی برای اول بودن یک عدد طبیعی مانند n به دست می‌دهد.

۱.۵.۳ نشان دهید که اگر n اول نباشد، آنگاه n عدد $(n-۱)!$ را عاد می‌کند، یعنی $(n-۱)!\equiv_n ۰$.

۲.۵.۳ از تمرین ۱.۵.۳ نتیجه بگیرید که[۲۵]

$$(n-۱)!\equiv_n -۱ \Leftrightarrow \text{اول است } n$$

۳.۵.۳ بررسی کنید که این محک برای $n=۷$ درست کار می‌کند.

متأسفانه این محک هیچ ارزش عملی برای n های بزرگ (مثلاً ۱۰۰ رقمی) ندارد چون در این حالت هیچ روش امکان پذیری برای محاسبهٔ $(n-۱)!$ به پیمانهٔ n نداریم.

---

[۲۴] Euler's criterion

[۲۵] البته باید حالت استثنایی $n=۱$ را کنار گذاشت. (م)

۶.۳ معکوس به پیمانه یک عدد طبیعی

همیشه درست نیست که یک $a \not\equiv_n ۰$ به پیمانهٔ k معکوس داشته باشد.
مثلاً $۲ \not\equiv_۴ ۰$ اما

$$۲ \times ۲ = ۴ \equiv_۴ ۰.$$

لذا ۲ هیچ معکوسی به پیمانهٔ ۴ ندارد چون اگر چنین می‌بود، می‌توانستیم طرفین

$$۲ \times ۲ \equiv_۴ ۰$$

را در معکوس ۲ ضرب کنیم تا به نتیجهٔ نادرست $۲ \equiv_۴ ۰$ برسیم.

محک برای وجود معکوسی به پیمانهٔ k. یک عدد صحیح مانند a معکوسی به پیمانهٔ k دارد فقط و فقط وقتی که $\gcd(a, k) = ۱$.

برهان. اگر $\gcd(a, k) = ۱$ آنگاه بنابر بخش ۳.۲ اعدادی صحیح مانند m و n موجودند که

$$\gcd(a, k) = ۱ = ma + nk.$$

این مطلب بیان می‌دارد که

$$ma \equiv_k ۱.$$

لذا m معکوسی به پیمانهٔ k برای a است.

بالعکس، اگر m معکوسی برای a به پیمانهٔ k باشد آنگاه

$$ma \equiv_k ۱.$$

از این رو n ی در $\mathbb{Z}$ هست که

$$ma + nk = ۱.$$

این نتیجه می‌دهد که $\gcd(a, k) = ۱$ چون هر مقسوم علیه مشترک a و k، عدد $ma + nk$ که برابر ۱ است را نیز عاد می‌کند. □

اگر a_1 و a_2 به ترتیب دارای معکوسهای m_1 و m_2 به پیمانهٔ k باشند آنگاه a_1a_2 نیز معکوس m_1m_2 دارد. این نتیجه می‌دهد که عناصر معکوس پذیربه پیمانهٔ k مجموعه‌ای بسته تحت ضرب است و لذا یک گروه تشکیل می‌دهند که با $(\frac{\mathbb{Z}}{k\mathbb{Z}})^\times$ نمایش داده می‌شود. (خواص گروهی را می‌توان همانند $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ در بخش ۳.۳ بررسی کرد.)

مثال. $(\frac{\mathbb{Z}}{8\mathbb{Z}})^\times$

۱ معکوس ۱ دارد، ۳ معکوس ۳ دارد، ۵ معکوس $-3 \equiv_8 5$ دارد و ۷ معکوس $-1 \equiv_8 7$ دارد. و می‌توان بررسی کرد که اینها تنها عناصر معکوس پذیرهستند. لذا $(\frac{\mathbb{Z}}{8\mathbb{Z}})^\times$ گروهی آبلی با چهار عنصر است. این گروه دوری نیست چون هر یک از عناصر آن دارای مرتبهٔ کمتر یا مساوی ۲ است.

مرتبهٔ $(\frac{\mathbb{Z}}{k\mathbb{Z}})^\times$، یعنی تعداد عناصر a در بین

$$1, 2, 3, \ldots, k$$

که در شرط $\gcd(a, k) = 1$ صدق می‌کنند، توسط $\varphi(k)$ نمایش داده می‌شود و تابع φ-اویلر نامیده می‌شود. مثلاً $\varphi(8) = 4$ چون چهار عنصر ۱، ۳، ۵، ۷ تنها اعداد طبیعی کوچک‌تر از ۸ هستند که برای آنها $\gcd(a, 8) = 1$.

خواص مشخصی از φ شناخته شده می‌باشند. مثلاً

- برای p ی اول $\varphi(p^i) = p^{i-1}(p-1)$،
- اگر $\gcd(m, n) = 1$ آنگاه $\varphi(mn) = \varphi(m)\varphi(n)$.

اگر تجزیه به اعداد اول را برای k بدانیم آنگاه این خواص، محاسبهٔ $\varphi(k)$ را آسان می‌سازد ولی در غیر این صورت محاسبهٔ آن سخت است.

اگر همان طور که در بخش ۴.۳ برای عنصر a از $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ عمل کردیم قضیهٔ لاگرانژ را برای عنصری مانند a از $(\frac{\mathbb{Z}}{k\mathbb{Z}})^\times$ به کار بریم قضیهٔ زیر را به دست می‌آوریم.

قضیهٔ اویلر. اگر a به پیمانهٔ k معکوس پذیرباشد آنگاه

$$a^{\varphi(k)} \equiv_k ۱.$$

برهان. همان استدلالی را که برای اثبات قضیهٔ کوچک فرما به کار بردیم استفاده می‌کنیم و فقط از این که اندازهٔ گروه $(\frac{\mathbb{Z}}{k\mathbb{Z}})^\times$ برابر $\varphi(k)$ است بهره می‌گیریم. □

مشابه آنچه قضیهٔ کوچک فرما برای حالت $k = p$ عمل می‌کرد، قضیهٔ اویلر نیز فرمولی را برای معکوس a به پیمانهٔ k به صورت $a^{\varphi(k)-۱}$ به دست می‌دهد. این فرمول برای k در حالت کلی چندان صریح نیست چون با تابع φ سر و کار دارد. این مطلب راه محاسبهٔ معکوس به پیمانهٔ k به وسیلهٔ به توان رساندن را می‌بندد زیرا هیچ راه کارآمد شناخته شده‌ای برای محاسبهٔ $\varphi(k)$ وجود ندارد. در حقیقت، سختی محاسبهٔ $\varphi(k)$ مسألهٔ مهمی در امنیت رمزنگاری RSA است که در فصل بعد مورد مطالعه قرار خواهد گرفت.

تمرینها

فرمول $\varphi(p^i) = p^{i-۱}(p-۱)$ (و حالت خاص آن برای $i = ۱$) را می‌توان به صورت زیر اثبات کرد.

۱.۶.۳ توضیح دهید که چرا وقتی p اول است داریم $\varphi(p) = p - ۱$.

۲.۶.۳ نشان دهید که تعداد $p^{i-۱}$ مضرب از مضارب p در بین اعداد ۱، ۲، ۳، ...، p^i وجود دارد.

۳.۶.۳ نتیجه بگیرید که هرگاه p اول باشد داریم $\varphi(p^i) = p^{i-۱}(p-۱)$.

فرمول $\varphi(mn) = \varphi(m)\varphi(n)$ (با شرط $\gcd(m,n) = ۱$) در بخش ۷.۹ اثبات خواهد شد. در حال حاضر صرفاً حالتی ساده را در نظر می‌گیریم.

۴.۶.۳ تحقیق کنید که $\varphi(۱۵) = \varphi(۳)\varphi(۵)$.

۷.۳ معادله‌های دیوفانتی مربعی

رفتار معادله‌های دیوفانتی مربعی پیچیده‌تر از معادله‌های دیوفانتی خطی بحث شده در فصل قبل است. با این حال، همنهشتیها ابزار خوبی برای این است که نشان دهیم اعداد خاصی در معادله‌هایی خاص صدق نمی‌کنند.

مثال ۱. معادلهٔ $x^2 + y^2 = p$ برای p هایی که به صورت $4n + 3$ می‌باشند هیچ جوابی ندارد.

این گزاره معادل این است که $x^2 + y^2 \not\equiv_4 3$ که می‌توانیم آن را با آزمودن مقادیر x و y به پیمانهٔ ۴ (که تعداد آنها متناهی است) اثبات کنیم. این مقادیر عبارتند از $x, y \equiv_4 0, 1, 2, -1$ که برای آنها داریم $x^2, y^2 \equiv_4 0, 1$. بنابراین داریم $x^2 + y^2 \equiv_4 0, 1, 2$ و لذا همان طور که ادعا شد $x^2 + y^2 \not\equiv_4 3$. □

مثال ۲. معادلهٔ $x^2 + 2y^2 = p$ برای p هایی که به صورت $8n + 5$ یا $8n + 7$ هستند هیچ جوابی ندارد.

این گزاره معادل این است که $x^2 + 2y^2 \not\equiv_8 5, 7$ که می‌توانیم آن را با آزمودن مقادیر x و y به پیمانهٔ ۸ (که تعداد آنها متناهی است) اثبات کنیم. این مقادیر عبارتند از $x, y \equiv_8 0, 1, 2, 3, 4, -3, -2, -1$ که برای آنها داریم $x^2, y^2 \equiv_8 0, 1, 4$. بنابراین داریم $x^2 + 2y^2 \equiv_8 0, 1, 2, 3, 4, 6$ و لذا همان طور که ادعا شد $x^2 + 2y^2 \not\equiv_8 5, 7$. □

مثال ۳. معادلهٔ $x^2 + 3y^2 = p$ برای p هایی که به صورت $3n + 2$ هستند هیچ جوابی ندارد.

این گزاره معادل این است که $x^2 + 3y^2 \not\equiv_3 2$ که می‌توانیم آن را با آزمودن مقادیر x و y به پیمانهٔ ۳ (که تعداد آنها متناهی است) اثبات کنیم. این مقادیر عبارتند از $x, y \equiv_3 0, 1, -1$ که برای آنها داریم $x^2, y^2 \equiv_3 0, 1$. بنابراین داریم $x^2 + 3y^2 \equiv_3 0, 1$ و لذا همان طور که ادعا شد $x^2 + 3y^2 \not\equiv_3 2$. □

این سه حکم اولین بار توسط فرما ادعا شد و گرچه با سلاح مرموز خود یعنی روش نزول نامتناهی به نبرد با آنها می‌پرداخت اما به نظر می‌رسد که به

برهانهای سادهٔ همنهشتی برای آنها اشراف داشته است. نزول، توپخانهٔ بسیار سهمگین‌تری است (از آن در بخش ۷.۷ استفاده می‌کنیم) و فرما از آن به شکلی مناسب برای اثبات متممهای سخت‌تری از احکامی که هم‌اکنون اشاره کردیم بهره می‌گرفت. مثلاً در حالی که (بنابر استدلال فوق) $x^۲ + y^۲$ هرگز مقدار اولی به صورت $۴n + ۳$ را نمی‌پذیرد، با این حال هر مقدار اولی به صورت $۴n + ۱$ را اختیار می‌کند.

فرما پس از خواندن تبصره‌ای از دیوفانتوس (حساب، کتاب III، مسألهٔ ۱۹)، به اعداد اول به صورت $x^۲ + y^۲$، $x^۲ + ۲y^۲$ و $x^۲ + ۳y^۲$ علاقه‌مند شد (و ما به همین دلیل از حرف p برای سمت راست معادله‌های بالا استفاده کردیم):

> ۶۵ به طور طبیعی به دو روش به صورت مجموع دو مجذور نوشته می‌شود، یعنی می‌توان آن را به صورت $۴^۲ + ۷^۲$ و $۱^۲ + ۸^۲$ نوشت. عدد ۶۵ این خاصیت خود را مدیون این حقیقت است که حاصل ضرب دو عدد اول ۱۳ و ۵ می‌باشد که هر کدام مجموع دو مجذور هستند.

واضح است که دیوفانتوس از فرمول

$$(a_۱^۲ + b_۱^۲)(a_۲^۲ + b_۲^۲) = (a_۱a_۲ \pm b_۱b_۲)^۲ + (b_۱a_۲ \pm a_۱b_۲)^۲$$

واقف بوده است. این فرمول نشان می‌دهد که حاصل ضرب مجموع دو مجذور در مجموع دو مجذور، خود مجموع دو مجذور است (به دو روش مختلف؛ متناظر با انتخاب علامتهای سمت راست).

فرما آنچه را این مطلب ایجاب می‌کرد دید: این که بدانیم چه اعدادی مجموع دو مجذور هستند وابسته به این است که بدانیم چه اعداد اولی مجموع دو مجذور می‌باشند. استدلال همنهشتی سادهٔ مثال ۱ نشان می‌دهد که اعداد اول به صورت $۴n + ۳$ مجموع دو مجذور نیستند؛ قسمت سخت مسأله این است که نشان دهیم همهٔ اعداد اول به صورت $۴n + ۱$ مجموع دو مجذور هستند. این قضیه به چیزی تماشایی در نظریه اعداد تبدیل می‌گردد که لاگرانژ، گاوس و بقیه با استفاده از آن نوآوریهای خود را به رخ کشیدند. در فصل ۶ برهانی را با

استفاده از اعداد صحیح گاوسی که منسوب به ددکیند است ارائه می‌دهیم.

همچنین این مطلب درست است که اعداد اول به صورت $x^۲ + ۲y^۲$ دقیقاً همان اعدادی هستند که به صورتهای $۸n + ۱$ و $۸n + ۳$ هستند؛ یعنی همان اعدادی که توسط استدلالهای همنهشتی بالا رد نشدند (البته اعدادی که به صورت $۸n + ۲$، $۸n + ۴$ یا $۸n + ٦$ هستند اول نیمی‌باشند چون بر ۲ بخش پذیرند). و به طور مشابه، اعداد اول به صورت $x^۲ + ۳y^۲$ دقیقاً همان اعدادی هستند که به صورت $۳n + ۱$ می‌باشند. این احکام را بعداً با تلفیق نتایج فصل ۷ و فصل ۹ اثبات می‌کنیم.

تمرینها

آزمودن قضیهٔ دو مجذور فرما برای اولین چند عدد اول به صورت $۴n + ۱$ و تحقیق در مورد قضایای متناظر در مورد اعداد اول به صورت $۸n + ۱$، $۸n + ۳$ و $۳n + ۱$ سرگرم کننده است.

۱.۷.۳ اولین ده عدد اول به صورت $۴n + ۱$ را بنویسید و بررسی کنید که همگی آنها مجموع دو مجذور هستند. (اولین آنها $۱^۲ + ۲^۲ = ۵$ است.)

۲.۷.۳ آیا در بین آنها عددی هست که به دو روش متفاوت مجموع دو مجذور باشد؟

۳.۷.۳ اولین ده عدد اول به صورت $۸n + ۱$ یا $۸n + ۳$ را بنویسید و بررسی کنید که همگی آنها به صورت $x^۲ + ۲y^۲$ هستند. (و ببینید که آیا در بین آنها عددی هست که به دو شکل مختلف به این صورت باشد یا نه.)

۴.۷.۳ اولین ده عدد اول به صورت $۳n + ۱$ را بنویسید و بررسی کنید که همگی آنها به صورت $x^۲ + ۳y^۲$ هستند. (و ببینید که آیا در بین آنها عددی هست که به دو شکل مختلف به این صورت باشد یا نه.)

۸.۳ * ریشه‌های اولیه

یک پدیدهٔ جالب و معماگونه در حساب مقدماتی، دورهٔ تناوب نمایش اعشاری[۲۶] کسر $\frac{۱}{n}$ می‌باشد. مثلاً می‌دانیم که

$$\frac{۱}{۳} = ۰/۳۳۳۳\ldots$$
$$\frac{۱}{۷} = ۰/۱۴۲۸۵۷۱۴۲۸۵۷\ldots$$
$$\frac{۱}{۱۳} = ۰/۰۷۶۹۲۳۰۷۶۹۲۳۰\ldots$$

می‌گوییم که طول دورهٔ تناوب[۲۷] کسر $\frac{۱}{۳}$ برابر ۱ است زیرا الگوی ۱ رقمی ۳ تکرار می‌شود؛ طول دورهٔ تناوب $\frac{۱}{۷}$ برابر ٦ است چون الگوی ٦ رقمی ۱۴۲۸۵۷ تکرار می‌شود؛ و به طور مشابه، طول دورهٔ تناوب $\frac{۱}{۱۳}$ برابر ٦ است چون الگوی ٦ رقمی ۰۷٦۹۲۳ تکرار می‌شود. با توجه به فرآیند تقسیم که در مدرسه آموخته‌ایم، روشن است که نهایتاً باید تکرار حاصل شود[۲۸]. لذا وجود تناوب در نمایش اعشاری $\frac{۱}{n}$ تعجب‌آور نیست[۲۹]. اما چرا طول دورهٔ تناوب حداکثر $n - ۱$ است و تحت چه شرایطی این حداکثر اتفاق می‌افتد؟

بخش اصلی پاسخ این است که طول دورهٔ تناوب $n - ۱$ هنگامی اتفاق می‌افتد که ۱۰ دارای مرتبهٔ $n - ۱$ در گروه $(\frac{\mathbb{Z}}{n\mathbb{Z}})^\times$ باشد، یعنی وقتی که $۱۰^{n-۱}$ کوچک‌ترین توان مثبت ۱۰ باشد که همنهشت با ۱ به پیمانهٔ n است. همچنین این شرط را می‌توان به این صورت نیز بیان کرد که ۱۰ باید ریشهٔ اولیه‌ای برای n باشد. در این صورت، نگاه نزدیک‌تری به $(\frac{\mathbb{Z}}{n\mathbb{Z}})^\times$ با استفاده از قضیهٔ اویلر نشان می‌دهد که چرا بیشترین طول دورهٔ تناوب ممکن برابر $n - ۱$ است.

مثال. $\frac{۱}{۷} = ۰/۱۴۲۸۵۷۱۴۲۸۵۷\ldots$.

---

[۲۶] period in the decimal expansion

[۲۷] length of period

[۲۸] چون تعداد باقیمانده‌ها متناهی است و نمی‌توانیم تا ابد باقیمانده‌هایی متفاوت را ببینیم. (م)

[۲۹] همین استدلال را در مورد هر کسری به صورت $\frac{m}{n}$ نیز می‌توان به کار برد. (م)

اگر این تساوی را در ۱۰، ۱۰۲، ۱۰۳، ... ضرب کنیم داریم

$$\begin{aligned}\frac{۱۰}{۷} &= ۱/۴۲۸۵۷۱۴۲۸۵۷\ldots\\ \frac{۱۰^{۲}}{۷} &= ۱۴/۲۸۵۷۱۴۲۸۵۷\ldots\\ &\vdots\\ \frac{۱۰^{٦}}{۷} &= ۱۴۲۸۵۷/۱۴۲۸۵۷\ldots = ۱۴۲۸۵۷+\frac{۱}{۷}.\end{aligned}$$

لذا $۱۰^{٦}$ در تقسیم بر ۷ شبیه $۱ = ۱۰^{۰}$ است و دارای باقیماندهٔ ۱ می‌باشد. همچنین در بین توانهای مثبت ۱۰ با این خاصیت، $۱۰^{٦}$ کوچک‌ترین عدد است (چون $\frac{۱۰^i}{۷}$ برای $i = ۱,۲,۳,۴,۵$ دارای بخش اعشاری متفاوتی است). این دقیقاً بدان معناست که ۱۰ ریشهٔ اولیه‌ای برای ۷ است.

تعمیمی از این استدلال، محک زیر را به دست می‌دهد.

محک برای طول دورهٔ تناوب بیشین. نمایش اعشاری $\frac{۱}{n}$ متناوب با طول $n-۱$ است، دقیقاً وقتی که ۱۰ ریشهٔ اولیه‌ای برای n باشد. همچنین $n-۱$ بیشترین طول دورهٔ تناوب ممکن است و در صورتی اتفاق می‌افتد که n اول باشد[۳۰].

برهان. فرض کنیم $\frac{۱}{n}$ نمایش اعشاری متناوبی با طول $n-۱$ داشته باشد،

$$\frac{۱}{n} = ۰/a_۱a_۲\ldots a_{n-۱}a_۱a_۲\ldots a_{n-۱}\ldots$$

اگر این تساوی را در ۱۰، ۱۰۲، ۱۰۳، ... ضرب کنیم داریم

$$\begin{aligned}\frac{۱۰}{n} &= a_۱/a_۲\ldots a_{n-۱}a_۱a_۲\ldots a_{n-۱}\ldots\\ \frac{۱۰^{۲}}{n} &= a_۱a_۲/\ldots a_{n-۱}a_۱a_۲\ldots a_{n-۱}\ldots\\ &\vdots\\ \frac{۱۰^{n-۱}}{n} &= a_۱a_۲\ldots a_{n-۱}/a_۱a_۲\ldots a_{n-۱}\ldots = a_۱a_۲\ldots a_{n-۱}+\frac{۱}{n}.\end{aligned}$$

[۳۰] البته توجه داریم که برای هر عدد اولی این طول دورهٔ تناوب اتفاق نمی‌افتد. (م)

لذا در بین توانهای مثبت ۱۰، عدد 10^{n-1} کوچک‌ترین عددی است که در تقسیم بر n دارای باقیماندهٔ ۱ می‌باشد (چون $\frac{10^i}{n}$ برای $i < n-1$ دارای بخش اعشاری متفاوتی است). یعنی مرتبهٔ ۱۰ برابر $n-1$ است و لذا ریشهٔ اولیه‌ای برای n می‌باشد.

بالعکس، اگر مرتبهٔ ۱۰ در $(\frac{\mathbb{Z}}{n\mathbb{Z}})^\times$ برابر $n-1$ باشد آنگاه n اول است. این مطلب از برهان قضیهٔ اویلر نتیجه می‌شود که نشان می‌دهد مرتبهٔ هر عضو $(\frac{\mathbb{Z}}{n\mathbb{Z}})^\times$ حداکثر $\varphi(n)$ است. از تعریف تابع φ-اویلر به سادگی نتیجه می‌شود که $\varphi(n) \leq n-1$[31] و تساوی فقط در صورتی برقرار است که n اول باشد.

باقی می‌ماند که نشان دهیم قسمت اعشاری $\frac{1}{n}$ متناوب با طول $n-1$ است هرگاه مرتبهٔ ۱۰ برابر $n-1$ باشد. این مطلب مجدداً با در نظر گرفتن $\frac{1}{n}$، $\frac{10}{n}$، $\frac{10^2}{n}$، ...، $\frac{10^{n-1}}{n}$ نتیجه می‌شود. این فرض که مرتبهٔ ۱۰ برابر $n-1$ است ایجاب می‌کند که 10^{n-1} در تقسیم بر n باقیماندهٔ ۱ داشته باشد و لذا

$$\frac{10^{n-1}}{n} = a_1a_2\dots a_{n-1} + \frac{1}{n} \qquad (*)$$

که در آن $a_1a_2\dots a_{n-1}$ همان $n-1$ رقم بعد از اعشار $\frac{1}{n}$ است. از تقسیم کردن دو طرف بر 10^{n-1} نتیجه می‌شود که

$$\frac{1}{n} = 0/a_1a_2\dots a_{n-1}\dots a_1a_2\dots a_{n-1}\dots \qquad (**)$$

گرچه واضح نیست که پس از اولین $2(n-1)$ رقم در سمت راست تساوی چه اتفاقی می‌افتد. مجدداً با جایگذاری (**) در (*) و تقسیم کردن بر 10^{n-1} می‌بینیم که دنبالهٔ $a_1a_2\dots a_{n-1}$ تکرار در اعشار $\frac{1}{n}$ را حفظ می‌کند. این دنباله نشان می‌دهد که طول دورهٔ تناوب $\frac{1}{n}$ برابر $n-1$ است چون اگر دورهٔ تناوبی با طول کوچک‌تر مانند k موجود می‌بود می‌توانستیم همانند استدلال بالا نتیجه

[31] بدیهی است که n باید بزرگ‌تر از ۱ باشد. در این صورت می‌دانیم که در بین اعداد ۱، ۲، ...، n خود عدد n نسبت به n اول نیست و لذا تعداد اعدادی که نسبت به n اول هستند و کوچک‌تر یا مساوی n می‌باشند حداکثر $n-1$ است. (م)

بگیریم که مرتبهٔ ۱۰ برابر k است که کوچک‌تر از $n-1$ می‌باشد و با فرض ما در تناقض است. □

در تمرینهای زیر از شما خواسته شده است که عددی اول مانند $p > 7$ را بیابید که ۱۰ ریشهٔ اولیه‌ای برای آن باشد و در نتیجه $\frac{1}{p}$ دارای طول دورهٔ تناوب $p-1$ باشد. در سال ۱۸۰۱ گاوس حدس زد که بیشترین طول دورهٔ تناوب، یعنی $p-1$ برای تعدادی نامتناهی عدد اول مانند p اتفاق می‌افتد اما هنوز نمی‌دانیم که این مطلب درست است یا نه. در حقیقت نمی‌دانیم که آیا هر عدد مشخص مانند ۲ یا ۳ ریشهٔ اولیهٔ تعدادی نامتناهی p است یا نه. با این حال می‌دانیم که هر عدد اول مانند p ریشهٔ اولیه دارد. برهانی از این قضیه را در بخش بعد ارائه می‌دهیم.

تمرینها

نمایش اعشاری $\frac{1}{n}$ هنگامی که n اول نباشد لزوماً متناوب نیست. مثلاً $\frac{1}{6} = 0/1666\ldots$. نمایش اعشاری اخیر نهایتاً متناوب[۳۲] نامیده می‌شود چون پس از ارقامی مشخص، متناوب است (در این مثال، بعد از اولین رقم).

۱.۸.۳ نمایشهای اعشاری $\frac{1}{12}$ و $\frac{1}{14}$ را محاسبه کنید و تحقیق کنید که نهایتاً متناوب هستند.

۲.۸.۳ در حالت کلی شرح دهیم که چرا $\frac{1}{n}$ نمایش اعشاری نهایتاً متناوب دارد.

ارتباط بین نمایشهای اعشاری و توانهای ۱۰ به ما این امکان را می‌دهد که خواص نمایش اعشاری $\frac{1}{n}$ را برای پیشگویی خواص توانهای ۱۰ به پیمانهٔ n و بالعکس، استفاده کنیم.

---
[۳۲] ultimately periodic

۳۸.۳ بدون استفاده از اعشار $\frac{۱}{۱۳}$ نشان دهید که مرتبهٔ ۱۰ در $(\frac{\mathbb{Z}}{۱۳\mathbb{Z}})^{\times}$ برابر ۶ است.

۴۸.۳ اولین عدد اول p بزرگ‌تر از ۷ که ۱۰ ریشهٔ اولیه‌ای برای آن است چند است؟ تحقیق کنید که طول دورهٔ تناوب اعشار $\frac{۱}{p}$ برابر $p-۱$ است.

۹.۳ * وجود ریشه‌های اولیه

وجود ریشهٔ اولیه برای p قضیه‌ای زیرکانه است زیرا هیچ روش جامعی برای مشخص کردن ریشهٔ اولیه به عنوان تابعی از p نمی‌شناسیم. مثلاً به نظر می‌رسد که کوچک‌ترین ریشهٔ اولیه به شکلی بسیار نامنظم بر حسب p تغییر می‌کند. همهٔ برهانهای شناخته شده حول این مسأله می‌گردند که فقط وجود ریشهٔ اولیه برای p را بدون سعی در یافتن آن نشان دهند.

این برهانها از قضیهٔ همنهشتی چندجمله‌ای لاگرانژ در بخش ۵.۳، که می‌گوید تعداد جوابهای یک همنهشتی درجهٔ n کمتر یا مساوی n می‌باشد، استفاده می‌کنند. این قضیه استفاده می‌شود تا نشان داده شود که وقتی n کمتر از $p-۱$ باشد، همنهشتیهای $x^n \equiv_p ۱$ آن قدر کم جواب دارند که نمی‌توانند شامل همهٔ $p-۱$ عدد ناهمنهشت ۱، ۲، ۳، ...، $p-۱$ باشند. لذا حداقل یکی از این اعداد فقط در $x^{p-۱} \equiv_p ۱$ صدق می‌کند و از این رو یک ریشهٔ اولیه است.

همراه این قضیه از قضیهٔ کوچک فرما در بخش ۴.۳ استفاده می‌کنیم. این قضیه نشان می‌دهد که هر $a \not\equiv_p ۰$ در یک همنهشتی مانند $x^n \equiv_p ۱$، که در آن n عددی طبیعی و مقسوم‌علیهی از $p-۱$ است، صدق می‌کند. این مطلب حکم زیر را در مورد تعداد جوابهای $x^n \equiv_p ۱$ به دست می‌دهد.

جوابهای $x^n \equiv_p ۱$. تعداد جوابهای همنهشتی $x^n \equiv_p ۱$ که جواب همنهشتی $x^m \equiv_p ۱$ برای m ی کوچک‌تر از n نباشد حداکثر $\varphi(n)$ است.

برهان. اگر a در $x^n \equiv_p ۱$ صدق کند ولی در هیچ همنهشتی مانند $x^m \equiv_p ۱$

از درجه‌ای کوچک‌تر صدق نکند آنگاه a از مرتبهٔ n است. در این صورت ۱، a، $a^۲$، ...، $a^{n-۱}$ همگی جوابهای متمایز $x^n \equiv_p ۱$ می‌باشند و لذا بنابر قضیهٔ همنهشتی چندجمله‌ای لاگرانژ، تنها جوابهای $x^n \equiv_p ۱$ هستند.

به علاوه یک توان از a مانند a^i، که $\gcd(i,n) > ۱$، در همنهشتی از درجهٔ کمتر $x^{\frac{n}{\gcd(i,n)}} \equiv_p ۱$ صدق می‌کند. لذا تعداد جوابهای $x^n \equiv_p ۱$ که در همنهشتیهای با درجهٔ کمتر مانند $x^m \equiv_p ۱$ صدق نمی‌کنند حداکثر برابر تعداد i هایی است که نسبت به n اول هستند؛ یعنی برابر $\varphi(n)$. □

نهایتاً برای اثبات وجود ریشه‌های اولیه از حکم فوق استفاده می‌کنیم تا نشان دهیم که تعداد عناصر از مرتبهٔ کمتر از $p-۱$ کافی نیست تا کل اعداد ۱، ۲، ۳، ...، $p-۱$ را پوشش دهد و لذا عنصری از مرتبهٔ $p-۱$ وجود خواهد داشت. برای مختصر کردن نمادگذاری به جای عبارت a عدد b را عاد می کند می‌نویسیم $a|b$.

وجود ریشه‌های اولیه. در بین اعداد ۱، ۲، ۳، ...، $p-۱$ تعداد آنهایی که مرتبهٔ کمتر از $p-۱$ دارند کمتر از $p-۱$ تا است و لذا یکی از این اعداد ریشهٔ اولیه است.

برهان. بنابر حکم قبلی تعداد کل عناصر از مرتبهٔ کمتر از $p-۱$ بیشتر از

$$\sum_{n|p-۱, n\neq p-۱} \varphi(n)$$

نیست. اگر اثبات کنیم که

$$\sum_{n|p-۱} \varphi(n) = p-۱,$$

آنگاه نتیجه می‌شود که تعداد عناصر از مرتبهٔ کمتر از $p-۱$ کمتر از $p-۱$ تا است.

در حقیقت برای هر عدد طبیعی مانند N داریم

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

برای این که دلیل این امر را بدانید کسرهای $\frac{1}{N}$، $\frac{2}{N}$، …، $\frac{N}{N}$ را در نظر بگیرید. هر یک از این کسرها صورت تحویل‌یافته‌ای مانند $\frac{n'}{n}$ دارد که از تقسیم کردن صورت و مخرج بر ب.م.م. حاصل می‌شود و $\gcd(n', n) = 1$. برای هر مقسوم‌علیه n از N تعداد کسرهای تحویل‌یافته مانند $\frac{n'}{n}$ برابر $\varphi(n)$ است و کسرهای متمایز $\frac{i}{N}$ و $\frac{j}{N}$ صورتهای تحویل‌یافتهٔ متمایز دارند. بنابراین همان گونه که انتظار داشتیم

$$N = \sum_{n|N} \varphi(n). \ \square$$

تمرینها

در اینجا روش دیگری برای اثبات وجود ریشه‌های اولیه را می‌بینیم که مجدداً از قضیهٔ همنهشتی چندجمله‌ای لاگرانژ استفاده می‌کند.

۱.۹.۳ فرض کنیم که عناصر غیر صفر به پیمانهٔ p حداکثر از درجهٔ n باشند که n کمتر از $p - 1$ است. نشان دهید این مطلب ایجاب می‌کند که برای هر x ناصفر به پیمانهٔ p داشته باشیم $x^n \equiv_p 1$ که در تناقض با قضیهٔ چندجمله‌ای لاگرانژ است.

۱۰.۳ بحث

مفهوم همنهشتی توسط گاوس (۱۸۰۱) معرفی شد. او اولین کسی بود که ارزش آن را در ساده کردن استدلالهای مربوط به تقسیم با باقیمانده (همانند قضیهٔ کوچک فرما و ویلسون) تشخیص داد. مثلاً به جای آن که بگوییم p عدد

a^{p-1} را با باقیماندهٔ ۱ عاد می‌کند می‌توانیم بنویسیم $a^{p-1} \equiv_p 1$ که شبیه یک معادله به نظر رسیده و رفتار می‌کند.

در حقیقت مفهوم ردهٔ همنهشتی که توسط ددکیند (۱۸۵۷) معرفی شد به همنهشتی

$$a \equiv_n b$$

اجازه می‌دهد که توسط معادلهٔ واقعی

$$n\mathbb{Z} + a = n\mathbb{Z} + b$$

بین اشیاء $n\mathbb{Z} + a = \{nk + a : k \in \mathbb{Z}\}$ و $n\mathbb{Z} + b = \{nk + b : k \in \mathbb{Z}\}$ که از قواعد حساب تبعیت می‌کند جایگزین گردد. این مطلب گرچه جلوتر از زمان خود بود با این حال گام مهمی در جهت تفکر جبری مدرن بود. تا قرن بیستم ریاضیدانان اندکی استفاده از مجموعه‌ها را به عنوان اشیائی ریاضی پذیرفته بودند.

قضیهٔ کوچک فرما، که از حالت خاص $2^{p-1} \equiv_p 1$ نشأت گرفت، توسط فرما در تحقیقاتی پیرامون اعداد تام و اعداد اولِ به صورت $2^p - 1$ کشف شد. وی در واقع این قضیه را به صورت $2^p \equiv_p 2$ بیان کرد و آن را با استفاده از خواص ضرایب دوجمله‌ای اثبات کرد. فرما نه از قضیهٔ دوجمله‌ای مدرن، یعنی

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \ldots + \binom{p}{p-1} ab^{p-1} + b^p$$

استفاده کرد و نه از فرمول

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

گرچه برهان مشابهی را از این دو می‌توان نتیجه گرفت. به سادگی می‌توان توجه کرد که

- برای $k \neq 1$ و عدد اول p، عامل اول p در صورت کسر $\binom{p}{k}$ ظاهر می‌شود ولی در مخرج آن نمی‌آید. از این رو p عدد $\binom{p}{k}$ را عاد می‌کند.

• بنابراین با توجه به قضیهٔ دوجمله‌ای

$$\begin{aligned} ۲^p &= (۱+۱)^p \\ &= ۱^p + \binom{p}{۱} + \binom{p}{۲} + \dots + \binom{p}{p-۱} + ۱^p \\ &\equiv_p ۲, \end{aligned}$$

چون p هر یک از اعداد $\binom{p}{۱}$، $\binom{p}{۲}$، ...، $\binom{p}{p-۱}$ را عاد می‌کند.

پس $a^p \equiv_p a$ را (که شکل معادلی از قضیهٔ کوچک فرما است) می‌توان به استقراء روی a به دست آورد، چون

$$\begin{aligned} ۳^p &= (۲+۱)^p \\ &\equiv_p ۲^p + ۱^p && \text{چون } \binom{p}{۱}, \binom{p}{۲}, \dots, \binom{p}{p-۱} \equiv_p ۰ \\ &\equiv_p ۲+۱ && \text{چون } ۲^p \equiv_p ۲ \\ &\equiv_p ۳. \end{aligned}$$

و به همین ترتیب.

اویلر در حدود سال ۱۷۵۰ برهانی از قضیهٔ کوچک فرما را ارائه داد که حکایت از برهان قضیهٔ لاگرانژ پیش از اثبات آن داشت (۲۰ سال قبل از برهان خود لاگرانژ که خود آن هم با اصطلاحات نظریهٔ گروهها بیان نشده بود؛ مفهوم گروه حدود سال ۱۸۳۰ توسط گالوا معرفی شد).

برای a ی داده شده با شرط $a \not\equiv_p ۰$، فرض کنیم $\{۱, a, a^۲, \dots, a^{n-۱}\}$ مجموعهٔ توانهای متمایز a باشد (که آن را به عنوان یک گروه مانند A می‌شناسیم). اویلر نشان داد که مجموعه‌های متمایز $\{b, ba, ba^۲, \dots, ba^{n-۱}\}$ برای b های مختلفِ ناهمنهشت با صفر به پیمانهٔ p (که آنها را به عنوان همرده‌های A می‌شناسیم) افرازی از مجموعهٔ $\{۱, ۲, \dots, p-۱\}$ را تشکیل می‌دهند. از این رو مرتبهٔ n برای a (که برابر مرتبهٔ هر یک از همرده‌هاست)

مقسوم‌علیهی از $p-1$ است. اویلر استدلالی مشابه را برای اثبات تعمیم خود بر قضیهٔ کوچک فرما به کار برد. تاریخچهٔ بیشتری در مورد قضیهٔ کوچک فرما و قضیهٔ اویلر را می‌توان در ویل[۳۳] (۱۹۸۴) یافت.

اعداد اول به صورت x^2+ny^2 سرنخ مهمی در تاریخ نظریه اعداد است و بارها در این کتاب به آن باز خواهیم گشت. منشأ حالت $n=1$ به دیوفانتوس و تبصرهٔ وی در مورد حاصل ضربهای مجموع مجذورات که در بخش ۷.۳ بحث کردیم باز می‌گردد (البته اگر پیش از آن در سه‌تایی‌های فیثاغورس نیامده باشد). تا سال ۱۶۴۰ فرما به طور کامل بر این حالت مسلط گردیده بود. او به وسیلهٔ تحویل آن به این سؤال که چه اعداد اولی به صورت x^2+y^2 هستند و با نشان دادن این که این اعداد دقیقاً اعداد اول به صورت $4n+1$ (همراه با استثناء بدیهی ۲) می‌باشند به این مطلب دست یافته بود. نمی‌دانیم که وی چگونه آن را اثبات کرد، اما می‌دانیم که از نزول (که روش اولیهٔ شناخته شده‌ای توسط اویلر (۱۷۵۵) نیز می‌باشد) بهره گرفته بود. تا سال ۱۶۵۴ فرما به طور مشابه با اعداد اول به صورت x^2+2y^2 و x^2+3y^2 نیز سر و کار داشته است. همان طور که در بخش ۷.۳ دیدیم به سادگی می‌توان نشان داد که رده‌های همنهشتی مشخصی به صورتی خاص نیستند. روشهای قدرتمندتری مورد نیاز است تا نشان دهیم که رده‌های همنهشتی دیگر به شکل مطلوب هستند. مجدداً در فصل ۶ به این داستان باز می‌گردیم.

موفقیت جزیی استدلالهای همنهشتی در مورد صورتهای x^2+y^2، x^2+2y^2 و x^2+3y^2 یک خوش‌اقبالی ساده نیست. این مطلب را می‌توان توسط اصلی کلی و خاتمه دهنده که توسط هس[۳۴] (۱۹۲۳) کشف شده است و اصل هس-مینکوفسکی[۳۵] نامیده می‌شود شرح داد. این اصل ایجاب می‌کند که امتناع مقادیر مشخص برای صورتهای مربعی $ax^2+bxy+cy^2$ را همواره می‌توان توسط استدلالهای همنهشتی تحقیق کرد.

---
[۳۳] Weil
[۳۴] Hasse
[۳۵] Hasse-Minkowski principle

۴

دستگاه رمز RSA

پیش‌نگاه

عمومی‌ترین کاربرد نظریه اعداد، و شاید بارزترین کاربرد هر نوع از ریاضیات پیشرفته، دستگاه رمز RSA است. در این فصل این دستگاه و چگونگی کار آن را مبتنی بر چند ایدهٔ کلیدی از فصل قبل توصیف می‌کنیم.

تنها ایده‌های نظری لازم عبارتند از عکس به پیمانهٔ n، تابع φ-اویلر و قضیهٔ اویلر مرتبط با آن یعنی $a^{\varphi(n)} \equiv_n 1$. در این راستا دو الگوریتم اساسی وجود دارد: الگوریتم محاسبهٔ اعداد دودویی، و الگوریتم اقلیدسی (صورتی از آن که عکس a را به پیمانهٔ b به دست می‌دهد).

الگوریتم اعداد دودویی، به توان رساندن به پیمانهٔ n برای توانهای بزرگ را امکان پذیر ساخته است. یک پیغام[1] (که به عنوان عددی صحیح مانند m مد نظر است) به صورت m^e به پیمانهٔ n برای مقادیر e و n (که برای همه شناخته شده است) رمز می‌شود؛ و با به توان رساندن نتیجهٔ حاصل به توانی مانند d (که عکس m به پیمانهٔ $\varphi(n)$ است و هر کسی از آن اطلاع ندارد) از رمز خارج

---

[1] message

می‌گردد. این مطلب، رمزخوانی را برای کسی که از مقدار $\varphi(n)$ اطلاع دارد آسان می‌سازد.

۱.۴ توابع دریچه‌ای

علم رمزنگاری در جست و جوی روشهایی برای کد کردن یا رمز کردن[۲] پیغامها، و روشهای متناظری برای از کد درآوردن یا رمزخواندن[۳] است. رمز کردن به طور شاخص از یک کلید[۴] عددی مشخص (که ممکن است رقمهای زیادی داشته باشد) استفاده می‌کند و همان عدد برای رمزخوانی به کار می‌رود. بدون این کلید، خواندن پیغامهای رمز شده ممکن نیست. بنابراین ایمنی دستگاه به سختیِ یافتن این کلید بستگی دارد. دو روش شناخته شده برای رمز کردن (در دو انتهای متضاد طیف ایمنی) عبارتند از

مثال ۱. به رمز درآوردن سزاری.

این روش در رمزنگاری (که گمان می‌رود توسط ژولیوس سزار[۵] استفاده شده بوده است) به طور ساده به هر حرف در پیغام، یک عدد صحیح ثابت به عنوان عدد کلیدی را (به پیمانهٔ ۲۶) می‌افزاید (با در نظر گرفتن حروف الفبای رومی، هر حرف به عنوان عددی بین ۱ تا ۲۶ در نظر گرفته می‌شود).

مثلاً اگر عدد کلیدی ۳ باشد آنگاه پیغام

Go to Zagreb tomorrow

به صورت

Jr wr Cdjuhe wrpruurz

---

[۲] encrypting
[۳] decrypting
[۴] key
[۵] Julius Caesar

رمز می‌شود و عبارت اخیر با کم کردن ۳ به پیمانهٔ ۲۶ از هر حرف رمزخوانی می‌گردد.

رمز کردن سزاری ایمنی کمی دارد چرا که فقط ۲۶ کلید ممکن وجود دارد و یافتن کلید درست وقت زیادی از دشمن نمی‌گیرد. به سادگی می‌توان کلیدهای ۱، ۲، ۳، ... را تا رسیدن به پیغامی قابل فهم، آزمود.

مثال ۲. لایهٔ یک بار مصرف.

در این روش، کلید، دنباله‌ای طولانی و اتفاقی مانند $x_1x_2x_3\ldots$ از اعدادی مانند x_i است که هر یک بین ۱ و ۲۶ می‌باشند. رقم x_i (به پیمانهٔ ۲۶) به i امین حرف پیغام افزوده می‌شود تا پیغام رمز شده حاصل شود و دریافت کننده به طور مشابه، x_i را (به پیمانهٔ ۲۶) کم می‌کند تا پیغام را بازسازی کند. همین که قطعه‌ای از کلید مانند $x_1x_2x_3\ldots x_n$ برای یک پیغام به کار گرفته شود این لایه کنار گذاشته می‌شود، یعنی بخش بعدی $x_{n+1}x_{n+2}\ldots$ برای پیغام بعدی استفاده می‌گردد.

روش لایهٔ یک بار مصرف کاملاً ایمن است (مشروط بر آن که نسخه‌ای از کلید لو نرود) چرا که همهٔ دنباله‌های $x_1x_2x_3\ldots$ به نظر یکسانند و از این رو همهٔ پیغامها نیز چنین هستند. هیچ سرنخی حتی برای سعی در حدس زدن کلید وجود ندارد. با این حال کلید باید شدیداً بزرگ باشد زیرا هر قطعه از آن فقط یک بار به کار می‌رود و این در عمل متداول نیست.

رویای رمزنگاری همواره سهولت در اجرا (همانند به رمز در آوردن سزاری) همراه با ایمنی (همانند لایهٔ یک بار مصرف) یا حداقل تلفیقی از این دو بوده است: رمزنگاری باید برای رمز کردن پیغامها، شدنی[۶] باشد، اما (بدون کلیدی در حد قابل قبول کوتاه) رمزخوانی آن باید نشدنی باشد. در گذر تاریخ این رویا بارها و بارها با شکست مواجه شده است اما در حدود سال ۱۹۷۰ به شکل دقیق‌تر و ریاضی‌گونهٔ توابع دریچه‌ای[۷] مجدداً احیا شد.

---

[۶] feasible

[۷] trapdoor functions

یک تابع دریچه‌ای عملی است که به سادگی انجام شود اما برگرداندن یا باز انجام دادن آن سخت باشد؛ مانند پایین افتادن از یک دریچه یا شکستن تخم مرغ. اما متفاوت با این مثالهای زندگی حقیقی، فرض بر این است که یک تابع دریچه‌ای به کمک یک کلید آسان برگردانده می‌شود. به نظر می‌رسد که چنین توابعی در ریاضیات وجود دارند و نظریهٔ محاسبه پذیری در زمان چندجمله‌ای[۸] برای بحث در مورد آنها گسترش یافته است. در اینجا با ذکر مهم‌ترین مثال رمزنگاری این مفاهیم را روشن می‌سازیم.

اگر دو عدد اول مانند

$$p_۱ = ۴۵۷۵۱۶۳$$

و

$$p_۲ = ۴۰۹۳۵۶۷$$

را در نظر بگیریم آنگاه به سادگی می‌توانیم حاصل ضرب آنها یعنی

$$p_۱p_۲ = ۱۸۷۲۸۷۳۶۲۷۶۴۲۱$$

را بیابیم (حتی با استفاده از روشهای مدرسه‌ای برای ضرب کردن که برای یک جفت عدد n رقمی در حدود $n^۲$ گام زمان می‌برد).

با این حال اگر عدد ۱۸۷۲۸۷۳۶۲۷۶۴۲۱ را به کسی بدهیم و از وی بخواهیم تا عوامل آن را بیابد، احتمالاً در حدود یک میلیون گام لازم دارد. این مطلب بدین دلیل است که هیچ روش شناخته شده‌ای برای یافتن مقسوم‌علیهی از یک عدد $۲n$ رقمی که ذاتاً سریع‌تر از تقسیم کردن آن بر همهٔ ۱۰^n عددِ با کمتر از n رقم باشد وجود ندارد.

لذا تابع $f(p_۱, p_۲) = p_۱p_۲$ از اعداد $p_۱$ و $p_۲$ در زمانی مربعی[۹] قابل محاسبه است اما فرآیند عکس آن یعنی تجزیه کردن به نظر نیاز به زمانی نمایی[۱۰] دارد.

[۸] polynomial time computability
[۹] quadratic time
[۱۰] exponential time

(این مفاهیم را می‌توان توسط صوری کردن مفهوم محاسبه کاملاً دقت بخشید ولی درکی غیر صوری از محاسبه برای اهداف ما کافی است.)

خاصیت به ظاهر صعب‌الرجوع عمل ضرب، مبنای معمولی‌ترین روش رمزنگاری استفاده شدهٔ امروزه یعنی دستگاه RSA است. این دستگاه پس از کارهای اولیهٔ سه ریاضیدان (که آن را اولین بار در سال **۱۹۷۸** منتشر کردند) نامگذاری گردید: ریوست[۱۱]، شامیر[۱۲] و ادلمن[۱۳]. این دستگاه متشکل است از

- یک تابع رمزنگاری[۱۴] مانند $E(m)$ از پیغامهای m که با حاصل ضرب $p_۱p_۲$[۱۵] سر و کار دارد که در آن $p_۱$ و $p_۲$ دو عدد اول بزرگ هستند،
- یک تابع رمزخوانی[۱۶] مانند $D(m)$ که با دو عدد $p_۱$ و $p_۲$ به طور مجزا سر و کار دارد.

تابع رمزنگاری به سادگی از روی پیغام و کلید $k = p_۱p_۲$[۱۷] محاسبه می‌شود ولی تابع رمزخوانی چنین نیست: به نظر نیازمند تجزیهٔ کلید به منظور استخراج دو عدد اول $p_۱$ و $p_۲$ است. به دلیل سختی ظاهری تجزیه، کلید k را می‌توان عمومی ساخت، که محاسبهٔ $E(m)$ را برای همگان آسان می‌سازد، در حالی که محاسبهٔ $D(m)$ تنها برای کسانی آسان است که $p_۱$ و $p_۲$ را می‌دانند.

لذا ظاهراً $E(m)$ یک تابع دریچه‌ای است. مجبوریم بگوییم ظاهراً زیرا هیچ کس هنوز نتوانسته است این ادعای ضمنی را اثبات کند که تجزیه کردن سخت است. این سؤال در پرتو حجم عظیمی از ارتباطاتی که RSA را استفاده می‌کنند (نظامی، تجاری و محرمانه) بسیار مهم است. صرف نظر از این که پاسخ چه

---

[۱۱] Rivest

[۱۲] Shamir

[۱۳] Adleman

[۱۴] encryption function

[۱۵] به جای $p_۱p_۲$ در نسخهٔ اصلی کتاب عبارت $(p_۱ - ۱)(p_۲ - ۱)$ آمده است که به نظر اشتباه می‌باشد چرا که امنیت رمزنگاری RSA وابسته به مخفی ماندن $\varphi(n) = (p_۱ - ۱)(p_۲ - ۱)$ است و لذا طبیعتاً نمی‌توان $(p_۱ - ۱)(p_۲ - ۱)$ را عمومی ساخت. (م)

[۱۶] decryption function

[۱۷] مجدداً $k = (p_۱ - ۱)(p_۲ - ۱)$ آمده که به نظر نمی‌رسد درست باشد. (م)

باشد نفوذ RSA بر نظریه اعداد به تنهایی برای تخصیص فصل کوتاهی به این موضوع کافی است.

۲.۴ اجزای RSA

یک استفاده کنندهٔ RSA، یک جفت عدد اول بزرگ مانند $p_۱$ و $p_۲$ برای خود بر می‌گزیند. اگر $p_۱$ و $p_۲$ مثلاً ۱۰۰ رقمی باشند آنگاه حاصل ضرب آنها یعنی $p_۱p_۲$ را می‌توان با حدود $۱۰۰^۲$ گام توسط روش مدرسه‌ای معمولی ضرب محاسبه کرد. در این صورت حاصل ضرب $p_۱p_۲$ تجزیهٔ منحصر به فردی به دو عامل کوچک‌تر یعنی $p_۱$ و $p_۲$ دارد اما هیچ روش شناخته شده‌ای برای محاسبهٔ آنها که ذاتاً بهتر از تقسیم کردن عدد ۲۰۰ رقمی $p_۱p_۲$ بر اکثر تقریباً $۱۰^{۱۰۰}$ عدد کوچک‌تر از جذر آن باشد وجود ندارد.

لذا استفاده کننده با اطمینان می‌تواند حاصل ضرب $n = p_۱p_۲$ را (بی آن که عوامل $p_۱$ و $p_۲$ از آن لو برود) فاش سازد.

اجزای نظری دستگاه رمز RSA، معکوس به پیمانهٔ k و قضیهٔ اویلر است که در قبل آنها را فراهم کرده‌ایم. تنها حکم دیگری که احتیاج داریم این است که برای دو عدد اول مانند $p_۱$ و $p_۲$ داریم

$$\varphi(p_۱p_۲) = (p_۱ - ۱)(p_۲ - ۱) \qquad (*)$$

برای اثبات $(*)$ می‌پرسیم چند عدد طبیعی مانند a کوچک‌تر از $p_۱p_۲$ موجود است که $\gcd(a, p_۱p_۲) = ۱$. تنها a هایی که برای آنها این حالت اتفاق نمی‌افتد $p_۲ - ۱$ مضرب $p_۱$ و نیز $p_۱ - ۱$ مضرب $p_۲$ هستند. این $۲ - (p_۱ + p_۲)$ عدد، متمایزند زیرا $p_۱p_۲$ کوچک‌ترین عدد طبیعی است که هم مضرب $p_۱$ و هم مضرب $p_۲$ می‌باشد. از این رو

$$\varphi(p_۱p_۲) \;=\; p_۱p_۲ - ۱ - (p_۱ + p_۲) + ۲$$

$$
\begin{aligned}
&= p_1p_2 - p_1 - p_2 + 1 \\
&= (p_1 - 1)(p_2 - 1). \square
\end{aligned}
$$

با دانستن اعداد اول p_1 و p_2 استفاده کنندهٔ RSA به سادگی می‌تواند $n = p_1p_2$ و $\varphi(n) = (p_1 - 1)(p_2 - 1)$ را محاسبه کند.

استفاده کننده همچنین توان رمزنگاری[۱۸]، یعنی e، را انتخاب می‌کند که می‌تواند هر عددی با شرط

$$\gcd(e, \varphi(n)) = 1$$

باشد؛ مثلاً عدد اولی کوچک‌تر از $\varphi(n)$. در عمل اعداد e و n را عمومی می‌سازند، بنابراین هر کسی می‌تواند آنها را برای ارسال پیغامهای رمز شده به استفاده کننده به کار ببرد.

مقدار $\varphi(n)$ (که فقط برای استفاده کننده مشخص است) محاسبهٔ توان رمزخوانی[۱۹] یعنی d را که معکوس e به پیمانهٔ $\varphi(n)$ است ممکن می‌سازد. همان گونه که می‌دانیم این معکوس به سادگی از روی e و $\varphi(n)$ توسط الگوریتم اقلیدسی محاسبه می‌شود.

کُنهِ ریاضی دستگاه RSA حکم زیر است که در بخش ۴.۴ اثبات شد. اگر d معکوس e به پیمانهٔ $\varphi(n)$[۲۰] باشد آنگاه $(m^e)^d \equiv_n m$. در اینجا m پیغام است؛ رمزنگاری، m را به توان e به پیمانهٔ n می‌رساند؛ و رمزخوانی، m را با به توان d رساندنِ پیغام رمز شده به پیمانهٔ n بازسازی می‌کند.

رمزنگاری و رمزخوانی شدنی هستند زیرا به توان رساندن به پیمانهٔ n به سادگی محاسبه می‌شود. در بخش بعد توضیح می‌دهیم که چرا چنین است. کلید موفقیت RSA سختی تجزیه کردن (که بنابر فرض پذیرفتیم) می‌باشد که محاسبهٔ $\varphi(n)$ و d را (برای کسی که اعداد اول p_1 و p_2 را نمی‌شناسد) دشوار می‌سازد.

---

[۱۸] encryption exponent

[۱۹] decryption exponent

[۲۰] در نسخهٔ اصلی، $\varphi(k)$ آمده که اشتباه تایپی است. (م)

تمرینها

برای آشنا شدن با دستگاه RSA، اعداد اول $p_1 = 7$ و $p_2 = 11$ را (که به طور غیر واقع‌بینانه‌ای کوچک هستند) در نظر بگیرید.

۱.۲.۴ شرح دهید که چرا $e = 5$ توان رمزنگاری معتبری نیست.

۲.۲.۴ نشان دهید که $e = 13$ توان رمزنگاری معتبری است و توان رمزخوانی متناظر با آن را با استفاده از الگوریتم اقلیدسی محاسبه کنید.

۳.۲.۴ نشان دهید که $e = 61$ نیز توان رمزنگاری معتبری است اما رضایت‌بخش نیست چون برای هر $m \not\equiv_{77} 0$ داریم $m^{61} \equiv_{77} m$.
چنین اتفاقاتی (که به توان e رساندن، پیغام را تغییر نمی‌دهد) با اعداد اول بزرگ p_1 و p_2 که در عمل به کار می‌روند نادر است. با این حال این مطلب نشان می‌دهد که موشکافیهایی در انتخاب صحیح توان رمزنگاری وجود دارد.

۳.۴ به توان رساندن به پیمانه یک عدد طبیعی

روش بدیهی محاسبهٔ m^k تشکیل دادنِ $m \times m \times \ldots \times m$ (k عامل) است که با $k - 1$ عمل ضرب سر و کار دارد. چون در RSA توان k با حدود ۱۰۰ رقم به کار می‌رود، تعداد اعمال ضرب در این روش چیزی در حدود 10^{100} است که به طور مأیوس‌کننده‌ای بزرگ است. لذا گام اول در به توان رساندنِ کارآمد، کاهش دادن تعداد اعمال ضرب به طور مؤثر، به امید رسیدن به عددی در حد و اندازهٔ $\log k$ است که متناسب با تعداد ارقام k می‌باشد. در بخش ۵.۱ دیدیم که با استفاده از محاسبات دودویی برای k چگونه این کار انجام می‌شود.

مثال. ساختن m^{91}.

به ترتیب زیر محاسبه می‌کنیم.

$$\begin{aligned} m &= ۱\times m \\ m^{۲} &= m^{۲} \\ m^{۵} &= (m^{۲})^{۲}\times m \\ m^{۱۱} &= (m^{۵})^{۲}\times m \\ m^{۲۲} &= (m^{۱۱})^{۲} \\ m^{۴۵} &= (m^{۲۲})^{۲}\times m \\ m^{۹۱} &= (m^{۴۵})^{۲}\times m. \end{aligned}$$

تعداد کل اعمال ضرب، برابر تعداد مجذور کردنها (یکی کمتر از تعداد ارقام k در مبنای ۲) به اضافهٔ تعداد ضرب در m کردنها (که بیش از تعداد ارقام k در مبنای ۲ نیست) می‌باشد. از این رو تعداد کل اعمال ضرب برای محاسبهٔ m^k بیش از دو برابر تعداد ارقام k در مبنای ۲ نیست. و می‌دانیم که تعداد ارقام k در مبنای ۲ حداکثر $\log_۲ k + ۱$ است.

هنوز این ایده برای محاسبهٔ m^k برای یک k که ۱۰۰ رقمی باشد خوب نیست گرچه حدود ۲۰۰ عمل ضرب لازم دارد، زیرا عددی که باید ضرب شود دارای طولی نجومی است.

آنچه RSA را شدنی می‌سازد این است که نیازی به محاسبهٔ خود m^k نداریم بلکه باقیماندهٔ آن را در تقسیم بر n می‌خواهیم. بدین دلیل در خلال محاسبه می‌توانیم (با استفاده از حساب همنهشتی) با باقیمانده‌ها کار کنیم. بالاخص، هرگز نیازی به ضرب اعداد بزرگ‌تر از n نیست و این چیزی است که به توان رساندن به پیمانهٔ n را شدنی می‌سازد. حتی با استفاده از روش ضرب کردن مدرسه‌ای (که کارآمدترین روش شناخته شده نیست)، ضرب کردن دو عدد n رقمی حدود $n^۲$ گام می‌خواهد. از این رو برای n ی در حدود ۱۰۰ رقم این کار حدود ۲۰۰ عمل ضرب می‌خواهد که به سادگی توسط رایانه انجام

می‌شود.

تمرینها

۱.۳.۴ بررسی کنید که مثال فوق امکان محاسبهٔ $m^{۹۱}$ را تنها با ۱۰ عمل ضرب (غیر از $m \times ۱$) فراهم می‌سازد.

۲.۳.۴ مقدار دودویی ۸۹ را محاسبه کنید و نشان دهید که $m^{۸۹}$ را می‌توان با ۹ عمل ضرب محاسبه کرد.

۴.۴ رمزنگاری و رمزخوانی RSA

اگر اعداد اول استفاده شده $p_۱$ و $p_۲$ باشد آنگاه یک پیغام (با استفاده از ترجمهٔ ساده‌ای از حروف به اعداد) به صورت عددی طبیعی مانند m کوچک‌تر از $n = p_۱p_۲$ (که برای عموم شناخته شده است) نوشته می‌شود. اگر پیغام واقعی بزرگ‌تر از این باشد به قطعات به اندازهٔ کافی کوچک شکسته شده و قطعه به قطعه رمز می‌شود.

همان گونه که در بخش ۲.۴ گفتیم، پیغام رمز شده که به استفاده کننده ارسال شده است برابر باقیماندهٔ m^e در تقسیم بر n می‌باشد که به صورت

$$m^e \text{ به پیمانه } n$$

آن را مختصر می‌کنیم. این نمادی طبیعی برای باقیمانده‌ها است و نباید ابهامی ایجاد کند چرا که

$$r = m^e \text{ به پیمانه } n \quad \Rightarrow \quad r \equiv_n m^e.$$

پس از آن که اعداد e و n از روی اعداد $p_۱$ و $p_۲$ توسط استفاده کننده محاسبه شد، آنها را عمومی می‌سازند: $n = p_۱p_۲$ و باید e نسبت به n اول باشد. گرچه ممکن است e و n صدها رقم داشته باشند، با استفاده از تکرار روش مجذور کردن که در بخش قبل توضیح داده شد، محاسبهٔ e و n شدنی است.

استفاده کننده پیغام رمز شدهٔ m^e به پیمانهٔ n را دریافت می‌کند و آن را به توان d به پیمانهٔ n می‌رساند. نتیجه، پیغام اولیهٔ m است چون d معکوسی برای e به پیمانهٔ $\varphi(n)$ است و لذا k یی هست که

$$ed = ۱ + k\varphi(n).$$

از این رو

$$\begin{aligned} m^{ed} &= m^{۱+k\varphi(n)} \\ &= m \cdot (m^{\varphi(n)})^k \\ &\equiv_n m \cdot (۱)^k \qquad m^{\varphi(n)} \equiv_n ۱ \text{ چون بنابر قضیه اویلر} \\ &\equiv_n m. \end{aligned}$$

همانند رمزنویسی، به توان d رساندن به پیمانهٔ n (مشروط بر آن که d مشخص باشد) به طور محاسبه‌ای شدنی است. توان رمزخوانی یعنی d را می‌توان توسط استفاده کننده محاسبه کرد چرا که استفاده کننده، عوامل $p_۱$ و $p_۲$ از n را می‌داند. این مطلب محاسبهٔ $\varphi(n) = (p_۱ - ۱)(p_۲ - ۱)$ را توسط الگوریتم اقلیدسی ممکن می‌سازد.

محاسبهٔ معکوس شدنی است چرا که الگوریتم اقلیدسی (همان طور که در بخش ۴.۳ نیز گفتیم) از نظر سرعت شبیه به توان رساندن به پیمانهٔ n با اندازه‌ای مشابه می‌باشد و در حقیقت وقتی $n = p_۱p_۲$ مقدار $\varphi(n)$ تنها اندکی کوچک‌تر از n است.

تمرینها

مثال RSA با اعداد $p_1 = ۷$، $p_2 = ۱۱$ و توان رمزنگاری $e = ۱۳$ را که مانند بازیچه‌ای ساده است ادامه دهید:

۱.۴.۴ نشان دهید که پیغام m به صورت $((m^۲ \cdot m)^۲)^۲ \cdot m$ به پیمانهٔ ۷۷ رمز می‌شود.

۲.۴.۴ وقتی $m = ۷$ تحقیق کنید که پیغام رمز شده برابر ۳۵ است.

با این حال تضمین نمی‌شود که هر پیغامی توسط فرآیند رمزنگاری تغییر یابد. بدیهی است که برای $m = ۱$ هیچ تغیری نداریم و نیز ممکن است برای مقادیر دیگر نیز چنین اتفاقی بیفتد:

۳.۴.۴ وقتی $m = ۱۲$ تحقیق کنید که پیغام رمز شده نیز ۱۲ است.

۴.۴.۴ با استفاده از توان رمزخوانی تمرین ۲.۴.۴ تحقیق کنید که رمزخوانی ۱۲ پیغام ۱۲ را باز می‌سازد.

۵.۴.۴ نتایج تمرینهای ۲.۴.۴ و ۳.۴.۴ را با استفاده از $۱۲^٦ \equiv_{۷۷} ۱$ شرح دهید.

۵.۴ امضاء رقمی

استفادهٔ دیگری از RSA ارسال امضاء رقمی[۲۱] می‌باشد (برای آن که استفاده کننده اثبات کند همان کسی است که ادعایش را دارد). بدین منظور، استفاده کننده می‌تواند احراز دانشی را نشان دهد که هیچ کس دیگر نمی‌تواند آن را دارا باشد؛ درست همانند توان رمزخوانی d که شخصی است و در مقابل اعداد عمومی e و n می‌آید.

[۲۱] digital signature

این مطلب را می‌توان توسط پیغامی شناخته شده مانند m و ارسال m^d به پیمانهٔ n، بدون فاش ساختن d، نمایش داد. این پیغامی مرموز است که فقط صاحب d می‌تواند آن را خلق کند. اما تمام دنیا e و n را می‌دانند و از این رو می‌توانند m^d به پیمانهٔ n را با به توان e رساندن به پیمانهٔ n باز کنند:

$$(m^d)^e = m^{ed} \equiv_n m.$$

از آنجایی که فقط m^d به پیمانهٔ n می‌تواند بدین روش به پیغام قابل تشخیص m تبدیل شود، همگان می‌توانند مطمئن باشند که ارسال کننده واقعاً مالک عدد محرمانهٔ d است.

۶.۴ نتایج محاسباتی دیگر

ایمنی RSA در وهلهٔ اول وابسته به داشتن موجودیِ بزرگی از اعداد اول ۱۰۰ رقمی است. اگر تنها مشتی از چنین اعداد اول در دسترس می‌بود، دشمن می‌توانست با آزمودن همهٔ زوجهایی همچون $p_۱$ و $p_۲$ تا رسیدن به $p_۱p_۲$ یی برابر n دستگاه را بشکنند. خوشبختانه این هیچ مشکلی نیست: تعداد زیادی عدد اول بزرگ وجود دارد و به طور محاسباتی یافتن آنها آسان نیست.

لذا مشکل حقیقی دشمن، محاسبهٔ توان رمزخوانی d از روی e و n ی است که توسط عموم شناخته شده می‌باشند.

چون d معکوس e به پیمانهٔ $\varphi(n)$ است و $\varphi(n) = (p_۱ - ۱)(p_۲ - ۱)$، این کار شدنی است هرگاه عوامل $p_۱$ و $p_۲$ از n شناخته شده باشند. در حقیقت نشان داده شده است که این کار شدنی است فقط اگر عوامل n شناخته شده باشند. از این رو رمزخوانی مشکل است مادامی که تجزیه کردن سخت باقی بماند.

با این حال نمی‌دانیم که تجزیه کردن حقیقتاً سخت است یا نه. هیچ روشی شدنی برای تجزیه کردن شناخته نشده است اما اثبات هم نشده است که اصلاً

چنین روشی وجود ندارد. برهانی برای این که هیچ روشی شدنی وجود ندارد پاسخی به سؤالی موسوم به $P \neq NP$ می‌باشد که جایزه‌ای معادل یک میلیون دلار برای آن پیشنهاد شده است.

به بیان عامیانه، مسائل از نوع P (زمان چندجمله‌ای[۲۲]) را می‌توان توسط محاسبات کوتاه (شبیه مسألهٔ ضرب کردن) حل کرد. مسائل از نوع NP (زمان غیر چندجمله‌ای[۲۳]) پاسخهایی دارند که توسط محاسبات کوتاه تحقیق می‌شوند، اما به خودی خود یافتن پاسخ، زمانی طولانی می‌خواهد. همان گونه که دیدیم، تجزیه کردن از این نوع است.

$P \neq NP$ می‌گوید مسائلی وجود دارند که به سختی حل می‌شوند اما پاسخ آنها به سادگی قابل تحقیق است. وجود مسأله‌ای از این دست تاکنون اثبات نشده است گرچه نامزدهای زیادی (همچون مسألهٔ تجزیه کردن) شناخته شده می‌باشند.

۷.۴ بحث

در اواسط دههٔ ۷۰، هنگامی که ریاضیدانان متوجه مسائل با راه حلهای ظاهراً سخت برای یافتن اما آسان برای تحقیق کردن شدند، پیشنهاد شد که از چنین مسائلی در دستگاه‌های رمزنگاری با کلید عمومی[۲۴] (یعنی دستگاه‌هایی که رمز کردن یک پیغام، آسان است اما رمزخوانی آن بدون داشتن اطلاعات محرمانه سخت است) استفاده شود.

ایدهٔ توابع دریچه‌ای و کاربرد آنها در دستگاه‌های رمزنگاری با کلید عمومی، اولین بار توسط دیفی[۲۵] و هلمن[۲۶] (۱۹۷۶) منتشر شد. آنها همچنین

---

[۲۲] polynomial time
[۲۳] nondeterministic polynomial time
[۲۴] public key cryptosystems
[۲۵] Diffie
[۲۶] Hellman

به توان رساندن به پیمانهٔ n را به عنوان فرآیندی به طور محاسباتی شدنی که ممکن است عکس آن سخت باشد مطرح کردند. اجرای این ایده در RSA اولین بار توسط ریوست و بقیه (۱۹۷۸) منتشر شد و از آن زمان تبدیل به متداول‌ترین دستگاه با کلید عمومی گردید. اخیراً فاش شد که همان دستگاه چند سال قبل از آن نیز توسط کلیفرد کاکز[۲۷] در انگلستان کشف شده بوده است. از آنجایی که این مطلب بخشی از کار وی برای ادارهٔ جاسوسی بریتانیا بود محرمانه ماند (گرچه این که چرا بعد از ۱۹۷۸ هیچ استفاده‌ای از آن نشده است به سختی قابل درک است). برای بحثی بیشتر در مورد تاریخ دستگاه‌های رمزنگاری با کلید عمومی، یان[۲۸] (۲۰۰۰) را ببینید.

بنیاد RSA، که بر اساس سخت بودن تجزیه کردن است، توسط کشف قابل توجهی از شور[۲۹] (۱۹۹۴) دچار خلل شد. شور دریافت که تجزیه کردن را می‌توان در زمان چندجمله‌ای توسط رایانه‌های کوانتومی انجام داد. نکته در این است که رایانه‌های کوانتومی هنوز وجود ندارند و شاید هرگز امکان وجود نداشته باشند. علی رغم این، نتیجهٔ شور پرتو جدید و غریبی بر مفهوم محاسبه می‌افکند.

در همهٔ رایانه‌های موجود سختی تجزیه کردن (و خیلی مسائل NP دیگر) در این است که فضای پاسخهای ممکن نسبت به مسأله به طور نمایی بزرگ است. برای یک عدد n رقمی مانند K حدود $10^{\frac{n}{2}}$ عدد کمتر از $\sqrt{K}$ وجود دارد و برای تجزیه کردن K راهی بهتر از آزمودن همهٔ مقسوم‌علیه‌های بالقوه نداریم. از آنجایی که چیزهای زیادی را یکی پس از دیگری مجبوریم بیازماییم، تجزیه کردن توسط روشهای شناخته شده، زمان نمایی می‌طلبد.

با این حال بنابر نظریهٔ کوانتوم، در دنیای اتم چیزهای زیادی در زمان واحد و مکان واحد واقعاً اتفاق می‌افتند. رایانهٔ کوانتومی فرضی، این امکان را فراهم می‌آورد که محاسبات زیادی را به طور همزمان انجام دهیم و بدین طریق

---
[۲۷] Clifford Cocks
[۲۸] Yan
[۲۹] Shor

می‌توان اعداد را در زمان چندجمله‌ای تجزیه کرد. ترجیحاً می‌گوییم فرضی چون نمی‌دانیم که آیا یک رایانهٔ مستحکم واقعاً می‌تواند مبتنی بر قطعات با اندازهٔ اتمی ساخته شود.

۵

معادله پل

پیش‌نگاه

معادلهٔ $x^۲ - ny^۲ = ۱$ موسوم به معادلهٔ پِل (که به اشتباه توسط اویلر به پِل نسبت داده شده است) یکی از قدیمی‌ترین معادله‌ها در ریاضیات است و برای مطالعهٔ معادله‌های دیوفانتی مربعی، اساسی است. یونانیان حالت خاص $x^۲ - ۲y^۲ = ۱$ را بررسی می‌کردند چون دریافته بودند که جوابهای طبیعی آن طبیعت $\sqrt{۲}$ را روشن می‌سازد. ارتباطی مشابه بین جوابهای طبیعی $x^۲ - ny^۲ = ۱$ و $\sqrt{n}$، که n یک نامربع طبیعی است، وجود دارد.

اصم بودن $\sqrt{n}$ برای n ی نامربع، رفتار عجیبی را در جوابهای $x^۲ - ny^۲ = ۱$ به وجود می‌آورد. علی رغم این، اصم بودن $\sqrt{n}$ پرتویی بر این معادله باز می‌تاباند؛ این مطلب به ساختار جبری ساده و فرمول کلی ساده‌ای برای همهٔ جوابهای صحیح $x^۲ - ny^۲ = ۱$ بر حسب کوچک‌ترین جواب طبیعی آن منجر می‌گردد[۱].

[۱] از آنجایی که یک جواب برای چنین معادله‌ای، یک زوج مرتب مانند (x,y) است شاید اصطلاح کوچک‌ترین جواب بی‌معنی باشد. در این گونه موارد عددی حقیقی (مانند $x^۲ + y^۲$) را به هر جواب نسبت می‌دهند و منظور از کوچک‌ترین جواب، جوابی است که مقدار نسبت داده

اما هیچ فرمول ساده‌ای برای کوچک‌ترین جواب طبیعی وجود ندارد و حتی اثبات وجود آن بدیهی نیست[۲]. در این فصل دو برهان ارائه می‌کنیم: اولی برهانی نسبتاً ساده منسوب به دیریکله است که مبتنی بر تقریب $\sqrt{n}$ توسط اعداد گویا می‌باشد. دومی (که در بخشهای ستاره‌دار آخر این فصل می‌آید) مبتنی بر یک نظریهٔ کلی در مورد صورتهای مربعی منسوب به کانوِی است.

نظریهٔ کانوی را بدین دلیل در کار می‌آوریم که توسیعی طبیعی از مطالعهٔ ما بر الگوریتم اقلیدسی می‌باشد (بالاخص احکام بخشهای آغازین فصل ۲) و نیز بدین دلیل که توصیف بسیار ساده‌ای از پدیدهٔ تناوب مرتبط با معادلهٔ پل و $\sqrt{n}$ به دست می‌دهد. همچنین رهیافتی بسیار شهودی با موضوع دارد که رفتار پیچیدهٔ معادلهٔ پل را به طور تعجب‌آوری برای درک کردن آسان می‌سازد.

۱.۵ اعداد ضلعی و قطری

یونانیان قدیم معادلهٔ $x^۲ - ۲y^۲ = ۱$ را در تلاشهای خود برای درک $\sqrt{۲}$ (که قطر مربع واحد است و از اصم بودن آن اطلاع داشتند) مشاهده کردند. آنها روشی برای تولید جوابهای به اندازهٔ دلخواه بزرگ مانند $(x_۱, y_۱)$، $(x_۲, y_۲)$، ... برای این معادله و در نتیجه تولید کسرهای $\frac{x_i}{y_i}$ را که به طور دلخواه نزدیک به $\sqrt{۲}$ باشند می‌دانستند. کسرهای $\frac{x_i}{y_i}$ به $\sqrt{۲}$ میل می‌کنند زیرا اگر $x_i^۲ - ۲y_i^۲ = ۱$ آنگاه

$$\frac{x_i^۲}{y_i^۲} = ۲ + \frac{۱}{y_i^۲} \to ۲$$

هرگاه $y_i \to \infty$.

لذا اگر y_i ضلع مربع باشد آنگاه x_i قطر را تقریب می‌زند. یونانیان جوابهای

شده به آن کمترین مقدار ممکن را داشته باشد. (م)

[۲] توجه کنید که اگر با مجموعه‌ای نامتناهی از جوابها سر و کار داشته باشیم صحبت کردن از مینیمم ناموجه است. (م)

(x_i, y_i) را در بین اعداد ضلعی[۳] مانند s_i و اعداد قطری[۴] مانند d_i که به وسیلهٔ

$$d_1 = 3, \qquad s_1 = 2$$
$$d_{i+1} = d_i + 2s_i, \qquad s_{i+1} = d_i + s_i$$

تعریف می‌شوند کشف کردند. از این معادله‌ها نتیجه می‌شود که

$$d_1^2 - 2s_1^2 = 1, \qquad d_{i+1}^2 - 2s_{i+1}^2 = -(d_i^2 - 2s_i^2).$$

از این رو جفتهای شمارهٔ فرد، یعنی (d_1, s_1)، (d_3, s_3)، (d_5, s_5)، ... در معادلهٔ $x^2 - 2y^2 = 1$ صدق می‌کنند در حالی که بقیه در $x^2 - 2y^2 = -1$ صادقند.

معادلهٔ اول، مثالی از معادلهٔ پل است که شکل کلی آن $x^2 - ny^2 = 1$ می‌باشد که در آن n عددی نامربع است. دومی خیلی مرتبط با اولی است؛ در حقیقت بعداً به دنبال همهٔ مقادیر $x^2 - ny^2$ خواهیم بود که ببینیم شامل مقدار ۱ است یا نه.

ریشه‌های دوم اصم

در کار با معادلهٔ $x^2 - ny^2 = 1$ که در آن n عددی نامربع است شدیداً بر اصم بودن $\sqrt{n}$ که در بخش ۵.۲ اثبات شد تکیه می‌کنیم.

اهمیت اصم بودن در این است که می‌توانیم یک زوج از اعداد صحیح مانند (a, b) را توسط یک عدد حقیقی یعنی $a + b\sqrt{n}$ کد کنیم؛ می‌گوییم که این عدد دارای بخش گویای a و بخش اصم b است. بخشهای گویا و اصم معنی دارند زیرا اگر $\sqrt{n}$ اصم باشد، $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ و

$$a_1 + b_1\sqrt{n} = a_2 + b_2\sqrt{n}$$

---

[۳] side numbers
[۴] diagonal numbers

آنگاه $a_۲ = a_۱$ و $b_۲ = b_۱$.

به برهان خلف فرض کنیم $b_۲ \neq b_۱$. در این صورت

$$a_۱ - a_۲ = (b_۲ - b_۱)\sqrt{n}$$

و چون $b_۲ - b_۱ \neq ۰$ داریم $\sqrt{n} = \frac{a_۱ - a_۲}{b_۲ - b_۱}$. این مطلب با اصم بودن $\sqrt{n}$ در تناقض است. از این رو $b_۲ = b_۱$ و در نتیجه $a_۲ = a_۱$. □

تمرینها

در بخشی که می‌آید اعداد $x_i + y_i\sqrt{n}$ را به کار می‌بریم تا جوابهای $x^۲ - ny^۲ = ۱$ را از کد خارج کنیم. برای آن که طعمی از چگونگی عملکرد این کار را بچشید، دو تمرین بعدی اعداد به صورت $a + b\sqrt{۲}$ را به کار می‌برند تا جفت (ضلع، قطر) را از کد خارج کنند.

۱.۱.۵ بررسی کنید که $(۱ + \sqrt{۲})^۲ = ۳ + ۲\sqrt{۲}$ و

$$(x + y\sqrt{۲})(۱ + \sqrt{۲}) = x + ۲y + (x + y)\sqrt{۲}.$$

۲.۱.۵ از استقراء و تمرین ۱.۱.۵ استفاده کنید تا نشان دهید که $(۱ + \sqrt{۲})^{n+۱} = d_n + s_n\sqrt{۲}$.

هنگامی که n مربع کامل باشد معادلهٔ $x^۲ - ny^۲ = ۱$ چندان جالب نیست. لذا هم‌اکنون تکلیفش را یکسره می‌کنیم.

۳.۱.۵ با تجزیه کردن سمت چپ $x^۲ - y^۲ = ۱$ نشان دهید که این معادله فقط دو جواب صحیح دارد.

۴.۱.۵ به طور مشابه نشان دهید که اگر n مربع کامل باشد آنگاه $x^۲ - ny^۲ = ۱$ فقط دو جواب صحیح دارد.

۲.۵ معادله $x^2 - 2y^2 = 1$

یافتن همهٔ جوابهای گویای $x^2 - ny^2 = 1$ به روش دیوفانتوس، خیلی سرراست است (خطی را که از نقطهٔ گویای $(1,0)$ می‌گذرد و شیب t دارد رسم کنید). لذا روش حل کاملاً مستقل از n است.

یافتنِ حتی یک جواب صحیح برای $x^2 - ny^2 = 1$ (غیر از جوابهای بدیهی $(\pm1, 0)$) امری دیگر است. کوچک‌ترین جواب مثبت غیر از $(\pm1, 0)$ به طریقی رمزآلود وابسته به n است. اما همین که این کوچک‌ترین جواب غیر بدیهی یافت شد، همهٔ جوابهای صحیح دیگر توسط فرمولی ساده تولید می‌شوند. این روش را برای حالت $n = 2$ روشن می‌سازیم.

برای $x^2 - 2y^2 = 1$ کوچک‌ترین جواب صحیح غیر بدیهی را می‌توان با آزمودن یافت که برابر $(3,2)$ است. جوابهای دیگر را می‌توان توسط قاعدهٔ ترکیب[5] به دست آورد: اگر (x_1, y_1) و (x_2, y_2) جوابهای $x^2 - ny^2 = 1$ باشند آنگاه (x_3, y_3) نیز چنین است که x_3 و y_3 توسط

$$(x_1 + y_1\sqrt{2})(x_2 + y_2\sqrt{2}) = x_3 + y_3\sqrt{2}$$

تعریف می‌شوند.

برای آن که نشان دهیم این قاعده جواب جدیدی به دست می‌دهد، ابتدا x_3 و y_3 را محاسبه می‌کنیم. با بسط دادن سمت چپ عبارت فوق و جدا کردن بخشهای گویا و اصم در می‌یابیم که

$$x_3 = x_1x_2 + 2y_1y_2, \qquad y_3 = x_1y_2 + y_1x_2.$$

سپس می‌توان با ضرب کردن بررسی کرد که

$$\begin{aligned}&(x_1x_2 + 2y_1y_2)^2 - 2(x_1y_2 + y_1x_2)^2\\ =\ &(x_1^2 - 2y_1^2)(x_2^2 - 2y_2^2)\end{aligned}$$

---
[5] composition rule

$$= \quad ۱ \times ۱ = ۱.$$

لذا همان طور که انتظارش را داشتیم ۱ = $x_۳^۲ - ۲y_۳^۲$. □

مثال. با ترکیب کردن جواب (۳,۲) با خودش به جواب جدید $(x_۳, y_۳)$ می‌رسیم که

$$x_۳ + y_۳\sqrt{۲} = (۳ + ۲\sqrt{۲})^۲ = ۹ + ۸ + ۱۲\sqrt{۲} = ۱۷ + ۱۲\sqrt{۲}.$$

با مساوی قرار دادن قسمتهای گویا و اصم داریم ۱۷ = $x_۳$ و ۱۲ = $y_۳$ که در حقیقت جوابی دیگر برای معادله است. سپس اگر (۱۷,۱۲) را با (۳,۲) ترکیب کنیم داریم

$$(۱۷ + ۱۲\sqrt{۲})(۳ + ۲\sqrt{۲}) = ۵۱ + ۴۸ + (۳۶ + ۳۴)\sqrt{۲} = ۹۹ + ۷۰\sqrt{۲}.$$

لذا جواب دیگر (۹۹,۷۰) است و به همین ترتیب می‌توان ادامه داد. با این فرآیند می‌توانیم بی‌نهایت جواب صحیح به دست آوریم اما روشن نیست که تا چه حد به یافتن همهٔ جوابها نزدیک شده‌ایم. این وضعیت روشن می‌گردد هرگاه مشاهده کنیم که یک ساختار گروهی در کار است.

تمرینها

روشی دیگر برای رسیدن به قاعدهٔ ترکیب، استفاده از تجزیهٔ اصم

$$x^۲ - ۲y^۲ = (x - y\sqrt{۲})(x + y\sqrt{۲}) \qquad (*)$$

است. فرض می‌کنیم که ۱ = $x_۱^۲ - ۲y_۱^۲$ و ۱ = $x_۲^۲ - ۲y_۲^۲$ که در نتیجه

$$۱ = ۱ \times ۱ = (x_۱^۲ - ۲y_۱^۲)(x_۲^۲ - ۲y_۲^۲) \qquad (**)$$

۱.۲.۵ تجزیهٔ (*) را برای هر یک از عوامل سمت راست (**) به کار برید، سپس عوامل را به روشی دیگر در هم ضرب کنید تا نشان دهید که

$$\begin{aligned} ۱ &= [x_۱x_۲ + ۲y_۱y_۲ - (x_۱y_۲ + y_۱x_۲)\sqrt{۲}] \\ &\times[x_۱x_۲ + ۲y_۱y_۲ + (x_۱y_۲ + y_۱x_۲)\sqrt{۲}]. \end{aligned}$$

۲.۲.۵ از تمرین ۱.۲.۵ نتیجه بگیرید که $x_۳ - ۲y_۳ = ۱$ که در آن

$$x_۳ = x_۱x_۲ + ۲y_۱y_۲, \qquad y_۳ = x_۱y_۲ + y_۱x_۲.$$

در بخش ۴.۵ این روش را برای یافتن قاعدهٔ ترکیب برای جوابهای $x^۲ - ny^۲ = ۱$ تعمیم می‌دهیم.

۳.۵ گروه جوابها

نه فقط جوابهای $(x_۱, y_۱)$ و $(x_۲, y_۲)$ از $x_۲ - ۲y_۲ = ۱$ حاصل ضرب $(x_۱x_۲ + ۲y_۱y_۲, x_۱y_۲ + y_۱x_۲)$ متناظر با ضرب دو عدد

$$(x_۱ + y_۱\sqrt{۲})(x_۲ + y_۲\sqrt{۲})$$

را دارند بلکه همهٔ اعداد به صورت $x + y\sqrt{۲}$ با شرط $x^۲ - ۲y^۲ = ۱$ (که شامل $۱ = ۱ + ۰\sqrt{۲}$ هستند)[۶] نیز همراه با معکوس ضربی خود یعنی $x - \sqrt{۲}$ چنین خاصیتی را دارند: چون با این فرض که (x, y) جوابی برای معادله است داریم

$$(x + y\sqrt{۲})(x - y\sqrt{۲}) = x^۲ - ۲y^۲ = ۱.$$

[۶] در نسخهٔ اصلی این قسمت به صورت بلکهٔ همهٔ اعداد به صورت $x + y\sqrt{n}$ با شرط $x^۲ - ny^۲ = ۱$ (که شامل $۱ = ۱ + ۰\sqrt{n}$ هستند) آمده است که به نظر می‌رسد اشتباه تایپی باشد. (م)

لذا جوابهای (x,y) با همان ساختار ضرب اعداد $x+y\sqrt{۲}$ (با شرط $x^۲-۲y^۲=۱$) یک گروه تشکیل می‌دهند. برای درک این گروه در ابتدا بر زیرگروه اعداد مثبت $x+y\sqrt{۲}$ (با شرط $x^۲-۲y^۲=۱$) متمرکز می‌شویم.

ساختار جوابهای مثبت. گروه اعداد مثبت $x+y\sqrt{۲}$، که در آن (x,y) جواب صحیحی از معادلهٔ $x^۲-۲y^۲=۱$ است، یک گروه دوری نامتناهی از توانهای $۳+۲\sqrt{۲}$ می‌باشد.

برای آن که دلیل این امر را بدانیم تابع لگاریتم را روی همهٔ اعداد مثبت $x+y\sqrt{۲}$ اثر می‌دهیم. چون $\log(ab)=\log a+\log b$، اعداد حاصله، یعنی $\log(x+y\sqrt{۲})$، تحت + یک گروه تشکیل می‌دهند.

این گروه دارای کوچک‌ترین عضو $\log(۳+۲\sqrt{۲})$ است زیرا

- $۳+۲\sqrt{۲}$ کمترین مقدار ممکن را در بین همهٔ $x+y\sqrt{۲}$ هایی که متناظر با جوابهایی مانند (x,y) با شرط $x,y>۰$ هستند، دارد.
- جوابهای $(x,-y)$ با شرط $y>۰$ معکوس جوابهای (x,y) با شرط $x,y>۰$ می‌باشند. از این رو $x-y\sqrt{۲}$ های متناظر با آنها کوچک‌تر از ۱ می‌باشند و لگاریتم آنها کوچک‌تر از ۰ است.

اما هر گروهی به این شکل شامل همهٔ مضارب صحیح کوچک‌ترین عضو مثبت خود (مثلاً m) می‌باشد: اگر عددی مانند k در بین دو مضرب متوالی m باشد، یعنی

$$mn<k<m(n+۱)$$

آنگاه $k-mn$ نیز در گروه است. اما

$$۰<k-mn<|m|$$

که متناقض با انتخاب m به عنوان کوچک‌ترین عضو گروه می‌باشد. □

لذا همهٔ جوابهای (x,y) از $x^۲-۲y^۲$ که برای آنها $x+y\sqrt{۲}>۰$ متناظر با توانهای $۳+۲\sqrt{۲}$ می‌باشند. حال برای هر جواب مانند (x,y)، یا $x+y\sqrt{۲}$

و یا $-x - y\sqrt{۲}$ مثبت هستند. از این رو جوابهای دیگر صرفاً قرینهٔ همان جوابهایی است که از توانهای $۳ + ۲\sqrt{۲}$ به دست می‌آید.

تمرینها

فرض کنیم زوجهای (u_k, v_k) از اعداد صحیح توسط

$$u_k + v_k\sqrt{۲} = (۳ + ۲\sqrt{۲})^k$$

برای k های صحیح، تعریف شوند. در این صورت آنچه هم‌اکنون اثبات کردیم این است که زوجهای (u_k, v_k) همهٔ جوابهای صحیح (x, y) از معادلهٔ $x^۲ - ۲y^۲ = ۱$ با شرط $x > ۰$ هستند. حال به سادگی می‌توانیم u_k و v_k را به صورت تابعی صریح بر حسب k بیان کنیم، گرچه این توابع (نه به شکلی غیر منتظره) با $\sqrt{۲}$ سر و کار دارند.

۱.۳.۵ با فرض آن که $u_k + v_k\sqrt{۲} = (۳ + ۲\sqrt{۲})^k$، مقدار $(۳ - ۲\sqrt{۲})^k$ چند است؟

۲.۳.۵ از تمرین ۱.۳.۵ نتیجه بگیرید که

$$\begin{aligned} u_k &= \frac{۱}{۲}[(۳ + ۲\sqrt{۲})^k + (۳ - ۲\sqrt{۲})^k], \\ v_k &= \frac{۱}{۲\sqrt{۲}}[(۳ + ۲\sqrt{۲})^k - (۳ - ۲\sqrt{۲})^k]. \end{aligned}$$

۳.۳.۵ از تمرین ۲.۳.۵ نتیجه بگیرید که u_k نزدیک‌ترین عدد صحیح به $\frac{(۳+۲\sqrt{۲})^k}{۲}$ است. و در مورد v_k چطور؟

۴.۵ معادلهٔ کلی پل

اگر n یک نامربع صحیح باشد، تعریف می‌کنیم

$$\mathbb{Z}[\sqrt{n}] = \{x + y\sqrt{n} : x, y \in \mathbb{Z}\}.$$

درست همان طور که برای مطالعهٔ $x^۲ - ۲y^۲ = ۱$ اعداد $x + y\sqrt{۲}$ را به کار بردیم، از اعداد $x + y\sqrt{n}$ نیز برای مطالعهٔ $x^۲ - ny^۲ = ۱$ بهره می‌گیریم.

در حقیقت $x^۲ - ny^۲$ چیزی است که آن را نرم $x + y\sqrt{n}$ در $\mathbb{Z}[\sqrt{n}]$ می‌نامیم و برابر حاصل ضرب $x + y\sqrt{n}$ در مزدوج[۷] آن یعنی $x - y\sqrt{n}$ می‌باشد:

$$\text{نرم } (x + y\sqrt{n}) = (x - y\sqrt{n})(x + y\sqrt{n}) = x^۲ - ny^۲.$$

لذا یافتن جوابهای معادلهٔ پل معادل است با یافتن عناصری از $\mathbb{Z}[\sqrt{n}]$ که نرم آنها ۱ است.

مزیت جست و جو در $\mathbb{Z}[\sqrt{n}]$ (به جای یافتن (x, y) های صحیحی که جواب معادله هستند) در این است که می‌توانیم جبر روی اعداد در $\mathbb{Z}[\sqrt{n}]$ را به کار بریم.

قاعدهٔ ترکیب براهماگوپتا[۸]. اگر $(x_۱, y_۱)$ و $(x_۲, y_۲)$ جوابهای معادلهٔ پل $x^۲ - ny^۲ = ۱$ باشند آنگاه

$$(x_۳, y_۳) = (x_۱x_۲ + ny_۱y_۲, x_۱y_۲ + y_۱x_۲)$$

نیز چنین است.

این مطلب قاعدهٔ ترکیب را که برای $n = ۲$ در بخش ۲.۵ استفاده شد تعمیم می‌دهد و می‌توان آن را به صورت زیر با استفاده از تجزیه در $\mathbb{Z}[\sqrt{n}]$ اثبات کرد.

چون $(x_۱, y_۱)$ و $(x_۲, y_۲)$ جواب هستند،

$$x_۱^۲ - ny_۱^۲ = ۱, \qquad x_۲^۲ - ny_۲^۲ = ۱.$$

---

[۷] conjugate

[۸] Brahmagupta composition rule

بنابراین

$$\begin{aligned}
۱ &= (x_۱^۲ - ny_۱^۲)(x_۲^۲ - ny_۲^۲) \\
&= (x_۱ - y_۱\sqrt{n})(x_۱ + y_۱\sqrt{n})(x_۲ - y_۲\sqrt{n})(x_۲ + y_۲\sqrt{n}) \\
&= (x_۱ - y_۱\sqrt{n})(x_۲ - y_۲\sqrt{n})(x_۱ + y_۱\sqrt{n})(x_۲ + y_۲\sqrt{n}) \\
&= [x_۱x_۲ + ny_۱y_۲ - (x_۱y_۲ + y_۱x_۲)\sqrt{n}] \\
&\quad \times [x_۱x_۲ + ny_۱y_۲ + (x_۱y_۲ + y_۱x_۲)\sqrt{n}] \\
&= (x_۱x_۲ + ny_۱y_۲)^۲ - n(x_۱y_۲ + y_۱x_۲)^۲ \\
&= x_۳^۲ - ny_۳^۲. \square
\end{aligned}$$

این ترکیب کردن جوابها برای تشکیل جوابی جدید توسط ریاضیدانی هندی به نام براهماگوپتا در حدود ۶۰۰ پس از میلاد کشف شد (اما بدون استفاده از $\sqrt{n}$).

همچنین یک جواب همانی $(۱, ۰)$ و یک معکوس $(x, -y)$ برای هر جواب مانند (x, y) داریم. از این رو همان طور که قبلاً در حالت خاص $n = ۲$ دیدیم، جوابها یک گروه تشکیل می‌دهند. همانند آن حالت می‌توانیم اثبات کنیم که همهٔ جوابها از توانهای کوچک‌ترین جواب مثبت معادله به دست می‌آیند.

مثال. جوابهای $x^۲ - ۳y^۲ = ۱$.

با آزمایش، کوچک‌ترین جواب مثبت $(۲, ۱)$ را می‌یابیم. با ترکیب کردن $(۲, ۱)$ با خودش جوابهای

$$\begin{aligned}
(۲ \times ۲ + ۳ \times ۱ \times ۱, ۲ \times ۱ + ۱ \times ۲) &= (۷, ۴) \\
(۲ \times ۷ + ۳ \times ۱ \times ۴, ۲ \times ۴ + ۱ \times ۷) &= (۲۶, ۱۵)
\end{aligned}$$

و الی‌آخر را داریم. این جوابها متناظر با توانهای $۲ + \sqrt{۳}$ هستند.

محاسبات به کار رفته برای اثبات قاعدهٔ ترکیب براهماگوپتا واقعاً خاصیتی کلی‌تر را نشان می‌دهد که نه تنها با ضرایب صحیح x و y بلکه با ضرایب گویا،

یعنی خارج قسمت اعداد صحیح، نیز برقرار است. نماد $\mathbb{Q}$ (خارج قسمت که از کلمهٔ quotient برگرفته شده است) را برای اعداد گویا به کار می‌بریم و تعمیم طبیعی $\mathbb{Z}[\sqrt{n}]$ را به

$$\mathbb{Q}[\sqrt{n}] = \{x + y\sqrt{n} : x, y \in \mathbb{Q}\}$$

می‌سازیم. این مجموعه از اعداد، مجموعهٔ خارج قسمتهای اعضای $\mathbb{Z}[\sqrt{n}]$ می‌باشد و یک میدان عددی است، یعنی تحت $+$، $-$، $\times$ و $\div$ (بر عناصر غیر صفر) بسته است. خواص بسته بودن به سادگی با محاسبه بررسی می‌شود (تمرین).

تعریف نرم را توسط همان فرمول

$$\text{نرم}\,(x + y\sqrt{n}) = x^{2} - ny^{2}$$

به $\mathbb{Q}[\sqrt{n}]$ توسیع می‌دهیم. این فرمول بامعنی باقی می‌ماند زیرا بنابر استدلال بخش ۱.۵ هر عنصر $\mathbb{Q}[\sqrt{n}]$ به طور منحصر به فردی به صورت $x + y\sqrt{n}$ برای x و y ی گویا قابل بیان است.

خاصیت ضربی نرم. برای هر α و β در $\mathbb{Q}[\sqrt{n}]$ داریم

$$\text{نرم}\,(\alpha\beta) = \text{نرم}\,(\alpha)\ \text{نرم}\,(\beta).$$

برهان. فرض کنیم $\alpha = x_{1} + y_{1}\sqrt{n}$ و $\beta = x_{2} + y_{2}\sqrt{n}$. در این صورت

$$\begin{aligned} \text{نرم}\,(\alpha)\ \text{نرم}\,(\beta) &= (x_{1}^{2} - ny_{1}^{2})(x_{2}^{2} - ny_{2}^{2}) \\ &= (x_{1}x_{2} + ny_{1}y_{2})^{2} - n(x_{1}y_{2} + y_{1}x_{2})^{2} \\ &= \text{نرم}\,(\alpha\beta). \quad \square \end{aligned}$$

تمرینها

۱.۴.۵ نشان دهید $\mathbb{Q}[\sqrt{n}]$ تحت +، − و × بسته است.

۲.۴.۵ نشان دهید که $\frac{1}{x+y\sqrt{n}}$ برای $x, y \in \mathbb{Q}$ (که هر دو با هم صفر نیستند) به صورت $x' + y'\sqrt{n}$ برای x' و y' ی گویا می‌باشد. نتیجه بگیرید که $\mathbb{Q}[\sqrt{n}]$ تحت تقسیم بر عناصر غیر صفر بسته است.

خاصیت ضربی نرم را می‌توان به صورت زیر مجدداً بیان کرد.

۳.۴.۵ اگر (x_1, y_1) در $x^2 - ny^2 = k_1$ و نیز (x_2, y_2) در $x^2 - ny^2 = k_2$ صدق کنند آنگاه نشان دهید که $(x_1x_2 + ny_1y_2, x_1y_2 + y_1x_2)$ در $x^2 - ny^2 = k_1k_2$ صدق می‌کند.

براهماگوپتا از این حقیقت برای حل $x^2 - ny^2 = 1$ با استفاده از معادله‌های ساده‌تری مانند $x^2 - ny^2 = k$ استفاده کرده است. روش وی هنگامی که جوابی واضح برای $x^2 - ny^2 = -1$ موجود باشد متداول‌تر است.

۴.۴.۵ با جست و جو جوابی غیر بدیهی برای $x^2 - 17y^2 = -1$ بیابید و از آن برای پیدا کردن جوابی غیر بدیهی برای $x^2 - 17y^2 = 14$ استفاده کنید.

۵.۴.۵ به طور مشابه جوابی غیر بدیهی برای $x^2 - 37y^2 = 1$ بیابید.

۵.۵ استدلال لانه کبوتری

کوچک‌ترین جواب غیر بدیهی $x^2 - ny^2 = 1$ همیشه به آسانی حالات $n = 2$ و $n = 3$ پیدا نمی‌شود. مثلاً کوچک‌ترین جواب غیر بدیهی $x^2 - 61y^2 = 1$ برابر

$$(x, y) = (1766319049, 226153980)$$

می‌باشد! این مثال جذاب توسط بهاسکارا[۹] II در قرن دوازدهم و مجدداً توسط فرما کشف شد.

کوچک‌ترین جواب غیر بدیهی، بسیار غیر قابل پیش‌بینی ظاهر می‌شود و لذا وجود آن در حالت کلی واضح نیست. با این حال لاگرانژ در سال ۱۷۶۸ اثبات کرد که اگر n عدد دلخواه مثبت صحیح و نامربعی باشد آنگاه معادلهٔ پل $x^۲ - ny^۲ = ۱$ جوابی صحیح غیر از $(\pm ۱, ۰)$ دارد.

برهانی جدید و جالب از این مطلب توسط دیریکله در حدود سال ۱۸۴۰ ارائه شد. وی چیزی را به کار برد که اکنون اصل لانه کبوتری نامیده می‌شود: اگر بیش از k کبوتر در k لانه بروند آنگاه حداقل یک لانه شامل حداقل دو کبوتر است (صورت متناهی)؛ اگر تعدادی نامتناهی کبوتر در k لانه بروند آنگاه حداقل یک لانه شامل تعدادی نامتناهی کبوتر است (صورت نامتناهی).

استدلال دیریکله را می‌توان به دو گام زیر تقسیم کرد. در ابتدا، قضیه‌ای در باب تقریب اعداد اصم:

قضیهٔ تقریب دیریکله. برای هر عدد اصم به صورت $\sqrt{n}$ و هر عدد صحیح مانند $B > ۰$، اعدادی صحیح مانند a و b با شرط $۰ < b < B$ موجودند که

$$|a - b\sqrt{n}| < \frac{۱}{B}.$$

برهان. برای هر عدد صحیح مانند $B > ۰$ تعداد $B - ۱$ عدد $\sqrt{n}$، $۲\sqrt{n}$، ...، $(B - ۱)\sqrt{n}$ را در نظر می‌گیریم. برای هر k، عدد صحیح A_k را که در شرط

$$۰ < A_k - k\sqrt{n} < ۱$$

صدق می‌کند انتخاب می‌کنیم[۱۰]. چون $\sqrt{n}$ اصم است، اعداد $A_k - k\sqrt{n}$ اکیداً بین ۰ و ۱ هستند و همگی به همین دلیل متفاوت می‌باشند (بنابر نتیجهٔ بخش

---

[۹] Bhaskara

[۱۰] در حقیقت A_k برابر جزء صحیح $k\sqrt{n}$ است. (م)

۱.۵). لذا $B+۱$ عدد متفاوت

$$۰, A_۱ - \sqrt{n}, A_۲ - ۲\sqrt{n}, \dots, A_{B-۱} - (B-۱)\sqrt{n}, ۱$$

در بازهٔ $[۰, ۱]$ قرار دارند.

اگر این بازه را به B زیربازه با طول $\frac{۱}{B}$ تقسیم کنیم، بنابر اصل لانه کبوتری متناهی نتیجه می‌شود که حداقل یکی از زیربازه‌ها شامل دو عدد است. بنابراین اختلاف این دو عدد (که برای a و b یی صحیح به صورت $a - b\sqrt{n}$ هستند) عدد اصمی است که در

$$|a - b\sqrt{n}| < \frac{۱}{B}$$

صدق می‌کند. همچنین $b < B$ زیرا b اختلافِ دو عدد صحیحِ کمتر از B است. □

چند گام زیر کاربردهای کوتاه و مستقیمی از اصل لانه کبوتری نامتناهی است.

۱. چون قضیهٔ تقریب دیریکله برای هر $B > ۰$ برقرار است می‌توانیم $\frac{۱}{B}$ را به طور دلخواه کوچک کنیم که باعث انتخاب مقادیر جدید a و b می‌گردد. لذا تعدادی نامتناهی زوج صحیح مانند (a, b) با شرط $|a - b\sqrt{n}| < \frac{۱}{B}$ وجود دارد. چون $۰ < b < B$ داریم

$$|a - b\sqrt{n}| < \frac{۱}{b}.$$

۲. از گام ۱ نتیجه می‌شود که

$$|a + b\sqrt{n}| \leq |a - b\sqrt{n}| + |۲b\sqrt{n}| \leq |۳b\sqrt{n}|$$

و بنابراین

$$|a^۲ - nb^۲| \leq \frac{۱}{b} \cdot ۳b\sqrt{n} = ۳\sqrt{n}.$$

از این رو تعدادی نامتناهی $a-b\sqrt{n}\in\mathbb{Z}[\sqrt{n}]$ با نرم کمتر یا مساوی $۳\sqrt{n}$ وجود دارد.

۳. بنابر اصل لانه کبوتری نامتناهی داریم

- تعدادی نامتناهی $a-b\sqrt{n}$ با نرم یکسان (مثلاً N) وجود دارد.
- تعدادی نامتناهی از این اعداد با a در یک ردهٔ همنهشتی به پیمانهٔ N قرار دارند.
- تعدادی نامتناهی از این اعداد با b در یک ردهٔ همنهشتی به پیمانهٔ N قرار دارند.

۴. بنابر گام ۳، دو عدد مثبت $a_۱-b_۱\sqrt{n}$ و $a_۲-b_۲\sqrt{n}$ وجود دارند که

- نرم آنها با هم برابر و مساوی N است،
- $a_۱\equiv_N a_۲$،
- $b_۱\equiv_N b_۲$.

آخرین گام از خارج قسمت $a-b\sqrt{n}$ (که از تقسیم کردن دو عددی که هم‌اکنون پیدا شد حاصل می‌شود) استفاده می‌کند. نرم این عدد برابر $a^۲-nb^۲$ است که بنابر خاصیت ضربی نرم، به وضوح برابر ۱ می‌باشد. چندان روشن نیست که a و b صحیح هستند اما اکنون صحیح بودن آنها از شرایط همنهشتی مذکور در گام ۴ نتیجه می‌شود.

جواب غیر بدیهی معادلهٔ پل. اگر n یک عدد صحیح مثبت نامربع باشد، آنگاه معادلهٔ $x^۲-ny^۲=۱$ جواب صحیحی مانند (a,b)، متمایز با $(\pm۱,۰)$ دارد.

برهان. خارج قسمت $a-b\sqrt{n}$ از دو عدد $a_۱-b_۱\sqrt{n}$ و $a_۲-b_۲\sqrt{n}$ را که در گام ۴ پیدا شد در نظر می‌گیریم. داریم

$$a-b\sqrt{n} \;=\; \frac{a_۱-b_۱\sqrt{n}}{a_۲-b_۲\sqrt{n}}$$

$$\begin{aligned} &= \frac{(a_۱ - b_۱\sqrt{n})(a_۲ + b_۲\sqrt{n})}{a_۲^۲ - nb_۲^۲} \\ &= \frac{a_۱a_۲ - nb_۱b_۲}{N} + \frac{a_۱b_۲ - b_۱a_۲}{N}\sqrt{n}, \end{aligned}$$

که در آن $N = a_۲^۲ - nb_۲^۲$ نرم مشترک $a_۱ - b_۱\sqrt{n}$ و $a_۲ - b_۲\sqrt{n}$ است. چون اعداد اخیر نرم یکسان دارند، خارج قسمت آنها، یعنی $a - b\sqrt{n}$ بنابر خاصیت ضربی نرم دارای نرم ۱ است (بخش ۴.۵).

چون $a_۱ - b_۱\sqrt{n}$ و $a_۲ - b_۲\sqrt{n}$ نامساوی و مثبت هستند، خارج قسمت آنها یعنی $a - b\sqrt{n}$ مخالف ± ۱ می‌باشد. باقی می‌ماند که نشان دهیم a و b صحیح هستند. این مطلب معادل این است که نشان دهیم N اعداد $a_۱a_۲ - nb_۱b_۲$ و $a_۱b_۲ - b_۱a_۲$ را عاد می‌کند؛ یا به عبارت دیگر

$$a_۱a_۲ - nb_۱b_۲ \equiv_N a_۱b_۲ - b_۱a_۲ \equiv_N ۰.$$

اولین همنهشتی با توجه به $a_۱^۲ - nb_۱^۲ = N$ و همنهشتیهای $a_۱ \equiv_N a_۲$ و $b_۱ \equiv_N b_۲$ که در گام ۴ گفته شد نتیجه می‌شود. در حقیقت داریم

$$۰ \equiv_N a_۱^۲ - nb_۱^۲ \equiv_N a_۱a_۱ - nb_۱b_۱ \equiv_N a_۱a_۲ - nb_۱b_۲.$$

برای اثبات همنهشتی دوم می‌توانیم طرفین همنهشتیهای $a_۱ \equiv_N a_۲$ و $b_۱ \equiv_N b_۲$ را در یکدیگر ضرب کنیم. □

۶.۵ * صورتهای مربعی

استدلال لانه کبوتری دیریکله یکی از شایسته‌ترین راه‌ها برای اثبات وجود جوابهای غیر بدیهی معادلهٔ پل است و شامل ایده‌هایی است که می‌توانند در وضعیتهای دیگر نیز به کار روند. علی رغم این، برهان دیریکله چندان مرتبط با معادله‌های دیوفانتی مربعی نیست و لذا دلیلی برای ارائهٔ برهانی دیگر وجود دارد: برهانی که مبتنی بر نظریه‌ای کلی در مورد صورتهای مربعی می‌باشد.

یک صورت مربعی دودویی[11] مانند $Ax^2 + Bxy + Cy^2$ (که در آن $A, B, C \in \mathbb{Z}$) را می‌توان به عنوان تابعی صحیح مقدار بر زوجهای صحیح یا بردارهای (x, y) تلقی کرد. بسیاری از معادله‌های کلاسیک در نظریه اعداد، با مقادیر صورتهای مربعی سر و کار دارند. مثلاً معادلهٔ پل سؤال می‌کند که آیا صورت $x^2 - ny^2$ مقداری برابر ۱ دارد یا نه. برای نزدیک شدن به این قبیل سؤالها، دو خاصیت مقدماتی صورتهای مربعی را که می‌توان توسط جبر ساده تأیید کرد به کار می‌بریم.

خواص صورتهای مربعی. اگر $f(x, y) = Ax^2 + Bxy + Cy^2$ و نیز $v = (x, y)$، آنگاه

۱. $f(kv) = k^2 f(v)$،

۲. $f(v_1 + v_2) + f(v_1 - v_2) = 2[f(v_1) + f(v_2)]$.

برهان. ۱. اگر $v = (x, y)$ آنگاه $kv = (kx, ky)$. از این رو

$$\begin{aligned} f(kv) &= A(kx)^2 + B(kx)(ky) + C(ky)^2 \\ &= k^2(Ax^2 + Bxy + Cy^2) \\ &= k^2 f(v). \end{aligned}$$

۲. اگر $v_1 = (x_1, y_1)$ و $v_2 = (x_2, y_2)$ آنگاه

$$\begin{aligned} f(v_1) &= Ax_1^2 + Bx_1y_1 + Cy_1^2, \\ f(v_2) &= Ax_2^2 + Bx_2y_2 + Cy_2^2. \end{aligned}$$

همچنین

$$f(v_1 + v_2) = A(x_1 + x_2)^2 + B(x_1 + x_2)(y_1 + y_2) + C(y_1 + y_2)^2$$

---

[11] binary quadratic form

$$\begin{aligned}
&= Ax_1^2 + Ax_2^2 + Bx_1y_1 + Bx_2y_2 + Cy_1^2 + Cy_2^2 \\
&\quad +2Ax_1x_2 + Bx_2y_1 + Bx_1y_2 + 2Cy_1y_2 \\
f(v_1 - v_2) &= A(x_1 - x_2)^2 + B(x_1 - x_2)(y_1 - y_2) + C(y_1 - y_2)^2 \\
&= Ax_1^2 + Ax_2^2 + Bx_1y_1 + Bx_2y_2 + Cy_1^2 + Cy_2^2 \\
&\quad -2Ax_1x_2 - Bx_2y_1 - Bx_1y_2 - 2Cy_1y_2
\end{aligned}$$

از این رو

$$\begin{aligned}
&f(v_1 + v_2) + f(v_1 - v_2) \\
&= 2Ax_1^2 + 2Ax_2^2 + 2Bx_1y_1 + 2Bx_2y_2 + 2Cy_1^2 + 2Cy_2^2 \\
&= 2[f(v_1) + f(v_2)]. \ \square
\end{aligned}$$

نتیجهٔ سادهای از خاصیت ۱ این است که $f(-v) = f(v)$. لذا یک صورت مربعی، بین برداری مانند v و قرینهٔ آن تمایزی قائل نمی‌شود. خاصیت ۱ همچنین می‌گوید که $f(kv)$ مضرب $f(v)$ است؛ بالاخص اگر $f(v)$ اول (یا ۱) باشد آنگاه $v = (x, y)$ مضرب صحیحی از برداری صحیح نیست؛ یعنی x و y نسبت به هم اول هستند. چنین بردارهایی را بردارهای اولیه[۱۲] می‌نامیم.

در بخش ۸.۲ نقشه‌ای از همهٔ بردارهای اولیه با x و y مثبت را یافتیم. همچنین دریافتیم که چنین بردارهایی توسط $\mathbf{i} = (1, 0)$ و $\mathbf{j} = (0, 1)$ به وسیلهٔ فرآیند $(v_1, v_2) \mapsto (v_1 + v_2, v_2)$ و $(v_1, v_2) \mapsto (v_1, v_1 + v_2)$ تولید می‌شوند.

در بخش بعد می‌بینیم بردارهایی که x و y آنها مختلف‌العلامه هستند به طور مشابه توسط $(0, -1)$ و $(1, 0)$ تولید می‌شوند. خاصیت ۲ نشان می‌دهد که ارتباطی ساده بین مقادیر f در مراحل متوالی این فرآیندها وجود دارد. این مطلب به نقشهٔ مقادیر f منجر می‌گردد.

---

[۱۲] primitive vectors

صورتهای معادل

نگاهی دیگر به صورت مربعی f (مرتبط با آنچه در بالا توصیف شد) همهٔ صورتهای معادل مانند $f^*(x,y) = f(px+qy, rx+sy)$ را به وسیلهٔ تعویض بردار سطری (x,y) با

$$(px+qy, rx+sy) = (x \quad y)\begin{pmatrix} p & r \\ q & s \end{pmatrix} = (x,y)M$$

به اختصار به دست می‌دهد که در آن ماتریس M و معکوس آن $M^{-۱}$ هر دو درایه‌های صحیح دارند. وقتی M در این شرایط صدق کند، زوج $(px+qy, rx+sy)$ در مجموعهٔ $\mathbb{Z}^۲$ متشکل از همهٔ زوجهای صحیح تغییر می‌کند. در حقیقت اگر (x', y') زوج صحیح دلخواهی باشد داریم

$$(x' \quad y') = (x \quad y)M \qquad \Longleftrightarrow \qquad (x \quad y) = (x' \quad y')M^{-۱}.$$

صورتهای معادل، مجموعهٔ مقادیر یکسانی دارند. مثلاً $x^۲ + y^۲$ و $x^۲ + ۲xy + y^۲$ مقادیر یکسانی دارند که صورت دوم را می‌توان از $x^۲ + y^۲$ با جایگذاری $(x+y, y)$ به جای (x,y) به دست آورد.

وقتی M و $M^{-۱}$ هر دو درایه‌های صحیح داشته باشند $\det M$ و $\det M^{-۱}$ هر دو صحیح هستند. حال چون

$$MM^{-۱} = \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix},$$

با دترمینان گرفتن از طرفین با توجه به خاصیت ضربی دترمینان داریم

$$\det M \cdot \det M^{-۱} = ۱.$$

بنابراین تنها مقادیر ممکن برای $\det M$ و $\det M^{-۱}$ عبارتند از ± ۱. لذا ماتریس M صورتهای مربعی معادلی تعریف می‌کند هرگاه درایه‌های صحیح داشته باشد و $\det M = ps - qr = \pm ۱$. چنین ماتریسی تک پیمانه‌ای[۱۳] نامیده می‌شود.

---
[۱۳] unimodular

حال یک صورت مربعی دلخواه را می‌توان به صورت حاصل ضرب ماتریسی

$$Ax^{2} + Bxy + Cy^{2} = (x \quad y)\begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \qquad (*)$$

نمایش داد. لذا از آنچه اکنون دیدیم نتیجه می‌شود که هر صورت معادل، با جایگذاری

$$M\begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix}M^{-1}$$

به جای $\begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix}$، که در آن M ماتریسی تک پیمانه‌ای است، به دست می‌آید. این مطلب بدان دلیل است که این ماتریس جدید بر تعویض $M(y \quad x)$ $(x \quad y)$ به جای $(x \quad y)$ اثر می‌گذارد.

فرمول $(*)$ مقداری پایا[14] از صورت $Ax^{2} + Bxy + Cy^{2}$ (یعنی دترمینان ماتریسش که برابر $AC - \frac{B^{2}}{4}$ است) را تحت معادل بودن نشان می‌دهد. در حقیقت دترمینان هر صورتی که معادل با آن باشد، یعنی

$$\det(M\begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix}M^{-1})$$

برابر

$$\begin{aligned} \det M \cdot \det\begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix} \cdot \det M^{-1} &= (\pm 1)^{2}\det\begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix} \\ &= \det\begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix} \end{aligned}$$

می‌باشد، چون بنابر فرض $\det M = \det M^{-1} = \pm 1$. لذا همهٔ صورتهای معادل صورت $Ax^{2} + Bxy + Cy^{2}$ دترمینان یکسان دارند.

---

[14] invariant

تمرینها

گرچه صورتهای مربعی معادل، دترمینان یکسان دارند، عکس این مطلب همواره درست نیست. مثلاً صورت $x^۲ + y^۲$ معادل همهٔ صورتهای دیگر با دترمینان ۱ است اما $x^۲ + ۵y^۲$ معادل همهٔ صورتهای دیگر با دترمینان ۵ نیست.

۱.۶.۵ نشان دهید که $۱۳x^۲ + ۱۶xy + ۵y^۲$ دترمینان ۱ دارد و از طریق ماتریس $M = \begin{pmatrix} ۲ & ۳ \\ ۱ & ۲ \end{pmatrix}$ معادل $x^۲ + y^۲$ می‌باشد.

۲.۶.۵ نشان دهید که دترمینان $۲x^۲ + ۲xy + ۳y^۲$ با $x^۲ + ۵y^۲$ یکی است اما با توجه به این که $x^۲ + ۵y^۲$ مقدار ۷ را نمی‌گیرد اثبات کنید که $۲x^۲ + ۲xy + ۳y^۲$، معادل $x^۲ + ۵y^۲$ نیست.

۳.۶.۵ به طور کلی با کار کردن روی مقادیر ممکن $x^۲ + ۵y^۲$ به پیمانهٔ ۲۰ نشان دهید که $x^۲ + ۵y^۲$ هیچ مقدار همنهشت با ۳ یا ۷ به پیمانهٔ ۲۰ را اختیار نمی‌کند.

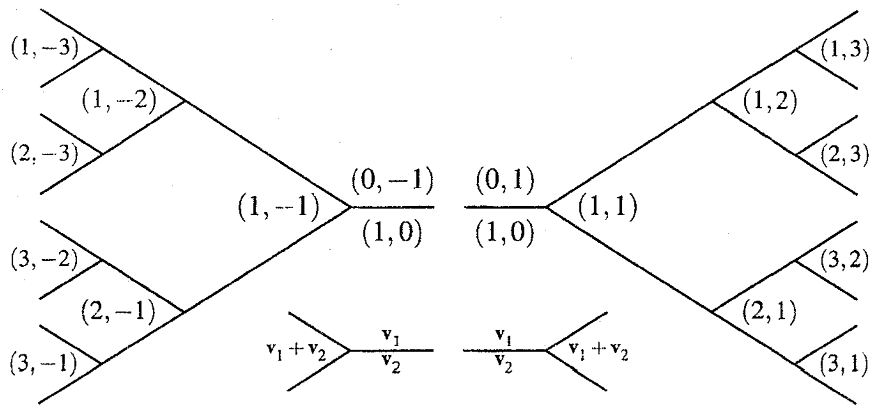
۷.۵ * نقشه بردارهای اولیه

در بخش ۸.۲ افرازی از صفحه (یک نقشه) به ناحیه‌های برچسب خورده توسط (۱, ۰)، (۰, ۱) و همهٔ بردارهای اولیه مانند (a, b) از اعداد طبیعی را توصیف کردیم. شکل ۱.۵ (نیمهٔ سمت راست) مجدداً این نقشه را (که °۹۰ چرخانده شده است) همراه با بازتاب نزدیکی از آن (نیمهٔ سمت چپ) نشان می‌دهد که در آن مختص دوم هر زوج علامت منفی دارد.

همچنین در نیمهٔ سمت راست شکل، قاعدهٔ جمع برداری نموداری را داریم که همهٔ برچسبها را به وسیلهٔ (۱, ۰) و (۰, ۱) تولید می‌کند و در نیمهٔ سمت چپ، قاعدهٔ تصویر بازتابی را که به طور بدیهی در آنجا به کار می‌رود داریم.

این دو نقشه را کنار هم می‌گذاریم زیرا می‌خواهیم آنها را به یکدیگر ملحق سازیم. اما به نظر می‌رسد توسط برچسبهای ناموافق (۱ ,۰) و (۱− ,۰) از انجام این کار در بخش مرکزی بالایی باز می‌مانیم.

این ناسازگاری را می‌توان با دادن یک علامت ± به هر برچسب از بین برد.



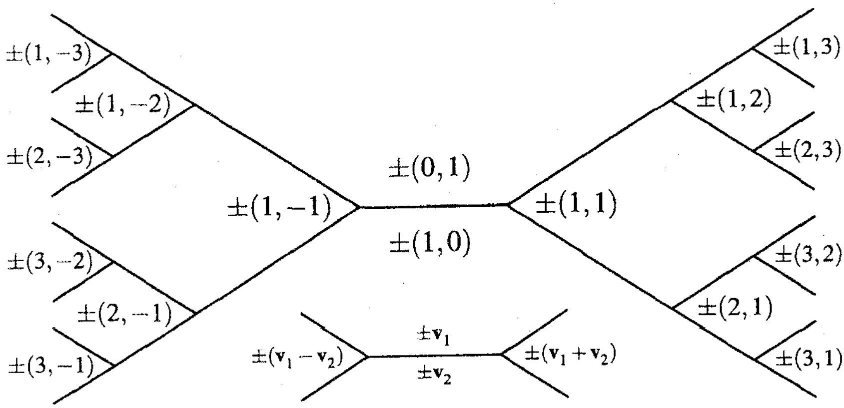
شکل ۱.۵: دو نقشهٔ جزیی از بردارهای اولیه

این کار شکل ۲.۵ را که نقشهٔ (کامل) بردارهای اولیه نامیده می‌شود به دست می‌دهد (بنا به این دلیل آشکار که شامل هر بردار اولیه‌ای می‌باشد). برچسب گذاری ±، دو قاعدهٔ جمع برداری را در یک قاعدهٔ تفاضل/جمع برداری[۱۵] که در زیرِ شکل آمده تلفیق می‌کند.

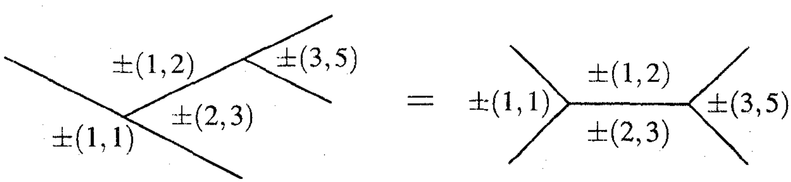
به خاطر علامتهای مبهم، این قاعده به توضیحی چند احتیاج دارد. در یک زوج ± از بردارها (مثلاً (۱, ۲)±) آزادیم که (۱, ۲) یا (۱, ۲)− را برای v_1 انتخاب کنیم. به طور مشابه برای این زوج (مثلاً (۲, ۳)±)، ناحیهٔ پایین یک یال برچسب $\pm v_1$ می‌گیرد: می‌توانیم (۲, ۳) یا (۲, ۳)− را برای v_2 انتخاب کنیم. قاعدهٔ جمع/تفاضل برداری می‌گوید که برای انتخابی از v_1 و v_2، ناحیهٔ بین v_1 و v_2 و در انتهای سمت چپ یال مشترک آنها برچسب $\pm(v_1 - v_2)$ می‌گیرد. در این مثال، ناحیه‌ها به صورت شکل ۳.۵ هستند.

[۱۵] vector difference/sum rule

شکل ۳.۵ نشان می‌دهد که چگونه ممکن است خطوط تغییر شکل یابند تا مؤید صورت نموداریِ قاعدهٔ جمع/تفاضل برداری گردند - بالاخص، یال مشترک ناحیه‌های $\pm(۱,۲)$ و $\pm(۲,۳)$ واقعاً افقی نیست - این قاعده‌ها در بین کرانهایی که مفاهیم بالا، پایین، انتهای راست و انتهای چپ را برای ناحیه‌های $\pm(۱,۲)$ و $\pm(۲,۳)$ حفظ می‌کنند قرار دارند.



شکل ۲.۵: نقشهٔ کامل بردارهای اولیه



شکل ۳.۵: ناحیه‌های بالا، پایین و دو انتهای یک یال

در اینجا انتخاب $v_۱ = (۱,۲)$ و $v_۲ = (۲,۳)$ مقادیر $v_۱ + v_۲ = (۳,۵)$ و $v_۱ - v_۲ = -(۱,۱)$ را به دست می‌دهند. لذا در انتهای سمت راست $\pm(v_۱ + v_۲) = \pm(۳,۵)$ و در انتهای سمت چپ $\pm(v_۱ - v_۲) = \pm(۱,۱)$ را (همان گونه که انتظار داشتیم) داریم.

از قاعده‌های جمع برداری در نقشه‌های چپ و راست مجزای شکل ۱.۵ نتیجه می‌شود که قاعدهٔ جمع/تفاضل برداری در نقشهٔ کامل برقرار است. این موضوع در حالت کلی توسط تعدادی متناهی بررسیهای ساده مشابه مثال فوق اثبات می‌شود. جزئیات برای تمرین باقی می‌ماند.

ابهام علامت $\pm(x,y)$ هیچ اثری بر مقدار یک صورت مربعی ندارد زیرا

$$Ax^۲ + Bxy + Cy^۲ = A(-x)^۲ + B(-x)(-y) + C(-y)^۲.$$

لذا نقشهٔ بردارهای اولیه، یک نقشهٔ غیر مبهم از همهٔ مقادیر صورت مربعی $f(x,y) = Ax^۲ + Bxy + Cy^۲$ برای اعداد نسبت به هم اول x و y به دست می‌دهد که با قرار دادن هر مقدار $f(a,b)$ در ناحیهٔ $\pm(a,b)$ به دست می‌آید. به علاوه ممکن است برخی الگوها را در این نقشه (با تشکر از توازی موجود بین قاعدهٔ جمع/تفاضل برداری و خاصیت ۲ صورتهای مربعی اثبات شده در بخش قبل) ببینیم. این مطلب را در بخش بعد با توجه به پایایی دترمینان $Ac - \frac{B^۲}{۴}$ تحت تعویض متغیرها، نشان خواهیم داد. همچنین نقشهٔ کامل، این تعویضها را همان طور که می‌بینیم نشان می‌دهد.

درخت پایه‌های صحیح

در بخش ۶.۵ صورتهای f و f^* را معادل خواندیم اگر $f^*(x,y)$ از $f(x,y)$ با جایگذاری برداری مانند $(px+qy, rx+sy)$ به جای (x,y) به دست بیاید. این مفهوم معادل است با این که وقتی (x,y) در $\mathbb{Z}^۲$ تغییر می‌کند $(px+qy, rx+sy)$ کل $\mathbb{Z}^۲$ را تولید کند. با توجه به آن که

$$(x,y) = x(۱,۰) + y(۰,۱), \qquad (px+qy, rx+sy) = x(p,r) + y(q,s)$$

می‌توان نتیجه گرفت که مطلب فوق‌الذکر معادل با تعویض بردارهای $(۱,۰)$ و $(۰,۱)$ با بردارهای (p,r) و (q,s) است. این زوج از بردارها (یعنی $(۱,۰)$ و

$((\circ, \mathsf{1}))$ را یک پایهٔ صحیح[۱۶] برای $\mathbb{Z}^{\mathsf{2}}$ می‌نامیم زیرا هر بردار صحیح مانند (x, y) ترکیبی خطی از این دو بردار با ضرایب صحیح (یعنی به صورت $x(\mathsf{1}, \circ) + y(\circ, \mathsf{1})$) می‌باشد.

معادل بودن می‌گوید که تعویض $M : (x, y) \mapsto (px + qy, rx + sy)$ معکوس پذیراست. بنابراین ماتریس معکوس آن یعنی $M^{-\mathsf{1}}$ درایه‌های صحیح دارد و بردارهای جدید نیز پایه‌ای صحیح تشکیل می‌دهند. لذا محکی که برای تشخیص پایهٔ صحیح بودن (p, r) و (q, s) داریم همان محکی است که در بخش ۶.۵ برای صحیح بودن M و $M^{-\mathsf{1}}$ به دست آمد؛ یعنی $ps - qr = \pm \mathsf{1}$.

در بخش ۷.۲ نشان دادیم که اگر (p, r) و (q, s) برچسبهای دو ناحیه با یال مشترک در نقشهٔ زوجهای نسبت به هم اول باشند، آنگاه

$$ps - rq = \pm \mathsf{1}.$$

به سادگی دیده می‌شود که این خاصیت به نقشهٔ کامل شکل ۲.۵ نیز توسیع می‌یابد. لذا هر یال در نقشهٔ بردارهای اولیه، پایهٔ صحیحی از $\mathbb{Z}^{\mathsf{2}}$ را نمایش می‌دهد، یعنی زوج برچسبهای ناحیه‌ها که در یک یال یکدیگر را قطع می‌کنند پایه‌ای صحیح می‌باشد. علامتهای $\pm$ روی برچسبها چهار پایهٔ مختلف که اساساً یکی هستند را به دست می‌دهد. چون یالهای نقشه یک درخت می‌سازند و هر یال به این روش با یک پایهٔ صحیح (تا حد علامت) شریک است، لذا ترکیب یالهای نقشهٔ بردارهای اولیه را درخت پایه‌های صحیح[۱۷] می‌نامیم.

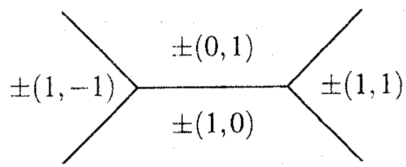
همان طور که این نام پیشنهاد می‌کند، این درخت همهٔ پایه‌های صحیح را نمایش می‌دهد؛ گرچه ما به این حقیقت نیازی نداریم. با این حال با استفاده از قاعدهٔ جمع/تفاضل برداری ایجاب نوعی الگوریتم اقلیدسی آسان اثبات می‌شود (تمرینها را ببینید).

---
[۱۶] integral basis
[۱۷] tree of integral bases

تمرینها

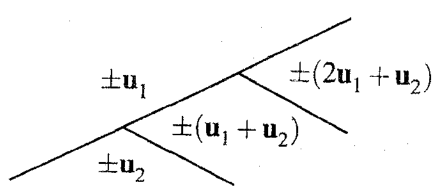
برای اثبات قاعدهٔ جمع/تفاضل برداری در نقشهٔ کامل بردارهای اولیه، بررسی می‌کنیم که این قاعده در میانه و قسمت کلیِ راست و چپ برقرار است.

۱.۷.۵ تحقیق کنید که قاعدهٔ جمع/تفاضل برداری در میانهٔ نقشه (شکل ۴.۵) با انتخاب $v_1 = (0, 1)$ و $v_2 = (1, 0)$ برقرار است.



شکل ۴.۵: میانهٔ نقشهٔ کامل

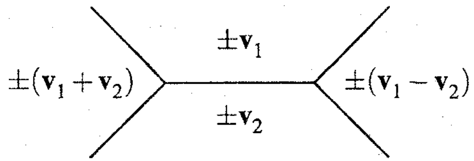
۲.۷.۵ شکل ۵.۵ قسمتی کلی از سمت راست نقشهٔ کامل را نشان می‌دهد. با انتخاب $v_1 = u_1$ و $v_2 = u_1 + u_2$ تحقیق کنید که قاعدهٔ جمع/تفاضل برداری در اینجا نیز برقرار است.



شکل ۵.۵: قسمتی کلی در سمت راست

۳.۷.۵ بررسی کنید که چه قسمتهای کلی دیگری در سمت راست و سمت چپ اتفاق می‌افتد و تحقیق کنید که قاعدهٔ جمع/تفاضل برداری برای هر یک از آنها برقرار است.

۴.۷.۵ قاعدهٔ جمع/تفاضل برداری نشان داده شده در شکل ٦.۵ نیز معتبر است. چرا؟



شکل ٦.۵: قاعدهٔ جمع/تفاضل برداری

برای اثبات این که درخت نقشهٔ کامل همهٔ پایه‌های صحیح را نشان می‌دهد قواعد جمع/تفاضل و تفاضل/جمع را برای ردیابی مسیری از پایه‌ای داده شده مانند $\{(p,r),(q,s)\}$ در جهت عقب به سوی $\{(۱,\circ),(\circ,۱)\}$ به کار می‌بریم. تمرین ۵.۷.۵ یک مثال است و تمرینهای ٦.۷.۵ تا ۸.۷.۵ نشان می‌دهند که چرا چنین مسیری را همواره می‌توان یافت.

۵.۷.۵ با تکرار کم کردن بردارِ کوچک‌تر از بزرگ‌تر، زوج $\{(۳۵,۳),(۲۳,۲)\}$ را به زوج $\{(۱۱,۱),(\circ,۱)\}$ تحویل کنید. زوج اخیر در درخت نمایش داده می‌شود (چرا؟). از این رو زوج اول نیز چنین است (چرا؟).

۶.۷.۵ نشان دهید اگر

$$(p',r')=(p+q,r+s),\qquad (q',s')=(q,s)$$

یا

$$(p',r')=(p,r)\qquad (q',s')=(p+q,r+s)$$

آنگاه

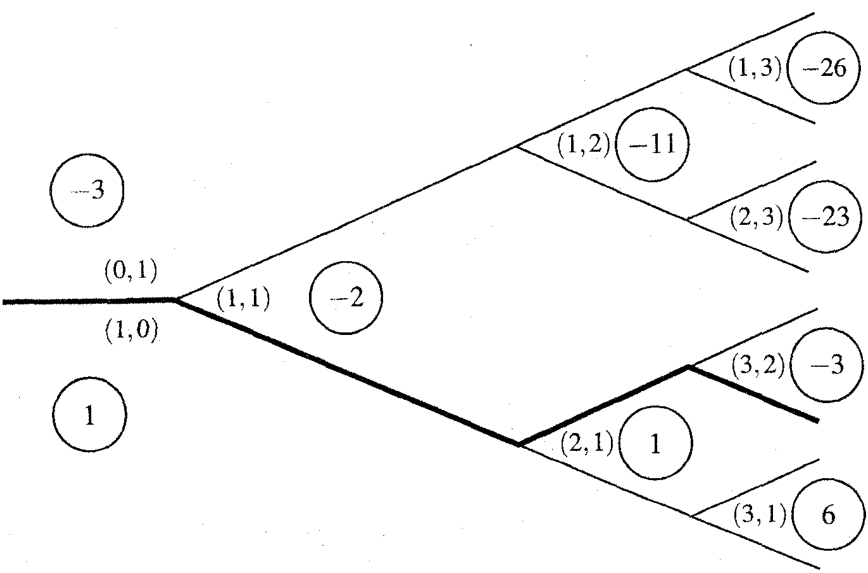
$$ps-qr=\pm ۱\qquad\Longleftrightarrow\qquad p's'-q'r'=\pm ۱.$$

۷.۷.۵ با تکرار جمع یا کم کردن یک بردار از دیگری نشان دهید که هر زوج مانند $\{(p,r),(q,s)\}$ با شرط $pr - qs = \pm ۱$ به زوجی به صورت $\{(p', ۰),(q', s')\}$ تحویل می‌شود. (راهنمایی: $\gcd(r,s) = ۱$. چرا؟) از تمرین **۶.۷.۵** نتیجه بگیرید که $p' = \pm ۱$، $q' = \pm ۱$.

۸.۷.۵ نتیجه بگیرید که $\{(p', ۰),(q', s')\}$ در تمرین **۷.۷.۵** توسط یالی در درخت نمایش داده می‌شود و لذا $\{(p,r),(q,s)\}$ نیز چنین است.

۸.۵ * تناوب در نقشه $x^۲ - ny^۲$

در بخش قبل به اختصار گفتیم که چگونه یک نقشه از صورتی مربعی مانند f را می‌توان با مشخص کردن ناحیهٔ $\pm v$ توسط مقدار $f(v) = f(-v)$ به نقشهٔ بردارهای اولیه تحمیل کرد.

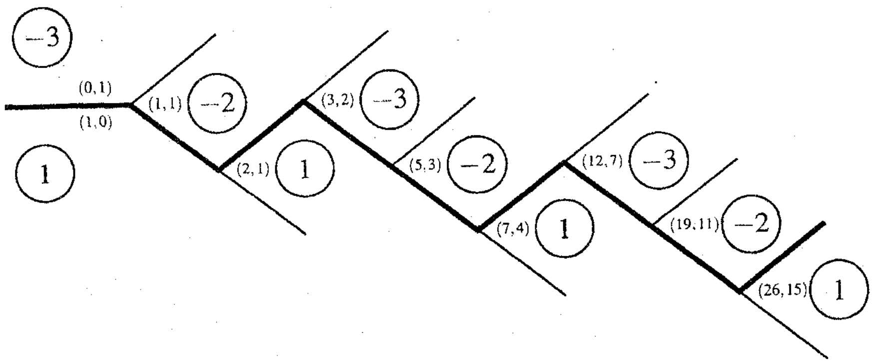


شکل **۷.۵**: نقشهٔ $x^۲ - ۳y^۲$

حال نقشه‌های صورتهای مربعی را عمیق‌تر مورد تحقیق قرار می‌دهیم تا ایده‌ای را از آنچه انتظار داریم به دست آوریم. در ابتدا نقشهٔ $x^۲ - ۳y^۲$ را در شکل ۷.۵ معرفی می‌کنیم. فقط نیمهٔ راست نشان داده شده است زیرا نیمهٔ چپ، تصویر بازتاب آن است. مقادیر، به صورت اعداد داخل دایره نشان داده شده‌اند.

به نظر می‌رسد که در این نقشه، خط جدا کننده‌ای بین مقادیر مثبت و منفی $x^۲ - ۳y^۲$ وجود دارد. کانوِی این خط را (که در شکل ۷.۵ پررنگ کشیده‌ایم) رودخانه[۱۸] می‌نامد. به نظر می‌رسد در هر طرف رودخانه همچنان که از آن دور می‌شویم مقادیر $x^۲ - ۳y^۲$ مطلقاً افزایش می‌یابد (و به همین دلیل است که انتظار داریم فقط یک رودخانه داشته باشیم).

و نسبتاً به طور غیر منتظره‌ای، مقادیر در راستای رودخانه به نظر متناوب هستند: در ناحیه‌های متوالی بالای رودخانه، مقادیر عبارتند از ۳−، ۲−، ۳−، ۲−، ... و در پایینِ هر زوج ناحیهٔ متوالی با مقادیر ۳− و ۲−، یک ناحیه با مقدار ۱ وجود دارد. شکل ۸.۵ این الگو را اندکی بیشتر تأیید می‌کند.



شکل ۸.۵: رودخانهٔ $x^۲ - ۳y^۲$

اگر این الگو ادامه یابد، آنگاه می‌توانیم دنبالهٔ جوابهای صحیح معادلهٔ پل $x^۲ - ۳y^۲$ یعنی (۲, ۱)، (۷, ۴)، (۲۶, ۱۵)، ... را با به کار بردن قاعدهٔ جمع

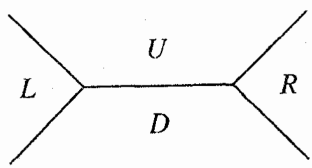
[۱۸] river

برداری برای نقشهٔ بردارهای اولیه که به عنوان ناحیه‌های متوالی با مقدار ۱ قرار گرفته‌اند تولید کنیم (تمرینها را ببینید).

مثال $x^۲ - ۳y^۲$ نمونهٔ خوبی از آنچه در مورد یک صورت مربعی نامعین[19] اتفاق می‌افتد می‌باشد.

یک صورت نامعین صورتی است که هر مقدار مثبت و منفی را اختیار می‌کند اما مقدار صفر را نمی‌پذیرد. به کمک حکم زیر می‌توانیم نشان دهیم که هر صورت مربعی نامعین دارای رودخانه‌ای یکتا با رفتار متناوب است.

قاعدهٔ تصاعد حسابی. اگر L، U، D و R (به ترتیب برای چپ، بالا، پایین و راست) مقادیر یک صورت مربعی حول یال نشان داده شده در شکل ۹.۵ باشند آنگاه



شکل ۹.۵: مقادیر ناحیه‌های حول یک یال

۱. $L, U+D, R$ یک تصاعد حسابی است.

۲. اگر (p,r) و (q,s) به ترتیب ناحیه‌های بالا و پایین یال باشند آنگاه قدرنسبت در این تصاعد برابر ضریب xy در صورت مربعی $f(px+qy, rx+sy)$ است.

برهان. قاعدهٔ جمع/تفاضل در نقشهٔ بردارهای اولیه (بخش ۷.۵) ایجاب می‌کند که

$$L = f(v_۱ - v_۲), \quad U = f(v_۱), \quad D = f(v_۲), \quad R = f(v_۱ + v_۲),$$

---
[19] indefinite

که در آن $v_۱$ و $v_۲$ ناحیه‌های بالا و پایین یال میانی هستند. لذا از خاصیت ۲ صورتهای مربعی (بخش ۶.۵) نتیجه می‌شود که

$$L + R = ۲(U + D) \quad \text{یا}\ (U + D) - L = R - (U + D),$$

و این می‌گوید که $L, U + D, R$ یک تصاعد حسابی است.

از بخش ۷.۵ یادآوری می‌کنیم که اگر به جای پایهٔ $\mathbf{i} = (۱, ۰)$، $\mathbf{j} = (۰, ۱)$ از $\mathbb{Z}^۲$ پایهٔ $v_۱ = (p, r)$، $v_۲ = (q, s)$ را قرار دهیم آنگاه صورت $f(x, y)$ توسط صورت معادل

$$f^*(x, y) = f(px + qy, rx + sy) = Ax^۲ + Bxy + Cy^۲$$

جایگزین می‌گردد. همچنین مقادیر f در $v_۱$، $v_۲$، $v_۱ + v_۲$ و $v_۱ - v_۲$ همان مقادیر f^* در $\mathbf{i}$، $\mathbf{j}$، $\mathbf{i}+\mathbf{j}$ و $\mathbf{i}-\mathbf{j}$ یعنی به ترتیب برابر A، C، $A + B + C$ و $A - B + C$ می‌باشد.

لذا قدر نسبت $(U + D) - L$ در تصاعد حسابی برابر $A + C - (A - B + C) = B$ است. □

بخش ۱ از قاعدهٔ تصاعد حسابی کافی است تا نشان دهیم که:

یکتایی رودخانه. برای هر صورت به شکل $x^۲ - ny^۲$ (که در آن n یک عدد طبیعی نامربع است) مسیر یالی یکتایی در نقشهٔ بردارهای اولیه وجود دارد که ناحیه‌های با مقدار مثبت را از ناحیه‌های با مقدار منفی جدا می‌سازد.

برهان. چنین صورتی هرگز صفر نیست چون $x^۲ - ny^۲ = ۰$ ایجاب می‌کند که $n = \frac{x^۲}{y^۲}$ یک مربع کامل باشد. به علاوه مطمئناً $x^۲ - ny^۲$ مقادیر مثبت و منفی را اختیار می‌کند. مکانی روی نقشه که یک ناحیه با مقدار $L < ۰$، دو ناحیه با مقادیر $U, D > ۰$ را ملاقات می‌کند همانند شکل ۹.۵ در نظر می‌گیریم. (اگر ناحیهٔ با مقدار L واقعاً سمت راست باشد کماکان $L, U + D, R$ یک تصاعد حسابی تشکیل می‌دهند.)

بخش ۱ ایجاب می‌کند که

$$R - (U + D) = (U + D) - L > U + D.$$

از این رو $R > \max\{U, D\}$. لذا کنار گذاشتن یک یال از مرز بین مقادیر مثبت و منفی منجر به ناحیه‌ای با مقدار مثبت بزرگ‌تر می‌شود.

به طور کلی‌تر، اگر $D > \max\{U, L\}$ آنگاه بنابر کاربرد مشابهی از خاصیت بخش ۱ داریم $R > D$. بنابراین همچنان که در ناحیهٔ منفی پیش رویم مقادیر ناحیه‌ها به طور مداوم زیاد می گردد. به طور مشابه مقادیر طرف منفی مداوماً کم می‌شوند هرگاه از مسیر مرزی بین ناحیه‌های مثبت و منفی پیش رویم. از این رو فقط یک مسیر یالی جدا کنندهٔ ناحیهٔ مثبت از منفی وجود دارد. □

بخش ۲ از قاعدهٔ تصاعد حسابی را برای اثبات خاصیت تناوبی سخت‌تری که وجود جوابهای غیر بدیهی معادلهٔ پل را تضمین می‌کند احتیاج داریم.

تناوب رودخانه. هرگاه n یک عدد طبیعی نامربع باشد، الگوی مقادیر در طرفین رودخانه برای $x^۲ - ny^۲$ متناوب است.

برهان. کافی است اثبات کنیم که ناحیه‌های مشترک در یال با رودخانه، از حیث قدرمطلق کراندار هستند. در حقیقت اگر چنین باشد مقادیر L، U و D در شکل ۹.۵ حول یالی از رودخانه تکرار خواهند شد؛ لذا مقدار R (که توسط L، U و D بر حسب قاعدهٔ تصاعد حسابی تعیین می‌شود) نیز چنین است. اما ناحیهٔ R نیز در یالی با رودخانه مشترک است و به همین ترتیب استدلال پیش می‌رود.

همان طور که در برهان بخش ۲ دیدیم، مقادیر U و D برابر C و A هستند که در آن $Ax^۲ + Bxy + Cy^۲$ صورتی مربعی مانند f^* است که با $f(x, y) = x^۲ - ny^۲$ معادل می‌باشد. اما از بخش ٦.۵ می‌دانیم که دترمینان $AC - \frac{B^۲}{۴}$ برای همهٔ معادلهای f^* از f یکسان است. در اینجا C و A که مقادیر ناحیه‌های دو سمت متفاوت رودخانه هستند علامت متفاوت دارند. از این رو

$$|AC - \frac{B^۲}{۴}| = |A||C| + \frac{B^۲}{۴}.$$

چون $AC - \frac{B^۲}{۴}$ ثابت است نتیجه می‌شود که $|A|$ و $|C|$ (قدرمطلقهای D و U) کراندار هستند. □

تمرینها

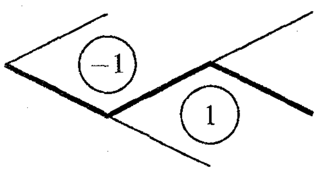
دلیلی ندارد که صورتهای مربعی پل یعنی $x^۲ - ny^۲$، تنها صورتهای نامعین باشند. یک مثال جالب دیگر $x^۲ + xy - y^۲$ است که مرتبط با نسبت طلایی[۲۰] یعنی $\frac{۱+\sqrt{۵}}{۲}$ و دنبالهٔ فیبوناچی ۱، ۱، ۲، ۳، ۵، ۸، ۱۳، ... می‌باشد.

۱.۸.۵ نشان دهید که

$$x^۲ + xy - y^۲ = (x + y\frac{۱+\sqrt{۵}}{۲})(x + y\frac{۱-\sqrt{۵}}{۲})$$

و نتیجه بگیرید که صورت $x^۲ + xy - y^۲$ نامعین است.

۲.۸.۵ ساختن رودخانهٔ $x^۲ + xy - y^۲$ را تا جایی ادامه دهید که بتوانید اثبات کنید تناوب آن شبیه شکل ۱۰.۵ است.



شکل ۱۰.۵: تناوب $x^۲ + xy - y^۲$

۳.۸.۵ نشان دهید برچسبهای مثبت (x_i, y_i) که متناوباً پایین و بالای رودخانه هستند (در ناحیه‌هایی که متناوباً ۱ و ۱− می‌باشند) در

$$(x_۱, y_۱) = (۱, ۱), \qquad (x_{i-۱}, y_{i-۱}) + (x_i, y_i) = (x_{i+۱}, y_{i+۱})$$

صدق می‌کنند.

---
[۲۰] golden ratio

۴۸.۵ از تمرین ۳.۸.۵ نتیجه بگیرید که زوجهای طبیعی صادق در معادلهٔ $x^۲ + xy - y^۲ = ۱$ عبارتند از $(F_{۲n+۱}, F_{۲n+۲})$ که در آن $F_۱ = F_۲ = ۱$ و $F_i + F_{i-۱} = F_{i+۱}$ (دنبالهٔ فیبوناچی).

تناوب در شکل رودخانه، به طور طبیعی به بازگشتی شدن روابط بین بردارهای برچسب زنندهٔ ناحیه‌های مجاور رودخانه منجر می‌گردد. رابطهٔ فیبوناچی به دست آمده از $x^۲ + xy - y^۲$، ساده‌ترین مثال از چنین روابط بازگشتی می‌باشد. مثالی دیگر، رابطهٔ بازگشتی برای $x^۲ - ۳y^۲$ است که رودخانهٔ آن در بالا ساخته شد.

۵۸.۵ دو تناوب متوالی در رودخانه برای $x^۲ - ۳y^۲$ را به کار ببرید تا نشان دهید که جوابهای نامنفی (x_i, y_i) از $x^۲ - ۳y^۲ = ۱$ در

$$(x_۰, y_۰) = (۱, ۰), \qquad (x_{i+۱}, y_{i+۱}) = ۴(x_i, y_i) - (x_{i-۱}, y_{i-۱})$$

صدق می‌کنند.

همچنین این رودخانه نشان می‌دهد که چرا برخی معادله‌ها هیچ جوابی ندارند.

۶۸.۵ شرح دهید که چرا معادلهٔ $x^۲ - ۳y^۲ = -۱$ هیچ جواب صحیحی ندارد.

۹.۵ بحث

معادلهٔ پل $x^۲ - ny^۲ = ۱$ یکی از قدیمی‌ترین و مهم‌ترین معادله‌های دیوفانتی مربعی می‌باشد که احتمالاً تنها رقیب آن معادلهٔ فیثاغورسی $x^۲ + y^۲ = z^۲$ است. همچنین معادلهٔ پل به زمان فیثاغورس (حدود ۵۰۰ قبل از میلاد) باز می‌گردد که وی حالت خاص $x^۲ - ۲y^۲ = ۱$ را در مورد $\sqrt{۲}$ (همان گونه که در بخش ۱.۵ اشاره شد) مطالعه می‌کرده است.

یک معادلهٔ پل معروف دیگر منسوب به ارشمیدس[۲۱] است. مسألهٔ احشام[۲۲] وی به معادلهٔ پل $x^۲ - ۴۷۲۹۴۹۴y^۲ = ۱$ منجر می‌گردد که کوچک‌ترین جواب غیر بدیهی آن x ی با ۲۰۶۵۴۵ رقم دارد! این جواب مطمئناً برای ارشمیدس شناخته شده نبوده است گرچه وی می‌دانسته که معادله‌های پل می‌توانند جوابهایی داشته باشند که به طور قابل توجهی بزرگ هستند. برای بحثی عالی در مورد مسألهٔ احشام و محاسباتی که به وجود می‌آورد لنسترا[۲۳] (۲۰۰۲) را ببینید.

معادلهٔ پل مجدداً در هندوستان کشف شد؛ جایی که ریاضیدانان شیفتهٔ مسائل کوتاه با جوابهای بزرگ بودند. در حدود سال 600 بعد از میلاد، براهماگوپتا فرمول ترکیب جوابها را که در بخش ۴.۵ استفاده کردیم کشف کرد. وی تعمیمی از آن را برای یافتن جواب کمین (۱۱۵۱, ۱۲۰) برای $x^۲ - ۹۲y^۲ = ۱$ به کار برد (وی معتقد بود که اگر شخصی بتواند این معادله را طی یک سال حل کند ریاضیدان است). در سال ۱۱۵۰ بعد از میلاد، بهاسکارا II ایدهٔ براهماگوپتا را به روشی که همهٔ معادله‌های پل را حل می‌کرد توسیع داد. او از مثال $x^۲ - ۶۱y^۲ = ۱$ که به خوبی انتخاب شده بود برای این کار بهره جست. وی کوچک‌ترین جواب آن یعنی (۱۷۶۶۳۱۹۰۴۹, ۲۲۶۱۵۳۹۸۰) را (که تاکنون بزرگ‌ترین مقدارِ کوچک‌ترین جواب معادلهٔ پل $x^۲ - ny^۲ = ۱$ برای $n \leq ۶۱$ می‌باشد) یافت.

در اروپا هیچ چیزی در مورد کشفیات هندیها نمی‌دانستند اما معادلهٔ پل مجدداً در قرن هفدهم (هنگامی که فرما به طور مستقل چگونگی حل آن را کشف کرد) پا به عرصه گذاشت. او روش خود را فاش نکرد اما به طور بدیهی می‌دانست چه می‌کند زیرا وی نیز $x^۲ - ۶۱y^۲ = ۱$ را برای مبارزه‌طلبی با ریاضیدانان دیگر مطرح کرد. وی همچنین معادلهٔ وحشتناک‌تر

[۲۱] Archimedes
[۲۲] cattle problem
[۲۳] Lenstra

$x^۲ - ۱۰۹y^۲ = ۱$ را که کوچک‌ترین جواب غیر بدیهی آن

$$(۱۵۸۰۷۰۶۷۱۹۸۶۲۴۹, ۱۵۱۴۰۴۲۴۴۵۵۱۰۰)$$

می‌باشد مطرح کرد. رقبای انگلیسی وی، والیس[۲۴] و برونکر[۲۵] مبارزه را با روشی که معادلهٔ پل را به شیوه‌ای متفاوت با بهاسکارا II حل می‌کرد در پیش گرفتند (ویل[۲۶] (۱۹۸۴) صفحهٔ ۹۴ را ببینید). در قرن هجدهم این روشها به صورت الگوریتم کسرهای مسلسل به شکلی زیباتر و ساده‌تر (که می‌توان آن را الگوریتم اقلیدسی به کار رفته برای زوج $(\sqrt{n}, ۱)$ تلقی کرد) شکل گرفت.

همهٔ این روشها مبتنی بر مشاهدهٔ متناوب بودن در محاسباتی خاص می‌باشد. چنین به نظر می‌رسد که یونانیان تناوب را در الگوریتم اقلیدسی مشاهده کرده‌اند زیرا استدلالهای هندسی ساده، تناوب آن را در زوجهایی از قبیل $(\sqrt{۲}, ۱)$ و $(\sqrt{۳}, ۱)$ نشان می‌دهد (مثلاً استیلول (۱۹۹۸) صفحهٔ ۲۶۸ یا آرتمن[۲۷] (۱۹۹۹) صفحهٔ ۲۴۲ را ببینید). در حالی که ممکن است افراد زیادی تناوب را برای حل نمونه‌های معادلهٔ پل استفاده کرده باشند، با این حال اولین کسی که اثبات کرد تناوب همیشه اتفاق می‌افتد لاگرانژ (۱۷۶۸) بود. وی بدینوسیله نشان داد که روش کسرهای مسلسل همیشه کار می‌کند. او با اثبات این که حل معادلهٔ پل به حل همهٔ معادله‌های دیوفانتی مربعی دو متغیره منجر می‌شود بر اهمیت این نتیجه صحه گذاشت.

رهیافت شهودی کانوِی که در بخشهای ۶.۵ تا ۸.۵ شرح داده شد، مطمئناً مرتبط با رهیافتهای قبلی با معادلهٔ پل است. اما این رهیافت اساساً از این جهت ساده‌تر است که یک فرآیند (الگوریتم اقلیدسی) را با یک تصویر (نقشهٔ بردارهای اولیه) عوض می‌کند. در این کتاب، سعی بر آن بوده است که این موضوع به اندازهٔ ممکن با به دست آوردن نقشهٔ بردارهای اولیه و خواص آن به

---

[۲۴] Wallis
[۲۵] Brouncker
[۲۶] Weil
[۲۷] Artmann

طور مستقیم از خواص الگوریتم اقلیدسی قبل از نشاندن یک صورت مربعی بر آن روشن گردد. (کانوی ساده‌ترین خواص نقشه یا طرحی از برهانهای توپولوژیکی را فرض می‌کند و بقیه را به کمک صورتهای مربعی اثبات می‌کند.) برای بصیرت بیشتری که از رهیافت کانوی قابل حصول است کتاب کانوی (۱۹۹۷) یا نوار ویدیویی او را در مورد $ax^۲ + hxy + by^۲$ که از طریق انجمن ریاضی امریکا در دسترس است ببینید.

۶

اعداد صحیح گاوسی

پیش‌نگاه

اعداد صحیح گاوسی، یعنی $\mathbb{Z}[\mathrm{i}]$، ساده‌ترین تعمیم اعداد صحیح هستند و در اکثر موارد این اعداد رفتاری یکسان با اعداد صحیح دارند. بالاخص، $\mathbb{Z}[\mathrm{i}]$ از یکتایی تجزیه به اعداد اول برخوردار است و این مطلب به ما اجازه می‌دهد که در مورد $\mathbb{Z}[\mathrm{i}]$ همانند $\mathbb{Z}$ استدلال کنیم. این کار را بدان جهت انجام می‌دهیم که $\mathbb{Z}[\mathrm{i}]$ مکانی طبیعی برای مطالعهٔ خواص مشخص $\mathbb{Z}$ است. به ویژه، بهترین مکان برای تجزیهٔ مجموع دو مجذور است چرا که در $\mathbb{Z}[\mathrm{i}]$ می‌توانیم مجموع دو مجذور صحیح را به صورت خطی تجزیه کنیم: $x^۲ + y^۲ = (x - y\mathrm{i})(x + y\mathrm{i})$.

در فصل حاضر این ایده را برای اثبات قضیهٔ معروف فرما به کار می‌بریم: اگر $p > ۲$ عددی اول باشد آنگاه اعدادی طبیعی مانند a و b موجودند که $p = a^۲ + b^۲$ فقط و فقط وقتی که عددی طبیعی مانند n موجود باشد که $p = ۴n + ۱$. قضیهٔ دو مجذور فرما نه تنها با یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\mathrm{i}]$ بلکه با اعداد اول واقعی در $\mathbb{Z}[\mathrm{i}]$ نیز که به اعداد اول گاوسی[۱] موسوم هستند،

[۱] Gaussian prime number

مرتبط از آب در می‌آید.

به سادگی نشان داده می‌شود که اعداد اول گاوسی شامل اعداد اول معمولی که مجموع دو مجذور نیستند و عوامل $a-b\mathrm{i}$ و $a+b\mathrm{i}$ از هر عدد اول به صورت $a^{۲}+b^{۲}$ می‌باشد. یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\mathrm{i}]$ نتیجه می‌دهد که این اعداد تنها اعداد اول گاوسی (تا حد مضربی توسط ۱± و $\pm\mathrm{i}$) هستند.

یک استدلال همنهشتی ساده نشان می‌دهد که اعداد اول معمولی به صورت $۴n+۳$ مجموع دو مجذور نیستند. لذا قضیهٔ دو مجذور نشان می‌دهد اعداد اولی که مجموع دو مجذور هستند ۲ و همهٔ اعداد اول دیگر (یعنی آنهایی که به صورت $۴n+۱$ هستند) می‌باشند.

برهان قضیهٔ دو مجذور با لم مهمی که به وسیلهٔ قضیهٔ ویلسون اثبات می‌شود سر و کار دارد: هر عدد اول مانند $p=۴n+۱$ عددی به صورت $m^{۲}+۱$ را عاد می‌کند. چون $m^{۲}+۱$ در $\mathbb{Z}[\mathrm{i}]$ تجزیه می‌شود از یکتایی تجزیه به اعداد اول نتیجه می‌شود که p نیز چنین است. تجزیهٔ p به صورت $(a-b\mathrm{i})(a+b\mathrm{i})$ است و از این رو همان گونه که ادعا شد $p=(a-b\mathrm{i})(a+b\mathrm{i})=a^{۲}+b^{۲}$.

۱.۶ اعداد صحیح گاوسی و نرم آنها

در فصل قبل دیدیم که سؤالهای خاصی در $\mathbb{Z}$ توسط کار کردن با اعداد صحیح تعمیم‌یافته توضیح داده می‌شوند؛ به ویژه، کار کردن در $\mathbb{Z}[\sqrt{n}]$ برای حل $x^{۲}-ny^{۲}=۱$ در $\mathbb{Z}$ را دیدیم. نقش $\mathbb{Z}[\sqrt{n}]$ در این حالت امکان تجزیهٔ

$$x^{۲}-ny^{۲}=(x-y\sqrt{n})(x+y\sqrt{n})$$

است. به طور مشابه، هنگام مطالعهٔ $x^{۲}+y^{۲}$ استفاده از اعداد صحیح گاوسی یعنی

$$\mathbb{Z}[\mathrm{i}]=\{a+b\mathrm{i}:a,b\in\mathbb{Z}\}$$

کمک می‌کند چون $x^۲ + y^۲ = (x - y\mathrm{i})$.

مجموع دو مجذور، یعنی $x^۲ + y^۲$، قدیمی‌ترین مبحث در نظریه اعداد است. قبلاً نتایجی در این باب را که توسط بابِلیها، اقلیدس و دیوفانتوس به دست آمده بود دیدیم. در حقیقت می‌توان گفت برخی از خواص $\mathbb{Z}[\mathrm{i}]$ تا این حد به عقب برمی‌گردد؛ حداقل تا زمان دیوفانتوس.

ظاهراً دیوفانتوس از اتحاد دو مجذور (بخش ۸.۱)

$$(a_۱^۲ + b_۱^۲)(a_۲^۲ + b_۲^۲) = (a_۱a_۲ - b_۱b_۲)^۲(a_۱b_۲ + b_۱a_۲)^۲$$

خبر داشته است چون وی می‌دانسته که حاصل ضرب مجموع دو مجذور در مجموع دو مجذور، خود مجموع دو مجذور است. امروزه این فرمول را به صورت معادل خاصیت ضربی نرم

$$|z_۱||z_۲| = |z_۱z_۲|$$

می‌شناسیم که در آن $z_۱ = a_۱ + b_۱\mathrm{i}$ و $z_۲ = a_۲ + b_۲\mathrm{i}$. و اتحاد دیوفانتوس دقیقاً فرمول

$$(*) \qquad \text{نرم}\,((a_۱ + b_۱\mathrm{i})(a_۲ + b_۲\mathrm{i})) = \text{نرم}\,(a_۲ + b_۲\mathrm{i})\ \text{نرم}\,(a_۱ + b_۱\mathrm{i})$$

می‌باشد که در آن نرم نشان‌دهندهٔ نرم در $\mathbb{Z}[\mathrm{i}]$ یعنی

$$\text{نرم}\,(a + b\mathrm{i}) = |a + b\mathrm{i}| = a^۲ + b^۲$$

است.

تمرینها

هنگامی که در مورد تجزیه بحث می‌کنیم همواره عواملی بدیهی وجود دارند که یکه نامیده می‌شوند و ترجیح می‌دهیم که از آنها چشم‌پوشی کنیم. مثلاً در $\mathbb{N}$

تنها یکه ۱ است، در $\mathbb{Z}$ یکه‌ها ۱ و ۱− هستند و در $\mathbb{Z}[\mathrm{i}]$ یکه‌ها عناصر با نرم ۱ می‌باشند.

۱.۱.۶ نشان دهید یکه‌های $\mathbb{Z}[\mathrm{i}]$ عبارتند از ۱± و $\pm\mathrm{i}$.

به طور مشابه، یکه‌های $\mathbb{Z}[\sqrt{n}]$ عناصر با نرم ۱ در آن، یعنی $a+b\sqrt{n}$ هایی که $a^{۲}-nb^{۲}=۱$، می‌باشند.

۲.۱.۶ یکه‌های $\mathbb{Z}[\sqrt{۲}]$ را توصیف کنید.

۳.۱.۶ نشان دهید که $\mathbb{Z}[\sqrt{n}]$ به ازای هر عدد طبیعی نامربع، بی‌نهایت یکه دارد.

۲.۶ عادپذیری و اعداد اول

نرم $\mathbb{Z}[\mathrm{i}]$ یعنی

$$\text{نرم}\ (a+b\mathrm{i}) = |a+b\mathrm{i}| = a^{۲}+b^{۲}$$

بیش از قدر مطلق در نظریه اعداد مفید است زیرا این نرم همواره یک عدد صحیح معمولی می‌باشد. خاصیت ضربی نرم یعنی (*) ایجاب می‌کند که اگر عدد صحیح گاوسی α، عدد صحیح گاوسی γ را عاد کند، یعنی اگر β یی در $\mathbb{Z}[\mathrm{i}]$ موجود باشد که

$$\gamma = \alpha\beta$$

آنگاه

$$\text{نرم}\ (\gamma) = \text{نرم}\ (\alpha)\ \text{نرم}\ (\beta),$$

یعنی نرم (α) باید نرم (γ) را عاد کند.

بدین دلیل، سؤالات مربوط به عادپذیری در $\mathbb{Z}[\mathrm{i}]$ اغلب به سؤالات عادپذیری در $\mathbb{Z}$ تحویل می‌شود. بالاخص، به طور طبیعی می‌توان یک عدد اول

گاوسی را به عنوان عددی گاوسی که حاصل ضرب اعداد صحیح گاوسی با نرم کوچک‌تر نیست تعریف کرد. پس می‌توانیم سؤالات گوناگونی را در مورد اعداد اول گاوسی با توجه به نرم آنها پاسخ دهیم.

مثالها.

۱. ۴+i یک عدد اول گاوسی است.

چون ۱۷ = ۱ + ۱۶ = نرم (۴+i)، که عدد اولی در $\mathbb{Z}$ است. از این رو ۴+i حاصل ضرب دو عدد صحیح گاوسی با نرم کمتر نیست، چرا که هیچ نرمی ۱۷ را عاد نمی‌کند.

۲. ۲ یک عدد گاوسی اول نیست.

چون (۱+i)(۱−i) = ۲ و نرم اعداد ۱−i و ۱+i برابر ۲ است که کمتر از ۴ = نرم (۲) می‌باشد.

۳. ۱−i و ۱+i عوامل اول گاوسی ۲ هستند.

چون ۲ = نرم (۱+i) = نرم (۱−i) عددی اول در $\mathbb{Z}$ است از این رو ۱−i و ۱+i حاصل ضرب اعداد صحیح گاوسی با نرم کمتر نیستند.

تجزیه به عوامل اول در $\mathbb{Z}[i]$. هر عدد صحیح گاوسی به اعداد اول گاوسی تجزیه می‌شود. برهان آن مشابه برهان در $\mathbb{Z}$ است.

برهان. عدد صحیح گاوسی دلخواهی مانند γ را در نظر می‌گیریم. اگر γ خود یک عدد اول گاوسی باشد کار تمام است. اگر چنین نباشد آنگاه α و β یی در $\mathbb{Z}[i]$ با نرم کمتر موجودند که $\gamma = \alpha\beta$. اگر α یا β اول گاوسی نباشد آن را به اعداد گاوسی با نرم کمتر تجزیه می‌کنیم و این کار را ادامه می‌دهیم. این فرآیند باید در جایی خاتمه یابد چون نرم عددی طبیعی است و نمی‌تواند تا ابد کوچک شود. از این رو سرانجام به تجزیهٔ γ به اعداد اول گاوسی می‌رسیم. □

همانند $\mathbb{Z}$، نمی‌توان بلادرنگ نتیجه گرفت که تجزیه به اعداد اول یکتاست. اما در بخش ۴.۶ می‌بینیم که یکتایی تجزیه به اعداد اول گاوسی با استدلالی

همانند آنچه در $\mathbb{Z}$ آمد برقرار است.

تمرینها

روشی معادل برای تعریف اعداد اول گاوسی به طریقی متداول همچون اعداد اول معمولی این است که بگوییم ϖ[۲] یک عدد اول گاوسی است هرگاه ϖ تنها توسط یکه‌ها و مضارب یکهٔ ϖ عاد شود. (همان طور که p برای نمایش اعداد اول معمولی به کار می‌رود، قرارداد بر این است که حرف یونانی π را برای نمایش اعداد اول در $\mathbb{Z}[\mathrm{i}]$ و دیگر تعمیمهای $\mathbb{Z}$ به کار برند. با این حال برای اجتناب از ابهام با $\pi = ۳/۱۴۱۵۹\ldots$ ترجیح می‌دهیم از ϖ که شکل دیگری از π است استفاده کنیم.)

۱.۲.۶ توضیح دهید که چرا این تعریف با آنچه قبلاً گفتیم معادل است.

۲.۲.۶ با در نظر گرفتن مقسوم‌علیه‌های نرم (۳) ثابت کنید که ۳ یک عدد اول گاوسی است.

همان طور که قبلاً در مثال ۲ دیدیم، اعداد اول معمولی همیشه اعداد اول گاوسی نیستند. در حقیقت ۲ تقریباً یک مربع کامل در $\mathbb{Z}[\mathrm{i}]$ است.

۳.۲.۶ نشان دهید مضرب یکه‌ای از ۲ یک مربع کامل در $\mathbb{Z}[\mathrm{i}]$ است.

۴.۲.۶ اعداد ۱۷ و ۵۳ را در $\mathbb{Z}[\mathrm{i}]$ تجزیه کنید.

۳.۶ مزدوجها

مزدوج عدد $z = a + b\mathrm{i}$ برابر $\bar{z} = a - b\mathrm{i}$ است. خواص مزدوجگیری (نه تنها در

[۲] این حرف رسم الخط دیگری از حرف یونانی π است و به همان شکل تلفظ می‌شود. (م)

$\mathbb{Z}[\mathrm{i}]$ بلکه برای همهٔ عددهای مختلط) عبارتند از

$$\begin{aligned} z\bar{z} &= |z|^2, \\ \overline{z_1 + z_2} &= \bar{z_1} + \bar{z_2}, \\ \overline{z_1 - z_2} &= \bar{z_1} - \bar{z_2}, \\ \overline{z_1 \times z_2} &= \bar{z_1} \times \bar{z_2}. \end{aligned}$$

این تساویها را می‌توان با نوشتن $z_1 = a_1 + b_1\mathrm{i}$ و $z_2 = a_2 + b_2\mathrm{i}$ و کار کردن روی دو طرف هر یک از اتحادها بررسی کرد. از این خواص مزدوجگیری برای گام اول به منظور رده‌بندی اعداد اول گاوسی بهره می‌گیریم.

اعداد اول گاوسی حقیقی. یک عدد اول معمولی مانند $p \in \mathbb{N}$ یک عدد اول گاوسی است $\Longleftrightarrow$ p مجموع دو مجذور نباشد. (و به طور بدیهی $p < 0$ یک عدد اول گاوسی است $\Longleftrightarrow$ $-p \in \mathbb{N}$ یک عدد اول گاوسی باشد.)

برهان. $(\Rightarrow)$ فرض کنیم یک عدد اول معمولی مانند p داریم که عدد اول گاوسی نیست. پس p در $\mathbb{Z}[\mathrm{i}]$ تجزیه می‌شود. لذا اعداد صحیح گاوسی $a + b\mathrm{i}$ و γ موجودند که نرم آنها کمتر از نرم p (یعنی p^2) است و

$$p = (a + b\mathrm{i})\gamma.$$

با مزدوجگیزی از طرفین داریم

$$p = (a - b\mathrm{i})\bar{\gamma},$$

چون p حقیقی است و $p = \bar{p}$. با ضرب کردن این دو عبارت در یکدیگر داریم

$$\begin{aligned} p^2 &= (a - b\mathrm{i})(a + b\mathrm{i})\gamma\bar{\gamma} \\ &= (a^2 + b^2)|\gamma|^2, \end{aligned}$$

که در آن هم $a^2 + b^2$ و هم $|\gamma|^2$ بزرگ‌تر از ۱ هستند. اما تنها تجزیهٔ p^2 به این صورت برابر $p \cdot p$ است. از این رو $p = a^2 + b^2$.

($\Leftarrow$) بالعکس، اگر عدد اول معمولی p به صورت $a^2 + b^2$ برای a و b یی در $\mathbb{Z}$ باشد آنگاه p یک عدد اول گاوسی نیست زیرا تجزیهٔ

$$p = (a - b\mathrm{i})(a + b\mathrm{i})$$

به اعداد اول گاوسی را دارد که عوامل آن با نرم $p = a^2 + b^2$ هستند که کمتر از نرم $p^2 = (p)$ است. $\square$

همچنین توجه کنید که عوامل $a - b\mathrm{i}$ و $a + b\mathrm{i}$ از p، اعداد اول گاوسی هستند زیرا نرم آنها برابر عدد اول $p = a^2 + b^2$ می‌باشد. به علاوه مزدوج هر عدد اول گاوسی مانند $a + b\mathrm{i}$، که $a, b \neq 0$، نیز یک عدد اول گاوسی است زیرا اگر عددی به صورت $\alpha\beta$ تجزیه شود آنگاه مزدوج آن نیز به صورت $\bar{\alpha}\bar{\beta}$ تجزیه می‌شود.

آنچه تاکنون روشن نیست این است که آیا هر عدد اول گاوسی مانند $a + b\mathrm{i}$، که $a, b \neq 0$، عامل یک عدد اول معمولی همچون $p = a^2 + b^2$ است. قابل تصور است که $a + b\mathrm{i}$ بتواند یک عدد اول گاوسی باشد در حالی که $a^2 + b^2$ حاصل ضربی از دو یا چند عدد اول معمولی باشد. در بخش ۴.٦ چنین اتفاقی را به کمک یکتایی تجزیه به عوامل اول در $\mathbb{Z}[\mathrm{i}]$ رد می‌کنیم.

به هر تقدیر می‌توانیم ببینیم که هر توضیح دیگری در مورد طبیعت اعداد اول گاوسی، بستگی به یافتن روشی دیگر برای توصیف اعداد اول معمولی که مجموع دو مجذور هستند دارد. در بخش ۷.۳ (مثال ۱) دیدیم که اعداد اول معمولی که مجموع دو مجذور نیستند به صورت $4n + 3$ می‌باشند. متمم این حکم (یعنی این که هر عدد اول به صورت $4n + 1$ مجموع دو مجذور است) قضیهٔ معروفی است که توسط فرما کشف شد. این مطلب در بخش ۵.٦ اثبات می‌شود.

تمرینها

۱.۳.۶ خواص مقدماتی مزدوجگیری را که در بالا اشاره شد تحقیق کنید.

برهان رده‌بندی اعداد اول گاوسی حقیقی نتایج جالب زیر را دارد.

۲.۳.۶ نشان دهید که برای هر عدد اول معمولی، عددی اول و گاوسی که شریک با آن است وجود دارد و برای دو عدد اول معمولی متمایز، اعداد اول گاوسی شریک با آنها متمایز است.

۳.۳.۶ نتیجه بگیرید که بی‌نهایت عدد اول گاوسی وجود دارد.

از آنجایی که اعداد اول گاوسی مثبت حقیقی به صورت $۴n + ۳$ هستند، روشی دیگر برای اثبات نامتناهی بودن اعداد اول گاوسی این است که نشان دهیم بی‌نهایت عدد اول معمولی به صورت $۴n + ۳$ وجود دارد. برهان این مطلب شبیه برهان اقلیدس است که در بخش ۱.۱ آمد.

۴.۳.۶ نشان دهید که حاصل ضرب اعداد به صورت $۴n + ۱$ به همین شکل است. نتیجه بگیرید که هر عدد به صورت $۴n + ۳$ مقسوم‌علیه اولی به صورت $۴n + ۳$ دارد.

۵.۳.۶ اگر $p_۱$، $p_۲$، ...، p_k اعداد اولی به صورت $۴n + ۳$ باشند آنگاه نشان دهید که $۲p_۱p_۲\cdots p_k + ۱$ نیز به صورت $۴n + ۳$ است.

۶.۳.۶ از تمرینهای ۴.۳.۶ و ۵.۳.۶ نتیجه بگیرید که بی‌نهایت عدد اول به صورت $۴n + ۳$ وجود دارد.

۴.۶ تقسیم کردن در اعداد صحیح گاوسی

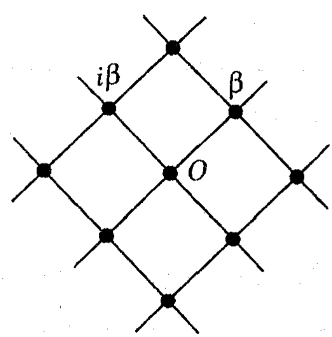
یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\mathrm{i}]$ همانند $\mathbb{Z}$ بر الگوریتم اقلیدسی تکیه می‌کند که وابسته به حقیقت زیر است.

خاصیت تقسیم در $\mathbb{Z}[\mathrm{i}]$. اگر $\alpha, \beta \neq ۰$ در $\mathbb{Z}[\mathrm{i}]$ آنگاه خارج قسمتی مانند μ و باقیمانده‌ای مانند ρ موجود است که

$$\alpha = \mu\beta + \rho, \qquad |\rho| < |\beta|.$$

برهان. با توجه به این که مضارب صحیح گاوسی $\mu\beta$ از هر عدد صحیح گاوسی مانند $\beta \neq ۰$ شبکه‌ای[۳] مربعی را در صفحهٔ مختلط پدید می‌آورد، حکم فوق بدیهی است.

این مطلب بدین دلیل است که ضرب کردن β در i بردار واصل از ۰ به β را ۹۰° دوران می‌دهد و از این رو ۰، β و $\mathrm{i}\beta$ سه گوشهٔ یک مربع هستند. همهٔ مضارب دیگر β مجموع (یا تفاضل) β و $\mathrm{i}\beta$ هستند و از این رو در گوشه‌های یک شبکهٔ مربعی قرار دارند. (شکل ۱.٦.)



شکل ۱.٦: مضارب یک عدد صحیح گاوسی

lattice[۳]

هر عدد صحیح گاوسی مانند α در یکی از این مربعها قرار دارد، و نزدیک‌ترین گوشه مانند $\mu\beta$ (که لزوماً منحصر به فرد نیست؛ گرچه اهمیتی ندارد) برای آن وجود دارد. بنابراین

$$\alpha = \mu\beta + \rho \quad \text{که در آن} \quad |\rho| = \text{فاصله تا نزدیک‌ترین گوشه}$$

لذا $|\rho|$ کمتر از ضلع مربع یعنی $|\beta|$ است. □

با تشکر از خاصیت تقسیم، نتایج زیر را داریم

۱. الگوریتمی اقلیدسی برای $\mathbb{Z}[\mathrm{i}]$.

۲. برای μ و ν یی در $\mathbb{Z}[\mathrm{i}]$ داریم $\gcd(\alpha, \beta) = \mu\alpha + \nu\beta$.

۳. خاصیت مقسوم علیه اول: اگر عددی اول مانند ϖ عدد $\alpha\beta$ را عاد کند آنگاه ϖ باید α یا β را عاد کند.

۴. یکتایی تجزیه به اعداد اول تا حد ترتیب و عوامل با نرم ۱ (یعنی ± 1 و $\pm\mathrm{i}$). عناصر با نرم ۱ یکه نامیده می‌شوند و یکتایی تجزیه به اعداد اول معمولاً با صفت تا حد عوامل یکه می‌آید. این مطلب حتی در $\mathbb{Z}$ نیز درست است که در آن یکه‌ها ± 1 هستند و از این رو اعداد اول تا حد علامت تغییر می‌کنند.

به عنوان اولین کاربرد از یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\mathrm{i}]$ توصیف اعداد اول گاوسی را که در بخش ۳.٦ شروع شد تکمیل می‌کنیم. در آنجا دریافتیم که اعداد اول گاوسی حقیقی، اعداد اول حقیقی که مجموع دو مجذور نیستند و قرینهٔ آنها می‌باشند. همچنین واضح است که اعداد اول گاوسیِ موهومی محض به صورت $\pm\mathrm{i}p$ هستند که p یک عدد اول گاوسی حقیقی است. لذا باقی می‌ماند که اعداد اول گاوسی مانند $a + b\mathrm{i}$ را که a و b ناصفر هستند توصیف کنیم.

اعداد گاوسی موهومی. اعداد اول گاوسی $a + b\mathrm{i}$ با شرط $a, b \neq 0$، عوامل اعداد اول معمولی مانند p که به صورت $a^2 + b^2$ هستند می‌باشند.

برهان. همان طور که در بخش ۳.٦ گفتیم، در ابتدا توجه می‌کنیم که اگر $a+b\mathrm{i}$ یک عدد اول گاوسی باشد آنگاه $a-b\mathrm{i}$ نیز چنین است (چون اگر $a-b\mathrm{i}=\alpha\beta$ اول نباشد آنگاه $a+b\mathrm{i}=\bar{\alpha}\bar{\beta}$ نیز چنین است.)

سپس توجه می‌کنیم که $(a-b\mathrm{i})(a+b\mathrm{i})$ تجزیهٔ (لزوماً منحصر به فردی) از

$$p=a^{۲}+b^{۲}=(a-b\mathrm{i})(a+b\mathrm{i})$$

به اعداد اول گاوسی است. اما در این صورت باید p یک عدد اول معمولی باشد. در حقیقت اگر

$$p=rs \qquad ۱<r,s<p,\ r,s\in\mathbb{Z},$$

آنگاه عوامل اول گاوسی r و s تجزیهٔ دیگری از p غیر از $(a-b\mathrm{i})(a+b\mathrm{i})$ را به اعداد اول گاوسی به دست می‌دهند (یا دو عامل حقیقی r و s یا حداقل چهار عامل مختلط). □

تمرینها

با استفاده از یکتایی تجزیه به اعداد اول می‌توانیم احکامی در مورد مربعها و مکعبهای کامل در $\mathbb{Z}[\mathrm{i}]$ را مشابه آنچه در بخش ۵.۲ در مورد $\mathbb{N}$ گفته شد اثبات کنیم. تنها تفاوت در این است که باید یکه‌ها را نیز به حساب آوریم، همان طور که در واقع قبلاً نیز در $\mathbb{Z}$ انجام دادیم.

۱.۴.۶ آیا در $\mathbb{Z}$ این مطلب درست است که عوامل نسبت به هم اول یک مربع کامل، خود مربع کامل هستند؟ اگر چنین نیست چگونه می‌توان این جمله را تعدیل کرد تا درست شود؟

۲.۴.۶ نشان دهید که عوامل نسبت به هم اول یک مکعب کامل در $\mathbb{Z}$، خود مکعب کاملند.

۳.۴.۶ قضیه‌ای را در مورد عوامل نسبت به هم اول یک مربع کامل در $\mathbb{Z}[i]$ بیان کنید.

۴.۴.۶ نشان دهید که عوامل نسبت به هم اول یک مکعب کامل در $\mathbb{Z}[i]$، خود مکعب کاملند.

۵.۶ قضیه دو مجذور فرما

در بخش ۷.۳ از همنهشتی به پیمانهٔ ۴ استفاده کردیم تا نشان دهیم که اعداد اول به صورت $۴n + ۳$ مجموع دو مجذور نیستند. قضیهٔ دو مجذور فرما بیان می‌دارد که بقیهٔ اعداد اول فرد (یعنی آنهایی که به صورت $۴n + ۱$ هستند) همگی مجموع دو مجذورند.

نظریهٔ اعداد صحیح گاوسی را برای یک عدد اول مانند $p + ۴n + ۱$ به کمک m ی که p مقسوم‌علیه $m^۲ + ۱$ است به کار می‌بریم. چنین m ی بنابر حکمی از لاگرانژ (۱۷۷۳) (که از قضیهٔ ویلسون

$$۱ \times ۲ \times ۳ \times \ldots \times (p - ۱) \equiv_p -۱$$

در بخش ۵.۳ نتیجه می‌شود) همواره وجود دارد.

لم لاگرانژ. برای هر عدد اول مانند $p = ۴n + ۱$ عددی مانند $m \in \mathbb{Z}$ موجود است که p عدد $m^۲ + ۱$ را عاد می‌کند.

برهان. اگر قضیهٔ ویلسون را در مورد عدد اول $p = ۴n + ۱$ به کار بریم داریم

$$\begin{aligned}
-۱ &\equiv_p ۱ \times ۲ \times ۳ \times \ldots \times ۴n \\
&\equiv_p (۱ \times ۲ \times ۳ \times \ldots \times ۲n) \times ((۲n + ۱) \times \ldots \times (۴n - ۱)(۴n)) \\
&\equiv_p (۱ \times ۲ \times ۳ \times \ldots \times ۲n) \times ((-۲n) \times \ldots \times (-۲)(-۱))
\end{aligned}$$

$$\equiv_p \quad (۱ \times ۲ \times ۳ \times \ldots \times ۲n)^۲(-۱)^{۲n}$$
$$\equiv_p \quad (۱ \times ۲ \times ۳ \times \ldots \times ۲n)^۲.$$

و لذا با فرض $m = (۲n)!$ داریم $-۱ \equiv_p m^۲$. یعنی p عدد $m^۲ + ۱$ را عاد می‌کند. □

قضیهٔ دو مجذور فرما. اگر $p = ۴n + ۱$ اول باشد آنگاه a و b یی در $\mathbb{Z}$ موجودند که $p = a^۲ + b^۲$.

برهان. برای p ی داده شده با توجه به لم فوق فرض می‌کنیم $m \in \mathbb{Z}$ به گونه‌ای باشد که p عدد $m^۲ + ۱$ را عاد کند. عدد $m^۲ + ۱$ تجزیه‌ای به صورت

$$m^۲ + ۱ = (m - \mathrm{i})(m + \mathrm{i})$$

در $\mathbb{Z}[\mathrm{i}]$ دارد. و گرچه p عدد $m^۲ + ۱$ را عاد می‌کند ولی $m-\mathrm{i}$ و $m+\mathrm{i}$ را عاد نمی‌کند چون $\frac{m}{p} - \frac{\mathrm{i}}{p}$ و $\frac{m}{p} + \frac{\mathrm{i}}{p}$ اعداد صحیح گاوسی نیستند.

بنابر خاصیت مقسوم‌علیه اول گاوسی از بخش ۴.۶ نتیجه می‌شود که p یک عدد اول گاوسی نیست. اما در این صورت همان گونه که در بخش ۳.۶ اثبات شد باید داشته باشیم $p = a^۲ + b^۲$. □

همچنین نتیجه می‌شود که

$$p = (a - b\mathrm{i})(a + b\mathrm{i})$$

تجزیه‌ای به اعداد اول گاوسی است و اکنون می‌دانیم که هر تجزیه‌ای از این نوع، منحصر به فرد است. لذا در حقیقت شکل قوی‌تری از قضیهٔ دو مجذور فرما را داریم: هر عدد اول مانند $۴n + ۱$ مجموعی به صورت $a^۲ + b^۲$ از دو مجذور برای زوجی منحصر به فرد از اعداد طبیعی مانند a و b است.

تمرینها

در اینجا پرتویی از $\mathbb{Z}[\mathrm{i}]$ بر مجموع دو مجذور را به طریقی دیگر مشاهده می‌کنید. تمرینهای زیر برهانی از قضیهٔ اویلر (۱۷۴۷) را شرح و بسط می‌دهد: اگر $\gcd(a,b)=۱$ آنگاه هر مقسوم‌علیه $a^۲+b^۲$ به صورت $c^۲+d^۲$ است که در آن $\gcd(c,d)=۱$. گام اصلی، مبتنی بر یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\mathrm{i}]$ است.

۱.۵.۶ مثالی ارائه دهید که نشان دهد چرا شرط $\gcd(a,b)=۱$ ضروری است.

۲.۵.۶ نشان دهید که هر مقسوم‌علیه صحیح از $a^۲+b^۲$ مانند $e>۱$، حاصل ضربی از مقسوم‌علیه‌های اول گاوسی به صورت $q+r\mathrm{i}$ از $a^۲+b^۲$ است که تا حد عوامل یکه منحصر به فرد می‌باشد.

۳.۵.۶ نشان دهید که هر یک از اعداد اول گاوسی $q+r\mathrm{i}$، یا $a-b\mathrm{i}$ را عاد می‌کند یا $a+b\mathrm{i}$ را. نتیجه بگیرید که هیچ یک از آنها یک عدد اول معمولی نیست.

۴.۵.۶ نشان دهید که برای هر عامل اول گاوسی از e مانند $q+r\mathrm{i}$، مزدوج آن یعنی $q-r\mathrm{i}$ نیز یک عامل است.

۵.۵.۶ از تمرین ۴.۵.٦ نتیجه بگیرید که e به صورت $c^۲+d^۲$ است که در آن $c+d\mathrm{i}$ عدد $a+b\mathrm{i}$ را عاد می‌کند.

۶.۵.۶ از تمرین ۵.۵.٦ نتیجه بگیرید که $\gcd(c,d)=۱$.

۶.۶ سه‌تایی‌های فیثاغورسی

اکنون زمان خوبی برای تجدید دیدار با سه‌تایی‌های فیثاغورسی اولیه است که ارتباط آن با $\mathbb{Z}[\mathrm{i}]$ در بخش ۸.۱ عنوان شد. چون مجذورهای فرد، همنهشت با ۱ (به پیمانهٔ ۴) و مجذورهای زوج، همنهشت با ۰ (به پیمانهٔ ۴) هستند، نتیجه می‌گیریم که مجموع دو مجذور فرد یک مربع کامل نیست. از این رو در یک سه‌تایی اولیه مانند (x,y,z) یکی از x و y زوج و z فرد است. استدلال بخش ۸.۱ این بود که اگر

$$x^{۲}+y^{۲}=z^{۲}$$

آنگاه

$$(x-y\mathrm{i})(x+y\mathrm{i})=z^{۲},$$

لذا $x-y\mathrm{i}$ و $x+y\mathrm{i}$ عوامل اول گاوسی[۴] مجذوری فرد یعنی $z^{۲}$ هستند. بنابراین می‌خواستیم بگوییم که:

۱. اگر x و y (در $\mathbb{Z}$) نسبت به هم اول باشند آنگاه $x-y\mathrm{i}$ و $x+y\mathrm{i}$ نیز (در $\mathbb{Z}[\mathrm{i}]$) چنین هستند.

۲. در $\mathbb{Z}[\mathrm{i}]$ عوامل نسبت به هم اول یک مربع کامل، خود مربع کامل هستند.

گزارهٔ اول درست است. اگر در $\mathbb{Z}$ داشته باشیم $\gcd(x,y)=۱$ آنگاه در $\mathbb{Z}[\mathrm{i}]$ نیز داریم $\gcd(x,y)=۱$. این مطلب برقرار است چون اگر x و y یک مقسوم‌علیه اول گاوسی مشترک داشته باشند آنگاه مزدوج آن نیز یک مقسوم‌علیه اول مشترک برای x و y است و لذا حاصل ضرب آنها نیز مقسوم‌علیه مشترکی است که عددی در $\mathbb{Z}$ و بزرگ‌تر از ۱ می‌باشد و این با $\gcd(x,y)=۱$ در تناقض

[۴] دلیلی ندارد که این دو عدد لزوماً اول باشند. لذا به نظر می‌رسد این عبارت درست نیست و باید گفته شود لذا $x-y\mathrm{i}$ و $x+y\mathrm{i}$ عوامل نسبت به هم اول گاوسی هستند؛ نه عوامل اول گاوسی. (م)

است. یک مقسوم‌علیه مشترک برای $x - y\mathrm{i}$ و $x + y\mathrm{i}$ باید مجموع این دو عدد یعنی $۲x$ و تفاضل آنها یعنی $۲\mathrm{i}y$ را نیز عاد کند. بنابراین (چون $\gcd(x,y) = ۱$) مقسوم‌علیه اول مشترک $x - y\mathrm{i}$ و $x + y\mathrm{i}$ اعداد $\pm۱\pm\mathrm{i}$ هستند که ۲ را عاد می‌کنند. چنین مقسوم‌علیه‌هایی نمی‌توانند وجود داشته باشند چون وجود آنها ایجاب می‌کند که $(x - y\mathrm{i})(x + y\mathrm{i}) = z^۲$ زوج باشد.

گزارهٔ دوم کاملاً درست نیست اما نسخهٔ اصلاحی زیر درست است:

عوامل نسبت به هم اول یک مربع کامل، خود مربع کامل هستند، تا حد عوامل یکه.

این مطلب از یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\mathrm{i}]$ نتیجه می‌شود.

از آنجایی که $x - y\mathrm{i}$ و $x + y\mathrm{i}$ هیچ عامل اول گاوسی مشترکی ندارند، در حالی که هر عامل اولی از $z^۲$ با توانی زوج ظاهر می‌شود، هر عامل اول $x - y\mathrm{i}$ و هر عامل اول $x + y\mathrm{i}$ نیز باید با توانی زوج ظاهر شوند. حاصل ضربی از اعداد اول که در آن هر عامل با توانی زوج ظاهر شده باشد به وضوح یک مربع کامل است (با همین استدلال که برای اعداد طبیعی در بخش ۵.۲ آمده بود مقایسه کنید). از این رو $x - y\mathrm{i}$ و $x + y\mathrm{i}$ مضرب یکه‌ای از یک مربع کامل هستند چون تنها عوامل غیر اول ممکن آنها عناصر یکه می‌باشند. □

شکل اصلاح شدهٔ گزارهٔ دوم برای رسیدن به نتیجه‌ای که انتظارش را داشتیم کافی است. آنچه نشان داده‌ایم این است که $x - y\mathrm{i}$ مضرب یکه‌ای از یک مربع کامل است و لذا برابر یکی از اعداد

$$(s - t\mathrm{i})^۲, -(s - t\mathrm{i})^۲, \mathrm{i}(s - t\mathrm{i})^۲, -\mathrm{i}(s - t\mathrm{i})^۲$$

برای s و t یی در $\mathbb{Z}$ می‌باشد؛ یعنی برابر یکی از اعداد

$$(s^۲ - t^۲) - ۲st\mathrm{i}, t^۲ - s^۲ + ۲st\mathrm{i}, ۲st + (s^۲ - t^۲)\mathrm{i}, -۲st + (t^۲ - s^۲)\mathrm{i}$$

است. در هر حالت با مساوی قرار دادن قسمتهای حقیقی و موهومی، یکی از x و y به صورت $u^۲ - v^۲$ و دیگری به صورت $۲uv$ است که u و v اعدادی

طبیعی می‌باشند. لذا حکم مورد نظر، اساساً همان است که توسط استدلال سست بخش ۸.۱ به دست آمد اما از آن بهتر است زیرا این حکم ما را مجبور نمی‌کند که x را برابر $۲uv$ اختیار کنیم (می‌توانیم y را برابر $۲uv$ در نظر بگیریم).

به علاوه داریم $\gcd(u,v) = ۱$ چون هر عامل اول مشترک u و v عامل مشترکی از $u^۲ - v^۲$ و $۲uv$ و لذا عامل مشترکی از x و y است. بنابراین ماحصلِ درستِ تحقیقات بخش ۸.۱ عبارت است از:

سه‌تایی‌های فیثاغورسی اولیه. اگر برای دو عدد طبیعی نسبت به هم اول مانند x و y داشته باشیم $x^۲ + y^۲ = z^۲$ آنگاه یکی از x و y به صورت $u^۲ - v^۲$ و دیگری به صورت $۲uv$ است که u و v دو عدد طبیعی نسبت به هم اول هستند. □

همچنین در هر حالت در می‌یابیم که $z = u^۲ + v^۲$ چون

$$(u^۲ - v^۲)^۲ + (۲uv)^۲ = u^۴ + ۲u^۲v^۲ + v^۴ = (u^۲ + v^۲)^۲.$$

لذا z مجموعی از دو مجذور است. چون u و v می‌توانند هر دو عدد دلخواهی با شرط $\gcd(u,v) = ۱$ باشند و از آنجایی که هر عدد اول به صورت $u^۲ + v^۲$ لزوماً شرط $\gcd(u,v) = ۱$ را دارد، لذا z می‌تواند هر عدد اولی که مجموع دو مجذور است باشد. لذا مشخص‌سازی هندسی اعداد اولی که مجموع دو مجذور هستند به شرح زیر به دست می‌آید.

وترهای اول. اعداد اولی که مجموع دو مجذور هستند همان اعدادی هستند که به عنوان وتر مثلثی قائم‌الزاویه با اضلاع صحیح ظاهر می‌شوند.

تمرینها

حکم اخیر، همراه با قضیهٔ دو مجذور فرما، نشان می‌دهد که اعداد اول به صورت $۴n + ۱$ دقیقاً همان اعدادی هستند که به عنوان وتر مثلثی قائم‌الزاویه با

اضلاع صحیح ظاهر می‌شوند.

۱.۶.۶ مثلثهای قائم‌الزاویه با اضلاع صحیح با وترهای ۵، ۱۳، ۱۷ (باید اینها را بشناسید) و ۲۹، ۳۷ و ۴۱ را بیابید.

۲.۶.۶ برای یک عدد اول داده شده مانند $p = ۴n + ۱$ آیا مثلث قائم‌الزاویهٔ با اضلاع صحیح و وتر p منحصر به فرد است؟

استدلال فوق نشان می‌دهد که اگر (x, y, z) یک سه‌تایی فیثاغورسی اولیه باشد آنگاه $x + y\mathrm{i}$ مضرب یکه‌ای از یک مربع کامل در $\mathbb{Z}[\mathrm{i}]$ است. اما همین که بدانیم $x = u^۲ - v^۲$ و $y = ۲uv$ آنگاه چیزهای بیشتری می‌توانیم بگوییم.

۳.۶.۶ اگر (x, y, z) یک سه‌تایی فیثاغورسی اولیه باشد که x فرد است آنگاه نشان دهید که $x + y\mathrm{i}$ مربع کاملی در $\mathbb{Z}[\mathrm{i}]$ است.

۴.۶.۶ مستقیماً تحقیق کنید که $۳ + ۴\mathrm{i}$ مربع کاملی در $\mathbb{Z}[\mathrm{i}]$ است.

از پاسخی که به سؤال ۳.٦.٦ می‌دهید باید واضح باشد که یافتن پارامترهای u و v برای یک سه‌تایی فیثاغورسی اولیه مانند (x, y, z) با شرط فرد بودن x معادل یافتن ریشه(های) دوم یک عدد مختلط است.

۵.۶.۶ ریشهٔ دوم $۵ + ۱۲\mathrm{i}$ را بیابید.

۶.۶.۶ اگر نرم‌افزاری دارید که ریشه‌های دوم اعداد مختلط را محاسبه می‌کند، تحقیق کنید که هر درایهٔ (x, y, z) در پلیمپتون ۳۲۲ (بخش ٦.١) غیر از سه‌تایی $(٦٠, ۴۵, ۷۵)$ یک $y + x\mathrm{i}$ به دست می‌دهد که مربع کاملی در $\mathbb{Z}[\mathrm{i}]$ است. (توجه: این مطلب در مورد سه‌تایی آخر یعنی $(۹٠, ۵٦, ١٠٦)$ نیز که به وضوح اولیه نیست درست می‌باشد.)

۷.۶.۶ شرح دهید که چگونه می‌توان ریشهٔ دوم یک عدد مختلط را با استفاده از معادلات درجه دوم محاسبه کرد.

۷.۶ * اعداد اول به صورت $۴n + ۱$

لم لاگرانژ که در بخش ۵.٦ اثبات شد در حقیقت نیمی از حکمی مهم در مورد چیزی موسوم به مشخصهٔ مربعی ۱−[5] است که آن را در فصل ۹ بیشتر مورد مطالعه قرار می‌دهیم. در اینجا از این مطلب برای اثبات نامتناهی بودن مجموعهٔ اعداد اول به صورت $۴n + ۱$ استفاده می‌کنیم که تتمیمی برای حکم سادهٔ متناظر با آن در مورد اعداد اول به صورت $۴n + ۳$ است که در تمرینهای ۴.۳.٦ تا ٦.۳.٦ اثبات شد.

مشخصهٔ مربعی ۱−. همنهشتی $x^۲ \equiv_p -۱$ (که در آن p یک عدد اول فرد است) دقیقاً وقتی دارای جواب است که $p = ۴n + ۱$.

برهان. وقتی $p = ۴n + ۱$ لم لاگرانژ x ی را به دست می‌دهد که $x^۲ \equiv_p -۱$. برای آن که نشان دهیم $x^۲ \equiv_p -۱$ در حالتی که p به صورت $۴n + ۳$ باشد جوابی ندارد، به برهان خلف فرض می‌کنیم که جواب داشته باشد.

فرض کنیم

$$x^۲ \equiv_p -۱, \qquad (p = ۴n + ۳).$$

در این صورت اگر طرفین عبارت فوق را به توان $۲n + ۱$ برسانیم داریم

$$(x^۲)^{۲n+۱} \equiv_p (-۱)^{۲n+۱} \equiv_p -۱.$$

چون $۲(۲n + ۱) = ۴n + ۲ = p - ۱$، این مطلب بیان می‌دارد که

$$x^{p-۱} \equiv_p -۱,$$

که متناقض با قضیهٔ کوچک فرما می‌باشد. از این رو وقتی $p = ۴n + ۳$ معادلهٔ $x^۲ \equiv_p -۱$ هیچ جوابی ندارد. □

---

[5] quadratic character of -1

لذا معادلهٔ $x^{\text{۲}} \equiv_p -\text{۱}$ دقیقاً وقتی جواب دارد که عدد فرد p به صورت $\text{۴}n+\text{۱}$ باشد. به بیان دیگر: اعداد اول فرد p که مقسوم‌علیهی از $x^{\text{۲}}+\text{۱}$ برای x ی صحیح باشند دقیقاً اعداد اول به صورت $\text{۴}n+\text{۱}$ هستند.

نامتناهی بودن اعداد اول به صورت $\text{۴}n+\text{۱}$. بی‌نهایت عدد اول به صورت $\text{۴}n+\text{۱}$ وجود دارد.

برهان. بنابر آنچه اکنون اثبات کردیم کافی است نشان دهیم که بی‌نهایت عدد اول وجود دارد که مقسوم‌علیهی از $x^{\text{۲}}+\text{۱}$ برای x ی صحیح هستند. به برهان خلف فرض کنیم فقط تعدادی متناهی عدد اول مانند $p_{\text{۱}}$، $p_{\text{۲}}$، ...، p_k مقادیر به صورت $x^{\text{۲}}+\text{۱}$ را عاد کنند.

حال چندجمله‌ای

$$(p_{\text{۱}}p_{\text{۲}}\cdots p_k y)^{\text{۲}}+\text{۱}=g(y)$$

را در نظر می‌گیریم. واضح است که هر عدد اول مانند p که مقداری از $g(y)$ را برای y یی صحیح عاد کند مقداری به صورت $x^{\text{۲}}+\text{۱}$ (یعنی برای $x=p_{\text{۱}}p_{\text{۲}}\cdots p_k y$) را عاد می‌کند. اما هیچ یک از $p_{\text{۱}}$، $p_{\text{۲}}$، ...، p_k مقدار $g(y)$ را عاد نمی‌کند چون $g(y)$ در تقسیم بر هر یک از آنها باقیمانده‌ای برابر ۱ دارد.

بنابراین هیچ عدد اولی $g(y)$ را برای y یی در $\mathbb{Z}$ عاد نمی‌کند و از این رو تنها مقادیر ممکن $g(y)$ برابر $\pm\text{۱}$ است. به بیان دیگر برای هر $y\in\mathbb{Z}$ داریم

$$(p_{\text{۱}}p_{\text{۲}}\cdots p_k y)^{\text{۲}}+\text{۱}=\pm\text{۱}.$$

اما این غیر ممکن است چون هر یک از معادلات مربعی

$$(p_{\text{۱}}p_{\text{۲}}\cdots p_k y)^{\text{۲}}+\text{۱}=-\text{۱} \qquad \text{و} \qquad (p_{\text{۱}}p_{\text{۲}}\cdots p_k y)^{\text{۲}}+\text{۱}=\text{۱}$$

حداکثر دو جواب y دارد. این تناقض نشان می‌دهد که مقادیر به صورت $x^{\text{۲}}+\text{۱}$ توسط تعدادی نامتناهی عدد اول عاد می‌شود. □

حال بنابر قضیهٔ دو مجذور فرما نتیجه می‌شود که بی‌نهایت عدد اول به صورت مجموع $a^۲ + b^۲$ از دو مربع کامل هستند. از این رو بی‌نهایت عدد اول گاوسی به صورت $a + bi$ وجود دارد که نه حقیقی هستند و نه موهومی محض.

تمرینها

اثباتی را که هم‌اکنون به کار رفت می‌توان به هر چندجمله‌ای غیر ثابت با ضرایب صحیح مانند $f(x)$ تعمیم داد. فرض کنیم

$$f(x) = a_m x^m + \ldots + a_۱ x + a_۰$$

که در آن $a_۰, a_۱, \ldots, a_m \in \mathbb{Z}$ و $a_۰, a_m \neq ۰$، دارای مقادیری است که فقط توسط اعداد اول $p_۱$، $p_۲$، ...، p_k عاد می‌شود و چندجمله‌ای

$$f(a_۰ p_۱ p_۲ \cdots p_k y) = a_۰ g(y)$$

را که در آن $g(y)$ یک چندجمله‌ای از درجهٔ m است در نظر می‌گیریم.

۱.۷.۶ نشان دهید که $g(y)$ با ضرایب صحیح است، جملهٔ ثابت آن ۱ است و هر عدد اول که مقداری از $g(y)$ را برای y یی صحیح عاد کند مقداری از $f(x)$ را برای x ی صحیح نیز عاد می‌کند.

۲.۷.۶ با این حال نشان دهید وقتی $y \in \mathbb{Z}$ هیچ یک از $p_۱$، $p_۲$، ...، p_k مقدار $g(y)$ را عاد نمی‌کند.

۳.۷.۶ از تمرین ۲.۷.۶ نتیجه بگیرید که برای هر $y \in \mathbb{Z}$ داریم $g(y) = \pm ۱$.

۴.۷.۶ نشان دهید که معادله‌های $g(y) = ۱$ و $g(y) = -۱$ فقط تعدادی متناهی جواب دارند که با تمرین ۳.۷.۶ در تناقض است. (کجا از فرض غیر ثابت بودن $f(x)$ استفاده کردید؟)

این تناقض نشان می‌دهد که $f(x)$ توسط تعدادی نامتناهی عدد اول عاد می‌شود. اما اکنون توجه کنید: فرض نکرده بودیم که بی‌نهایت عدد اول وجود دارد. از این رو این مطلب به خودی خود برهانی برای قضیهٔ اقلیدس است که می‌گوید بی‌نهایت عدد اول وجود دارد.

۵.۷.۶ آیا این استدلال اساساً متفاوت با برهان اقلیدس است؟

۸.۶ بحث

قضیهٔ دو مجذور توسط فرما در سال ۱۶۴۰ بدون برهان بیان شد؛ گرچه وی ادعا می‌کرد که برهانی مبتنی بر نزول دارد: با فرض آن که عددی اول به صورت $۴n + ۱$ وجود دارد که مجموع دو مجذور نیست، وی توانست نشان دهد که عدد اول کوچک‌تری با همین خاصیت وجود دارد. اولین برهان شناخته شده برای این قضیه در حقیقت مبتنی بر نزول بود و توسط اویلر (۱۷۵۵) منتشر شد. این قضیه برای او به اندازهٔ سالها تلاش ارزش داشت.

امروزه ارائهٔ برهانهایی کاملاً ساده به کمک حکمی که در بخش ۵.٦ آن را لم لاگرانژ نامیدیم امکان پذیر است. خود لاگرانژ این لم را به کمک قضیهٔ کوچک فرما و قضیهٔ خود در مورد تعداد جوابهای همنهشتیهای به پیمانهٔ p (بخش ۵.۳) اثبات کرد.

لاگرانژ (۱۷۷۳) لم خود را با نظریه‌اش در مورد هم‌ارزی صورتهای مربعی (بخش ٦.۵) برای ارائهٔ برهانی جدید از قضیهٔ دو مجذور به کار بست. بخشی از آن برهان با صورتهای مربعی سر و کار داشت که توسط گاوس (۱۸۰۱) (مدتها قبل از خلق اعداد صحیح گاوسی توسط خود وی) ساده شده بود. به نظر می‌رسد که گاوس نتایج اصلی در مورد $\mathbb{Z}[i]$ را (مشتمل بر یکتایی تجزیه به اعداد اول) در حدود سال ۱۸۱۵ داشته است، اما اولین بار آن را در سال ۱۸۲۳ منتشر کرد. برهانی که در این فصل آمد با تلفیق یکتایی تجزیه به اعداد

اول در $\mathbb{Z}[i]$ همراه با لم لاگرانژ مدیون ددکیند (۱۸۹۴) هستیم.

کماکان برهانی که عمومیت بیشتری دارد از هندسهٔ اعداد[۶] که در سالهای ۱۸۹۰ توسط مینکوفسکی گسترش یافت استفاده می‌کند. می‌توان این برهان را در اسکارلا[۷] و اپلکا[۸] (۱۹۸۵) همراه با مقدمه‌ای تاریخی بر نتایج مینکوفسکی یافت.

موازی با همهٔ برهانهای متداول برای قضیهٔ دو مجذور، برهانهای مشابهی برای قضیهٔ چهار مجذور لاگرانژ[۹] (۱۷۷۰) وجود دارد: هر عدد طبیعی مجموع (حداکثر) چهار مجذور طبیعی است. اغلب این برهانها از همتای لم لاگرانژ استفاده می‌کنند: هر عدد اول مانند p عددی به صورت $\ell^۲ + m^۲ + ۱$ را عاد می‌کند. این همتای لم لاگرانژ آسان‌تر از آب در می‌آید. آنچه سخت‌تر است اتحاد چهار مجذور[۱۰] است که توسط اویلر (۱۷۴۸b) کشف شد. این اتحاد، مشابه اتحاد دو مجذور بخش ۱.٦ است اما بسیار پیچیده‌تر از آن می‌باشد (بخش ۳.۸ را ببینید). می‌توان آن را توسط ضرب کردن هر یک از دو طرف معادله بررسی کرد، اما معنی آن چیست؟

برهان اعداد صحیح گاوسی در این کتاب از آن جهت مورد توجه است که $\mathbb{Z}[i]$ ساختاری طبیعی دارد و اتحاد دو مجذور، بخشی طبیعی از آن (خاصیت ضربی نرم) به جای اتحادی تصادفی از عبارتهای صوری می‌باشد. در فصل ۸ برهان ساختاریِ[۱۱] مشابهی از قضیهٔ چهار مجذور را که از چهارگانهای صحیح[۱۲] استفاده می‌کند ارائه می‌دهیم. این مجموعه از اعداد، ساختار چهار بعدی قابل توجهی است که از آن اتحاد چهار مجذور به طور طبیعی به عنوان خاصیت ضربیِ نرم چهارگانها[۱۳] پدیدار می‌شود. مجدداً کلید برهان، یکتایی

---

[۶] geometry of numbers
[۷] Scharlau
[۸] Opolka
[۹] four square theorem of Lagrange
[۱۰] four square identity
[۱۱] structural
[۱۲] quaternion integers
[۱۳] quaternion norm

تجزیه به اعداد اول (یا به جای آن، خاصیت مقسوم‌علیه اول که در مورد چهارگانها به عنوان چیزی ساده‌تر از یکتایی تجزیه به اعداد اول است) می‌باشد.

قضیهٔ دو مجذور فرما در جهتی دیگر توسط خود فرما تعمیم داده شد. فرما در سال ۱٦۵۴ قضایای مشابهی را در مورد اعداد به صورت $x^۲ + ۲y^۲$ و $x^۲ + ۳y^۲$ اعلام کرد:

$$p = x^۲ + ۲y^۲ \iff p = ۸n + ۱ \quad \text{یا} \quad p = ۸n + ۳$$

$$p = x^۲ + ۳y^۲ \iff p = ۳n + ۱.$$

برهان ما برای قضیهٔ دو مجذور در بخش ۵.٦ را می‌توان به اثباتی برای قضایای $x^۲ + ۲y^۲$ و $x^۲ + ۳y^۲$ ی فرما (به کمک قضایای یکتایی تجزیه به اعداد اول، به ترتیب برای اعداد به صورت $a + b\sqrt{-۲}$ و $a + b\sqrt{-۳}$) تبدیل کرد. این قضایا در فصل بعد اثبات خواهد شد.

چیز دیگری که لازم داریم شکل مناسبی از لم لاگرانژ است: اگر $p = ۴n + ۱$ آنگاه p عددی به صورت $m^۲ + ۱$ را برای m ی صحیح عاد می‌کند. در بخش ۷.٦ این لم را (همراه با عکس آن) به عنوان مشخصهٔ مربعی ۱− توصیف کردیم چرا که بیان می‌دارد ۱− با مربع کاملی به پیمانهٔ p همنهشت است دقیقاً وقتی که $p = ۴n + ۱$.

به طور مشابه برای اثبات قضیهٔ فرما در مورد اعداد اول به صورت $x^۲ + ۲y^۲$ و $x^۲ + ۳y^۲$ به مشخصهٔ مربعی ۲− و ۳− نیاز داریم. اینها عبارتند از:

$$-۲ \equiv_p \text{مربع کامل} \iff p = ۸n + ۱ \quad \text{یا} \quad p = ۸n + ۳$$

$$-۳ \equiv_p \text{مربع کامل} \iff p = ۳n + ۱.$$

به جای یکی یکی یافتن مشخصه‌های مربعی، در فصل ۹ قانون تقابل مربعی[۱۴] را اثبات می‌کنیم که به یکباره به ما امکان می‌دهد بگوییم چه وقت عددی صحیح همنهشت با یک مربع کامل به پیمانهٔ p است. تقابل مربعی اولین بار

[۱۴] quadratic reciprocity law

توسط اویلر مشاهده شد و در حالات خاص (از قبیل آنهایی که با قضیهٔ فرما سر و کار دارند) توسط وی اثبات شد. اولین برهان کلی منسوب به گاوس (۱۸۰۱) است و پس از آن، قانون تقابل مربعی به روشهای متفاوتی اثبات شده است. در حقیقت این مطلب بیش از هر قضیهٔ دیگری (غیر از جد بزرگ آن یعنی قضیهٔ فیثاغورس) اثبات شده است.

۷

اعداد صحیح مربعی

پیش‌نگاه

درست همانند اعداد صحیح گاوسی که تجزیهٔ $x^۲+y^۲$ را ممکن می‌سازند، بقیهٔ عبارتهای مربعی از اعداد صحیح معمولی نیز به کمک اعداد صحیح مربعی[۱] تجزیه می‌شوند. مثالهای این فصل عبارتند از

$$\begin{aligned} x^۲+۲ &= (x-\sqrt{-۲})(x+\sqrt{-۲}) \\ x^۲-xy+y^۲ &= (x+\frac{-۱+\sqrt{-۳}}{۲}y)(x+\frac{-۱-\sqrt{-۳}}{۲}y). \end{aligned}$$

در مثال اول عوامل ظاهر شده متعلق به

$$\mathbb{Z}[\sqrt{-۲}]=\{a+b\sqrt{-۲}:a,b\in\mathbb{Z}\}$$

می‌باشند. شبیه اعداد صحیح گاوسی $a+bi$، اعداد $a+b\sqrt{-۲}$ نیز از یکتایی تجزیه به اعداد اول برخوردار هستند. این خاصیت را برای یافتن همهٔ جوابهای صحیح (معمولی) معادلهٔ $y^۳=x^۲+۲$ به کار می‌بریم.

---

[۱] quadratic integers

اعداد $\frac{-۱+\sqrt{-۳}}{۲}$ و $\frac{-۱-\sqrt{-۳}}{۲}$ در مثال دوم، در ابتدا کسری به نظر می‌رسند و ممکن است ترجیح دهیم که عبارت صحیح را برای اعداد

$$\mathbb{Z}[\sqrt{-۳}] = \{a + b\sqrt{-۳} : a, b \in \mathbb{Z}\}$$

برگزینیم. اما یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\sqrt{-۳}]$ شکست می‌خورد و دقیقاً با افزودن $\frac{-۱+\sqrt{-۳}}{۲}$ است که مجدداً چیره می‌شود.

این مطلب به بحثی از مفهوم کلی اعداد صحیح مربعی و کاربردهای آن (که بخشی از آن در تمرین آمده است) منجر می‌شود. این فصل با دو کاربرد قابل توجه خاتمه می‌یابد: فرمول پارامتری برای (بی‌نهایت) جواب گویای $x^۳ + y^۳ = z^۳ + w^۳$ و برهان این که هیچ جواب ناصفری برای $x^۳ + y^۳ = z^۳$ وجود ندارد.

۱.۷ معادله $y^۳ = x^۲ + ۲$

دیوفانتوس معمولاً به جوابهای گویای معادله‌ها علاقه‌مند بود که معادلهٔ $y^۳ = x^۲ + ۲$ تعدادی نامتناهی از این گونه جوابها دارد (تمرینهای ۱.۷.۱ و ۴.۷.۱ را ببینید). اما در حساب[۲]، کتاب VI، مسألهٔ ۱۷، دیوفانتوس متذکر می‌شود که $y^۳ = x^۲ + ۲$ دارای جواب $x = ۵$ و $y = ۳$ است. وی به طور بدیهی فکر می‌کرده است که این جواب طبیعی جالب است. در سال ۱۶۵۷ فرما این ادعا را به آن افزود که هیچ جواب طبیعی دیگری برای $x^۳ = x^۲ + ۲$ وجود ندارد.

ادعای فرما توسط اویلر (۱۷۷۰) با فرض یکتایی تجزیه در

$$\mathbb{Z}[\sqrt{-۲}] = \{a + b\sqrt{-۲} : a, b \in \mathbb{Z}\}$$

[۲] Arithmetics

اثبات شد. اویلر هیچ برهانی برای این حقیقت (که مشابه برهان ارائه شده در بخش ۴.۶ برای $\mathbb{Z}[i]$ است) ارائه نداد اما اگر برای لحظه‌ای مسألهٔ یکتایی تجزیه را کنار بگذاریم استدلال وی به شرح زیر است.

فرض کنیم برای x و y یی صحیح داشته باشیم $y^۳ = x^۲ + ۲$. در این صورت تجزیهٔ زیر را در $\mathbb{Z}[\sqrt{-۲}]$ داریم

$$y^۳ = (x - \sqrt{-۲})(x + \sqrt{-۲}) \qquad (*)$$

حال یکتایی تجزیه به اعداد اول را در $\mathbb{Z}[\sqrt{-۲}]$ فرض می‌کنیم و همچنین فرض می‌کنیم که

$$\gcd(x - \sqrt{-۲}, x + \sqrt{-۲}) = ۱$$

(این هم مسأله‌ای دیگر است که فعلاً بدون دلیل می‌پذیریم). بنابراین با در نظر گرفتن تجزیه به اعداد اول طرفین عبارت $(*)$ نتیجه می‌گیریم که عوامل $x - \sqrt{-۲}$ و $x + \sqrt{-۲}$ مکعبهای کاملی در $\mathbb{Z}[\sqrt{-۲}]$ هستند.

گزارهٔ اخیر بدان معنی است که برای a و b یی در $\mathbb{Z}$ داریم

$$\begin{aligned} x - \sqrt{-۲} &= (a + b\sqrt{-۲})^۳ \\ &= a^۳ + ۳a^۲b\sqrt{-۲} - ٦ab^۲ - ۲\sqrt{-۲}b^۳ \\ &= a^۳ - ٦a^۲b + (۳a^۲b - ۲b^۳)\sqrt{-۲}. \end{aligned}$$

با مساوی قرار دادن قسمتهای حقیقی و موهومی داریم

$$\begin{aligned} x &= a^۳ - ٦ab^۲ \\ ۱ &= ۲b^۳ - ۳a^۲b = b(۲b^۲ - ۳a^۲). \end{aligned}$$

معادلهٔ اخیر می‌گوید که عدد طبیعی b[۳] عدد ۱ را عاد می‌کند. از این رو

[۳] ظاهراً اشتباه تایپی است و باید نوشته شود عدد صحیح b. (م)

$b = \pm ۱$. بنابراین مقسوم‌علیه دیگر یعنی $۳a^۲ - ۲b^۲$ باید برابر ۱– باشد[۴]. لذا $a = \pm b = \pm ۱$.[۵]

این مطلب نتیجه می‌دهد که $x = \pm ۵$ و لذا $y = ۳$. □

تمرینها

روش مشابهی (با استفاده از $\mathbb{Z}[\mathrm{i}]$) برای معادلهٔ $y^۳ = x^۲ + ۱$ وجود دارد که نشان می‌دهد تنها جواب صحیح آن $x = ۰$ و $y = ۱$ است.

۱.۱.۷ با فرض آن که عوامل $x \pm \mathrm{i}$ از تجزیهٔ

$$y^۳ = x^۲ + ۱ = (x - \mathrm{i})(x + \mathrm{i})$$

مکعبهایی مانند $(a \pm b\mathrm{i})^۳$ در $\mathbb{Z}[\mathrm{i}]$ باشند نتیجه بگیرید که $۱ = b(۳a^۲ - b^۲)$.

۲.۱.۷ از تمرین ۱.۱.۷ نتیجه بگیرید که $a = ۰$. از این رو $x = ۰$ و لذا $y = ۱$.

یک معادلهٔ چالش‌برانگیزتر که می‌توان به کمک $\mathbb{Z}[\mathrm{i}]$ بر آن نیز چیره شد معادلهٔ $y^۳ = x^۲ + ۴$ می‌باشد. فرما ادعا کرد که تنها جوابهای طبیعی آن عبارتند از $x = ۲$، $y = ۲$ و $x = ۱۱$، $y = ۵$. اویلر (۱۷۷۰) این معادله را با استفاده از $\mathbb{Z}[\mathrm{i}]$ حل کرد اما باز هم بدون اثبات یکتایی تجزیه به اعداد اول. در حالتی که x فرد باشد استدلال همانند آنچه در بالا آمد پیش می‌رود که در این حالت فرض مکعب کامل بودن عوامل $x - ۲\mathrm{i}$ و $x + ۲\mathrm{i}$ درست است.

۳.۱.۷ با فرض آن که $x \pm ۲\mathrm{i}$ مکعبهای کاملی مانند $(a \pm b\mathrm{i})^۳$ در $\mathbb{Z}[\mathrm{i}]$ باشند نشان دهید که $۲ = b(۳a^۲ - b^۲)$ و در حالتی که x عددی فرد و مثبت باشد نتیجه بگیرید که $x = ۱۱$.

---

[۴] توجه کنید که در حقیقت $۳a^۲ - ۲b^۲$ باید برابر ± ۱ باشد اما حالت $۳a^۲ - ۲b^۲ = ۱$ امکان ندارد. (م)

[۵] این نیز ظاهراً اشتباهی دیگر است و باید به صورت $a = b = \pm ۱$ نوشته شود. (م)

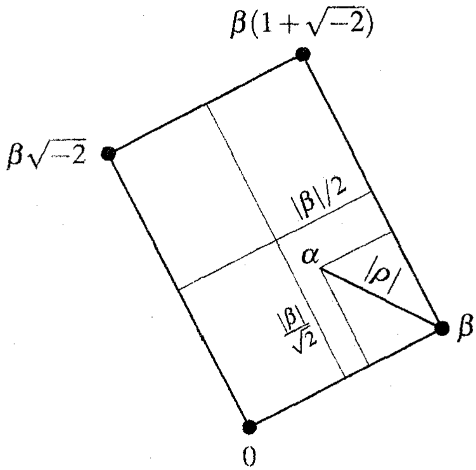
۲.۷ خاصیت تقسیم

یکتایی تجزیه به اعداد اول همانند $\mathbb{Z}$ و $\mathbb{Z}[i]$ نتیجه می‌شود: از خاصیت مقسوم‌علیه اول که آن هم از الگوریتم اقلیدسی توسط یک خاصیت تقسیم ساخته می‌شود حاصل می‌گردد.

خاصیت تقسیم برای $\mathbb{Z}[\sqrt{-۲}]$. برای هر $\alpha, \beta \neq ۰$ در $\mathbb{Z}[\sqrt{-۲}]$، اعداد ρ و μ در $\mathbb{Z}[\sqrt{-۲}]$ موجودند به قسمی که

$$\alpha = \mu\beta + \rho, \qquad |\rho| < |\beta|.$$

برهان. برای آن که ببینیم چرا خاصیت تقسیم در $\mathbb{Z}[\sqrt{-۲}]$ برقرار است به مضارب $\mu\beta$ از عدد غیر صفر $\beta \in \mathbb{Z}[\sqrt{-۲}]$ توجه می‌کنیم. این اعداد در گوشه‌های یک شبکه از مستطیلها قرار دارند که گوشه‌های اولین مستطیل ۰، β، $\beta\sqrt{-۲}$ و $\beta(۱ + \sqrt{-۲})$ است (شکل ۱.۷).



شکل ۱.۷: خاصیت تقسیم در $\mathbb{Z}[\sqrt{-۲}]$

هر $\alpha \in \mathbb{Z}[\sqrt{-۲}]$ در یکی از این مستطیلها قرار دارد و همان طور که شکل نشان می‌دهد فاصلهٔ α تا نزدیک‌ترین مضرب β (مانند $\mu\beta$)، که آن را با $|\rho|$ نمایش

می‌دهیم در شرط

$$\begin{aligned} |\rho|^۲ &\leq (\frac{|\beta|}{۲})^۲ + (\frac{|\beta|}{\sqrt{۲}})^۲ \\ &= \frac{|\beta|^۲ + ۲|\beta|^۲}{۴} = \frac{۳|\beta|^۲}{۴} \end{aligned}$$

صدق می‌کند.

از این رو همان طور که می‌خواستیم $|\beta| > |\rho|$. □

یکه‌های $\mathbb{Z}[\sqrt{-۲}]$ همانند یکه‌های $\mathbb{Z}$ صرفاً برابر ± ۱ می‌باشند. این مطلب را با استفاده از نرم $a + b\sqrt{-۲}$ که برابر $a^۲ + ۲b^۲$ تعریف می‌شود اثبات می‌کنیم. یکه‌ها عناصر با نرم ۱ هستند و $a^۲ + ۲b^۲$ تنها در صورتی برابر ۱ است که $a = \pm ۱$ و $b = ۰$.

حال فرض کنیم تجزیه‌ای از یک مکعب کامل در $\mathbb{Z}[\sqrt{-۲}]$ به عوامل نسبت به هم اول s و t به صورت

$$y^۳ = st$$

داشته باشیم. چون s و t عامل مشترکی ندارند، عوامل مکعبی $y^۳$ باید به عواملی مکعبی در s و عواملی مکعبی در t تفکیک شود. می‌توانست عوامل یکه‌ای نیز در s و t وجود داشته باشد اما یکه‌ها فقط ۱ یا ۱− هستند که هر دو مکعب هستند. از این رو عوامل نسبت به هم اول یک مکعب، خود مکعب هستند.

این مطلب خلل دیگری را که در حل اویلر برای $y^۳ = x^۲ + ۲$ وجود داشت پر می‌کند. تنها خلأیی که اکنون باقی می‌ماند این است که نشان دهیم $\gcd(x - \sqrt{-۲}, x + \sqrt{-۲}) = ۱$.

تمرینها

معادلهٔ $y^۳ = x^۲ + ۱$ که در مجموعه تمرینهای قبلی به آن پرداختیم مطالعهٔ مشابهی از یکه‌ها را در $\mathbb{Z}[\mathrm{i}]$ می‌طلبد. از بخش ۴.۶ یادآوری می‌کنیم که یکه‌های

$\mathbb{Z}[\mathrm{i}]$ عبارتند از ۱± ، i±.

۱.۲.۷ بررسی کنید که هر یک از یکه‌های $\mathbb{Z}[\mathrm{i}]$ مکعب کامل هستند.

۲.۲.۷ از تمرین ۱.۲.۷ و یکتایی تجزیه به اعداد اول نتیجه بگیرید که عوامل نسبت به هم اول یک مکعب کامل در $\mathbb{Z}[\mathrm{i}]$، خود مکعب کامل هستند.

این خواص یکه‌ها و مکعبهای کامل را می‌توان برای حل معادلهٔ $y^۳ = x^۲ + ۴$ به کار برد. هنگامی که سمت راست این معادله را تجزیه کنیم به $(x - ۲\mathrm{i})(x + ۲\mathrm{i})$ می‌رسیم. اما اگر x زوج باشد (مثلاً $x = ۲X$) مشکل دیگری داریم.

۳.۲.۷ نشان دهید که در این حالت y نیز زوج است (مثلاً $y = ۲Y$). از این رو معادلهٔ $y^۳ = x^۲ + ۴$ معادل $۲Y^۳ = X^۲ + ۱ = (X-\mathrm{i})(X+\mathrm{i})$ می‌باشد.

۴.۲.۷ نشان دهید که در هر جوابی برای $۲Y^۳ = X^۲ + ۱$ باید X فرد باشد و در این حالت $۱-\mathrm{i}$ باید $X-\mathrm{i}$ را عاد کند.

با مزدوجگیری نتیجه می‌شود که $۱+\mathrm{i}$ نیز باید $X+\mathrm{i}$ را برای هر X فرد عاد کند. در حقیقت چون $۱+\mathrm{i} = \mathrm{i}(۱-\mathrm{i})$ نتیجه می‌گیریم که $۱-\mathrm{i}$ مقسوم‌علیه مشترک $X-\mathrm{i}$ و $X+\mathrm{i}$ در $\mathbb{Z}[\mathrm{i}]$ است. در مجموعه تمرینهای بعدی می‌بینیم که آیا $۱-\mathrm{i}$ ب.م.م. است یا نه.

۳.۷ ب.م.م.

مجدداً نرم در $\mathbb{Z}[\sqrt{-۲}]$ یعنی

$$\text{نرم}\ (a + b\sqrt{-۲}) = |a + b\sqrt{-۲}|^۲ = a^۲ + ۲b^۲$$

را که بنابر خاصیت ضربی قدرمطلق ضربی می‌باشد به کار می‌بریم.

همانند $\mathbb{Z}[i]$ این مطلب درست است که اگر α عدد γ را عاد کند آنگاه نرم (α) باید نرم (γ) را عاد کند. بنابراین اگر δ مقسوم‌علیه مشترک α و β باشد آنگاه نرم (δ) مقسوم علیه مشترک نرم (α) و نرم (β) خواهد بود.

حال می‌توانیم به معادلهٔ

$$y^{۳} = x^{۲} + ۲ = (x - \sqrt{-۲})(x + \sqrt{-۲})$$

بازگردیم و $\gcd(x - \sqrt{-۲}, x + \sqrt{-۲})$ را محاسبه کنیم.

نسبت به هم اول بودن عوامل. اگر $x, y \in \mathbb{Z}$ به قسمی باشند که $y^{۳} = x^{۲} + ۲$ آنگاه $\gcd(x - \sqrt{-۲}, x + \sqrt{-۲}) = ۱$.

برهان. اگر $y^{۳} = x^{۲} + ۲$ آنگاه x باید فرد باشد. در حقیقت برای x زوج داریم

$$x^{۲} + ۲ \equiv_{۴} ۲$$

در حالتی که

$$y^{۳} \equiv_{۴} ۰, ۱ \text{ یا } ۳.$$

این مطلب را می‌توان با آزمودن $y \equiv_{۴} ۰, ۱, ۲, ۳$ تحقیق کرد. نتیجه می‌شود که نرم $x \pm \sqrt{-۲}$ که برابر $x^{۲} + ۲$ است باید فرد باشد.

حال می‌بینیم که ب.م.م. $x - \sqrt{-۲}$ و $x + \sqrt{-۲}$ تفاضل این دو عدد را نیز که برابر $۲\sqrt{-۲}$ است و نرم آن برابر ۸ می‌باشد عاد می‌کند. اما ب.ب.م. ۸ و $x^{۲} + ۲$ (که فرد است) برابر ۱ می‌باشد. بنابراین

$$\gcd(x - \sqrt{-۲}, x + \sqrt{-۲}) = ۱. \ \square$$

اکنون دیگر خلل آخر در برهان اویلر را که می‌گوید $x = ۵$ و $y = ۳$ تنها جواب طبیعی $y^{۳} = x^{۲} + ۲$ هستند پر کرده‌ایم: $y^{۳}$ که مکعب کامل است به حاصل ضرب دو عدد نسبت به هم اول $x - \sqrt{-۲}$ و $x + \sqrt{-۲}$ تجزیه می‌شود که بنابر یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\sqrt{-۲}]$ و این حقیقت که یکه‌های $\mathbb{Z}[\sqrt{-۲}]$ نیز مکعب کامل هستند، خود باید مکعب کامل باشند. بنابراین

می‌توانیم بنویسیم $x-\sqrt{-۲}=(a+b\sqrt{-۲})^۳$ و برهان را همان طور که قبلاً در بخش ۱.۷ مشخص کردیم تمام کنیم.

تمرینها

به طور مشابه می‌توانیم از $\mathbb{Z}[\mathrm{i}]$ برای تکمیل برهانی که در مجموعه تمرینهای قبلی شروع شده بود استفاده کنیم و نشان دهیم که $x=۰$ و $y=۱$ تنها جواب صحیح $y^۳=x^۲+۱$ است.

۱.۳.۷ از همنهشتی به پیمانهٔ ۴ استفاده کنید و نشان دهید که x برای هر جواب صحیح از $y^۳=x^۲+۱$ زوج است. از حالا به بعد فرض می‌کنیم که (x,y) چنین جوابی باشد.

۲.۳.۷ شرح دهید که چرا $\gcd(x-\mathrm{i},x+\mathrm{i})=\gcd(x+\mathrm{i},۲)$ و از تمرین ۱.۳.۷ استفاده کنید تا نشان دهید که نرم $(x+i)$ فرد است.

۳.۳.۷ از تمرین ۲.۳.۷ نتیجه بگیرید که $\gcd(x-\mathrm{i},x+\mathrm{i})=۱$.

۴.۳.۷ از تمرینهای قبلی و یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\mathrm{i}]$ نتیجه بگیرید که عوامل ظاهر شده در سمت راست $y^۳=(x-\mathrm{i})(x+\mathrm{i})$ در $\mathbb{Z}[\mathrm{i}]$ مکعب کامل هستند.

به طور مشابه می‌توانیم $\gcd(X-\mathrm{i},X+\mathrm{i})$ را وقتی که X فرد است بیابیم و لذا راه حل $y^۳=x^۲+۴$ را برای حالتی که $x=۲X$ تکمیل کنیم.

۵.۳.۷ نشان دهید که ۲ اعداد $X-\mathrm{i}$ یا $X+\mathrm{i}$ را عاد نمی‌کند و از تمرین ۴.۲.۷ نتیجه بگیرید که $\gcd(X-\mathrm{i},X+\mathrm{i})=۱-\mathrm{i}$.

۶.۳.۷ از یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\mathrm{i}]$ استفاده کنید و از $۲Y^۳=(X-\mathrm{i})(X+\mathrm{i})$ نتیجه بگیرید که برای a و b یی در $\mathbb{Z}$ داریم

$$X - \mathrm{i} = (۱ - \mathrm{i})(a - b\mathrm{i})^۳.$$

۷.۳.۷ از تمرین ٦.۳.۷ نتیجه بگیرید که

$$۱ = a^۳ - b^۳ + ۳ab(a - b) = (a - b)(a^۲ + ۴ab + b^۲)$$

و لذا $X = ۱$. از این رو $x = ۲$.

۴.۷ ریشه دوم ۳− و ریشه سوم واحد

یک گام طبیعی بعد از تحقیق در مورد $\mathbb{Z}[\mathrm{i}]$ و $\mathbb{Z}[\sqrt{-۲}]$، مطالعهٔ

$$\mathbb{Z}[\sqrt{-۳}] = \{a + b\sqrt{-۳} : a, b \in \mathbb{Z}\}$$

خواهد بود. اما یک شگفتی در اینجا هست: یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\sqrt{-۳}]$ شکست می‌خورد!

تجزیه‌های زیر از ۴ را در نظر بگیرید:

$$۴ = ۲ \times ۲ = (۱ - \sqrt{-۳})(۱ + \sqrt{-۳}).$$

در $\mathbb{Z}[\sqrt{-۳}]$ نرم عبارت است از

$$\text{نرم}\ (a + b\sqrt{-۳}) = |a + b\sqrt{-۳}|^۲ = a^۲ + ۳b^۲$$

و طبق معمول اگر α عدد γ را عاد کند آنگاه نرم (α) باید نرم (γ) را عاد کند.

اما اکنون ۴ = نرم (۲) که هیچ مقسوم‌علیه کوچک‌تری به صورت $a^۲ + ۳b^۲$ غیر از ۱ ندارد. از این رو ۲ عددی اول در $\mathbb{Z}[\sqrt{-۳}]$ است. و

$$\text{نرم}\ (۱ - \sqrt{-۳}) = ۱ + ۳ = ۴.$$

بنابراین $\sqrt{-۳} - ۱$ (و به همین دلیل $\sqrt{-۳} + ۱$) نیز اول است. لذا ۴ دو تجزیهٔ متمایز به اعداد اول در $\mathbb{Z}[\sqrt{-۳}]$ دارد. □

این کاستی را می‌توان با وسعت دادن $\mathbb{Z}[\sqrt{-۳}]$ به

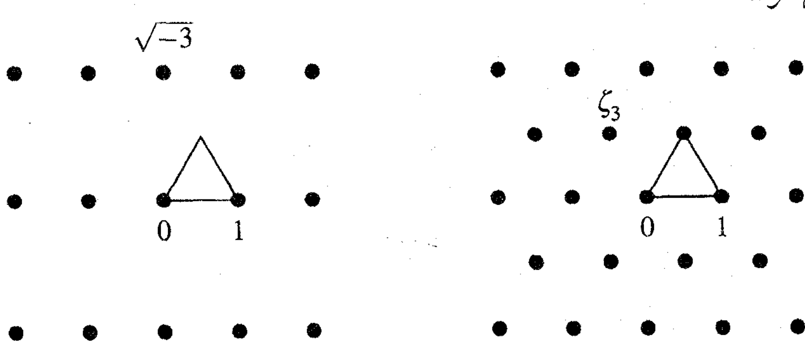
$$\mathbb{Z}[\zeta_۳] = \{a + b\zeta_۳ : a, b \in \mathbb{Z}\}$$

برطرف نمود که در آن

$$\zeta_۳ = \frac{-۱ + \sqrt{-۳}}{۲}$$

یکی از ریشه‌های سوم واحد می‌باشد. (به همین دلیل است که از زیرنویس ۳ استفاده کرده‌ایم. در حالت کلی عدد ζ_n یعنی $\cos\frac{۲\pi}{n} + i\sin\frac{۲\pi}{n}$ ریشهٔ nام واحد را نشان می‌دهد.) عناصر $\mathbb{Z}[\zeta_۳]$ در گوشه‌های یک کاشیکاری از صفحه توسط مثلثها قرار دارند و اعداد صحیح آیزنشتین[۶] نامیده می‌شوند.

بنابر استدلالهای هندسی، مشابه آنچه برای $\mathbb{Z}[i]$ و $\mathbb{Z}[\sqrt{-۲}]$ به کار رفت، می‌توانیم ببینیم که $\mathbb{Z}[\zeta_۳]$ خاصیت تقسیم دارد و از این رو حائز الگوریتمی اقلیدسی و یکتایی تجزیه به اعداد اول است. شکل ۲.۷ نقاط مجموعه‌های $\mathbb{Z}[\sqrt{-۳}]$ و $\mathbb{Z}[\zeta_۳]$ را در صفحه با یکدیگر مقایسه می‌کند که نشان می‌دهد چرا خاصیت تقسیم در اولی شکست می‌خورد اما در دومی با موفقیت مواجه می‌شود.



شکل ۲.۷: $\mathbb{Z}[\zeta_۳]$ (سمت راست) و $\mathbb{Z}[\sqrt{-۳}]$ (سمت چپ)

[۶] Eisenstein integers

در مستطیلهای $\mathbb{Z}[\sqrt{-۳}]$ هر نقطهٔ مرکزی (شبیه آنچه در بالای مثلث نشان داده شده است) در فاصلهٔ ۱ از دو نزدیک‌ترین گوشه قرار دارد و از این رو فاصلهٔ آن از نزدیک‌ترین گوشه کمتر از طول ضلع کوچک‌تر مثلث نیست. $\mathbb{Z}[\zeta_۳]$ این حفره‌های $\mathbb{Z}[\sqrt{-۳}]$ را با تولید کاشیکاری صفحه به وسیلهٔ مثلثهای متساوی‌الاضلاع پر می‌کند.

خاصیت تقسیم برای $\mathbb{Z}[\zeta_۳]$. برای هر $\alpha, \beta \neq ۰$ در $\mathbb{Z}[\zeta_۳]$ اعداد μ و ρ در $\mathbb{Z}[\zeta_۳]$ وجود دارند به قسمی که

$$\alpha = \mu\beta + \rho, \qquad |\rho| < |\beta|.$$

برهان. در کاشیکاری مثلثهای متساوی‌الاضلاع، هر نقطهٔ صفحه در یک مثلث واقع است و فاصلهٔ آن از نزدیک‌ترین رأس، کمتر از طول ضلع مثلث است. در حقیقت فاصلهٔ این نقطه از هر رأس مثلثی که آن را محاصره می‌کند کمتر از طول ضلع است. این مطلب بدان دلیل درست است که یک دایره به مرکز یک رأس و ضلعی به عنوان شعاع، کل مثلث را در بر می‌گیرد.

این خاصیت هندسی اساس خاصیت تقسیم است زیرا طبق معمول، مجموعهٔ همهٔ $\mu\beta$ ها برای β یی غیر صفر در $\mathbb{Z}[\zeta_۳]$ به همان صورت $\mathbb{Z}[\zeta_۳]$ است. نقاط این مجموعه، رئوس یک کاشیکاری با مثلثهای متساوی‌الاضلاع به ضلع $|\beta|$ می‌باشد. از این رو فاصلهٔ $|\alpha - \mu\beta| = |\rho|$ از هر $\alpha \in \mathbb{Z}[\zeta_۳]$ تا نزدیک‌ترین $\mu\beta$ کمتر از طول ضلع یعنی $|\beta|$ است. □

شش یکه در $\mathbb{Z}[\zeta_۳]$ وجود دارد: ± ۱، $\pm\zeta_۳$ و $\pm\zeta_۳^۲$ که رئوس یک شش ضلعی منتظم روی دایرهٔ واحد به مرکز مبدأ هستند (مجدداً شکل ۲.۷ را ببینید). شبیه یکه‌های $\mathbb{Z}$ و $\mathbb{Z}[i]$، همهٔ این اعداد ۱ را عاد می‌کنند. با تشکر از این یکه‌های جدید در $\mathbb{Z}[\zeta_۳]$، دو تجزیهٔ متمایز ۴ در $\mathbb{Z}[\sqrt{-۳}]$ همان تجزیه‌ها در $\mathbb{Z}[\zeta_۳]$ تا حد عوامل یکه هستند (تمرین).

اعداد صحیح مربعی

این که قادر هستیم شکست یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\sqrt{-۳}]$ را با توسیع آن به $\mathbb{Z}[\zeta_۳]$ برطرف کنیم، رضایت‌بخش است. اما آیا موجه است که $\zeta_۳ = \frac{-۱+\sqrt{-۳}}{۲}$ را صحیح تلقی کنیم؟ تعریفی کلی که به ما اجازه می‌دهد پاسخ مثبت دهیم به شرح زیر است.

تعریف. یک عدد مانند $\alpha \in \mathbb{C}$ یک عدد صحیح جبری[۷] است هرگاه در یک معادلهٔ چندجمله‌ای تکین[۸] با ضرایب صحیح، یعنی معادله‌ای به صورت

$$\alpha^m + a_{m-۱}\alpha^{m-۱} + \ldots + a_۱\alpha + a_۰ = ۰$$

که در آن $a_۰, a_۱, \ldots, a_{m-۱} \in \mathbb{Z}$، صدق کند. یک عدد صحیح مربعی[۹] یک عدد صحیح جبری است که در یک معادلهٔ مربعی تکین با ضرایب صحیح صدق کند.

مفهوم کلی اعداد صحیح جبری را در فصل ۱۰ مطالعه می‌کنیم. در آنجا نشان داده شده است که جمع، تفاضل و حاصل ضرب اعداد صحیح جبری، خود اعداد صحیح جبری هستند. $\zeta_۳$ یک عدد صحیح جبری است زیرا در معادلهٔ $x^۲ + x + ۱ = ۰$ که از تجزیهٔ $x^۳ - ۱$ به دست می‌آید صدق می‌کند. همهٔ عناصر $\mathbb{Z}[\zeta_۳]$ که از اعداد صحیح جبری ۱ و $\zeta_۳$ توسط جمع و تفاضل به دست می‌آیند صحیح جبری هستند. مستقیماً می‌توان نشان داد که این اعداد، مربعی هستند (تمرین).

بسته بودن تحت +، − و × مطمئناً لازمه‌ای طبیعی برای اعداد صحیح است اما شاید تعریف اعداد صحیح جبری خیلی وسعت یافته باشد و اعدادی که نباید صحیح تلقی شوند را شامل شود. دلیلی برای آن که این تعریف چنین نیست بدین شرح است: هر عدد صحیح جبری گویا، یک عدد صحیح معمولی است. این دلیل هنگامی قاطعیت پیدا می‌کند که احکام مربوط به اعداد صحیح معمولی

---

[۷] algebraic integer

[۸] monic

[۹] quadratic integer

به عنوان حالتی خاص از احکام مربوط به اعداد صحیح جبری نتیجه شوند.

اعداد صحیح جبری گویا. اگر عددی گویا مانند r در یک معادلهٔ چندجمله‌ای تکین با ضرایب صحیح صدق کند آنگاه r یک عدد صحیح معمولی است.

برهان. فرض کنیم $r = \frac{s}{t}$ که در آن $s, t \in \mathbb{Z}$ و نیز $\gcd(s,t) = ۱$. همچنین فرض کنیم r در معادلهٔ

$$x^m + a_{m-۱}x^{m-۱} + \ldots + a_۱ x + a_۰ = ۰$$

که در آن $a_۰, a_۱, \ldots, a_{m-۱} \in \mathbb{Z}$، صدق کند. با قرار دادن $\frac{s}{t}$ به جای x داریم

$$\frac{s^m}{t^m} = -a_{m-۱}\frac{s^{m-۱}}{t^{m-۱}} - \ldots - a_۱\frac{s}{t} - a_۰.$$

با ضرب کردن طرفین در t^m داریم

$$\begin{aligned} s^m &= -a_{m-۱}s^{m-۱}t - \ldots - a_۱ st^{m-۱} - a_۰ t^m \\ &= (-a_{m-۱}s^{m-۱} - \ldots - a_۱ st^{m-۲} - a_۰ t^{m-۱})t \qquad (*) \end{aligned}$$

چون $\gcd(s,t) = ۱$، هر عامل اول t (در صورت وجود) که سمت راست را عاد می‌کند باید سمت چپ را نیز عاد کند. از این رو بنابر یکتایی تجزیه به اعداد اول در $\mathbb{Z}$ داریم $t = \pm ۱$. لذا r یک عدد صحیح معمولی است. □

تبصره. از این حکم نتیجه می‌شود که ریشه‌های یک معادلهٔ چندجمله‌ای تکین با ضرایب صحیح یا صحیح هستند یا اصم. این مطلب آنچه را در بخش ۱.۵ در مورد اصم بودن $\sqrt{n}$ برای یک عدد طبیعی نامربع مانند n اثبات کردیم تعمیم می‌دهد زیرا $\sqrt{n}$ ریشهٔ معادلهٔ $x^۲ - n = ۰$ است.

تمرینها

دو تجزیهٔ یافت شده برای ۴ در $\mathbb{Z}[\sqrt{-۳}]$، یعنی ۲ × ۲ و $(۱ + \sqrt{-۳})(۱ - \sqrt{-۳})$، فقط در عوامل یکهٔ $\mathbb{Z}[\zeta_۳]$ با هم تفاوت دارند.

۱.۴.۷ یکه‌های u و $\bar{u}$ ی در $\mathbb{Z}[\zeta_۳]$ بیابید که

$$۲u \times ۲\bar{u} = (۱ - \sqrt{-۳})(۱ + \sqrt{-۳}).$$

۲.۴.۷ بررسی کنید که یکه‌های $\pm\zeta_۳$ و $\pm\zeta_۳^۲$ از $\mathbb{Z}[\zeta_۳]$ در چندجمله‌ای‌های تکینی با ضرایب صحیح صدق می‌کنند.

۵.۷ * جوابهای گویای $x^۳ + y^۳ = z^۳ + w^۳$

شبیه معادلهٔ فیثاغورسی $x^۲ + y^۲ = z^۲$ معادلهٔ $x^۳ + y^۳ = z^۳ + w^۳$ نیز تعدادی نامتناهی جواب صحیح دارد که برخی از آنها پرآوازه‌اند. در اینجا یکی از آنها را که در مورد رامانوجان[۱۰] (نظریه اعداد دان بزرگ هندی) است می‌آوریم.

> این لیتلوود[۱۱] بود که گفت هر عدد صحیح مثبت یکی از دوستان شخصی رامانوجان بوده است. به یاد می‌آورم که یک بار وقتی در پاتنی[۱۲] بیمار بود برای ملاقات وی رفته بودم. روی بدنهٔ تاکسی عدد ۱۷۲۹ نوشته شده بود و به وی گفتم که این عدد به نظر مزخرف می‌آید، امیدوارم برایم بدشگون نباشد. او پاسخ داد: " نه. این عدد بسیار جالبی است؛ این عدد کوچک‌ترین عددی است که به دو صورت می‌توان آن را به شکل مجموع دو مکعب بیان کرد."

هاردی[۱۳] (۱۹۷۳)

---

[۱۰] Ramanujan
[۱۳] Hardy

دو روش متفاوتی که رامانوجان به آن اشاره داشت عبارتند از

$$۱۷۲۹ = ۹^۳ + ۱۰^۳ = ۱^۳ + ۱۲^۳$$

که متناظر با جواب صحیحی از $x^۳ + y^۳ = z^۳ + w^۳$ هستند. به گفتهٔ برونکر[۱۴] (۱۶۵۷) همین جوابها توسط فرنیکل[۱۵] همراه با اعداد دیگر

$$\begin{aligned} ۹^۳ + ۱۵^۳ &= ۲^۳ + ۱۶^۳, \\ ۱۵^۳ + ۳۳^۳ &= ۲^۳ + ۳۴^۳, \\ ۱۶^۳ + ۳۳^۳ &= ۹^۳ + ۳۴^۳, \\ ۱۹^۳ + ۲۴^۳ &= ۱۰^۳ + ۲۷^۳ \end{aligned}$$

یافت شده بود. جواب تکان‌دهندهٔ دیگر این معادله $x = ۳$، $y = ۴$، $z = -۵$ و $w = ۶$ است. به بیان دیگر $۶^۳ = ۵^۳ + ۴^۳ + ۳^۳$. این نتیجه که به نظر می‌رسد $۳^۲ + ۴^۲ = ۵^۲$ را تعمیم می‌دهد واقعاً متعلق به معادلهٔ $x^۳ + y^۳ = z^۳ + w^۳$ است، اما این معادله از جهتی به معادلهٔ فیثاغورسی شبیه است - فرمولی پارامتری برای همهٔ جوابهای گویای آن وجود دارد.

این فرمول منسوب به اویلر (۱۷۵۶) می‌باشد. روش وی را می‌توان با استفاده از اعداد مختلط، یعنی نرم در

$$\mathbb{Q}[\sqrt{-۳}] = \{a + b\sqrt{-۳} : a, b \in \mathbb{Q}\},$$

ساده‌تر کرد.

جوابهای پارامتری $x^۳ + y^۳ = z^۳ + w^۳$. جوابهای گویا عبارتند از

$$\begin{aligned} x &= [(p + ۳q)(p^۲ + ۳q^۲) - ۱]r, \\ y &= [(-p + ۳q)(p^۲ + ۳q^۲) + ۱]r, \end{aligned}$$

[۱۴] Brouncker
[۱۵] Frenicle

$$\begin{aligned} z &= [-p+۳q+(p^۲+۳q^۲)^۲]r, \\ w &= [p+۳q-(p^۲+۳q^۲)^۲]r, \end{aligned}$$

که در آن p، q و r در اعداد گویا تغییر می‌کنند.

برهان. اگر جایگذاریهای $x=X+Y$، $y=X-Y$، $z=Z+W$ و $w=Z-W$ را انجام دهیم آنگاه معادلهٔ $x^۳+y^۳=z^۳+w^۳$ به صورت

$$X(X^۲+۳Y^۲)=Z(Z^۲+۳W^۲)$$

تبدیل می‌شود و X، Y، Z و W گویا هستند فقط و فقط وقتی که x، y، z و w چنین باشند.

لذا مسألهٔ ما یافتن جوابهای گویای معادلهٔ $X(X^۲+۳Y^۲)=Z(Z^۲+۳W^۲)$ می‌باشد. همچنین می‌توانیم این معادله را به حالت خاص $Z=۱$ تحویل کنیم (اگر بعداً جوابها را در یک عدد گویای دلخواه ضرب کنیم). لذا کافی است جوابهای گویای

$$X=\frac{۱+۳W^۲}{X^۲+۳Y^۲}$$

را بیابیم. حال داریم $a^۲+۳b^۲=|a+b\sqrt{-۳}|^۲$. از این رو

$$\begin{aligned} X &= \frac{|۱+W\sqrt{-۳}|^۲}{|X+Y\sqrt{-۳}|^۲} \\ &= \left|\frac{۱+W\sqrt{-۳}}{X+Y\sqrt{-۳}}\right|^۲ \\ &= |p+q\sqrt{-۳}|^۲=p^۲+۳q^۲ \end{aligned}$$

که در آن p و q گویا هستند مشروط بر آن که X، Y و W چنین باشند.

می‌توانیم p و q را به عنوان قسمتهای حقیقی و موهومی

$$p+q\sqrt{-۳}=\frac{۱+W\sqrt{-۳}}{X+Y\sqrt{-۳}}$$

تعریف کنیم. ضرب کردن طرفین در $X+Y\sqrt{-۳}$ نتیجه می‌دهد که

$$pX-۳qY+(qX+pY)\sqrt{-۳}=۱+W\sqrt{-۳}.$$

بنابراین با مساوی قرار دادن قسمتهای حقیقی و موهومی داریم

$$pX-۳qY=۱, \qquad qX+pY=W.$$

از آنجایی که دو معادلهٔ فوق بر حسب Y و W خطی هستند می‌توانیم آنها را برای Y و W بر حسب p و q حل کنیم. همچنین می‌دانیم که $X=p^۲+۳q^۲$. بدین ترتیب تناظری یک به یک بین زوجهای گویای (p,q) و سه‌تایی‌های گویای (X,Y,W) برقرار می‌شود که $X(X^۲+۳Y^۲)=Z(Z^۲+۳W^۲)$.

با جایگذاری این مقادیر X، Y، $Z=۱$ و W به جای x، y، z و w درمی‌یابیم که جوابهای گویای $x^۳+y^۳=z^۳+w^۳$ همان طور که ادعا کردیم همگی مضارب گویای

$$\begin{aligned} x &= (p+۳q)(p^۲+۳q^۲)-۱, \\ y &= (-p+۳q)(p^۲+۳q^۲)+۱, \\ z &= -p+۳q+(p^۲+۳q^۲)^۲, \\ w &= p+۳q-(p^۲+۳q^۲)^۲ \end{aligned}$$

هستند. □

مثال. $p=۱$، $q=۱$ نتیجه می‌دهد

$$۱۵^۳+۹^۳=۱۸^۳+(-۱۲)^۳$$

که مضربی از $۶^۳=۵^۳+۴^۳+۳^۳$ می‌باشد.

تمرینها

۱.۵.۷ اعداد p و q ی ساده‌تری بیابید که آنها هم (مضربی از) $۶^۳ = ۵^۳ + ۴^۳ + ۳^۳$ را به دست دهند.

روشن نیست که آیا جواب گویای پارامتری $x^۳ + y^۳ = z^۳ + w^۳$ جوابی پارامتری و صحیح را نیز به دست می‌دهد یا نه. با این حال داونپورت[۱۶] (۱۹۶۰)، صفحهٔ ۱۶۲، رده‌ای نامتناهی از جوابهای صحیح کشف شده توسط ماهلر[۱۷] در ۱۹۳۶ را ارائه می‌دهد.

۲.۵.۷ با قرار دادن $p = ۳q$ و اِعمال تغییری خطی از متغیر q به t، خانواده‌ای نامتناهی از جوابهای صحیح را به صورت

$$x = ۹t^۳ - ۱, \quad y = ۱, \quad z = ۹t^۴, \quad w = ۳t - ۹t^۴$$

به دست آورید.

۳.۵.۷ مقادیر t یی را بیابید که $۹^۳ = ۸^۳ + ۶^۳ + ۱^۳$ و $۱۲^۳ + ۱^۳ = ۱۰^۳ + ۹^۳$ را به دست دهند.

۶.۷ * عدد اول ریشهٔ دوم ۳-

شاید مهم‌ترین معادلهٔ دیوفانتی که می‌توان آن را به کمک $\mathbb{Z}[\zeta_۳]$ تجزیه و تحلیل کرد معادلهٔ فرما

$$x^۳ + y^۳ = z^۳ \qquad (*)$$

باشد. بدین وسیله حالت $n = ۳$ از قضیهٔ آخر فرما[۱۸] را تحقیق می‌کنیم: $x^n + y^n \neq z^n$ برای هر عدد طبیعی x، y، z و $n > ۲$.

---

[۱۶] Davenport

[۱۷] Mahler

[۱۸] Fermat's last theorem

برای رسیدن به تناقض، با فرض آن که (*) برای اعدادی طبیعی مانند x، y و z برقرار باشد، سمت چپ را تجزیه می‌کنیم:

$$x^{۳}+y^{۳} = (x+y)(x^{۲}-xy+y^{۲}) \qquad \text{در } \mathbb{Z}$$
$$= (x+y)(x+\zeta_{۳}y)(x+\zeta_{۳}^{۲}y) \qquad \text{در } \mathbb{Z}[\zeta_{۳}]$$

اگر x، y و z نسبت به هم اول باشند آنگاه می‌توان امید داشت که $x+y$، $x+\zeta_{۳}y$ و $x+\zeta_{۳}^{۲}y$ نیز نسبت به هم اول باشند. اگر چنین باشد می‌توانیم یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\zeta_{۳}]$ را به کار بریم و نتیجه بگیریم که $x+y$، $x+\zeta_{۳}y$ و $x+\zeta_{۳}^{۲}y$ مضارب یکه‌ای از مکعبهای کاملی در $\mathbb{Z}[\zeta_{۳}]$ هستند و به این روش می‌توانیم طرحی برای رسیدن به تناقض را در سر بپرورانیم.

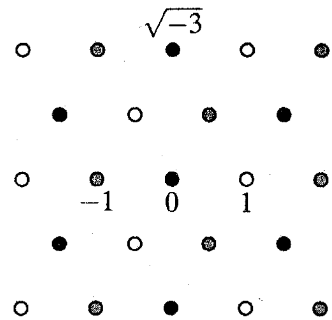
به طور تعجب‌آوری دقیقاً همین فرضِ $x^{۳}+y^{۳}=z^{۳}$ عاملی چون $\sqrt{-۳}$ را در معادله به اجبار ایجاد می‌کند. با نامگذاری مناسب جملات نتیجه می‌گیریم که $\sqrt{-۳}$ هم z و هم هر یک از اعداد $x+y$، $x+\zeta_{۳}y$ و $x+\zeta_{۳}^{۲}y$ را عاد می‌کند. این مطلب طرح اولیهٔ ما را که مبتنی بر نسبت به هم اول بودن عوامل بود تباه می‌سازد اما طرح جدیدی را پیشنهاد می‌کند: طرفین معادلهٔ (*) را بر $(\sqrt{-۳})^{۳}$ تقسیم کنید و معادله‌ای جدید را به همان صورت اما با عوامل کمتری از $\sqrt{-۳}$ بسازید. با اندک تعمیمی در معادلهٔ فرما می‌توان این طرح جدید را کارساز کرد. این مطلب بنابر نزول نامتناهی به تناقض می‌انجامد زیرا یک معادلهٔ صحیح در $\mathbb{Z}[\zeta_{۳}]$ را نمی‌توان بی‌نهایت بار بر $\sqrt{-۳}$ تقسیم کرد.

برای آن که ببینیم $\sqrt{-۳}$ چگونه خودش را در معادلهٔ فرما، یعنی (*)، جا می‌کند در ابتدا برخی از خواص مقدماتی آن را بسط می‌دهیم. این خواص با همنهشتی به پیمانهٔ $\sqrt{-۳}$ سر و کار دارد که طبق معمول

$$\sigma \equiv_{\nu} \tau$$

بدان معنی است که ν عدد $\sigma-\tau$ را عاد می‌کند. بالاخص، $\sigma \equiv_{\sqrt{-۳}} ۰$ یعنی $\sqrt{-۳}$ عدد σ را عاد می‌کند.

شکل ۳.۷ رده‌های همنهشتی به پیمانهٔ $\sqrt{-۳}$ را در $\mathbb{Z}[\zeta_۳]$ نشان می‌دهد. این رده‌ها سه تا هستند: رده‌های ۰ (سیاه)، ۱ (سفید) و ۱− (خاکستری).



شکل ۳.۷: رده‌های همنهشتی به پیمانهٔ $\sqrt{-۳}$

این مطلب را می‌توان با محاسبه بررسی کرد. کافی است به باقیمانده‌های ممکن تقسیم بر $\sqrt{-۳}$ که قدرمطلقی کوچک‌تر از $\sqrt{۳}$ دارند توجه کنیم. حال می‌توانیم خواص زیر را اثبات کنیم:

مکعبهای کامل به پیمانهٔ ۹. برای هر $\sigma \in \mathbb{Z}[\zeta_۳]$ اگر $\sigma \not\equiv_{\sqrt{-۳}} ۰$ آنگاه $\sigma^۳ \equiv_۹ \pm ۱$.

برهان. چون $\sigma \not\equiv_{\sqrt{-۳}} ۰$ پس $\sigma \equiv_{\sqrt{-۳}} \pm ۱$. قرار می‌دهیم $\tau = \pm\sigma$ که $\tau \equiv_{\sqrt{-۳}} ۱$. لذا برای μ یی در $\mathbb{Z}[\zeta_۳]$ داریم $\tau = ۱ + \mu\sqrt{-۳}$. در این صورت

$$\begin{aligned}
\tau^۳ - ۱ &= (۱ + \mu\sqrt{-۳})^۳ - ۱ \\
&= ۳\mu\sqrt{-۳} + ۳(\mu\sqrt{-۳})^۲ + (\mu\sqrt{-۳})^۳ \\
&= ۳\sqrt{-۳}(\mu + \mu^۲\sqrt{-۳} - \mu^۳) \\
&\equiv_{\sqrt{-۳}} ۳\sqrt{-۳}(\mu - \mu^۳) \\
&\equiv_{\sqrt{-۳}} -۳\sqrt{-۳}\mu(\mu - ۱)(\mu + ۱).
\end{aligned}$$

حال μ، $\mu - ۱$ و $\mu + ۱$ در رده‌های همنهشتی متفاوتی هستند و از این رو یکی از آنها بر $\sqrt{-۳}$ بخش پذیر است. لذا $\tau^۳ - ۱$ بر $۹ = -۳\sqrt{-۳}\sqrt{-۳}$

بخش پذیر می‌باشد یعنی $\tau^{۳} \equiv_{۹} ۱$ و در نتیجه $\sigma^{۳} \equiv_{۹} \pm ۱$. □

از این خاصیت نتیجه می‌شود که اگر $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta_{۳}]$ و

$$\alpha^{۳} + \beta^{۳} + \gamma^{۳} = ۰ \qquad (**)$$

(که صورت معادلی از $x^{۳} + y^{۳} = z^{۳}$ می‌باشد؛ چون $(-z)^{۳} = -z^{۳}$)، آنگاه $\sqrt{-۳}$ حداقل یکی از α، β یا γ را عاد می‌کند. اگر چنین نباشد آنگاه با همنهشتی گرفتن به پیمانهٔ ۹ داریم

$$\pm ۱ \pm ۱ \pm ۱ \equiv_{۹} ۰$$

و به سادگی با بررسی هشت حالت ممکن برای علامتهای + و − می‌بینیم که این همنهشتی غیر ممکن است. با تغییر نام مناسب α، β و γ می‌توانیم فرض کنیم که γ بر $\sqrt{-۳}$ بخش پذیر است؛ مثلاً $\gamma = \delta(\sqrt{-۳})^{n}$. در این صورت معادلهٔ سه مکعب (**) به صورت

$$\alpha^{۳} + \beta^{۳} + \delta^{۳}(\sqrt{-۳})^{۳n} = ۰ \qquad (***)$$

تبدیل می‌شود. اکنون خاصیت مهم دیگری از همنهشتی به پیمانهٔ $\sqrt{-۳}$ وارد بازی می‌شود.

همنهشتی عوامل در مجموعی از دو مکعب. برای هر $\alpha, \beta \in \mathbb{Z}[\zeta_{۳}]$، عوامل $\alpha + \beta$، $\alpha + \zeta_{۳}\beta$، $\alpha + \zeta_{۳}^{۲}\beta$ از $\alpha^{۳} + \beta^{۳}$ با یکدیگر به پیمانهٔ $\sqrt{-۳}$ همنهشت هستند.

برهان. چون $\zeta_{۳} = \frac{-۱+\sqrt{-۳}}{۲}$، داریم

$$\begin{aligned} \alpha + \zeta_{۳}\beta &= \alpha + \frac{-۱ + \sqrt{-۳}}{۲}\beta \\ &= \alpha + \beta + \frac{-۳ + \sqrt{-۳}}{۲}\beta \\ &= \alpha + \beta + \frac{۱ + \sqrt{-۳}}{۲}\beta\sqrt{-۳} \\ &\equiv_{\sqrt{-۳}} \alpha + \beta. \end{aligned}$$

به طور مشابه

$$\alpha+\zeta_3^2\beta=\alpha+\frac{-1-\sqrt{-3}}{2}\beta\equiv_{\sqrt{-3}}\alpha+\beta. \ \square$$

حال این خاصیت را برای صورت تجزیه شدهٔ معادلهٔ $(***)$ به کار می‌بریم:

$$(\alpha+\beta)(\alpha+\zeta_3\beta)(\alpha+\zeta_3^2\beta)+\delta^3(\sqrt{-3})^{3n}=0.$$

عدد $\sqrt{-3}$ در $\mathbb{Z}[\zeta_3]$ اول است زیرا نرم آن یعنی ۳ در $\mathbb{Z}$ اول است. چون $\sqrt{-3}$ عدد $\delta^3(\sqrt{-3})^{3n}$ را عاد می‌کند، حداقل یکی از عوامل $\alpha+\beta$، $\alpha+\zeta_3\beta$، $\alpha+\zeta_3^2\beta$ را عاد خواهد کرد. اما در این صورت باید هر سهٔ آنها را عاد کند چون این اعداد به پیمانهٔ $\sqrt{-3}$ با یکدیگر همنهشت هستند. در مجموع داریم: اگر اعداد $\alpha,\beta,\gamma\in\mathbb{Z}[\zeta_3]$ در معادلهٔ

$$\alpha^3+\beta^3+\gamma^3=0$$

صدق کنند آنگاه (با تغییر نام مناسب اعداد در صورت لزوم) $\sqrt{-3}$ عدد γ و همهٔ عوامل $\alpha+\beta$، $\alpha+\zeta_3\beta$، $\alpha+\zeta_3^2\beta$ از $\alpha^3+\beta^3$ را عاد خواهد کرد.

تمرینها

در روشهای دیگری که برای معادلهٔ $\alpha^3+\beta^3+\gamma^3=0$ سراغ داریم (ناگل[19] (۱۹۵۱) صفحهٔ ۲۴۱، گراسوالد[20] (۱۹۶۶) صفحهٔ ۱۶۹، ردموند[21] (۱۹۹۶) صفحهٔ ۶۹۷ و طرحی اجمالی در بیکر[22] (۱۹۸۴) صفحهٔ ۸۶) عدد $\lambda=\zeta_3-1$ به جای $\sqrt{-3}$ استفاده شده است. این مطلب احتمالاً بدین دلیل است که با معادلهٔ $\alpha^n+\beta^n+\gamma^n=0$ می‌توان به طور مشابه با استفاده از

[19] Nagell
[20] Grosswald
[21] Redmond
[22] Baker

$\lambda = \zeta_n - 1$ برای مقادیر مشخص دیگری از n مانند $n = 5$ رفتار کرد، گرچه به ادراک می‌بینیم که $\lambda = \zeta_3 - 1$ اساساً همان کار را انجام می‌دهد. دلیل آن به صورت زیر است.

۱.۶.۷ نشان دهید که λ مضرب یکه‌ای از $\sqrt{-3}$ است.

۲.۶.۷ از تمرین ۱.۶.۷ نتیجه بگیرید که

$$\sigma \equiv_{\lambda} \tau \Leftrightarrow \sigma \equiv_{\sqrt{-3}} \tau$$

و نیز

$$\sigma \equiv_{\lambda^4} \tau \Leftrightarrow \sigma \equiv_{9} \tau.$$

۷.۷ * قضیه آخر فرما برای $n = 3$

اکنون این تصور را که معادلهٔ $\alpha^3 + \beta^3 + \gamma^3 = 0$ برای $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta_3]$ غیر ممکن است مدلل می‌سازیم چرا که به نظر می‌رسد به تعدادی نامحدود بر $\sqrt{-3}$ بخش پذیر است. حال فرض می‌کنیم که γ جملهٔ قابل قسمت بر $\sqrt{-3}$ باشد. لذا $\gamma = \delta(\sqrt{-3})^n$ که δ بر $\sqrt{-3}$ تقسیم‌پذیر نیست. در این صورت می‌توان معادله را به صورت

$$\alpha^3 + \beta^3 + \delta^3(\sqrt{-3})^{3n} = 0$$

نوشت که n عددی طبیعی است و فرض می‌کنیم که کمترین مقدار ممکن را دارد. در حقیقت باید داشته باشیم $n \geq 2$. دلیل این امر این است که α، β و γ نسبت به هم اول هستند و لذا α و β (همانند δ) بر $\sqrt{-3}$ قابل قسمت نیستند. اما در این صورت (بنابر شماره‌گذاری رده‌های همنهشتی در بخش قبل) هر یک

از آنها همنهشت با ± ۱ به پیمانهٔ $\sqrt{-۳}$ می‌باشد. از این رو اگر $n = ۱$ و معادله را به پیمانهٔ ۹ بنویسیم خاصیت مکعبهای کامل به پیمانهٔ ۹ نتیجه می‌دهد که

$$\pm ۱ \pm ۱ \pm (\sqrt{-۳})^۳ \equiv_۹ ۰$$

که به وضوح برای هر ترکیبی از علامتها غیر ممکن است.

بنابراین می‌توانیم فرض کنیم که $n \geq ۲$. از آنجایی که می‌توانیم تقسیم کردن بر $\sqrt{-۳}$ را تکرار کنیم، فرض می‌کنیم که معادلهٔ کمی کلی‌تر

$$\alpha^۳ + \beta^۳ + \varepsilon(\sqrt{-۳})^{۳n}\delta^۳ = ۰ \qquad (*)$$

برقرار است که در آن $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta_۳]$ نسبت به هم اول هستند و ε یکه‌ای از $\mathbb{Z}[\zeta_۳]$ می‌باشد. وجود یکهٔ ε در اینجا بدین دلیل است که تقسیم کردن باعث به وجود آمدن یکه‌هایی می‌گردد که نمی‌توانند کاملاً حذف شوند.

امتناع معادلهٔ $\alpha^۳ + \beta^۳ + \varepsilon(\sqrt{-۳})^{۳n}\delta^۳ = ۰$. فرض کنیم $\alpha, \beta, \delta \in \mathbb{Z}[\zeta_۳]$ نسبت به هم اول باشند و بر $\sqrt{-۳}$ بخش پذیر نباشند. نیز فرض کنیم ε یکه باشد و $n \geq ۲$. در این صورت

$$\alpha^۳ + \beta^۳ + \varepsilon(\sqrt{-۳})^{۳n}\delta^۳ \neq ۰.$$

برهان. به برهان خلف فرض کنیم که اعداد نسبت به هم اول α، β و δ که بر $\sqrt{-۳}$ بخش پذیر نیستند وجود دارند که معادلهٔ $(*)$ برای آنها برقرار است. از یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\zeta_۳]$ نتیجه می‌شود که عدد اول $\sqrt{-۳}$ باید $\alpha^۳ + \beta^۳$ را عاد کند. از این رو $\sqrt{-۳}$ لااقل یکی از اعداد $\alpha + \beta$، $\alpha + \zeta_۳\beta$، $\alpha + \zeta_۳^۲\beta$ را عاد خواهد کرد.

اما همان طور که در بخش قبل دیدیم، این سه عامل به پیمانهٔ $\sqrt{-۳}$ همنهشت هستند و لذا در حقیقت $\sqrt{-۳}$ همهٔ آنها را عاد می‌کند. بنابراین

$$\frac{\alpha+\beta}{\sqrt{-۳}}, \frac{\alpha+\zeta_۳\beta}{\sqrt{-۳}}, \frac{\alpha+\zeta_۳^۲\beta}{\sqrt{-۳}} \in \mathbb{Z}[\zeta_۳].$$

این سه عدد مقسوم‌علیه اول مشترکی در $\mathbb{Z}[\zeta_3]$ ندارند. هر مقسوم‌علیه مشترک از $\frac{\alpha+\beta}{\sqrt{-3}}$ و $\frac{\alpha+\zeta_3\beta}{\sqrt{-3}}$ تفاضل آنها یعنی

$$\frac{1-\zeta_3}{\sqrt{-3}}\beta = \frac{3-\sqrt{-3}}{2\sqrt{-3}}\beta = \frac{1+\sqrt{-3}}{2}\beta = \text{یکه } \times \beta$$

را نیز عاد می‌کند. از این رو هر مقسوم‌علیه مشترک از $\frac{\alpha+\beta}{\sqrt{-3}}$ و $\frac{\alpha+\zeta_3\beta}{\sqrt{-3}}$ باید β را عاد کند. با در نظر گرفتن $\zeta_3\frac{\alpha+\beta}{\sqrt{-3}} - \frac{\alpha+\zeta_3\beta}{\sqrt{-3}}$ به طور مشابه درمی‌یابیم که α را نیز عاد می‌کند. اما هیچ مقسوم‌علیه اول مشترکی برای α و β و از این رو برای $\frac{\alpha+\beta}{\sqrt{-3}}$ و $\frac{\alpha+\zeta_3\beta}{\sqrt{-3}}$ وجود ندارد. محاسباتی مشابه این، همین نتیجه را برای دیگر زوجهای متشکل از $\frac{\alpha+\beta}{\sqrt{-3}}$، $\frac{\alpha+\zeta_3\beta}{\sqrt{-3}}$ و $\frac{\alpha+\zeta_3^2\beta}{\sqrt{-3}}$ به دست می‌دهد.

لذا می‌توانیم یکتایی تجزیه به اعداد اول را برای تغییر شکل یافتهٔ معادلهٔ (*)، یعنی

$$\frac{\alpha+\beta}{\sqrt{-3}}\cdot\frac{\alpha+\zeta_3\beta}{\sqrt{-3}}\cdot\frac{\alpha+\zeta_3^2\beta}{\sqrt{-3}} = -\varepsilon(\sqrt{-3})^{3n-3}\delta^3$$

به کار بریم و نتیجه بگیریم که هر عامل سمت چپ، حاصل ضرب یکه‌ای در یک مکعب کامل است؛ مثلاً

$$\frac{\alpha+\beta}{\sqrt{-3}} = \varepsilon_1\alpha_1^3, \quad \frac{\alpha+\zeta_3\beta}{\sqrt{-3}} = \varepsilon_2\beta_1^3, \quad \frac{\alpha+\zeta_3^2\beta}{\sqrt{-3}} = \varepsilon_3\gamma_1^3$$

که α_1، β_1 و γ_1 نسبت به هم اولند زیرا $\frac{\alpha+\beta}{\sqrt{-3}}$، $\frac{\alpha+\zeta_3\beta}{\sqrt{-3}}$ و $\frac{\alpha+\zeta_3^2\beta}{\sqrt{-3}}$ چنین هستند. نتیجه می‌شود $(\sqrt{-3})^{3n-3}$ (که توانی از یک عدد اول است) دقیقاً در یکی از سه عدد α_1^3، β_1^3، γ_1^3 ظاهر می‌شود. با تغییر نام (در صورت لزوم) می‌توانیم فرض کنیم که $(\sqrt{-3})^{3n-3}$ مقسوم‌علیهی از γ_1^3 است. لذا می‌توان نوشت $\gamma_1^3 = (\sqrt{-3})^{3n-3}\delta_1^3$.

حال به این حقیقت دلپذیر توجه می‌کنیم که

$$\zeta_3^2\frac{\alpha+\beta}{\sqrt{-3}} + \frac{\alpha+\zeta_3\beta}{\sqrt{-3}} + \zeta_3\frac{\alpha+\zeta_3^2\beta}{\sqrt{-3}} = 0$$

زیرا $\zeta_3^2 + \zeta_3 + 1 = 0$. این حقیقت بر حسب α_1، β_1 و δ_1 عبارت است از

$$\zeta_3^2\varepsilon_1\alpha_1^3 + \varepsilon_2\beta_1^3 + \zeta_3\varepsilon_3(\sqrt{-3})^{3n-3}\delta_1^3 = 0$$

که وقتی بر یکهٔ $\zeta_3^2\varepsilon_1$ تقسیم شود به صورت

$$\alpha_1^3 + \varepsilon_4\beta_1^3 + \varepsilon_5(\sqrt{-3})^{3n-3}\delta_1^3 = 0 \qquad (**)$$

تبدیل می‌گردد. در اینجا ε_4 و ε_5 یکه هستند و α_1، β_1، δ_1 نسبت به هم اول و غیر قابل‌قسمت بر $\sqrt{-3}$ می‌باشند. معادلهٔ (**) تقریباً همان شکل (*) را دارد جز این که یکهٔ ε_4 در آن ظاهر شده است. خوشبختانه می‌توانیم با استدلال زیر نشان دهیم که $\varepsilon_4 = \pm 1$.

چون $n \geq 2$ عدد $(\sqrt{-3})^{3n-3}$ بر $3\sqrt{-3}$ بخش پذیر است، در حالی که $\alpha_1^3, \beta_1^3 \equiv_9 \pm 1$ (بنابر خاصیت مکعبهای کامل به پیمانهٔ ۹) و از این رو به پیمانهٔ $3\sqrt{-3}$ نیز چنین است. لذا اگر (**) را به پیمانهٔ $3\sqrt{-3}$ بنویسیم داریم

$$\pm 1 \pm \varepsilon_4 \equiv_{3\sqrt{-3}} 0.$$

همان گونه که می‌خواستیم تنها یکه‌هایی که در این همنهشتی صدق می‌کنند ± 1 هستند. بنابراین معادلهٔ (*) به شکل ساده‌تر

$$\alpha_1^3 \pm \beta_1^3 + \varepsilon_5(\sqrt{-3})^{3n-3}\delta_1^3 = 0 \qquad (***)$$

تبدیل می‌شود که α_1، β_1، δ_1 نسبت به هم اول و غیر قابل‌قسمت بر $\sqrt{-3}$ می‌باشند. چون $(-\beta_1)^3 = -\beta_1^3$، معادلهٔ (***) در حقیقت به همان شکل (*) است با این تفاوت که توان $\sqrt{-3}$ در آن کوچک‌تر است.

این مطلب در تناقض با این فرض است که توان $\sqrt{-3}$ در (*) کوچک‌ترین مقدار ممکن را دارد. از این رو (*) برقرار نیست. □

نتیجه. معادلهٔ $x^3 + y^3 = z^3$ برای اعداد صحیح $x, y, z \neq 0$ جواب ندارد.

برهان. به برهان خلف فرض کنیم که برای x، y و z ی صحیح و ناصفر داشته باشیم $x^۳ + y^۳ = z^۳$. با تقسیم کردن بر هر مقسوم‌علیه مشترک در $\mathbb{Z}[\zeta_۳]$ معادله‌ای به صورت

$$\alpha^۳ + \beta^۳ + \gamma^۳ = ۰$$

حاصل می‌شود که در آن $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta_۳]$ نسبت به هم اول هستند. با تغییر نام مناسب اعداد (در صورت لزوم) می‌توانیم فرض کنیم عددی که مضرب $\sqrt{-۳}$ است $\gamma = (\sqrt{-۳})^n \delta$ می‌باشد که در آن δ بر $\sqrt{-۳}$ بخش پذیر نیست. بنابراین معادلهٔ

$$\alpha^۳ + \beta^۳ + (\sqrt{-۳})^{۳n} \delta^۳ = ۰$$

را داریم که در آن $\alpha, \beta, \delta \in \mathbb{Z}[\zeta_۳]$ نسبت به هم اول و غیر قابل‌قسمت بر $\sqrt{-۳}$ می‌باشند. این حالت خاصی از معادله‌ای است که هم‌اکنون امتناع آن اثبات شد. بنابراین $x^۳ + y^۳ = z^۳$ برای اعداد صحیح $x, y, z \neq ۰$ جواب ندارد. □

تمرینها

امتناع معادلهٔ $\alpha^۳ + \beta^۳ + \gamma^۳ = ۰$ برای α، β و γ ی ناصفر در $\mathbb{Z}[\zeta_۳]$ شاید سخت‌ترین حکم این کتاب باشد. لذا خواننده ممکن است برهان آن را به سختی دریابد. تمرینهای زیر قصد دارند دریافت بهتری را با استفاده از ایده‌های برهان در مثالی مشابه مهیا سازند. این تمرینها قضیه‌ای از لژاندر را اثبات می‌کنند که می‌گوید

$$\alpha^۳ + \beta^۳ + ۳\gamma^۳ = ۰$$

برای α، β و γ ی ناصفر در $\mathbb{Z}[\zeta_۳]$ جواب ندارد.

همانند بالا، این استدلال یکه‌های مجهولی را معرفی می‌کند. لذا احتیاج

داریم امتناع معادلهٔ کلی‌تر

$$\alpha^{۳} + \beta^{۳} + \varepsilon(\sqrt{-۳})^{۳n+۲}\gamma^{۳} = ۰ \qquad (*)$$

را اثبات کنیم که در آن γ مضرب $\sqrt{-۳}$ نیست و ε یکه‌ای در $\mathbb{Z}[\zeta_۳]$ است. گام پیشنیاز (که به طور معمول با تقسیم کردن بر عوامل مشترک صورت می‌گیرد) به ما این امکان را می‌دهد که فرض کنیم $\alpha_۱$، $\beta_۱$، $\delta_۱$ نسبت به هم اول و غیر قابل‌قسمت بر $\sqrt{-۳}$ می‌باشند. همچنین فرض می‌کنیم که توان $\sqrt{-۳}$ در $(*)$ کمترین مقدار ممکن را دارد.

۱.۷.۷ شرح دهید که چرا $\alpha^{۳} + \beta^{۳} + ۳\gamma^{۳} = ۰$ حالت خاصی از $(*)$ است.

۲.۷.۷ معادلهٔ $(*)$ را به پیمانهٔ ۹ بنویسید و با استفاده از خاصیت مکعبهای کامل نشان دهید که در $(*)$ داریم $n \geq ۱$.

۳.۷.۷ حال از همنهشت بودن عوامل $\alpha^{۳} + \beta^{۳}$، نسبت به هم اول بودن آنها و یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\zeta_۳]$ استفاده کنید و از $(*)$ نتیجه بگیرید که دو تا از اعداد

$$\frac{\alpha+\beta}{\sqrt{-۳}}, \frac{\alpha+\zeta_۳\beta}{\sqrt{-۳}}, \frac{\alpha+\zeta_۳^{۲}\beta}{\sqrt{-۳}} \in \mathbb{Z}[\zeta_۳]$$

مضرب یکه‌ای از یک مکعب کامل هستند و سومی مضرب یکه‌ای از $(\sqrt{-۳})^{۳n-۱}$ می‌باشد.

۴.۷.۷ از تمرین ۳.۷.۷ و حقیقت دلپذیر نتیجه بگیرید که معادلهٔ معتبری به صورت

$$\varepsilon_۱\alpha_۱^{۳} + \varepsilon_۲\beta_۱^{۳} + \varepsilon_۳(\sqrt{-۳})^{۳n-۱}\gamma_۱^{۳} = ۰$$

یا به طور معادل به صورت

$$\alpha_۱^{۳} + \varepsilon_۴\beta_۱^{۳} + \varepsilon_۵(\sqrt{-۳})^{۳n-۱}\gamma_۱^{۳} = ۰ \qquad (**)$$

وجود دارد که در آن $\varepsilon_۴$ و $\varepsilon_۵$ یکه‌هایی در $\mathbb{Z}[\zeta_۳]$ هستند و $\alpha_۱$، $\beta_۱$، $\gamma_۱$ غیر قابل‌قسمت بر $\sqrt{-۳}$ می‌باشند.

۵.۷.۷ با نوشتن (**) به پیمانهٔ ۳ نشان دهید که $\varepsilon_{۴} = \pm ۱$ (در کجا از $n \geq ۱$ استفاده می‌شود؟). نتیجه بگیرید که (**) با معادله‌ای به صورت (*) اما با توان کوچک‌تری از $\sqrt{-۳}$ معادل است.

۶.۷.۷ نتیجه بگیرید که معادلهٔ (*) برای $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta_{۳}]$ ی ناصفر برقرار نیست.

۸.۷ بحث

در فصلهای اخیر روشهای بسیاری که در آن اعداد صحیح جبری، اعداد صحیح معمولی و بالاخص معادله‌های دیوفانتی را نمایان می‌سازند دیده‌ایم. به عنوان ساده‌ترین مرحله، نرم ضربی ما را قادر می‌سازد که چیزهایی از این قبیل را انجام دهیم:

- تولید جوابهای معادلهٔ پل $x^{۲} - ny^{۲} = ۱$ از توانهای $x_{۱} + y_{۱}\sqrt{n}$ که در آن $(x_{۱}, y_{۱})$ کوچک‌ترین جواب طبیعی است.
- یافتن همهٔ جوابهای گویای $x^{۳} + y^{۳} = z^{۳} + w^{۳}$.

در مرحله‌ای پیچیده‌تر می‌توان نشان داد که حلقه‌های مشخصی از اعداد صحیح جبری از یکتایی تجزیه به اعداد اول برخوردار هستند که در بین آنها می‌توان $\mathbb{Z}[i]$، $\mathbb{Z}[\sqrt{-۲}]$ و $\mathbb{Z}[\zeta_{۳}]$ را نام برد. این مطلب ما را قارد می‌سازد که تجزیه‌هایی جبری از قبیل

$$\begin{aligned} x^{۲} + y^{۲} &= (x - y\mathrm{i})(x + y\mathrm{i}) \\ x^{۳} + y^{۳} &= (x + y)(x + \zeta_{۳} y)(x + \zeta_{۳}^{۲} y) \end{aligned}$$

را تجزیه و تحلیل کنیم و جوابهای معادله‌های مشخصی را که در آنها ظاهر می‌شوند بیابیم. مثلاً

- جوابهای اولیهٔ معادلهٔ فیثاغورسی $x^۲ + y^۲ = z^۲$ را می‌توان با تجزیه کردن $x^۲ + y^۲$ در $\mathbb{Z}[\mathrm{i}]$ یافت.
- قضیهٔ فرما را (که می‌گوید هر عدد اول مانند $p = ۴n + ۱$ مجموعی از دو مجذور است) می‌توان با نشان دادن این که p عددی به صورت $m^۲ + ۱$ را عاد می‌کند و سپس با تجزیه کردن $m^۲ + ۱$ در $\mathbb{Z}[\mathrm{i}]$ اثبات کرد.
- جوابهای صحیح معادلهٔ باشه $y^۳ = x^۲ + ۲$ را می‌توان با تجزیه کردن $x^۲ + ۲$ در $\mathbb{Z}[\sqrt{-۲}]$ یافت.
- امتناع وجود جوابهای طبیعی $x^۳ + y^۳ = z^۳$ را می‌توان با تجزیه کردن $x^۳ + y^۳$ در $\mathbb{Z}[\zeta_۳]$ اثبات کرد.

اما تا اینجا اثبات کرده‌ایم که یکتایی تجزیه به اعداد اول فقط در $\mathbb{Z}$، $\mathbb{Z}[\mathrm{i}]$، $\mathbb{Z}[\sqrt{-۲}]$ و $\mathbb{Z}[\zeta_۳]$ برقرار است و دیدیم که در $\mathbb{Z}[\sqrt{-۳}]$ برقرار نیست. بنابراین هیچ تضمینی وجود ندارد که بتوانیم این برخورد را با $\mathbb{Z}[\sqrt{-۵}]$، $\mathbb{Z}[\sqrt{-۶}]$، ... یا $\mathbb{Z}[\zeta_n]$ برای مقادیر بزرگ‌تر n داشته باشیم.

در فصل ۱۱ نشان می‌دهیم که یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\sqrt{-۵}]$ شکست می‌خورد و این بار با پر کردن حفره‌های بدیهی $\mathbb{Z}[\sqrt{-۵}]$ (همانند آنچه در $\mathbb{Z}[\sqrt{-۳}]$ انجام دادیم) این خلل برطرف نخواهد شد. این وضعیت، اعدادی ایده‌آلی را از فضایی بیرونی در ریاضیات فرا می‌خواند (روشن نیست که این اعداد در $\mathbb{C}$ که اعداد جبری معمولی در آنجا ظاهر می‌شوند وجود داشته باشند).

این وضعیت وخیم اولین بار توسط کومر در سالهای ۱۸۴۰ تشخیص داده شد و هنگامی روشن‌تر گردید که لامه[۲۳] (۱۸۴۷) برهانی غلط از قضیهٔ آخر فرما را (که می‌گوید برای اعداد طبیعی x، y، z و $n \geq ۲$ داریم $x^n + y^n \neq z^n$

---

[۲۳] Lamé

منتشر کرد. لامه تجزیهٔ

$$x^n + y^n = (x+y)(x+\zeta_n y)\cdots(x+\zeta_n^{n-۱}y)$$

را (همانند روش ما در بخش ۷.۷ برای حالت $n = ۳$) به کار برد که در آن $\zeta_n = \cos\frac{۲\pi}{n} + \mathrm{i}\sin\frac{۲\pi}{n}$. اما او فرض کرده بود که $\mathbb{Z}[\zeta_n]$ از یکتایی تجزیه به اعداد اول برخوردار است و کومر نشان داد که برای $n \geq ۲۳$ این مطلب غلط است. کومر بی هیچ شکی مطلع بود که یکتایی تجزیه به اعداد اول در حلقه‌های اعداد صحیح مربعی مانند $\mathbb{Z}[\sqrt{-۵}]$ نیز شکست می‌خورد اما به $\mathbb{Z}[\zeta_n]$ بیشتر علاقه‌مند بود. $\mathbb{Z}[\zeta_n]$ اعداد صحیح دایره‌بُر[۲۴] نامیده می‌شود زیرا ۱، ζ_n، $\zeta_n^۲$، ...، $\zeta_n^{n-۱}$ دایرهٔ واحد را به n قسمت مساوی می‌بُرند.

وی اعداد ایده‌آلی را برای احراز یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\zeta_n]$ معرفی کرد که او را قادر می‌ساخت تا قضیهٔ آخر فرما را برای بسیاری از مقادیر n (گرچه نه همهٔ آنها) اثبات کند. با اهمیتی بیشتر، مفهوم ایده‌آل، اعداد صحیح دایره‌بر را به دست داد و به جبر و هندسهٔ جبری و نیز نظریه اعداد گسترش پیدا کرد. مثالهای ساده‌تر همچون $\mathbb{Z}[\sqrt{-۳}]$ و $\mathbb{Z}[\sqrt{-۵}]$ توسط ددکیند در سالهای ۱۸۷۰ در درسی که توصیفی از اعداد ایده‌آلی را از شیر مرغ تا جان آدمیزاد ارائه می‌داد، تأکید گردید. در فصل ۱۱ رهیافت ددکیند را پی می‌گیریم. ترجمه‌ای انگلیسی از تفسیر خود ددکیند را می‌توان در ددکیند (۱۸۷۷) یافت.

باید متذکر شد که قضیهٔ آخر فرما را برای $n = ۴$ و $n = ۷$ می‌توان صرفاً با استفاده از اعداد صحیح معمولی اثبات کرد. برهانی برای $n = ۴$ توسط خود فرما ارائه شده است (برهانی در نظریه اعداد که او واقعاً خودش آن را نوشته بود) و صورتهایی از آن در بسیاری از کتابها آمده است. دو شکل از آن را می‌توان در استیلول (۱۹۹۸) صفحات ۱۳۱ تا ۱۳۴ یافت. یک برهان مقدماتی برای $n = ۷$ توسط و. ا. لبگ[۲۵] (۱۸۴۰) کشف شد که توسط جنوچی[۲۶]

---

[۲۴] cyclotomic (*circle-cutting*) integers

[۲۵] V. A. Lebesgue

[۲۶] Genocchi

(۱۸۷٦) با پیگیری ترفند قابل توجه تشکیل مجموع دو توان هفتم ریشه‌های یک معادلهٔ مکعبی، بسیار ساده شد. این برهان غیر مشهور را می‌توان در ناگل (۱۹۵۱) صفحات ۲۴۸ تا ۲۵۱ و ریبنبویم[۲۷] (۱۹۹۹) صفحات ۵۷ تا ٦۲ یافت.

---

[۲۷] Ribenboim

۸

قضیه چهار مجذور

پیش‌نگاه

در این فصل با پیگیری برهان هرویتز[۱] اثبات می‌کنیم که هر عدد طبیعی، مجموع چهار مجذور صحیح است. این برهان بدان جهت انتخاب شده است که با برهان قضیهٔ دو مجذور که قبلاً در فصل ٦ اثبات شد شباهت دارد و چهارگانها را که دارای ساختاری ریاضی با نمود جبری و هندسی بسیار زیبا هستند معرفی می‌کند.

با مشاهدهٔ این مطلب که ماتریسهای به صورت $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ رفتاری شبیه اعداد مختلط دارند، چهارگانها را به صورت ماتریسهای $\begin{pmatrix} a+d\mathrm{i} & b+c\mathrm{i} \\ -b+c\mathrm{i} & a-d\mathrm{i} \end{pmatrix}$ که در آن $a, b, c, d \in\mathbb{R}$ تعریف می‌کنیم. در این نمایش، نرم صرفاً همان دترمینان است و خاصیت ضربی نرم از خاصیت ضربی دترمینانها نتیجه می‌شود. دترمینان، در حالت ماتریسهای اعداد مختلط اتحاد دو مجذور و در حالت چهارگانها، اتحاد چهار مجذور را به دست می‌دهد.

---

[۱] Hurwitz

چهارگانهای صحیح می‌باید چهارگانهایی با شرط $a, b, c, d \in \mathbb{Z}$ تعریف شوند اما این اعداد فاقد خاصیت تقسیم هستند. برای برقراری این خاصیت، این اعداد را با نقاط نیم‌صحیح[۲] برای تشکیل اعدادی موسوم به اعداد صحیح هرویتز[۳] قوت می‌بخشیم. سپس می‌توانیم الگوریتم اقلیدسی و خاصیت مقسوم‌علیه اول را به وجود آوریم. (ضرب چهارگانها غیر تعویض‌پذیر است که اندکی مشکل ایجاد می‌کند اما توجه می‌کنیم که همواره ضرب و تقسیمها را از یک طرف انجام دهیم و این مشکل را برطرف می‌کنیم.)

در این صورت برهان قضیهٔ چهار مجذور از برهان قضیهٔ دو مجذور به شکلی بسیار تنگاتنگ نتیجه می‌شود.

- با استفاده از مزدوج، نشان داده می‌شود که هر عدد اول معمولی که عدد اول هرویتز نباشد مجموع چهار مجذور است.

- اگر یک عدد اول معمولی مانند p حاصل ضرب $\alpha\beta$ از اعداد صحیح هرویتز را عاد کند آنگاه p باید α یا β را عاد کند.

- هر عدد اول فرد معمولی عددی طبیعی به صورت $۱ + \ell^۲ + m^۲$ را عاد می‌کند (مشابه لم لاگرانژ در بخش ۵.۶ ولی با اثبات آسان‌تر).

- اعداد به صورت $۱ + \ell^۲ + m^۲$ در اعداد صحیح هرویتز تجزیه می‌شوند. از این رو p مجموع چهار مجذور است.

- چون هر عدد طبیعی مانند n حاصل ضربی از اعداد اول فرد و عدد اول ۲ است (که برابر $۱^۲ + ۱^۲ + ۰^۲ + ۰^۱$ می‌باشد)، اتحاد چهار مجذور نشان می‌دهد که n مجموع چهار مجذور است.

---

[۲] half integer points

[۳] Hurwitz integers

۱.۸ ماتریسهای حقیقی و اعداد مختلط

در این فصل اعداد اَبَر مختلط[۴] ۴-بعدی را که چهارگان نامیده می‌شوند معرفی می‌کنیم. یک چهارگان به سادگی به صورت یک ماتریس ۲ × ۲ از اعداد مختلط تعریف می‌شود. اما برای آن که ببینیم چرا توقع داریم که ماتریسها رفتاری شبیه اعداد مختلط داشته باشند در ابتدا نشان می‌دهیم که چگونه می‌توان اعداد مختلط را با ماتریسهای ۲ × ۲ ی حقیقی صورت‌بندی کرد.

برای هر $a + b\mathrm{i} \in \mathbb{C}$ با a و b ی حقیقی، ماتریس

$$M(s + b\mathrm{i}) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

را در نظر بگیرید. به سادگی می‌توان بررسی کرد که (تمرین)

$$\begin{aligned} M(a_۱ + b_۱\mathrm{i}) + M(a_۲ + b_۲\mathrm{i}) &= M(a_۱ + a_۲ + (b_۱ + b_۲)\mathrm{i}) \\ &= M((a_۱ + b_۱\mathrm{i}) + (a_۲ + b_۲\mathrm{i})), \\ M(a_۱ + b_۱\mathrm{i})M(a_۲ + b_۲\mathrm{i}) &= M(a_۱a_۲ - b_۱b_۲ + (a_۱b_۲ + b_۱a_۲)\mathrm{i}) \\ &= M((a_۱ + b_۱\mathrm{i})(a_۲ + b_۲\mathrm{i})). \end{aligned}$$

لذا جمع و ضرب ماتریسی متناظر با جمع و ضرب اعداد مختلط است. بنابراین ماتریسهای

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \qquad a, b \in \mathbb{R}$$

دقیقاً شبیه اعداد مختلط $a + b\mathrm{i}$ رفتار می‌کنند.

روش دیگر برای مشاهدهٔ این مطلب این است که بنویسیم

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a\begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} + b\begin{pmatrix} ۰ & ۱ \\ -۱ & ۰ \end{pmatrix} = a\mathbf{1} + b\mathbf{i}.$$

---

[۴] hypercomplex numbers

ماتریس همانی

$$\mathbf{1} = \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix}$$

شبیه عدد ۱ رفتار می‌کند و

$$\mathbf{i} = \begin{pmatrix} ۰ & ۱ \\ -۱ & ۰ \end{pmatrix}$$

شبیه $\sqrt{-۱}$. در حقیقت

$$\mathbf{i}^۲ = \begin{pmatrix} -۱ & ۰ \\ ۰ & -۱ \end{pmatrix} = -\mathbf{1}.$$

نه تنها در این نمایش ماتریسی برای $\mathbb{C}$ نسخه‌های $\mathbf{1}$ و $\mathbf{i}$ را به طور طبیعی برای ۱ و i داریم بلکه برای نرم نیز تعبیری طبیعی داریم که همان دترمینان ماتریس می‌باشد. زیرا

$$(a+b\mathrm{i})\ \text{نرم} = a^۲ + b^۲ = \det \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

خاصیت ضربی نرم از خاصیت ضربی دترمینان نتیجه می‌شود:

$$\begin{aligned} &\det \begin{pmatrix} a_۱ & b_۱ \\ -b_۱ & a_۱ \end{pmatrix} \det \begin{pmatrix} a_۲ & b_۲ \\ -b_۲ & a_۲ \end{pmatrix} \\ = \ &\det \left(\begin{pmatrix} a_۱ & b_۱ \\ -b_۱ & a_۱ \end{pmatrix} \begin{pmatrix} a_۲ & b_۲ \\ -b_۲ & a_۲ \end{pmatrix} \right) \qquad (*) \end{aligned}$$

و از آنجایی که ضرب ماتریسهای سمت راست برابر

$$\begin{pmatrix} a_۱a_۲ - b_۱b_۲ & a_۱b_۲ + b_۱a_۲ \\ -a_۱b_۲ - b_۱a_۲ & a_۱a_۲ - b_۱b_۲ \end{pmatrix}$$

است، معادلهٔ $(*)$ روشی جدید را برای به دست آوردن اتحاد دو مجذور دیوفانتوس به دست می‌دهد. با جایگذاری $a^۲ + b^۲$ به جای $\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ در هر یک از ماتریسهای $(*)$، داریم

$$(a_۱^۲ + b_۱^۲)(a_۲^۲ + b_۲^۲) = (a_۱a_۲ - b_۱b_۲)^۲ + (a_۱b_۲ + b_۱a_۲)^۲.$$

خاصیتی هندسی از ضرب

اکنون موقعیت خوبی است تا خاصیتی از ضرب را که در حالتهای خاص در فصلهای ٦ و ۷ مشاهده کردیم متذکر شویم: ضرب همهٔ اعضای $\mathbb{C}$ در عدد ناصفر ثابتی مانند $z_0 \in \mathbb{C}$ یک تشابه[5] یا نگاشتی حافظ شکل[6] است؛ یعنی همهٔ فواصل را در عددی ثابت ($|z_0|$) ضرب می‌کند.

این مطلب بدان دلیل است که فاصلهٔ بین دو عدد مختلط z_1 و z_2 برابر $|z_2 - z_1|$ است. وقتی اعداد را در z_0 ضرب کنیم، z_1 و z_2 به $z_0 z_1$ و $z_0 z_2$ برده می‌شوند که فاصلهٔ آنها بنابر خاصیت ضربی نرم برابر

$$|z_0 z_2 - z_0 z_1| = |z_0(z_2 - z_1)| = |z_0||z_2 - z_1|$$

است.

حالتهایی از این مطلب را در فصل ٦ دیدیم. در آنجا ضرب کردن در $\mathbb{Z}[i]$ توسط β یی ناصفر، شبکه‌ای با همان صورت مربعی را به دست می‌داد. همچنین در فصل ۷ دیدیم که ضرب کردن در $\mathbb{Z}[\sqrt{-2}]$ توسط β یی ناصفر، شبکه‌ای با همان شکل مستطیلی را به دست می‌دهد. در بخش ۴.۸ از خاصیت ضربی نرم چهارگانها استفاده می‌کنیم تا به طور مشابه نشان دهیم که هر مضرب ناصفر چهارگانهای صحیح، شبکه‌ای با همان شکل در $\mathbb{R}^4$ است. (کلمهٔ شبکه که در اینجا به کار می‌بریم نسبتاً ضعیف است چرا که چهارگانهای صحیح به سادگیِ شبکه‌ای ۴-بعدی از مکعبها نیست.)

تمرینها

---

[5] similarity

[6] shape preserving map

۱.۱۸ بررسی کنید که

$$\begin{aligned} M(a_1+b_1\mathrm{i})+M(a_2+b_2\mathrm{i}) &= M(a_1+a_2+(b_1+b_2)\mathrm{i}) \\ &= M((a_1+b_1\mathrm{i})+(a_2+b_2\mathrm{i})), \\ M(a_1+b_1\mathrm{i})M(a_2+b_2\mathrm{i}) &= M(a_1a_2-b_1b_2+(a_1b_2+b_1a_2)\mathrm{i}) \\ &= M((a_1+b_1\mathrm{i})(a_2+b_2\mathrm{i})). \end{aligned}$$

گرچه ضرب کردن در z_0 ظاهر هر شکلی در صفحهٔ $\mathbb{C}$ را بدون تغییر نگه می‌دارد، با این حال شکل ممکن است دوران یابد.

۲.۱۸ میزان دوران بر حسب z_0 چه قدر است؟

۲۸ ماتریسهای مختلط و چهارگانها

برای هر جفت $\alpha,\beta\in\mathbb{C}$ ماتریس

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$$

را که چهارگان می‌نامیم در نظر می‌گیریم.

پس از همیلتون[۷] که چهارگانها را در ۱۸۴۳ کشف کرد، مجموعهٔ چهارگانها را با $\mathbb{H}$ نمایش می‌دهیم (با این حال این تعریف ماتریسی را مدیون کیلی[۸] (۱۸۵۸) هستیم).

به سادگی می‌توان بررسی کرد که مجموع و تفاضل چهارگانها نیز چهارگان است. لذا حاصل ضرب نیز چنین است چون

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ -\bar{\beta}_1 & \bar{\alpha}_1 \end{pmatrix}\begin{pmatrix} \alpha_2 & \beta_2 \\ -\bar{\beta}_2 & \bar{\alpha}_2 \end{pmatrix}=\begin{pmatrix} \alpha_3 & \beta_3 \\ -\bar{\beta}_3 & \bar{\alpha}_3 \end{pmatrix},$$

[۷] Hamilton
[۸] Cayley

که در آن

$$\alpha_3 = \alpha_1\alpha_2 - \beta_1\bar{\beta_2}, \qquad \beta_3 = \alpha_1\beta_2 + \beta_1\bar{\alpha_2}.$$

این مطلب را می‌توان توسط ضرب ماتریسی و مزودج مختلط تحقیق کرد.

نرم یک چهارگان مانند q برابر دترمینان آن تعریف می‌شود. از این رو اگر $q = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ آنگاه نرم (q) برابر

$$\det \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = \alpha\bar{\alpha} + \beta\bar{\beta} = |\alpha|^2 + |\beta|^2$$

است. حال خاصیت ضربی دترمینان یک اتحاد دو مجذور مختلط را مشابه اتحاد دو مجذور دیوفانتوس به دست می‌دهد:

$$(|\alpha|^2 + |\beta_1|^2)(|\alpha|^2 + |\beta|^2) = |\alpha_1\alpha_2 - \beta_1\bar{\beta_2}|^2 + |\alpha_1\beta_2 + \beta\bar{\alpha_2}|^2.$$

این اتحاد حدود سال ۱۸۲۰ توسط گاوس کشف شد اما منتشر نشده باقی ماند.

تبصره در مورد شرکت پذیری

به سادگی می‌توان چهارگانهای q_1 و q_2 یی یافت که $q_1q_2 \neq q_2q_1$ (تمرین). در حقیقت چهارگانها شامل چهارگانهای یکه که در بخش بعدی مورد بحث واقع می‌شوند می‌باشند. با این حال حداقل چیزی که می‌دانیم این است که ضرب چهارگانها شرکت پذیر است یعنی

$$q_1(q_2q_3) = (q_1q_2)q_3,$$

چون ضرب ماتریسها شرکت پذیر می‌باشد. این خاصیت را می‌توان به شکلی طاقت‌فرسا با محاسبهٔ ماتریسهای دو طرف تساوی بررسی کرد اما ترجیح

می‌دهیم یادآوری کنیم که هر ماتریس، نمایش‌دهندهٔ یک تابع[۹]، یعنی نگاشتی خطی به صورت

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ y \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

است و ضرب ماتریسی، نمایش‌دهندهٔ ترکیب توابع می‌باشد.

بنا به این دلیل ساده که $f_۱(f_۲f_۳)$ و $(f_۱f_۲)f_۳$ هر دو یک تابع هستند چون هر دو X را به $f_۱(f_۲(f_۳(X)))$ می‌برند، نتیجه می‌گیریم که ترکیب توابع همواره شرکت پذیر است.

تمرینها

۱.۲۸ تحقیق کنید که حاصل ضرب دو چهارگان، همان ماتریسی است که ادعا شد.

۲.۲۸ چهارگانهای $q_۱$ و $q_۲$ یی را بیابید که $q_۱q_۲ \neq q_۲q_۱$.

همچنین نمایش ماتریسی چهارگانها نشان می‌دهد که هر چهارگان غیر صفر دارای معکوس ضربی (یعنی معکوس ماتریسی آن) است.

۳.۲۸ معکوس یک چهارگان غیر صفر مانند $q = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ را محاسبه کنید و تحقیق کنید که $q^{-۱}$ نیز یک چهارگان است.

اتحاد دو مجذور مختلط روشی برای به دست آوردن اتحاد چهار مجذور است که در بخش بعد آمده است.

۴.۲۸ با استفاده از

$$\alpha_۱ = a_۱ + d_۱\mathrm{i}, \quad \beta_۱ = b_۱ + c_۱\mathrm{i}, \quad \alpha_۲ = a_۲ + d_۲\mathrm{i}, \quad \beta_۲ = b_۲ + c_۲\mathrm{i},$$

---
[۹] function

عبارت $(a_1^2+b_1^2+c_1^2+d_1^2)(a_2^2+b_2^2+c_2^2+d_2^2)$ را به صورت مجموع چهار مجذور بنویسید.

۳۸ چهارگانهای یکه

اگر بنویسیم $\alpha = a + d\mathrm{i}$ و $\beta = b + c\mathrm{i}$ که در آن $a, b, c, d \in \mathbb{R}$ آنگاه هر چهارگان را می‌توان به عنوان ترکیبی خطی از چهار ماتریس خاص $\mathbf{1}$، $\mathbf{i}$، $\mathbf{j}$ و $\mathbf{k}$ که چهارگان یکه نامیده می‌شوند تلقی کرد.

$$\begin{aligned}
\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} &= \begin{pmatrix} a+d\mathrm{i} & b+c\mathrm{i} \\ -b+c\mathrm{i} & a-d\mathrm{i} \end{pmatrix} \\
&= a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\
&\quad + c\begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} + d\begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix} \\
&= a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}.
\end{aligned}$$

ماتریسهای $\mathbf{1}$، $\mathbf{i}$، $\mathbf{j}$ و $\mathbf{k}$ چهارگانهای با نرم ۱ هستند و در روابط زیر که به سادگی تحقیق می‌شوند صدق می‌کنند:

$$\begin{aligned}
\mathbf{i}^2 &= \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}, \\
\mathbf{ij} &= \mathbf{k} = -\mathbf{ji}, \\
\mathbf{jk} &= \mathbf{i} = -\mathbf{kj}, \\
\mathbf{ki} &= \mathbf{j} = -\mathbf{ik}.
\end{aligned}$$

لذا حاصل ضرب چهارگانها در حالت کلی غیر تعویض پذیر است:

$$q_۱ q_۲ \neq q_۲ q_۱.$$

گذشته از این مطلب، چهارگانها همان خواص مقدماتی اعداد را دارند. آنها گروهی آبلی تحت جمع را تشکیل می‌دهند. چهارگانهای غیر صفر نیز تحت ضرب یک گروه تشکیل می‌دهند و به علاوه داریم

$$\begin{aligned} q_۱(q_۲+q_۳) &= q_۱ q_۲ + q_۱ + q_۳, \\ (q_۲+q_۳)q_۱ &= q_۲ q_۱ + q_۳ q_۱ \end{aligned}$$

(قانون توزیع پذیری از چپ و راست).

اتحاد چهار مجذور

اگر $q = a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ آنگاه نرم (q) برابر

$$\det \begin{pmatrix} a+di & b+ci \\ -b+ci & a-di \end{pmatrix} = a^۲ + b^۲ + c^۲ + d^۲$$

است. از آنجایی که $\det(q_۱)\det(q_۲) = \det(q_۱ q_۲)$، اتحاد دو مجذور مختلط را می‌توانیم به صورت اتحاد چهار مجذور حقیقی نیز بنویسیم که به شکل

$$\begin{aligned} & (a_۱^۲ + b_۱^۲ + c_۱^۲ + d_۱^۲)(a_۲^۲ + b_۲^۲ + c_۲^۲ + d_۲^۲) \\ = \; & (a_۱ a_۲ - b_۱ b_۲ - c_۱ c_۲ - d_۱ d_۲)^۲ \\ & +(a_۱ b_۲ + b_۱ a_۲ + c_۱ d_۲ - d_۱ c_۲)^۲ \\ & +(a_۱ c_۲ - b_۱ d_۲ + c_۱ a_۲ + d_۱ b_۲)^۲ \\ & +(a_۱ d_۲ + b_۱ c_۲ - c_۱ b_۲ + d_۱ a_۲)^۲ \end{aligned}$$

در می‌آید.

قابل توجه است که اتحاد چهار مجذور توسط اویلر در سال ۱۷۴۸ (نزدیک به ۱۰۰ سال قبل از کشف چهارگانها) کشف شد. اویلر امیدوار بود که با استفاده از آن و با اثبات این مطلب که هر عدد اول مجموع چهار مجذور است بتواند نشان دهد که هر عدد طبیعی مجموع چهار مجذور می‌باشد. این مطلب اولین بار توسط لاگرانژ در سال ۱۷۷۰ اثبات شد. اکنون به کمک چهارگانها می‌توانیم برهان ساده‌تری ارائه دهیم. این کار را در چند بخش بعد انجام خواهیم داد.

تمرینها

همان گونه که در بخش قبل متذکر شدیم، همیلتون چهارگانها را به صورت ماتریسهای ۲ × ۲ ی خاص معرفی نکرد. وی آنها را مستقیماً به عنوان اشیائی مجرد به شکل $a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ با ضربی تحت قواعد

$$\mathbf{i}^۲=\mathbf{j}^۲=\mathbf{k}^۲=-\mathbf{1}$$

تعریف کرد.

۱.۳۸ از این روابط نتیجه بگیرید که $\mathbf{ij}=\mathbf{k}$. کجا در محاسبات خود شرکت پذیری را فرض می‌گیرید؟

به طور مشابه می‌توان حاصل ضرب هر دو یکه و سپس حاصل ضرب هر دو چهارگان دلخواه را یافت.

۲.۳۸ نقش قانون توزیع پذیری را در محاسبهٔ حاصل ضربها شرح دهید.

این هشت عنصر، یعنی یکه‌ها و قرینهٔ آنها، گروه متناهی جالبی را تشکیل می‌دهند.

۳.۳۸ نشان دهید $Q = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ تحت ضرب و معکوس بسته است و از این رو گروهی (غیر آبلی) را تحت ضرب چهارگانها تشکیل می‌دهد.

۴.۳۸ نشان دهید که حاصل ضرب هر دو تا از $\mathbf{i}$، $\mathbf{j}$، $\mathbf{k}$ و قرینهٔ آنها همهٔ Q را می‌سازد.

۵.۳۸ از تمرین ۴.۳.۸ نتیجه بگیرید که هر زیرگروه سَره[۱۰] از Q (یعنی هر زیرگروهی غیر از خود Q) آبلی است.

در حقیقت Q کوچک‌ترین گروه غیر آبلی است که زیرگروههای سرهٔ آن همگی آبلی هستند.

۴.۸ ترکیبهای خطی با ضرایب صحیح

از حالا به بعد چهارگان $\mathbf{1}$ را به صورت سادهٔ ۱ می‌نویسیم و از آن به عنوان جمله‌ای در یک حاصل ضرب صرف نظر می‌کنیم. لذا نمونه‌ای از یک چهارگان به صورت

$$q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}, \qquad a, b, c, d \in \mathbb{R}$$

نوشته خواهد شد. کدام یک از این اشیاء باید صحیح تلقی شوند؟

اولین تلقی این است که

$$\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}] = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{Z}\}$$

در مشابهت با اعداد صحیح گاوسی، یعنی $\mathbb{Z}[i]$، باید چهارگانهای صحیح باشد. مجموع، تفاضل و حاصل ضرب اعضای $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ نیز اعضایی از $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ هستند و

---
[۱۰] proper

$$\text{نرم}\ (a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}) = a^{۲}+b^{۲}+c^{۲}+d^{۲}$$

یک عدد صحیح معمولی است که می‌توانیم آن را برای تعریف عدد اول در $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ به کار ببریم.

مثال. $۲+\mathbf{i}+\mathbf{j}+\mathbf{k}$ عددی اول در $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ است.

این مطلب از آن رو درست است که

$$\text{نرم}\ (۲+\mathbf{i}+\mathbf{j}+\mathbf{k}) = ۲^{۲}+۱^{۲}+۱^{۲}+۱^{۲}=۷$$

عددی اول در $\mathbb{Z}$ است. از این رو $۲+\mathbf{i}+\mathbf{j}+\mathbf{k}$ حاصل ضرب اعضایی از $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ با نرم کمتر نیست.

با این حال هنگامی که سعی داریم تقسیم با باقیمانده را انجام دهیم دچار مشکل می‌شویم: مجموعهٔ مضارب صحیح چهارگانی ثابت، شکل غلطی دارد. گرچه تصوری شهودی از ضرب کردن (همانند $\mathbb{Z}[\mathrm{i}]$) نداریم (چون چهارگانهای

$$\mathbb{H}[\mathbf{i},\mathbf{j},\mathbf{k}] = \{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} : a,b,c,d\in\mathbb{R}\}$$

در فضای ۴-بعدی $\mathbb{R}^{۴}$ هستند)، علی رغم این می‌توانیم در مورد فاصله و زاویه در $\mathbb{R}^{۴}$ صحبت کنیم و دلایلی هندسی برای اثبات احکام بیاوریم.

مضارب یک عدد

۱، $\mathbf{i}$، $\mathbf{j}$ و $\mathbf{k}$ را به عنوان نقاط یکهٔ محورهای متعامد چهارگانهٔ $\mathbb{R}^{۴}$ تعبیر می‌کنیم. در این صورت نرم چهارگان یعنی $a^{۲}+b^{۲}+c^{۲}+d^{۲}$ صرفاً مجذور فاصلهٔ نقطهٔ $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ تا ۰ یعنی $|a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}|^{۲}$ است.

در حالت کلی، نرم $(q_۱-q_۲)$ مجذور فاصلهٔ بین چهارگانهای $q_۱$ و $q_۲$ یعنی $|q_۱-q_۲|^{۲}$ است.

حال چون نرم ضربی است داریم

$$|qq_1 - qq_2| = |q(q_1 - q_2)| = |q||q_1 - q_2|.$$

لذا ضرب کردن همهٔ $\mathbb{H} = \mathbb{R}^4$ در یک چهارگان مانند q، همهٔ فواصل را در عدد ثابت $|q|$ ضرب می‌کند. (چون $q \cdot 0 = 0$، ضرب کردن در q مبدأ را ثابت نگه می‌دارد. لذا وقتی $|q| = 1$ می‌توان این عمل را به عنوان دوران[11] $\mathbb{R}^4$ حول مبدأ تلقی کرد.)

نتیجه می‌شود که اگر $q \neq 0$ آنگاه ضرب کردن در q زاویه را بدون تغییر نگه می‌دارد. بالاخص، هر کدام از مضارب β، $\beta\mathbf{i}$، $\beta\mathbf{j}$ و $\beta\mathbf{k}$ از ۱، $\mathbf{i}$، $\mathbf{j}$ و $\mathbf{k}$ در چهارگانی مانند $\beta \neq 0$، فاصله‌ای برابر $|\beta|$ تا 0 دارند و در جهتهایی متعامد مانند ۱، $\mathbf{i}$، $\mathbf{j}$ و $\mathbf{k}$ هستند.

هر مضرب β از عضوی از $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ صرفاً مجموعی از عناصر $\pm\beta$، $\pm\beta\mathbf{i}$، $\pm\beta\mathbf{j}$ و $\pm\beta\mathbf{k}$ است. از این رو مضارب β در گوشه‌های یک شبکه شبیه نقاط خود $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ قرار دارند؛ شبکه‌ای که آن را ۴-مکعبها[12] می‌نامیم. تنها تفاوت در این است که شبکهٔ مضارب β توسط $|\beta|$ بزرگ می‌شوند و ممکن است دوران یابند.

تمرینها

دوران $\mathbb{R}^4$ که توسط ضرب کردن هر نقطه در چهارگانی مانند $q \neq 1$ با شرط $|q| = 1$ به دست آمد شبیه دورانهای $\mathbb{R}^3$ نیست، به این دلیل که هیچ محوری از نقاط ثابت نداریم.

۱.۴۸ نشان دهید که ضرب کردن در یک چهارگان مانند $q \neq 1$ تنها مبدأ را ثابت نگه می‌دارد.

---

[11] rotation
[12] 4-cubes

شناسایی چهارگانهای اول توسط نرم آنها (که برابر مجموع مجذورات است) این امکان را به ما می‌دهد تا از پیش اثبات کنیم که بی‌نهایت از آنها وجود دارد.

۲.۴.۸ بدون فرض آن که هر عدد طبیعی مجموعی از چهار مجذور است، نشان دهید که بی‌نهایت چهارگان اول وجود دارد.

۵.۸ اعداد صحیح هرویتز

تقسیم با باقیمانده

درست همانند $\mathbb{Z}[\mathrm{i}]$، در $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ نیز به شبکهٔ مضارب β برای یافتن باقیماندهٔ تقسیم α بر β توجه می‌کنیم. این باقیمانده برابر $\alpha - \mu\beta$ است که در آن $\mu\beta$ نزدیک‌ترین گوشهٔ شبکه است.

متأسفانه همواره $|\alpha - \mu\beta| < |\beta|$ را نداریم. یک موقعیت استثنایی وجود دارد: اگر α در گوشهٔ یک ۴-مکعب باشد آنگاه $|\alpha - \mu\beta| = |\beta|$. این مطلب بدان دلیل روی می‌دهد که فاصلهٔ یک گوشه تا گوشه‌ای دیگر از یک ۴-مکعب برابر طول ضلع آن است. مثلاً گوشهٔ

$$\frac{۱}{۲} + \frac{\mathbf{i}}{۲} + \frac{\mathbf{j}}{۲} + \frac{\mathbf{k}}{۲}$$

از ۴-مکعب یکه با یالهای روی محورها، دارای فاصله‌ای برابر

$$\sqrt{(\frac{۱}{۲})^۲ + (\frac{۱}{۲})^۲ + (\frac{۱}{۲})^۲ + (\frac{۱}{۲})^۲} = \sqrt{۱} = ۱$$

از مبدأ می‌باشد.

لذا خاصیت تقسیم برای $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ با شکست مواجه می‌شود. از این جنبه $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ بیشتر شبیه $\mathbb{Z}[\sqrt{-۳}]$ است تا $\mathbb{Z}[\mathrm{i}]$. در حقیقت این مشکل را دقیقاً همان

طور که برای $\mathbb{Z}[\sqrt{-۳}]$ برطرف کردیم با افزودن نقاطی استثنایی به عنوان اعداد صحیح اضافی حل می‌کنیم.

چون هر نقطهٔ میانی با افزودن $\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲}$ به عضوی از $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ به دست می‌آید، مجموعهٔ چهارگانهایی به صورت

$$\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲}+a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \qquad a,b,c,d\in\mathbb{Z}$$

را همراه با آنهایی که در $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ هستند، یعنی

$$a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \qquad a,b,c,d\in\mathbb{Z}$$

احتیاج داریم. فرمول واحدی که شامل هر دوی این مجموعه نقاط باشد عبارت است از

$$A\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲}+B\mathbf{i}+C\mathbf{j}+D\mathbf{k} \qquad A,B,C,D\in\mathbb{Z}.$$

نقاط میانی توسط A های فرد و نقاط $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ توسط A های زوج به دست می‌آیند. لذا چهارگانهایی که برای اطمینان از برقراری خاصیت تقسیم ساخته‌ایم مجموعهٔ $\mathbb{Z}[\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲},\mathbf{i},\mathbf{j},\mathbf{k}]$ متشکل از همهٔ ترکیبهای صحیح

$$\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲},\mathbf{i},\mathbf{j},\mathbf{k}$$

می‌باشند.

پس از هرویتز که چنین مجموعه‌ای را در سال ۱۸۹۶ معرفی کرد، چهارگانهای عضو $\mathbb{Z}[\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲},\mathbf{i},\mathbf{j},\mathbf{k}]$ اعداد صحیح هرویتز[۱۳] نامیده می‌شوند. می‌خواهیم ایده‌ای را که وی استفاده کرده بود تعقیب کنیم تا نشان دهیم که هر عدد طبیعی مجموع چهار مجذور است. (این شیوه را می‌توان در هاردی و رایت (۱۹۷۹) و ساموئل[۱۴] (۱۹۷۰) نیز یافت.)

اما در ابتدا ببینیم که چرا باید این اعداد را صحیح تلقی کنیم.

---

[۱۳] Hurwitz integers

[۱۴] Samuel

۱. بدیهی است که مجموع و تفاضل اعداد صحیح هرویتز، خود اعداد صحیح هرویتز هستند.

۲. می‌توان (اندکی سخت‌تر) بررسی کرد که حاصل ضرب اعداد صحیح هرویتز نیز عدد صحیح هرویتز است.

۳. همچنین می‌توان بررسی کرد که نرم یک عدد صحیح هرویتز، یک عدد صحیح معمولی است.

مثال. $۳+\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲}=\frac{۷+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲}$.

این عدد صحیح هرویتز دارای نرم

$$\frac{۷^۲+۱^۲+۱^۱+۱^۲}{۴}=\frac{۵۲}{۴}=۱۳$$

است. چون ۱۳ یک عدد اول معمولی است، $\frac{۷+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲}$ حاصل ضربی از اعداد صحیح هرویتز با نرم کمتر نیست و از این رو یک عدد اول هرویتز می‌باشد.

تمرینها

۱.۵۸ هر یک از $\mathbf{1}$، $\mathbf{i}$، $\mathbf{j}$ و $\mathbf{k}$ را به صورت

$$A\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲}+B\mathbf{i}+C\mathbf{j}+D\mathbf{k} \qquad A,B,C,D\in\mathbb{Z}$$

بنویسید و با توجه به آن نتیجه بگیرید که $\mathbb{Z}[\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲},\mathbf{i},\mathbf{j},\mathbf{k}]$ شامل $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ است. همچنین نشان دهید که نرم هر عدد صحیح هرویتز یک عدد صحیح معمولی می‌باشد.

یکه‌های $\mathbb{Z}[\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲},\mathbf{i},\mathbf{j},\mathbf{k}]$ عبارتند از هشت یکهٔ ± ۱، $\pm\mathbf{i}$، $\pm\mathbf{j}$ و $\pm\mathbf{k}$ از $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ همراه با ۱۶ نقطهٔ میانی $\pm\frac{۱}{۲}\pm\frac{\mathbf{i}}{۲}\pm\frac{\mathbf{j}}{۲}\pm\frac{\mathbf{k}}{۲}$ که به مبدأ نزدیک‌ترند. شبیه

یکه‌های $\mathbb{Z}[i]$ یا $\mathbb{Z}[\zeta_3]$ این یکه‌ها نیز یک گروه تشکیل می‌دهند چون مجموعهٔ آنها تحت ضرب و معکوس بسته است. با این حال گروه یکه‌های اعداد صحیح هرویتز جالب‌تر است چون هم بزرگ‌تر است و هم غیر آبلی می‌باشد.

۲.۵۸ نشان دهید که ۲۴ یکهٔ فهرست شده در بالا، شامل حاصل ضرب هر دو تا از آنهاست.

۳.۵۸ از محاسبات حاصل ضربی در تمرین ۲.۵.۸ نتیجه بگیرید که این ۲۴ یکه شامل معکوس هر یک از آنها می‌باشد.

۶.۸ مزدوجها

برای هر چهارگان مانند $q = a + \mathbf{i} + c\mathbf{j} + d\mathbf{k}$ عدد

$$\bar{q} = a - \mathbf{i} - c\mathbf{j} - d\mathbf{k}$$

را مزدوج q می‌نامیم. این مزدوج تقریباً خواص مقدماتی مزدوج مختلط را دارد:

$$\begin{aligned} q\bar{q} &= |q|^2, \\ \overline{q_1 + q_2} &= \bar{q_1} + \bar{q_2}, \\ \overline{q_1 - q_2} &= \bar{q_1} - \bar{q_2}, \\ \overline{q_1 q_2} &= \bar{q_2}\bar{q_1}. \end{aligned}$$

(تعویض جای q_1 و q_2 در آخرین عبارت، به دلیل غیر تعویض پذیر بودن ضرب چهارگانها می‌باشد.)

همانند $\mathbb{C}$ خواص مزدوجگیری در $\mathbb{H}$ را می‌توان با کار کردن روی هر دو طرف تساویها بررسی کرد. از این خواص (کاملاً به همان شکلی که در بخش

۳.٦ انجام دادیم) برای اثبات قضیهٔ چهار مجذور مشروط استفاده می‌کنیم: اگر p یک عدد اول معمولی باشد که عدد اول هرویتز نیست، آنگاه

$$p = a^{۲} + b^{۲} + c^{۲} + d^{۲}, \qquad ۲a, ۲b, ۲c, ۲d \in \mathbb{Z}.$$

فرض کنیم p تجزیه‌ای نابدیهی به اعداد صحیح هرویتز مانند

$$p = (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\gamma$$

داشته باشد. در این صورت با مزدوجگیری از هر دو طرف داریم

$$p = \bar{\gamma}(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})$$

چون $\bar{p} = p$. با ضرب کردن این دو عبارت داریم

$$\begin{aligned} p^{۲} &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\gamma\bar{\gamma}(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) \\ &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})\gamma\bar{\gamma} \quad \text{چون } \gamma\bar{\gamma} \text{ حقیقی است} \\ &= (a^{۲} + b^{۲} + c^{۲} + d^{۲})|\gamma|^{۲}, \end{aligned}$$

که در آن هم $a^{۲} + b^{۲} + c^{۲} + d^{۲}$ و هم $|\gamma|^{۲}$ بزرگ‌تر از ۱ هستند.

اما تنها تجزیهٔ $p^{۲}$ به اعداد صحیح مثبت pp است[15]. از این رو $p = a^{۲} + b^{۲} + c^{۲} + d^{۲}$.

سرانجام چون a، b، c و d ضرایب یک عدد صحیح هرویتز هستند می‌توانند اعدادی نیم‌صحیح باشند. اما در هر صورت داریم $۲a, ۲b, ۲c, ۲d \in \mathbb{Z}$. □

[15] باید گفت تنها تجزیه به اعداد صحیح مثبت نابدیهی این گونه است. بدیهی است که $p^{۲} = p^{۲} \times ۱$ نیز تجزیه‌ای به اعداد صحیح مثبت است. (م)

تغییر عوامل p

اکنون با یافتن تجزیه‌ای جدید برای p نشان می‌دهیم هر عدد اول معمولی که یک عدد اول هرویتز نباشد مجموع چهار مجذور است.

یک عدد صحیح هرویتز مانند α با مختصات نیم‌صحیح را همواره می‌توان به صورت

$$\alpha = \omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$$

نوشت که در آن a'، b'، c' و d' اعداد صحیح زوجی هستند و با انتخاب مناسبی از علامتها در عدد صحیح هرویتز

$$\omega = \frac{\pm ۱ \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}}{۲}.$$

نرم ω برابر ۱ است و در نتیجه $\omega\bar{\omega} = ۱$

حال همانند زیربخش قبل، برای یک عدد اول معمولی مانند p داریم $p = a^۲ + b^۲ + c^۲ + d^۲$ که a، b، c و d نیم‌صحیح هستند. در ابتدا می‌نویسیم

$$\begin{aligned} p &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) \\ &= (\omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) \times (\bar{\omega} + a' - b'\mathbf{i} - c'\mathbf{j} - d'\mathbf{k}) \end{aligned}$$

که در آن a'، b'، c' و d' زوج هستند و ω همانند فوق است؛ لذا $\omega\bar{\omega} = ۱$. سپس بین عواملی که هم‌اکنون یافتیم $\omega\bar{\omega} = ۱$ را درج می‌کنیم و بدین طریق عوامل مزدوج جدیدی برای p می‌یابیم،

$$p = (\omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k})\bar{\omega} \times \omega(\bar{\omega} + a' - b'\mathbf{i} - c'\mathbf{j} - d'\mathbf{k}).$$

در عامل اول، وقتی $\bar{\omega}$ را در ω به علاوهٔ جملات با ضرایب صحیح زوج ضرب کنیم عبارتی برابر ۱ به علاوهٔ جملاتی با ضرایب صحیح به دست

می‌آید. از این رو حاصل این ضرب کردن به صورت $A+B\mathbf{i}+C\mathbf{j}+D\mathbf{k}$ برای A، B، C و D یی صحیح می‌باشد. اما عامل دوم مزدوج آن است و لذا $p=A^۲+B^۲+C^۲+D^۲$ که $A,B,C,D\in\mathbb{Z}$. □

تمرینها

برهان فوق نشان می‌دهد که هر مجموعی از مجذورات صحیح، تجزیه‌ای غیر بدیهی به چهارگانهای صحیح دارد.

۱.۶.۸ برای اعداد اول گاوسی ۳، ۷ و ۱۱، تجزیه‌ای به چهارگانهای صحیح بیابید.

۲.۶.۸ چرا اعداد فوق‌الذکر اول گاوسی هستند؟

خواص مزدوجها را که در بالا برشمرده شد می‌توان با استفاده از ماتریسها یا قواعد ضرب برای $\mathbf{i}$، $\mathbf{j}$ و $\mathbf{k}$ اثبات کرد.

۳.۶.۸ اگر $q=\begin{pmatrix}\alpha & \beta\\ -\bar\beta & \bar\alpha\end{pmatrix}$ آنگاه $\bar q$ چیست؟

۴.۶.۸ از ماتریسی که هم‌اکنون برای $\bar q$ یافتید استفاده کنید و $\bar q_۲\bar q_۱$ را محاسبه کنید. نتیجه بگیرید که $\bar q_۲\bar q_۱=\overline{q_۱q_۲}$.

۷.۸ یک خاصیت مقسوم‌علیه اول

در بخش ۵.۸ نشان داده شد که $\mathbb{Z}[\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲},\mathbf{i},\mathbf{j},\mathbf{k}]$ خاصیت تقسیم دارد. این ما را قادر می‌سازد که بزرگ‌ترین مقسوم‌علیه مشترک دو عدد هرویتز دلخواه را توسط الگوریتم اقلیدسی بیابیم.

با این حال چون ضرب چهارگانها در حالت کلی غیر تعویض پذیر است باید بین مقسوم‌علیه چپ و راست تمایز قائل شویم و به یک نوع بپردازیم. δ را یک مقسوم‌علیه راستِ[۱۶] α می‌نامیم هرگاه برای γ یی داشته باشیم $\alpha = \gamma\delta$.

بنابراین اگر α و β مقسوم‌علیه راست مشترکی مانند δ داشته باشند آنگاه برای γ و ε ی داریم $\alpha = \gamma\delta$ و $\beta = \varepsilon\delta$. لذا

$$\rho = \alpha - \mu\beta = \gamma\delta - \mu\varepsilon\delta = (\gamma - \mu\varepsilon)\delta.$$

این مطلب نشان می‌دهد که δ نیز مقسوم‌علیه راستی از باقیماندهٔ ρ در تقسیم (راست) α بر β است.

لذا اگر در الگوریتم اقلیدسی همواره از راست تقسیم کنیم، بزرگ‌ترین مقسوم‌علیه مشترک راست α و β را می‌یابیم که آن را با $\mathrm{rgcd}(\alpha, \beta)$ نمایش می‌دهیم.

در این صورت با الهام از جملات تولید شده توسط الگوریتم اقلیدسی نتیجه می‌شود اعداد صحیح هرویتزی مانند μ و ν موجودند که

$$\mathrm{rgcd}(\alpha, \beta) = \mu\alpha + \nu\beta.$$

این مطلب به ما اجازه می‌دهد که خاصیت مقسوم‌علیه اول زیر را (که کاملاً مشابه نظیر آن برای $\mathbb{Z}$ و $\mathbb{Z}[\mathrm{i}]$ نیست اما برای اهداف ما به اندازهٔ کافی قوی است) اثبات کنیم: اگر p یک عدد اول حقیقی باشد و اگر p حاصل ضربی از اعداد صحیح هرویتز مانند $\alpha\beta$ را عاد کند آنگاه p باید α یا β را عاد کند.

(حقیقی بودن p به آن کمک می‌کند زیرا اعداد حقیقی با همهٔ چهارگانها جابجا می‌شوند. از این رو p هم مقسوم‌علیه راست و هم مقسوم‌علیه چپ هر عددی است که p آن را عاد می‌کند.)

همانند معمول، برهان با فرض آن که p عدد α را عاد نکند شروع می‌شود. در این صورت اعداد صحیح هرویتزی مانند μ و ν موجودند که

[۱۶] right divisor

$$۱ = \mathrm{rgcd}(p, \alpha) = \mu p + \nu\alpha.$$

با ضرب کردن طرفین در β از سمت راست، داریم

$$\beta = \mu p\beta + \nu\alpha\beta.$$

چون p عدد $\mu p\beta$ را (به طور بدیهی) و عدد $\nu\alpha\beta$ را (بنابر فرض) عاد می‌کند نتیجه می‌گیریم که p سمت راست تساوی را عاد می‌کند. از این رو همان طور که می‌خواستیم p عدد β را عاد می‌کند. □

۸.۸ برهان قضیه چهار مجذور

در بخش ۳.۸ دیدیم که کلید قضیهٔ چهار مجذور لاگرانژ اثبات این امر است که هر عدد اول مجموع چهار مجذور صحیح است، چون اتحاد چهار مجذور مواظب است تا همهٔ حاصل ضربهای اعداد اول (یعنی همهٔ عددهای طبیعی غیر از $۱^۲ + ۰^۲ + ۰^۲ + ۰^۲ = ۱$) نیز چنین خاصیتی را داشته باشند.

عدد اول زوج ۲ به صورت $۱^۲ + ۱^۲ + ۰^۲ + ۰^۲ = ۱$ است. لذا باقی می‌ماند اثبات کنیم که هر عدد اول فرد مانند p مجموع چهار مجذور صحیح است. این مطلب را به کمک حکم زیر اثبات می‌کنیم:

اگر $p = ۲n + ۱$ آنگاه $\ell, m \in\mathbb{Z}$ ی موجودند که p عدد $۱ + \ell^۲ + m^۲$ را عاد می‌کند.

این مطلب مشابه لم لاگرانژ در بخش ۵.٦ اما ساده‌تر از آن است. برهان آن را در اینجا می‌آوریم.

اگر در بین اعداد $\ell = ۰, ۱, ۲, \ldots, n$ دو عدد دلخواه مانند x و y را در نظر بگیریم آنگاه مجذورهای $x^۲$ و $y^۲$ به پیمانهٔ p ناهمنهشت هستند، زیرا

$$x^۲ \equiv_p y^۲ \Longrightarrow x^۲ - y^۲ \equiv_p ۰$$

$$\Longrightarrow \quad (x-y)(x+y) \equiv_p \circ$$

$$\Longrightarrow \quad x \equiv_p \circ \quad \text{یا} \quad x+y \equiv_p \circ.$$

و $x+y \not\equiv_p \circ$ چون $\circ < x+y < p$. لذا اعداد $\ell = \circ, ۱, ۲, \ldots, n$ تعداد $n+۱$ عدد ناهمنهشت به پیمانهٔ p مانند $\ell^۲$ را به دست می‌دهند.

به طور مشابه با در نظر گرفتن اعداد $m = \circ, ۱, ۲, \ldots, n$ می‌بینیم که $n+۱$ عدد ناهمنهشت مانند $m^۲$، یا به طور معادل، $n+۱$ عدد ناهمنهشت مانند $-m^۲$، یا به طور معادل، $n+۱$ عدد ناهمنهشت مانند $-۱-m^۲$ به پیمانهٔ p داریم.

اما تنها $۲n+۱$ مقدار ناهمنهشت به پیمانهٔ $p = ۲n+۱$ وجود دارد. بنابراین ℓ و m ی موجودند که

$$\ell^۲ \equiv_p -۱ - m^۲.$$

یعنی p عدد $۱+\ell^۲+m^۲$ را عاد می‌کند[۱۷]. □

قضیهٔ چهار مجذور. هر عدد طبیعی مجموع چهار مجذور است.

برهان. بنابر تبصرهٔ فوق باقی می‌ماند که قضیه را برای هر عدد اول فرد مانند p اثبات کنیم؛ عددی که هم‌اکنون دیدیم مقسوم‌علیهی از مقداری به صورت $۱+\ell^۲+m^۲$ است.

برای تکمیل برهان، $۱+\ell^۲+m^۲$ را به اعداد صحیح هرویتز به صورت

$$(۱-\ell\mathbf{i}-m\mathbf{j})(۱+\ell\mathbf{i}+m\mathbf{j})$$

تجزیه می‌کنیم و خاصیت مقسوم‌علیه اول را از بخش قبل به کار می‌بریم. اگر p یک عدد اول هرویتز باشد آنگاه p باید $(۱-\ell\mathbf{i}-m\mathbf{j})$ یا $(۱+\ell\mathbf{i}+m\mathbf{j})$ را عاد

---

[۱۷] در اینجا در حقیقت از اصل لانه‌کبوتری استفاده شده است. چون $n+۱$ مقدار دو به دو ناهمنهشت مانند $\ell^۲$ و نیز $n+۱$ مقدار دو به دو ناهمنهشت مانند $-۱-m^۲$ داریم پس $۲n+۲$ عدد داریم. اما تعداد مقادیر دو به دو ناهمنهشت به پیمانهٔ p برابر $۲n+۱$ است و لذا $۲n+۱$ لانه داریم که $۲n+۲$ کبوتر $\ell^۲$ و $-۱-m^۲$ می‌خواهند در آنها قرار بگیرند. در نتیجه دو تا از این کبوترها باید در یک لانه باشند. اما می‌دانیم که $\ell^۲$ ها با هم در یک لانه قرار نمی‌گیرند و $-۱-m^۲$ ها نیز به همین ترتیب. پس باید $\ell^۲$ یی با $-۱-m^۲$ یی در یک لانه باشند. (م)

کند. اما هیچ یک از این دو حالت درست نیست چون هیچ یک از دو عدد

$$\frac{۱}{p} - \frac{\ell \mathbf{i}}{p} - \frac{m\mathbf{j}}{p}, \qquad \frac{۱}{p} + \frac{\ell \mathbf{i}}{p} + \frac{m\mathbf{j}}{p}$$

یک عدد صحیح هرویتز نیست. از این رو عدد اول دلخواه ما، یعنی p، یک عدد اول هرویتز نیست. بنابراین با توجه به مطالب بخش ۶.۸ داریم

$$p = A^{۲} + B^{۲} + C^{۲} + D^{۲}, \qquad A, B, C, D \in \mathbb{Z}. \ \square$$

تمرینها

از قضیهٔ چهار مجذور نتیجه می‌شود که هر عدد طبیعی تجزیه‌ای به اعداد صحیح هرویتز دارد.

۱.۸.۸ توضیح دهید که چرا. (آیا اگر برخی از مجذورات صفر باشند اهمیتی دارد؟)

لذا نباید چندان شگفت‌انگیز باشد که برخی اعداد اول گاوسی حقیقی، اعداد اول هرویتز نیستند (هیچ یک از آنها چنین نیست). با این حال هنوز می‌توانیم در مورد اعداد اول گاوسی مختلط محض مانند $a + b\mathrm{i}$ (با شرط $a, b \neq ۰$) پرسشی مطرح کنیم.

۲.۸.۸ توضیح دهید که چرا چهارگانهای به صورت $a + b\mathbf{i}$ (برای $a, b \in \mathbb{R}$) را می‌توان با اعداد مختلط $a + bi = a + b\sqrt{-۱}$ یکی دانست.

۳.۸.۸ نشان دهید که یک عدد اول گاوسی سره مانند $a + b\mathbf{i}$، یک عدد اول هرویتز نیز می‌باشد.

تا اینجا چیزی در مورد مجموع سه مجذور نگفتیم چون داستان آن چندان کامل و زیبا نیست. برای شروع، هیچ نوع اتحاد سه مجذوری وجود ندارد چون مجموعی از سه مجذور در مجموعی از سه مجذور، لزوماً مجموعی از سه مجذور نیست.

۴.۸.۸ اعداد طبیعی کوچک‌تر از ۲۰ را که مجموع سه مجذور نیستند بیابید و از این طریق آنهایی را که به دو صورت به شکل مجموع سه مجذور هستند پیدا کنید.

۵.۸.۸ روی مقادیر ممکن $x^۲$ به پیمانهٔ ۸ کار کنید و نشان دهید که هیچ عدد طبیعی به صورت $۸n+۷$ مجموع سه مجذور نیست.

با اندکی کار بیشتر می‌توانیم این حکم کلی‌تر را اثبات کنیم که هیچ عدد طبیعی به صورت $۴^m(۸n+۷)$ مجموع سه مجذور نیست.

۶.۸.۸ با در نظر گرفتن مقادیر مجذورات به پیمانهٔ ۴ نشان دهید که

$$x^۲+y^۲+z^۲\equiv_۴ ۰$$

تنها هنگامی امکان پذیر است که x، y و z همگی زوج باشند.

۷.۸.۸ از تمرین ٦.۸.۸ نتیجه بگیرید که که اگر $۴^m(۸n+۷)$ مجموع سه مجذور باشد آنگاه $۴^{m-۱}(۸n+۷)$ نیز چنین است.

۸.۸.۸ تمرینهای ۷.۸.۸ و ۵.۸.۸ نتیجه می‌دهند که هیچ عدد طبیعی مانند $۴^m(۸n+۷)$ مجموع سه مجذور نیست. چرا؟

پایان شادی‌آور این داستان این است که اعداد به صورت $۴^m(۸n+۷)$ دقیقاً همان اعدادی هستند که مجموع سه مجذور نمی‌باشند. این مطلب اولین بار توسط لژاندر اثبات شد و برهانی از آن را می‌توان در مُردل (١٩٦٩)، صفحات ۱۷۵ تا ۱۷۸ یافت. همان طور که مُردل متذکر گردیده است هیچ راه حلی که واقعاً مقدماتی باشد تاکنون شناخته نشده است.

۹۸ بحث

کاربرد هرویتز از چهارگانها در قضیهٔ چهار مجذور رویدادی به طور تاریخی طبیعی می‌باشد که بسیار مشابه کاربرد ددکیند از اعداد گاوسی در قضیهٔ دو مجذور است. در هر دو حالت یک اتحاد مجموع مجذورات در ابتدا کشف شده بود که پس از آن به طور قابل توجهی با کشف اعداد تعمیم‌یافته با یک نرم ضربی ادامه یافت (خاصیت ضربی صرفاً یک بازگویی از اتحاد مجموع مجذورات است). سرانجام اعداد صحیح و اعداد اول مناسبی در بین اعداد تعمیم‌یافته پیدا شد تا نمایش اعداد صحیح معمولی را به صورت مجذورات شرح دهد.

توازی تاریخی بین اعداد مختلط $\mathbb{C}$ و چهارگانهای $\mathbb{H}$ حتی از این هم قوی‌تر است زیرا هر دو داستان، حلقهٔ مفقودهٔ مشابهی دارند که تاکنون چیزی در این باب نگفته‌ایم. کشف اتحاد مجموع مجذورات منجر به خلق اعداد تعمیم‌یافته از طریق تجزیه و تحلیلی جبری از دَوَران است[۱۸].

در مورد اعداد مختلط، داستان به طور خلاصه چنین است.

- دیوفانتوس (در حدود ۲۰۰ سال قبل از میلاد) اتحاد

$$(a_1^2+b_1^2)(a_2^2+b_2^2)=(a_1a_2-b_1b_2)^2+(a_1b_2+b_1a_2)^2$$

را مشاهده کرد و آن را به عنوان قاعده‌ای برای در نظر گرفتن دو مثلث قائم‌الزاویه با جفت اضلاع (a_1,b_1) و (a_2,b_2) و تولید مثلث سومی با جفت اضلاع $(a_1a_2-b_1b_2, a_1b_2+b_1a_2)$ که وتر آن حاصل ضرب وترهای مثلثهای با اضلاع (a_1,b_1) و (a_2,b_2) است تعبیر کرد.

- ویت[۱۹] (۱۹۵۳) توجه کرد که زاویه در مثلث سوم مجموع زوایای دو

[۱۸] آنچه در مورد اعتقاد نویسنده نسبت به مسألهٔ کشف و خلق در این بند از نوشته‌هایش به چشم می‌خورد قابل توجه است. گرچه او پیدا شدن اتحاد مجذورات را کشف می‌داند با این حال معتقد است که اعداد تعمیم‌یافته خلق شده‌اند. (م)

[۱۹] Viéte

مثلث اول است. در نمادگذاری ما این مطلب بدان دلیل است که نسبت اضلاع در مثلث سوم برابر

$$\frac{a_1 b_2 + b_1 a_2}{a_1 a_2 - b_1 b_2} = \frac{\frac{b_1}{a_1} + \frac{b_2}{a_2}}{1 - \frac{b_1}{a_1}\frac{b_2}{a_2}} = \tan(\theta_1 + \theta_2)$$

است که در آن $\theta_1 = \tan^{-1}\frac{b_1}{a_1}$ و $\theta_2 = \tan^{-1}\frac{b_2}{a_2}$ زوایای دو مثلث اول هستند.

- در قرن هجدهم کوتز[20]، دموآور[21] و دیگران، مجدداً خاصیت جمع زاویه را به طور صوری با ضرب کردن $\cos\theta + i \sin\theta$ و $\cos\varphi + i \sin\varphi$ برای به دست آوردن $\cos(\theta+\varphi) + i \sin(\theta+\varphi)$ کشف کردند. بنابراین ضرب کردن در اعداد مختلط با نرم ۱ دوران صفحه حول مبدأ را به دست می‌دهد. این مطلب و تعبیر واضح‌تر جمع، به عنوان جمع برداری، به یکی انگاشتن اعداد مختلط با نقاط صفحه توسط وسل[22] (۱۷۹۷)، آرگاند[23] (۱۸۰۶) و (به شکل معتبرتری) توسط گاوس منجر گردید.

- همیلتون (۱۸۳۵) اعداد مختلط را به صورت جفتهای (a,b) از اعداد حقیقی با جمع و ضربی به صورت

$$\begin{aligned}(a_1,b_1)+(a_2,b_2) &= (a_1+a_2, b_1+b_2)\\ (a_1,b_1)\times(a_2,b_2) &= (a_1a_2-b_1b_2, a_1b_2+b_1a_2)\end{aligned}$$

تعریف کرد.

البته همیلتون در ۱۸۳۵ با ششدانگ حواسش در مورد اعداد مختلط عمل می‌کرد. لذا او می‌دانست که این تعاریف جمع و ضرب باید همهٔ خواص

[20] Cotes
[21] de Moivre
[22] Wessel
[23] Argand

معمولی را داشته باشد و می‌دانست که تابع $a^۲ + b^۲ =$ نرم $((a,b))$ باید ضربی باشد. با این حال امیدوار بود که با دوباره‌نویسی تاریخ اعداد مختلط بدین طریق باید چگونگی ضرب کردن سه‌تایی‌ها را ببیند. در حقیقت وی امیدوار بود یک قاعدهٔ ضرب کردن برای n-تایی‌ها بیابد که نرم آنها یعنی

$$((a_۱, a_۲, \ldots, a_n)) \text{ نرم } = a_۱^۲ + a_۲^۲ + \ldots + a_n^۲$$

را ضربی سازد. اما نرمی ضربی برای n-تایی‌ها، اتحادی از مجموع n مجذور را ایجاب خواهد کرد. لذا عاقلانه است که در ابتدا به دنبال اتحادی از مجموع سه مجذور باشیم.

این مطلب اتفاق نیفتاد. در عوض همیلتون ۱۳ سال را بیهوده صرف سعی در یافتن قاعده‌ای برای ضرب سه‌تایی‌ها کرد. همهٔ آنچه وی به طور مجازی از تحقیقاتش دریافته بود این بود که قاعدهٔ تعویض پذیری ضرب را باید کنار گذاشت. هنگامی که سه‌تایی‌ها را نیز کنار گذاشت و چهارگانها را آزمود همه چیز در جای خود جا افتاد. در شانزده اکتبر ۱۸۴۳ او قاعدهٔ

$$\mathbf{i}^۲ = \mathbf{j}^۲ = \mathbf{k}^۲ = \mathbf{ijk} = -۱$$

را نوشت که ضرب چهارگانها را تعریف می‌کند و از آن اتحاد چهار مجذور را به دست آورد. سپس وی فقط شروع به جمع‌آوری اخبار کرد؛ این که اویلر در ۱۷۴۸ اتحاد چهار مجذور را می‌دانست، این که لژاندر می‌دانست هیچ اتحاد سه مجذوری وجود ندارد و این که ضرب چهارگانها قبلاً توسط ردریگز[۲۴] در سال ۱۸۴۰ برای محاسبهٔ حاصل ضرب دورانها در $\mathbb{R}^۴$ استفاده شده بود.

البته یافته‌های پیشین منحصراً نگاهی اجمالی به ساختار کامل و زیبای کشف شده به وسیلهٔ همیلتون بود. چهارگانها حتی از آنچه وی می‌دانست نیز قابل توجه‌تر بود، زیرا پس از مرگ وی نشان داده شد که ضرب n-تایی‌ها فقط برای $n = ۱, ۲, ۴, ۸$ امکان پذیر است. به عبارت دقیق‌تر، اینها تنها

[۲۴] Rodrigues

n-تایی‌هایی هستند که برای آنها $\mathbb{R}^n$ نرمی ضربی و نیز ضربی که روی جمع برداری تعویض پذیر می‌باشد دارد. حکمی در این مورد، منسوب به هرویتز است که بیان می‌دارد اتحاد n-مجذوری فقط برای $n = ۱, ۲, ۴, ۸$ وجود دارد.

برای $n = ۱, ۲, ۴$ ساختارهای متناظر $\mathbb{R}$، $\mathbb{C}$ و $\mathbb{H}$ هستند و برای $n = ۸$ ساختار متناظر هشتگانها[۲۵] نامیده می‌شود. این مطلب تنها چند ماه بعد از کشف چهارگانها و بر مبنای اتحاد هشت مجذور توسط دوست همیلتون، جان گریوز[۲۶]، کشف شد. شبیه چهارگانها، هشتگانها نیز فاقد یک ضرب تعویض پذیر هستند. همچنین ضرب آنها شرکت پذیر نیز نمی‌باشد. بحثی بیشتر در باب این دستگاه اعداد تعمیم‌یافته را می‌توان در کتاب عالی اعداد[۲۷]، نوشتهٔ ابینگهاوس[۲۸] و بقیه (۱۹۹۱)، یافت.

اعداد صحیح هرویتز شبیه چهارگانها فرآیند جالبی در هندسه دارند. در سال ۱۸۵۲ شلافلی[۲۹] کشف کرد که دو بُعد استثنا مانند n هست که برای آنها $\mathbb{R}^n$ را می‌توان توسط شکلهایی غیر از مکعب کاشیکاری کرد. این اعداد $n = ۲$ (که در آن کاشیکاریهای استثنایی توسط مثلثهای متساوی‌الاضلاع یا هشت‌ضلعیهای منتظم انجام می‌شود) و $n = ۴$ هستند. در $\mathbb{C}= \mathbb{R}^۲$ این دو کاشیکاری استثنایی را می‌توان از اعداد صحیح آیزنشتینی $\mathbb{Z}[\zeta_۳]$ به دست آورد. کاشیکاری مثلثی توسط وصل کردن هر نقطهٔ صحیح به نزدیک‌ترین همسایه‌های آن و کاشیکاری هشت ضلعی با در نظر گرفتن هر نقطهٔ صحیح به عنوان مرکز ناحیه‌ای که اضلاع آن خطوط میانی بین همسایه‌های صحیحش می‌باشد به دست می‌آید. در $\mathbb{R}^۴$ دو کاشیکاری استثنایی به همین طریق از اعداد صحیح هرویتز به دست می‌آیند. برای بحثی بیشتر در باب این کاشیکاریهای قابل توجه کاکستر[۳۰] (۱۹۴۸) را ببینید.

---

[۲۵] octonions
[۲۶] John Graves
[۲۷] Numbers
[۲۸] Ebbinghaus
[۲۹] Schläfli
[۳۰] Coxeter

۹

تقابل مربعی

پیش‌نگاه

اکتشاف فرما مبنی بر این که اعداد اول فرد مربعی (یعنی به صورت $x^۲ + y^۲$) در حقیقت خطی (یعنی به صورت $۴n + ۱$) هستند به مسأله‌ای کلی‌تر در باب تعیین اعداد اول به صورت $x^۲ + dy^۲$ برای یک عدد نامربع مانند d منجر گردید. آیا برای هر d این مطلب درست است که اعداد اول به صورت $x^۲ + dy^۲$ همانهایی هستند که ترکیبی خطی و متناهی از صورتهایی خطی می‌باشند؟

فرما این صورتها را برای اعداد اول به صورت $x^۲ + ۲y^۲$ و $x^۲ + ۳y^۲$ به خوبی پیدا کرد. در هر یک از حالات، یافتن مشخصهٔ مربعی d- یعنی یافتن اعداد اول q که d- به پیمانهٔ q یک مربع کامل است، گامی سخت در تعیین صورتهای خطی اعداد اول $x^۲ + dy^۲$ می‌باشد.

قانون تقابل مربعی[۱] به همهٔ این قبیل سؤالها پاسخ می‌دهد. این قانون، توصیف می‌کند که چه موقع p یک مربع کامل به پیمانهٔ q است، که در آن p و q اعداد اول فردی می‌باشند؛ و مکملهای این قانون با حالات $p = -۱$ و $p = ۲$

[۱] quadratic reciprocity law

سر و کار دارد.

برای اثبات آن ابتدا محک اویلر[۲] را اثبات می‌کنیم که می‌گوید p یک مربع کامل به پیمانهٔ q است $\Longleftrightarrow$ $p^{\frac{q-1}{2}} \equiv_q 1$. این مطلب مکملهای قانون تقابل مربعی را نسبتاً آسان به دست می‌دهد و در برهان خودِ قانون تقابل مربعی نیز کمک می‌کند.

همچنین به قضیهٔ باقیماندهٔ چینی[۳] احتیاج داریم. این قضیه به خودی خود و همچنین برای آنچه در مورد تابع φ-اویلر می‌گوید جالب است اما هدف اصلی ما، استفاده از آن برای اثبات تقابل مربعی برای اعداد اول فرد p و q می‌باشد.

برای مختصر شدن بحث تقابل مربعی، نماد لژاندر[۴] $\left(\frac{P}{q}\right)$ را به کار می‌بریم که برابر ۱ است هرگاه P مربعی به پیمانهٔ q باشد و در غیر این صورت برابر ۱− می‌باشد. همهٔ مقادیر $\left(\frac{P}{q}\right)$ از مقادیر $\left(\frac{p}{q}\right)$ برای اعداد اول p (بنابر تقابل مربعی) و مقادیر خاص $\left(\frac{-1}{q}\right)$ و $\left(\frac{2}{q}\right)$ (از مکملهای قانون تقابل) نتیجه می‌شود.

۱.۹ اعداد اول x^2+y^2، x^2+2y^2، x^2+3y^2

مجدداً اعداد اول x^2+y^2

در برهان قضیهٔ دو مجذور فرما (که می‌گفت یک عدد اول فرد مانند p به صورت x^2+y^2 است فقط و فقط وقتی که p به صورت $4n+1$ باشد) یک گام کلیدی این بود که نشان دهیم هر عدد اول مانند $p=4n+1$، عددی به صورت m^2+1 را عاد می‌کند. این مطلب را در بخش ۵.۶ با استفاده از قضیهٔ ویلسون برای ساختن m ی مناسب، اثبات کردیم.

[۲] Euler's criterion
[۳] Chinese remainder theorem
[۴] Legendre's symbol

حال این گام را مجدداً می‌آزماییم تا ببینیم که چگونه ممکن است تعمیم یابد. این گزاره که p عدد $m^۲+۱$ را عاد می‌کند معادل این است که

$$-۱ \equiv_p m^۲.$$

به بیان دیگر، ۱− باید یک مربع کامل به پیمانهٔ $p=۴n+۱$ باشد. و در حقیقت برهان ما این بود که بنابر قضیهٔ ویلسون عبارتی برای ۱− اختیار کنیم و نشان دهیم که واقعاً یک مربع کامل به پیمانهٔ $p=۴n+۱$ است.

این مطلب این سؤال کلی را به وجود می‌آورد که آیا q یک مربع کامل به پیمانهٔ p است، که در آن p و q اعداد صحیح دلخواهی می‌باشند. این سؤال را به صورت زیر نیز می‌توان بیان کرد:

مشخصهٔ مربعی q به پیمانهٔ p چیست؟

همان طور که اکنون نشان می‌دهیم مسائلی چند به این سؤال منجر می‌شوند.

صورت $x^۲+۲y^۲$

فرما پس از توصیف اعداد اول به صورت $x^۲+y^۲$ از عهدهٔ اعداد اول به صورت $x^۲+۲y^۲$ نیز برآمد. وی ادعا کرد که

$$p=x^۲+۲y^۲ \Longleftrightarrow p=۸n+۱ \quad \text{یا} \quad p=۸n+۳.$$

همانند برهان ما برای قضیهٔ دو مجذور، در اینجا نیز می‌توان برهانی ارائه داد.

در $\mathbb{Z}[\sqrt{-۲}]$ کار می‌کنیم و ابتدا اثبات می‌کنیم اگر p یک عدد اول معمولی باشد که در $\mathbb{Z}[\sqrt{-۲}]$ اول نیست آنگاه برای a و b یی در $\mathbb{Z}$ داریم

$$p=a^۲+۲b^۲.$$

برهان، شبیه اعداد اول غیر گاوسی (بخش ۳.٦) است. اگر p عددی اول در $\mathbb{Z}[\sqrt{-۲}]$ نباشد آنگاه عواملی با نرم بیشتر از ۱ دارد. مثلاً

$$p=(a+b\sqrt{-۲})\gamma.$$

ضرب کردن این معادله در مزدوج آن به $p = a^۲ + ۲b^۲$ منجر می‌شود.

اکنون گام کلیدی این است که اثبات کنیم هر عدد اول مانند $۸n + ۳$ یا $p = ۸n + ۱$، عددی به صورت $m^۲ + ۲$ را عاد می‌کند. همین که این کار انجام شود تجزیهٔ

$$m^۲ + ۲ = (m - \sqrt{-۲})(m + \sqrt{-۲})$$

و یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\sqrt{-۲}]$ برای تکمیل برهان (همانند آنچه در بخش ۵.۶ برای $\mathbb{Z}[i]$ انجام دادیم) به کار می‌رود.

این ادعا که p عددی به صورت $m^۲ + ۲$ را عاد می‌کند معادل این است که

$$-۲ \equiv_p m^۲.$$

لذا مجبوریم اثبات کنیم که ۲− یک مربع کامل به پیمانهٔ p است هرگاه p عدد اولی به صورت $۸n + ۱$ یا $۸n + ۳$ باشد.

صورت $x^۲ + ۳y^۲$

سپس فرما اعداد اول به صورت $x^۲ + ۳y^۲$ را توصیف کرد:

$$p = x^۲ + ۳y^۲ \iff p = ۳n + ۱.$$

این مطلب را می‌توان همانند برهان برای $x^۲ + y^۲$ و $x^۲ + ۲y^۲$ (ولی این بار با استفاده از تجزیه‌هایی در $\mathbb{Z}[\frac{-۱+\sqrt{-۳}}{۲}]$) اثبات کرد. گام خالی از لطف این است که اثبات کنیم هر عدد اول مانند $p = ۳n + ۱$، عددی به صورت $m^۲ + ۳$ را عاد می‌کند. به طور معادل باید نشان دهیم که

$$-۳ \equiv_p m^۲.$$

لذا اکنون باید اثبات کنیم که ۳− یک مربع کامل به پیمانهٔ $p = ۳n + ۱$ است.

تمرینها

فرما در نامه‌ای به فرنیکل در پانزدهم ژوئن ۱۶۴۱ پرسید که کدام اعداد طبیعی، مجموع دو عدد کوچک‌تر در یک سه‌تایی فیثاغورسی هستند. چنین اعدادی باید به صورت $۲XY + X^۲ - Y^۲ = (X+Y)^۲ - ۲Y^۲$ باشند و فرانکل به درستی پاسخ داد که اعداد اول به صورت $x^۲ - ۲y^۲$ دقیقاً همانهایی هستند که به صورت $۸n \pm ۱$ می‌باشند. این مطلب را می‌توان به همان روش احکام فرما در مورد $x^۲ + y^۲$، $x^۲ + ۲y^۲$ و $x^۲ + ۳y^۲$ با استفاده از موارد زیر اثبات کرد.

- مزدوجگیری در $\mathbb{Z}[\sqrt{۲}]$،
- مشخصهٔ مربعی ۲،
- یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\sqrt{۲}]$.

مشخصهٔ مربعی ۲ در بخش ۴.۹ پایه‌ریزی خواهد شد اما گامهای دیگر را می‌توان در اینجا انجام داد.

۱.۱.۹ فرض کنیم p عدد اول دلخواهی باشد که در $\mathbb{Z}[\sqrt{۲}]$ اول نیست. لذا $p = (a + b\sqrt{۲})\gamma$، که در آن قدرمطلق نرم $a + b\sqrt{۲}$ و γ بزرگ‌تر از ۱ است. با مزدوجگیری از طرفین نشان دهید که $p = a^۲ - ۲b^۲$.

۲.۱.۹ با استفاده از این حقیقت که $x^۲ \equiv_۸ ۰, ۱, ۴$ نشان دهید که همهٔ اعداد اول به صورت $x^۲ - ۲y^۲$، به صورت $۸n \pm ۱$ می‌باشند.

حال از مشخصهٔ مربعی ۲ (بخش ۴.۹ را ببینید) استفاده می‌شود تا اثبات شود که هر عدد اول به صورت $۸n \pm ۱$ عددی طبیعی به صورت $m^۲ - ۲$ را عاد می‌کند. همچنین با فرض وجود یک خاصیت مقسوم‌علیه اول در $\mathbb{Z}[\sqrt{۲}]$، استدلال به شکل زیر پیش می‌رود.

۳.۱.۹ نشان دهید که اگر p عدد $(m-\sqrt{۲})(m+\sqrt{۲}) = m^{۲}-۲$ را عاد کند آنگاه p عددی اول در $\mathbb{Z}[\sqrt{۲}]$ نیست. (از این رو بنابر تمرین ۱.۱.۹ عدد p به صورت $x^{۲}-۲y^{۲}$ می‌باشد.)

حال تنها اطلاعاتی که صرف نظر از مشخصهٔ مربعی ۲ جا مانده است این است که اثبات کنیم $\mathbb{Z}[\sqrt{۲}]$ خاصیت مقسوم‌علیه اول دارد. با اثبات این مطلب که $\mathbb{Z}[\sqrt{۲}]$ خاصیت تقسیم و در نتیجه الگوریتم اقلیدسی دارد حکم حاصل می‌شود.

نرم $a^{۲}-۲b^{۲}$ از $a+b\sqrt{۲}\in\mathbb{Z}[\sqrt{۲}]$ برابر $|a+b\sqrt{۲}|^{۲}$ نیست. لذا استدلال هندسی استفاده شده برای $\mathbb{Z}[i]$ و $\mathbb{Z}[\sqrt{۲}]$ به کار نمی‌رود و ما در آرزوی یافتن یک روش جبری محض هستیم. در ابتدا خاصیت تقسیم در $\mathbb{Z}[\sqrt{۲}]$ را به صورت زیر بیان می‌کنیم:

اگر $\alpha,\beta\in\mathbb{Z}[\sqrt{۲}]$ و نیز $\beta\neq ۰$ آنگاه $\mu,\rho\in\mathbb{Z}[\sqrt{۲}]$ یی وجود دارند که

$$\alpha=\mu\beta+\rho,\qquad |\text{نرم }(\rho)|<|\text{نرم }(\beta)|.$$

۴.۱.۹ نشان دهید که خاصیت تقسیم از وجود μ یی در $\mathbb{Z}[\sqrt{۲}]$ با شرط $|\text{نرم }(\frac{\alpha}{\beta}-\mu)|<۱$ نتیجه می‌شود. (اکنون داریم نرم را به $\mathbb{Q}[\sqrt{۲}]$ توسیع می‌دهیم. آیا این کار موجه است؟)

۵.۱.۹ اگر $\alpha,\beta\in\mathbb{Z}[\sqrt{۲}]$ و نیز $\beta\neq ۰$، آنگاه به وسیلهٔ گویا کردن مخرج نشان دهید که برای $A_{۱}$ و $A_{۲}$ یی در $\mathbb{Z}$ داریم

$$\frac{\alpha}{\beta}=\frac{A_{۱}}{\text{نرم }(\beta)}+\frac{A_{۲}}{\text{نرم }(\beta)}\sqrt{۲}.$$

۶.۱.۹ با ادامهٔ نمادگذاری تمرین ۵.۱.۹ نشان دهید که اگر

$m_{۱}=$ نزدیک‌ترین عدد به $\frac{A_{۱}}{\text{نرم }(\beta)}$ ، $m_{۲}=$ نزدیک‌ترین عدد به $\frac{A_{۲}}{\text{نرم }(\beta)}$,

و $\mu = m_1 + m_2\sqrt{2}$ آنگاه ۱ > | نرم $(\frac{\alpha}{\beta} - \mu)$|. لذا $\mathbb{Z}[\sqrt{2}]$ خاصیت تقسیم دارد.

۲.۹ بیان تقابل مربعی

در اواسط قرن هجدهم اویلر دریافت که شناخت اعداد اول به صورتهایی از قبیل $x^2 + y^2$، $x^2 + 2y^2$ و $x^2 + 3y^2$ وابسته به این است که برای اعداد صحیح مشخصی مانند p و q بدانیم آیا p یک مربع کامل به پیمانهٔ q است یا نه. در حالتی که p و q اعداد اول و فردی باشند وی حدس زد که پاسخ عبارت است از:

هنگامی که p و q هر دو به صورت $4n + 3$ باشند آنگاه

p یک مربع کامل به پیمانهٔ q است فقط و فقط وقتی که q یک مربع کامل به پیمانهٔ p نباشد.

در غیر این صورت

p یک مربع کامل به پیمانهٔ q است فقط و فقط وقتی که q یک مربع کامل به پیمانهٔ p باشد.

به دلیل ارتباط متقابل بین p و q، این گزاره قانون تقابل مربعی نامیده می‌شود. (کلمهٔ مربعی در این حالت واقعاً به معنی مجذور است. در اغلب متون، اصطلاح قدیمی ماندهٔ مربعی به پیمانهٔ p[5] را به جای مربعهای به پیمانهٔ p به کار می‌برند[6].)

اویلر قادر نبود که قانون تقابل مربعی را اثبات کند. اولین برهانها توسط گاوس در ۱۸۰۱ ارائه شد. از آن موقع حدود ۲۰۰ برهان مختلف ارائه شده است که پس از قضیهٔ فیثاغورس، تقابل مربعی را به دومین قضیهٔ اثبات شده در ریاضیات تبدیل می‌کند.

---

[5] quadratic residues mod p

[6] اصطلاح ماندهٔ مربعی بر این حقیقت دلالت دارد که اگر p یک ماندهٔ مربعی به پیمانهٔ q باشد آنگاه باقیماندهٔ تقسیم p بر q یک مربع کامل است. (م)

نمادگذاری و مثالها

در بخش ۸.۹ برهان جدیدی از تقابل مربعی را ارائه می‌دهیم که برهان گاوس را ساده می‌سازد. اما در ابتدا نمادی را معرفی می‌کنیم و با ذکر مثالهایی، استفادهٔ آن را روشن می‌سازیم.

برای هر دو عدد اول مانند p و q، نماد لژاندر یا نماد مشخصهٔ مربعی توسط

$$\left(\frac{p}{q}\right) = \begin{cases} ۱ & \text{اگر } p \text{ یک مانده مربعی به پیمانه } q \text{ باشد} \\ -۱ & \text{اگر } p \text{ یک مانده مربعی به پیمانه } q \text{ نباشد} \end{cases}$$

تعریف می‌شود[۷]. به کمک این نماد، تقابل مربعی را می‌توان به صورت خیلی مختصرتر

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-۱)^{\frac{p-۱}{۲}.\frac{q-۱}{۲}}$$

برای اعداد اول[۸] p و q بیان کرد.

نماد لژاندر را می‌توان به $\left(\frac{P}{q}\right)$ برای هر عدد صحیح دلخواه مانند P توسیع داد. این نماد برابر ± ۱ است بسته به این که P یک مربع کامل به پیمانهٔ q باشد یا نباشد[۹]. این کار توسط خاصیت ضربی

$$\left(\frac{P}{q}\right) = \left(\frac{p_۱ p_۲ \cdots p_k}{q}\right) = \left(\frac{p_۱}{q}\right)\left(\frac{p_۲}{q}\right)\cdots\left(\frac{p_k}{q}\right)$$

امکان پذیر است، که در آن $p_۱ p_۲ \cdots p_k$ تجزیهٔ P به اعداد اول (که ممکن است شامل ۲ و یکهٔ ۱− نیز باشد[۱۰]) است. برای ارزیابی عوامل ممکن $\left(\frac{-۱}{q}\right)$ و $\left(\frac{۲}{q}\right)$ که از این تجزیه حاصل می‌شود به چیزی موسوم به مکملهای تقابل مربعی احتیاج داریم،

---

[۷] بهتر است p و q متمایز تلقی شوند. در حالت کلی اگر a مضربی از q باشد بهتر است نماد لژاندر $\left(\frac{a}{q}\right)$ تعریف نشود. (م)

[۸] متمایز (م)

[۹] بهتر است P مضرب q نباشد. (م)

[۱۰] و ممکن است p_iها تکراری نیز باشند (م)

$$\left(\frac{-۱}{q}\right) = ۱ \Longleftrightarrow q = ۴n + ۱ \qquad (\mathrm{I})$$

$$\left(\frac{۲}{q}\right) = ۱ \Longleftrightarrow q = ۸n \pm ۱ \qquad (\mathrm{II})$$

این موارد همراه با خاصیت ضربی، در چند بخش بعدی اثبات خواهند شد. حال از آنها برای اثبات خواص مطرح شده در بخش ۱.۹ استفاده می‌کنیم.

مثالها.

برای آن که نشان دهیم ۲− یک مربع کامل به پیمانهٔ $۸n + ۳$ یا $p = ۸n + ۱$ است مقادیر زیر را محاسبه می‌کنیم

$$\begin{aligned} \left(\frac{-۲}{۸n+۱}\right) &= \left(\frac{-۱}{۸n+۱}\right)\left(\frac{۲}{۸n+۱}\right) && \text{بنابر خاصیت ضربی} \\ &= ۱ \times ۱ = ۱ && \text{بنابر مکملها} \\ \left(\frac{-۲}{۸n+۳}\right) &= \left(\frac{-۱}{۸n+۳}\right)\left(\frac{۲}{۸n+۳}\right) && \text{بنابر خاصیت ضربی} \\ &= (-۱) \times (-۱) = ۱ && \text{بنابر مکملها} \end{aligned}$$

برای آن که نشان دهیم ۳− یک مربع کامل به پیمانهٔ $p = ۳n + ۱$ است داریم

$$\begin{aligned} &\left(\frac{-۳}{۳n+۱}\right) \\ &= \left(\frac{-۱}{۳n+۱}\right)\left(\frac{۳}{۳n+۱}\right) && \text{بنابر خاصیت ضربی} \\ &= ۱ \times \left(\frac{۳n+۱}{۳}\right) \end{aligned}$$

بنابر مکملها و قانون تقابل مربعی $\qquad (-۱) \times (-۱)\left(\frac{۳n+۱}{۳}\right)$ یا

با قرار دادن علامت + یا − بر حسب آن که $۳n + ۱$ به صورت $۴n' + ۱$ باشد

یا نباشد داریم

$$\text{چون}\ ۱ \equiv_۳ ۳n+۱ \quad \left(\frac{۱}{۳}\right) (-۱)\times(-۱)\ \text{یا}\ ۱\times\left(\frac{۱}{۳}\right) =$$
$$۱ = (-۱)\times(-۱)\ \text{یا}\ ۱\times ۱ =$$

چون ۱ یک مربع کامل به پیمانهٔ ۳ است.

تمرینها

توجه کنید که مشخصهٔ مربعی ۲ که توسط مکمل (II) ارائه می‌شود دقیقاً همان چیزی است که برای پر کردن خلل موجود در مجموعه تمرینهای قبلی بدان احتیاج داشتیم و اثبات می‌کند که اعداد اول به صورت $x^۲ - ۲y^۲$ همانهایی هستند که به صورت $۸n \pm ۱$ می‌باشند. حال از مشخصهٔ مربعی ۳ به روشی مشابه برای مشخص کردن اعداد اول به صورت $x^۲ - ۳y^۲$ استفاده می‌کنیم.

۱.۲.۹ فرض کنیم p یک عدد اول معمولی باشد که در $\mathbb{Z}[\sqrt{۳}]$ اول نیست. لذا $p = (a+b\sqrt{۳})\gamma$ که در آن قدرمطلق نرم $a+b\sqrt{۳}$ و γ بزرگ‌تر از ۱ است. با مزدوجگیری از طرفین نشان دهید که $p = a^۲ - ۳b^۲$.

۲.۲.۹ از همنهشتی به پیمانهٔ ۱۲ استفاده کنید و نشان دهید که ۳ یک مربع کامل به پیمانهٔ هر عدد اول مانند $p = ۱۲n + ۱$ می‌باشد. نتیجه بگیرید که چنین p یی عددی طبیعی به صورت $m^۲ - ۳$ را عاد می‌کند.

۳.۲.۹ بررسی کنید که استدلال تمرین ٦.۱.۹ برای $\mathbb{Z}[\sqrt{۳}]$ نیز کار می‌کند و لذا $\mathbb{Z}[\sqrt{۳}]$ خاصیت مقسوم‌علیه اول دارد.

۴.۲.۹ از تمرینهای ۳.۲.۹ و ۴.۲.۹ و این که

$$m^۲ - ۳ = (m - \sqrt{۳})(m + \sqrt{۳})$$

استفاده کنید و اثبات کنید که $p = ۱۲n + ۱$ عددی اول در $\mathbb{Z}[\sqrt{۳}]$ نیست. بنابر تمرین ۱.۲.۹ نتیجه بگیرید که p به صورت $x^۲ - ۳y^۲$ است.

لذا صورت $x^۲ - ۳y^۲$ همهٔ اعداد اول به صورت $۱۲n + ۱$ را نمایش می‌دهد. این صورت، عدد اول زوج ۲ را نمایش نمی‌دهد چرا که اگر چنین باشد با مشخصهٔ مربعی ۲ در تناقض است.

۵.۲.۹ نشان دهید وجود جوابی صحیح برای $x^۲ - ۳y^۲ = ۲$ ایجاب می‌کند که ۲ یک مربع کامل به پیمانهٔ عددی اول باشد که این با توجه به مکمل (II) امکان پذیر نیست.

به طور مشابه، مشخصهٔ مربعی ۱− راه حل دیگری برای تمرین **۶.۸.۵** ارائه می‌دهد.

۶.۲.۹ نشان دهید وجود جوابی صحیح برای $x^۲ - ۳y^۲ = -۱$ ایجاب می‌کند که ۱− یک مربع کامل به پیمانهٔ عددی اول باشد که این با توجه به مکمل (I) امکان پذیر نیست.

۳.۹ محک اویلر

اگر q اول باشد و $a \not\equiv_q ۰$ آنگاه بنابر قضیهٔ کوچک فرما $a^{q-۱} \equiv_q ۱$. اویلر از این مطلب برای رسیدن به فرمول زیر استفاده کرد:

محک اویلر. برای یک عدد اول فرد مانند p داریم $\left(\frac{p}{q}\right) \equiv_q p^{\frac{q-۱}{۲}}$. از این رو p یک مربع کامل به پیمانهٔ q است فقط و فقط وقتی که $p^{\frac{q-۱}{۲}} \equiv_q ۱$.

برهان. در ابتدا فرض کنیم p یک مربع کامل به پیمانهٔ q باشد؛ مثلاً $p \equiv_q a^۲$. در این صورت بنابر تعریف، $\left(\frac{p}{q}\right) = ۱$ و

$$p^{\frac{q-۱}{۲}} \equiv_q a^{q-۱} \equiv_q ۱ \qquad \text{بنابر قضیه کوچک فرما}$$

بالعکس، اگر p یک مربع کامل به پیمانهٔ q نباشد کافی است نشان دهیم که

$$p^{\frac{q-۱}{۲}} \not\equiv_q ۱.$$

این مطلب بدان دلیل است که بنابر قضیهٔ کوچک فرما $x = p^{\frac{q-۱}{۲}}$ در $x^۲ \equiv_q p^{q-۱} \equiv_q ۱$ صدق می‌کند و بنابر قضیهٔ همنهشتی چندجمله‌ای لاگرانژ، معادلهٔ $x^۲ \equiv_q ۱$ فقط دو جواب $x \equiv_q \pm ۱$ دارد.

بنابر همان قضیه، $p^{\frac{q-۱}{۲}} \equiv_q ۱$ حداکثر $\frac{q-۱}{۲}$ جواب دارد و می‌دانیم که این جوابها شامل مربعهای $p = ۱^۲, ۲^۲, \dots, (\frac{q-۱}{۲})^۲$ می‌باشد. این $\frac{q-۱}{۲}$ مربع کامل متمایزند. در حقیقت اگر $x^۲$ و $y^۲$ دو مربع دلخواه از بین این اعداد باشند، داریم

$$\begin{aligned} x^۲ \equiv_q y^۲ &\iff x^۲ - y^۲ \equiv_q ۰ \\ &\iff (x-y)(x+y) \equiv_q ۰ \\ &\iff x = y. \end{aligned}$$

این مطلب بدان دلیل است که $۱ < x + y < q$ و از این رو $x + y \not\equiv_q ۰$. لذا هنگامی که $p \equiv_q a^۲$ داریم $p^{\frac{q-۱}{۲}} \not\equiv_q ۱$. بنابراین $\left(\frac{p}{q}\right) \equiv_q -۱ \equiv_q p^{\frac{q-۱}{۲}}$. $\square$

توجه کنید که برهان این محک فرض نمی‌کند که p واقعاً یک عدد اول باشد. از این موقعیت برای تعریف $\left(\frac{P}{q}\right)$ به ازای هر $P \not\equiv_q ۰$ استفاده می‌کنیم و اگر P یک مربع کامل به پیمانهٔ q باشد $\left(\frac{P}{q}\right)$ را برابر ۱ و در غیر این صورت برابر ۱− تعریف می‌کنیم. بنابراین محک اویلر برهانی ساده برای خاصیت زیر است.

خاصیت ضربی $\left(\frac{P}{q}\right)$. برای هر $P_۱, P_۲ \equiv_q ۰$ داریم

$$\left(\frac{P_۱}{q}\right)\left(\frac{P_۲}{q}\right) = \left(\frac{P_۱ P_۲}{q}\right).$$

برهان. بنابر محک اویلر داریم

$$\begin{aligned} \left(\frac{P_۱}{q}\right) &\equiv_q P_۱^{\frac{q-۱}{۲}}, \\ \left(\frac{P_۲}{q}\right) &\equiv_q P_۲^{\frac{q-۱}{۲}}. \end{aligned}$$

بنابراین

$$\begin{aligned}\left(\frac{P_۱}{q}\right)\left(\frac{P_۲}{q}\right) &\equiv_q P_۱^{\frac{q-۱}{۲}} P_۲^{\frac{q-۱}{۲}}\\ &\equiv_q (P_۱ P_۲)^{\frac{q-۱}{۲}}\\ &\equiv_q \left(\frac{P_۱ P_۲}{q}\right). \square\end{aligned}$$

برهان خاصیت ضربی نیز فرض نمی‌کند که P ها اول باشند. لذا می‌توانیم $\left(\frac{P}{q}\right)$ را برای هر عدد صحیح مانند P ارزیابی کنیم مشروط بر آن که $\left(\frac{p}{q}\right)$ را برای عوامل اول p از P بدانیم. می‌توانیم فرض کنیم که این عوامل از بین ۱−، ۲ و اعداد اول فرد هستند.

قانون تقابل مربعی (اثبات شده در بخش ۸.۹) اطلاعاتی در مورد $\left(\frac{p}{q}\right)$ برای p های اول فرد می‌دهد. لذا به اطلاعاتی در مورد $\left(\frac{-۱}{q}\right)$ و $\left(\frac{۲}{q}\right)$ نیز احتیاج داریم. این مطلب را از مکملهای تقابل مربعی که در اینجا و بخش بعد اثبات شده‌اند به دست می‌آوریم که مقادیر $\left(\frac{-۱}{q}\right)$ و $\left(\frac{۲}{q}\right)$ را مستقیماً به دست می‌دهند. (قبلاً روش دیگری برای تعیین $\left(\frac{-۱}{q}\right)$ را در بخش ۷.۶ ارائه داده بودیم.)

مقدار $\left(\frac{-۱}{q}\right)$. برای یک عدد اول فرد مانند q،

$$\left(\frac{-۱}{q}\right)=\begin{cases} ۱ & q=۴n+۱ \text{ اگر } \\ -۱ & q=۴n+۳ \text{ اگر } \end{cases}$$

برهان. محک اویلر می‌گوید که

$$\left(\frac{-۱}{q}\right)\equiv_q (-۱)^{\frac{q-۱}{۲}}.$$

لذا اگر $q=۴n+۱$ داریم

$$\left(\frac{-۱}{q}\right)\equiv_q (-۱)^{۲n}\equiv_q ۱$$

و اگر $q=۴n+۳$ آنگاه

$$\left(\frac{-۱}{q}\right)\equiv_q (-۱)^{۲n+۱}\equiv_q -۱. \square$$

تمرینها

اگر وجود ریشهٔ اولیه برای یک عدد اول مانند q را (که در بخش ۹.۳ اثبات شد) فرض کنیم آنگاه ارائهٔ برهانی برای محک اویلر ساده‌تر خواهد بود.

۱.۳.۹ اگر a ریشهٔ اولیه‌ای برای q باشد (که در نتیجه ۱، a، $a^۲$، ...، $a^{q-۲}$ عناصر ناصفر متمایزی به پیمانهٔ q هستند) آنگاه نشان دهید که مربعهای کامل به پیمانهٔ q عبارتند از ۱، $a^۲$، $a^۴$، ...، $a^{q-۳}$.

۲.۳.۹ از تمرین ۱.۳.۹ نتیجه بگیرید که b یک مربع کامل به پیمانهٔ q است فقط و فقط وقتی که $b^{\frac{q-۱}{۲}} \equiv_q ۱$.

یک نتیجهٔ سادهٔ دیگر از تمرین ۱.۳.۹ خاصیت نصف نصف[۱۱] مربعها به پیمانهٔ q است.

۳.۳.۹ نشان دهید که دقیقاً نصف اعداد ۱، ۲، ۳، ...، $q-۱$ به پیمانهٔ q مربع کامل هستند.

خاصیت نصف نصف را می‌توان بدون فرض وجود ریشهٔ اولیه نیز اثبات کرد؛ گرچه کاملاً ساده نیست. برای این کار لازم است که حکم زیر اثبات شود:

۴.۳.۹ نشان دهید که ۱^۲، ۲^۲، ۳^۲، ...، $(q-۱)^۲$ شامل حداکثر نصف اعداد ناهمنهشت با صفر به پیمانهٔ q می‌باشد.

۴.۹ مقدار $\left(\frac{۲}{q}\right)$

محک اویلر می‌گوید که $\left(\frac{۲}{q}\right) \equiv_q ۲^{\frac{q-۱}{۲}}$. اما محاسبهٔ $۲^{\frac{q-۱}{۲}}$ سخت‌تر از $(-۱)^{\frac{q-۱}{۲}}$ می‌باشد. به نظر می‌رسد که فرما $\left(\frac{۲}{q}\right)$ را می‌دانسته است (تمرینهای بخش ۱.۹

---
[۱۱] half and half

را ببینید)، اما نمی‌دانیم چگونه. می‌توانیم این مطلب را که

$$۲^{\frac{q-۱}{۲}} = \begin{cases} (-۱)^{\frac{q-۱}{۴}} & q = ۴n + ۱ \text{ اگر} \\ (-۱)^{\frac{q+۱}{۴}} & q = ۴n + ۳ \text{ اگر} \end{cases}$$

با محاسبهٔ حاصل ضرب $(q - ۱) \times \ldots \times ۳ \times ۲ \times ۱$ به پیمانهٔ q اثبات کنیم. این کار، اندکی شبیه محاسبهٔ مذکور در بخش ۵.٦ است که مشخصهٔ مربعی ۱− را در بخش ۷.٦ به دست داد.

هنگامی که $q = ۴n + ۱$، محاسبهٔ ما از نصف آنها عامل ۲ و از یک چهارم آنها عامل ۱− را خارج می‌کند و عوامل منفی حاصله را مجدداً به پیمانهٔ $۴n + ۱$ می‌نویسیم تا آنها را مثبت سازیم. این کار حاصل ضربی را که با آن شروع کردیم به شکل دیگری باز می‌سازد که سپس می‌توان آن را از طرفین معادله حذف کرد.

$$\begin{aligned}
& ۱ \times ۲ \times \ldots \times ۴n \\
\equiv_q \quad & (۱ \times ۳ \times \ldots \times (۴n - ۱)) \times (۲ \times ۴ \times \ldots \times ۴n) \\
\equiv_q \quad & (۱ \times ۳ \times \ldots \times (۴n - ۱))(۱ \times ۲ \times \ldots \times ۲n)۲^{۲n} \\
\equiv_q \quad & (۱ \times ۳ \times \ldots \times (۲n - ۱)) \\
& ((۲n + ۱)(۲n + ۳) \ldots (۴n - ۱))(۱ \times ۲ \times \ldots \times ۲n)۲^{۲n} \\
\equiv_q \quad & ((-۱) \times (-۳) \times \ldots \times (-۲n + ۱))(-۱)^n \\
& ((۲n + ۱)(۲n + ۳) \ldots (۴n - ۱))(۱ \times ۲ \times \ldots \times ۲n)۲^{۲n} \\
\equiv_q \quad & ((۴n) \times (۴n - ۲) \times \ldots \times (۲n + ۲))(-۱)^n \\
& ((۲n + ۱)(۲n + ۳) \ldots (۴n - ۱))(۱ \times ۲ \times \ldots \times ۲n)۲^{۲n} \\
\equiv_q \quad & ((۲n + ۱) \times (۲n + ۲) \times \ldots \times (۴n))(-۱)^n \\
& \times(۱ \times ۲ \times \ldots \times ۲n)۲^{۲n} \\
\equiv_q \quad & (-۱)^n ۲^{۲n}(۱ \times \times ۲ \times \ldots \times ۴n).
\end{aligned}$$

با حذف کردن $۱ \times ۲ \times \ldots \times ۴n$ از سطر اول وآخر داریم

$$۱ \equiv_q (-۱)^n ۲^{۲n} \equiv_q (-۱)^{\frac{q-۱}{۴}} ۲^{\frac{q-۱}{۲}}.$$

یعنی اگر $q = ۴n + ۱$ آنگاه

$$۲^{\frac{q-۱}{۲}} \equiv_q (-۱)^{\frac{q-۱}{۴}}.$$

با برهانی مشابه (تمرین) می‌توان نشان داد که اگر $q۴n + ۳$ آنگاه

$$۲^{\frac{q-۱}{۲}} \equiv_q (-۱)^{\frac{q+۱}{۴}}.$$

بنابراین برای این که تصمیم بگیریم چه زمانی ۲ به پیمانهٔ q یک مربع کامل است باید به دو حالت توجه کنیم:

اگر $q = ۴n + ۱$ آنگاه $\frac{q-۱}{۴} = n$. لذا $\left(\frac{۲}{q}\right) = (-۱)^{\frac{q-۱}{۴}}$ برابر ۱ است هرگاه $n = ۲m$ و برابر ۱− است هرگاه $n = ۲m + ۱$. یعنی ۲ یک مربع کامل به پیمانهٔ q است هرگاه $q = ۸m + ۱$ و نه هرگاه $q = ۸m + ۵$.

اگر $q = ۴n + ۳$ آنگاه $\frac{q+۱}{۴} = n + ۱$. لذا $\left(\frac{۲}{q}\right) = (-۱)^{\frac{q+۱}{۴}}$ برابر ۱ است هرگاه $n = ۲m + ۱$ و برابر ۱− است هرگاه $n = ۲m$. یعنی ۲ یک مربع کامل به پیمانهٔ q است هرگاه $q = ۸m + ۷$ و نه هرگاه $q = ۸m + ۳$.

به عنوان جمع‌بندی: ۲ یک مربع کامل به پیمانهٔ q است فقط و فقط وقتی که $q = ۸m \pm ۱$.

تمرینها

برهان حالت $q = ۴n+۳$، حاصل ضرب $۱\times۲\times\ldots\times۴n\times(۴n+۱)\times(۴n+۲)$ را به روش اندکی کم‌نظم‌تر می‌شکنند. این کار لازم است زیرا تعداد جملات در این حالت، بر ۴ قابل قسمت نیست. روش انجام این کار را می‌توان در ابتدا توسط یک مثال، مثلاً $q = ۱۱$، آزمود.

۱.۴.۹ با افراز $۱۰! = ۱ \times ۲ \times ۳ \times ۴ \times ۵ \times ۶ \times ۷ \times ۸ \times ۹ \times ۱۰$ به صورت

$$(۱ \times ۳ \times ۵)(۷ \times ۹)(۲ \times ۴ \times ۶ \times ۸ \times ۱۰)$$

و خارج کردن ۱− و ۲ از عوامل مناسب و سپس تبدیل عوامل منفی مانند $-k$ به عوامل مثبت $۱۱ - k$ نشان دهید که

$$۱۰! \equiv_{۱۱} ۱۰!(-۱)^{۳}۲^{۵},$$

و از این رو $\left(\frac{۲}{۱۱}\right) = -۱$.

۲.۴.۹ با افراز $(۴n+۲)! = ۱ \times ۲ \times \ldots \times ۴n \times (۴n+۱) \times (۴n+۲)$ به صورت

$$(۱ \times ۳ \times ۵ \times \ldots \times (۲n+۱))((۲n+۳)(۲n+۵)\ldots(۴n+۱))$$
$$\times(۲ \times ۴ \times ۶ \times \ldots ۸ \times ۴n \times (۴n+۲))$$

و خارج کردن ۱− و ۲ از عوامل مناسب و سپس تبدیل عوامل منفی مانند $-k$ به عوامل مثبت $۴n + ۳ - k$ نشان دهید که

$$(۴n+۲)! \equiv_{۴n+۳} (۴n+۲)!(-۱)^{n+۱}۲^{۲n+۱},$$

و از این رو $\left(\frac{۲}{۴n+۳}\right) = (-۱)^{n+۱}$.

۳.۴.۹ از تمرین ۲.۴.۹ نتیجه بگیرید که وقتی $q = ۴n + ۳$ داریم $\left(\frac{۲}{q}\right) = (-۱)^{\frac{q+۱}{۴}}$.

۵.۹ این قصه سر دراز دارد

در بخش ۱.۹ مشاهده کردیم که رده‌بندی اعداد اول به صورتهای $x^۲ + y^۲$، $x^۲ + ۲y^۲$، $x^۲ + ۳y^۲$ وابسته به دانستن این مطلب است که اعدادی مشخص به

پیمانهٔ اعداد اول خاصی مربع کامل هستند یا نه. برای اثبات چنین احکامی نماد لژاندر را معرفی کردیم که برای هر عدد صحیح مانند $P \not\equiv_q 0$ و عدد اول q به صورت

$$\left(\frac{P}{q}\right)=\begin{cases} 1 & \text{اگر } P \text{ یک مانده مربعی به پیمانه } q \text{ باشد} \\ -1 & \text{اگر } P \text{ یک مانده مربعی به پیمانه } q \text{ نباشد} \end{cases}$$

تعریف می‌شود. با تشکر از محک اویلر همنهشتی

$$\left(\frac{P}{q}\right) \equiv_q P^{\frac{q-1}{2}}$$

برای هر $P \not\equiv_q 0$ معتبر است و می‌توانیم خاصیت ضربی

$$\left(\frac{P_1}{q}\right)\left(\frac{P_2}{q}\right)=\left(\frac{P_1P_2}{q}\right)$$

را اثبات کنیم. از این رو $\left(\frac{P}{q}\right)$ را برای هر $P \not\equiv_q 0$ با شکستن P به عوامل p_1، p_2، ... (که -1 یا عدد اول هستند) و سپس با ضرب کردن $\left(\frac{p_1}{q}\right)$، $\left(\frac{p_2}{q}\right)$، ... در یکدیگر می‌یابیم.

در بخشهای ۳.۹ و ۴.۹ از محک اویلر برای اثبات مکملهای تقابل مربعی استفاده کردیم:

$$\begin{aligned} \left(\frac{-1}{q}\right) &= 1 \Longleftrightarrow q=4n+1 && \text{(I)} \\ \left(\frac{2}{q}\right) &= 1 \Longleftrightarrow q=8n\pm 1 && \text{(II)} \end{aligned}$$

لذا باقی می‌ماند که $\left(\frac{p}{q}\right)$ را برای p و q های اول و فرد ارزیابی کنیم. این کار توسط قانون تقابل مربعی که در بخش ۸.۹ اثبات خواهد شد انجام می‌شود:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

استفاده از تقابل مربعی

تقابل مربعی می‌گوید که اگر یکی از p و q به صورت $۴n + ۱$ باشد آنگاه

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

و در غیر این صورت

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

نکتهٔ دیگری که در ذهن داریم این است که اگر $p \equiv_q p'$ آنگاه p یک مربع کامل به پیمانهٔ q است فقط و فقط وقتی که p' چنین باشد.

لذا می‌توانیم p را در $\left(\frac{p}{q}\right)$ با باقیماندهٔ تقسیم p بر q (مثلاً p') عوض کنیم. در این صورت $\left(\frac{p'}{q}\right)$ توسط تقابل مربعی با $\pm\left(\frac{q}{p'}\right)$ تقابل می‌یابد، سپس باقیماندهٔ تقسیم q بر p (مثلاً q') به جای q قرار می‌گیرد و به همین ترتیب این کار ادامه پیدا می‌کند. در نتیجه می‌توانیم الگوریتم اقلیدسی را با کاربردهای ضربی بودن برای تحویل سریع اعداد در هم بیامیزیم تا به نقطه‌ای برسیم که بتوانیم مکملهای I و II را به کار ببریم.

مثال. می‌خواهیم ببینیم که آیا ۳۷ یک مربع کامل به پیمانهٔ ۵۹ است.

$$\begin{aligned}\left(\frac{۳۷}{۵۹}\right) &= \left(\frac{۵۹}{۳۷}\right) && \text{بنابر تقابل}\\ &= \left(\frac{۲۲}{۳۷}\right) && \text{بنابر باقیمانده گرفتن}\\ &= \left(\frac{۲}{۳۷}\right)\left(\frac{۱۱}{۳۷}\right) && \text{بنابر ضربی‌بودن}\\ &= -\left(\frac{۱۱}{۳۷}\right) && \text{بنابر مکمل II}\\ &= -\left(\frac{۳۷}{۱۱}\right) && \text{بنابر تقابل}\end{aligned}$$

$$
\begin{aligned}
&= -\left(\frac{۴}{۱۱}\right) && \text{بنابر باقیمانده گرفتن}\\
&= -\left(\frac{۲}{۱۱}\right)^{۲} && \text{بنابر ضربی بودن}\\
&= -۱.
\end{aligned}
$$

از این رو ۳۷ مربعی کامل به پیمانهٔ ۵۹ نیست.

تمرینها

۱.۵.۹ با استفاده از ضربی بودن و الگوریتم اقلیدسی نشان دهید که $\left(\frac{۵۵}{۸۹}\right) = ۱$.

۲.۵.۹ مستقیماً با یافتن یک مربع کامل همنهشت با ۵۵ به پیمانهٔ ۸۹ تحقیق کنید که $\left(\frac{۵۵}{۸۹}\right) = ۱$.

۳.۵.۹ نشان دهید $\left(\frac{۵۶}{۸۹}\right) = ۱$.

۶.۹ قضیه باقیمانده چینی

یک مثال

قضیهٔ باقیماندهٔ چینی در مورد نمایش اعداد به وسیلهٔ باقیماندهٔ آنهاست. مثلاً در اینجا اعداد $n = ۰, ۱, ۲, \ldots, ۱۴$ و باقیماندههای آنها را به پیمانهٔ ۳ و به پیمانهٔ ۵ به ترتیب در تقسیم بر ۳ و ۵ داریم.

n	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴
n به پیمانه ۳	۰	۱	۲	۰	۱	۲	۰	۱	۲	۰	۱	۲	۰	۱	۲
n به پیمانه ۵	۰	۱	۲	۳	۴	۰	۱	۲	۳	۴	۰	۱	۲	۳	۴

می‌توان بررسی کرد که هر یک از این ۱۵ عدد $n = ۰, ۱, ۲, \ldots, ۱۴$، زوج متفاوتی از باقیمانده‌ها را به دست می‌دهند و از این رو هر چنین n ی به وسیلهٔ زوج باقیمانده‌اش معین می‌شود. مثلاً تنها عدد با زوج باقیماندهٔ $(۲, ۳)$ عبارت است از ۸.

همچنین به سادگی می‌توان فهمید که چرا چنین است.

- اولین مؤلفهٔ هر زوج، یعنی n به پیمانهٔ ۳ در دنبالهٔ ...۰۱۲۰۱۲۰۱۲ تغییر می‌کند که هر سه گام یک بار تکرار می‌شود.

- دومین مؤلفهٔ هر زوج، یعنی n به پیمانهٔ ۵ در دنبالهٔ ...۰۱۲۳۴۰۱۲۳۴ تغییر می‌کند که هر پنج گام یک بار تکرار می‌شود.

- بنابراین هیچ زوجی تا $\mathrm{lcm}(۳, ۵) = ۱۵$ گام تکرار نمی‌شود و از این رو اولین ۱۵ زوج متفاوتند.

قضیه باقیمانده چینی کلاسیک

شکل اصلی قضیهٔ باقیمانده که در حدود 300 بعد از میلاد در چین یافت شده است بدین شکل است: اگر $\gcd(a, b) = ۱$ آنگاه هر $n = ۰, ۱, ۲, \ldots, ab - ۱$ زوجی متمایز از باقیمانده‌ها را در تقسیم بر a و b به دست می‌دهد.

این مطلب را می‌توان توسط تعمیم استدلال فوق اثبات کرد.

- اولین باقیماندهٔ هر زوج، یعنی n به پیمانهٔ a در دنبالهٔ

$$۰۱۲\ldots(a-۱)۰۱۲\ldots(a-۱)\ldots$$

تغییر می‌کند که هر a گام یک بار تکرار می‌شود.

- دومین مؤلفهٔ هر زوج، یعنی n به پیمانهٔ b در دنبالهٔ

$$۰۱۲\ldots(b-۱)۰۱۲\ldots(b-۱)\ldots$$

تغییر می‌کند که هر b گام یک بار تکرار می‌شود.

- بنابراین هیچ زوجی از باقیمانده‌ها تا $\mathrm{lcm}(a,b)=ab$ گام تکرار نمی‌شود و از این رو اولین ab زوج متفاوتند. □

شرط $\gcd(a,b)=۱$ می‌گوید که a و b هیچ عامل اول مشترکی ندارند. لذا مضارب مشترک آنها شامل همهٔ عوامل اولشان می‌باشد و از این رو $\mathrm{lcm}(a,b)=ab$.

تمرینها

مثال کلاسیک مسألهٔ باقیماندهٔ چینی در کتاب دستی ریاضیات سون زی[۱۲] که قدمت آن به قرن سوم پس از میلاد بر می‌گردد آمده است. در این مسأله خواسته شده است عددی را بیابید که در تقسیم بر ۳ باقیماندهٔ ۲، در تقسیم بر ۵ باقیماندهٔ ۳ و در تقسیم بر ۷ باقیماندهٔ ۲ دارد.

۱.۶.۹ نشان دهید که اعداد ۱، ۲، ۳، ...، ۲۱۰ همگی سه‌تایی‌های متمایزی از باقیمانده‌ها را در تقسیم بر ۳، ۵ و ۷ دارند.

۲.۶.۹ تعمیمی از این حکم را به سه‌تایی‌های باقیمانده‌های تقسیم بر a، b و c با شرطی مناسب روی پیمانه‌های a، b و c پیدا کنید.

۳.۶.۹ کوچک‌ترین جواب مسألهٔ سون زی را بیابید.

---

[۱۲] Mathematical Manual of Sun Zi

۴.۶.۹ اعداد با باقیماندهٔ ۱ در تقسیم بر ۳ و با باقیماندهٔ ۲ در تقسیم بر ۵ را توصیف کنید و سپس کوچک‌ترین آنها را که در تقسیم بر ۷ باقیماندهٔ ۳ دارد بیابید.

۷.۹ قضیه باقیمانده چینی کامل

شکل مدرن این قضیه نه تنها هر یک از اعداد $n = ۰, ۱, ۲, \ldots, ab - ۱$ را توسط یک زوج (n به پیمانهٔ n, b به پیمانهٔ a) نمایش می‌دهد بلکه همچنین مشخص می‌سازد که این n ها را می‌توان با جمع کردن و ضرب کردن زوجهای متناظر، با یکدیگر جمع و یا در یکدیگر ضرب کرد.

به طور طبیعی، اولین مؤلفهٔ زوجها به پیمانهٔ a جمع و یا ضرب می‌شوند و دومین مؤلفه‌ها به پیمانهٔ b. لذا صحبت از زوجهایی است که به پیمانهٔ (a, b) محاسبه می‌شوند.

مثال. جمع و ضرب کردن به پیمانهٔ ۱۵.

اعداد ۸ و ۹ و مجموع و حاصل ضرب آنها را به پیمانهٔ ۱۵ در نظر می‌گیریم. داریم

۸ توسط $(۲, ۳)$ نمایش داده می‌شود،

۹ توسط $(۰, ۴)$ نمایش داده می‌شود.

با جمع کردن این زوجها به پیمانهٔ ۳ در مؤلفهٔ اول و به پیمانهٔ ۵ در مؤلفهٔ دوم، داریم

$$(۲, ۳) + (۰, ۴) = (۲ + ۰, ۳ + ۴) = (۲, ۷) \equiv_{(۳,۵)} (۲, ۲).$$

$(۲, ۲)$ زوج نمایش دهندهٔ ۲ می‌باشد و در حقیقت داریم $۸ + ۹ \equiv_{۱۵} ۲$.

به طور مشابه اگر $(۲,۳)$ را در $(۰,۴)$ به پیمانهٔ ۳ در مؤلفهٔ اول و به پیمانهٔ ۵ در مؤلفهٔ دوم ضرب کنیم، داریم

$$(۲,۳) \times (۰,۴) = (۲ \times ۰, ۳ \times ۴) = (۰, ۱۲) \equiv_{(۳,۵)} (۰,۲).$$

$(۰,۲)$ زوج نمایش دهندهٔ ۱۲ می‌باشد و در حقیقت $۸ \times ۹ \equiv_{۱۵} ۱۲$.

قضیهٔ باقیماندهٔ چینی کامل می‌گوید که زوج $(m$ به پیمانهٔ m, b به پیمانهٔ $a)$ متناظر با m به پیمانهٔ ab است و

$$\begin{aligned}(m \text{ به پیمانه } a, m \text{ به پیمانه } b) + (n \text{ به پیمانه } a, n \text{ به پیمانه } b) \\ \equiv_{(a,b)} \quad (m+n \text{ به پیمانه } a, m+n \text{ به پیمانه } b)\end{aligned}$$

و

$$\begin{aligned}(m \text{ به پیمانه } a, m \text{ به پیمانه } b) \times (n \text{ به پیمانه } a, n \text{ به پیمانه } b) \\ \equiv_{(a,b)} \quad (mn \text{ به پیمانه } a, mn \text{ به پیمانه } b)\end{aligned}$$

این مطلب به سادگی از جمع و ضرب همنهشتیها نتیجه می‌شود.

$$\begin{aligned} m \text{ به پیمانه } a &\equiv_a m, \\ n \text{ به پیمانه } a &\equiv_a n. \end{aligned}$$

بنابراین با جمع کردن همنهشتیها داریم

$$m \text{ به پیمانه } a + n \text{ به پیمانه } a \equiv_a m+n.$$

به طور مشابه برای جمع به پیمانهٔ b و برای ضرب به پیمانهٔ a و به پیمانهٔ b می‌توان عمل کرد. □

این نسخه از قضیه نشان می‌دهد که زوجهای $(n$ به پیمانهٔ n, b به پیمانهٔ $a)$ نه تنها در تناظر یک به یک با n های به پیمانهٔ ab هستند بلکه تحت + و × به پیمانهٔ (a,b) نیز همان طور رفتار می‌کنند.

عناصر معکوس‌پذیر

قضیهٔ باقیماندهٔ چینی مدرن تصویر بسیار واضحی از $(\frac{\mathbb{Z}}{ab\mathbb{Z}})^{\times}$ متشکل از همهٔ عناصر معکوس پذیرتحت ضرب به پیمانهٔ ab ارائه می‌کند.

همان گونه که هم‌اکنون دیدیم وقتی $\gcd(a,b) = ۱$، عدد n به پیمانهٔ ab همانند زوج (n به پیمانهٔ n, b به پیمانهٔ a) در پیمانهٔ (a,b) رفتار می‌کند. بالاخص، n به پیمانهٔ ab معکوس دارد فقط و فقط وقتی که n به پیمانهٔ a و نیز به پیمانهٔ b معکوس داشته باشد.

مثال. عناصر معکوس‌پذیر به پیمانهٔ ۱۵.

این اعداد، n هایی هستند که زوج باقیماندهٔ آنها به پیمانهٔ $(۳,۵)$ معکوس دارند. چون ۳ و ۵ اول هستند، این اعداد دقیقاً زوجهایی هستند که در آنها هم n به پیمانهٔ ۳ و هم n به پیمانهٔ ۵ ناصفر هستند.

دو عنصر غیر صفر به پیمانهٔ ۳ (یعنی ۱ و ۲) و چهار عنصر غیر صفر به پیمانهٔ ۵ (یعنی ۱، ۲، ۳ و ۴) وجود دارد. از این رو

$$۲ \times ۴ = ۸$$

زوج (n به پیمانهٔ $n, ۵$ به پیمانهٔ ۳) از عناصر غیر صفر وجود دارد و لذا هشت عنصر معکوس پذیرمانند n به پیمانهٔ ۱۵ داریم. این اعداد را می‌توان از روی جدول بخش ٦.۹ خواند که ۱، ۲، ۴، ۷، ۸، ۱۱، ۱۳ و ۱۴ هستند؛ اعدادی که در زوجهای متناظر آنها صفر ظاهر نشده است.

این موضوع به قضیهٔ کلیدی تابع φ-اویلر تعمیم می‌یابد.

خاصیت ضربی φ. وقتی $\gcd(a,b) = ۱$ داریم $\varphi(ab) = \varphi(a)\varphi(b)$.

برهان. بنابر محک معکوسها در بخش ٦.۳، تعداد عناصر معکوس‌پذیر به پیمانهٔ a برابر $\varphi(a)$ و تعداد عناصر معکوس‌پذیر به پیمانهٔ b برابر $\varphi(b)$ است. بنابراین اگر $\gcd(a,b) = ۱$ آنگاه $\varphi(a)\varphi(b)$ زوج معکوس‌پذیر مانند (n به پیمانهٔ n, b به پیمانهٔ a) داریم؛ یعنی $\varphi(a)\varphi(b)$ عنصر معکوس‌پذیر به پیمانهٔ ab. اما

تعداد عناصر معکوس‌پذیر به پیمانهٔ ab برابر $\varphi(ab)$ است. از این رو اگر $\gcd(a,b)=۱$ آنگاه

$$\varphi(ab)=\varphi(a)\varphi(b). \ \square$$

تمرینها

با تشکر از خاصیت ضربی، می‌توانیم جست و جوی خود را برای یافتن فرمولی صریح برای $\varphi(n)$ که در تمرینهای بخش ۶.۳ شروع شده بود تکمیل کنیم.

۱.۷.۹ با استفاده از تمرین ۳.۶.۳ نشان دهید $\varphi(n)=n(۱-\frac{۱}{p_۱})\cdots(۱-\frac{۱}{p_k})$ که در آن $p_۱$، ...، p_k مقسوم‌علیه‌های اول متمایز n هستند.

۲.۷.۹ از این فرمول استفاده کنید و نشان دهید که $\varphi(۶۰)=۱۶$.

۸.۹ برهان تقابل مربعی

فرمولی برای $\left(\frac{p}{q}\right)$ و $\left(\frac{q}{p}\right)$

حال فرمولی را که به طور همزمان $\left(\frac{p}{q}\right)$ و $\left(\frac{q}{p}\right)$ را به صورت حاصل ضربی از زوجهای به پیمانهٔ (p,q) نمایش می‌دهد ارائه می‌کنیم. از این فرمول استفاده می‌شود تا تقابل مربعی با پیگیری استدلال روسو[۱۳] (۱۹۹۱) در زیر اثبات شود.

اگر p و q اعداد اول فرد متفاوتی باشند، عناصر معکوس‌پذیر به پیمانهٔ pq را در نظر می‌گیریم که نه بر p بخش‌پذیرند و نه بر q. عناصر معکوس‌پذیر به

[۱۳] Rousseau

پیمانهٔ pq مانند x در فاصلهٔ $\frac{pq-1}{2} \geq x \geq 1$ که به پیمانهٔ p محاسبه شوند عبارتند از $\frac{q-1}{2}$ بار عددهای ۱، ۲، ...، $p-1$ همراه با نیم‌دنبالهٔ ۱، ۲، ...، $\frac{p-1}{2}$ غیر از اعداد q، $2q$، ...، $\frac{p-1}{2}q$ که در این فاصله قرار گرفته‌اند[14].

بنابراین حاصل ضرب این x های معکوس‌پذیر که به پیمانهٔ p محاسبه شود عبارت است از

$$\prod_{1 \leq x \leq \frac{pq-1}{2}}^{x\ \text{معکوس‌پذیر}} x \equiv_p \frac{(p-1)!^{\frac{q-1}{2}} (\frac{p-1}{2})!}{q^{\frac{p-1}{2}} (\frac{p-1}{2})!}$$

$$\equiv_p (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right),$$

زیرا می‌توان $(\frac{p-1}{2})!$ را حذف کرد و بنابر قضیهٔ ویلسون داریم $(p-1)! \equiv_p -1$ و همچنین بنابر محک اویلر داریم $q^{\frac{p-1}{2}} \equiv_p \left(\frac{q}{p}\right)$.

به طور مشابه اگر حاصل ضرب این x های معکوس‌پذیر را به پیمانهٔ q

---

[14] برای آن که موضوع بهتر روشن شود اجازه دهید که یک مثال عددی را بررسی کنیم. اگر مثلاً $p = 13$ و $q = 7$ آنگاه در بین اعداد ۱ تا $\frac{13\times 7-1}{2} = 45$ آنهایی که به پیمانهٔ 7×13 معکوس‌پذیرند عبارتند از همهٔ اعداد بین ۱ تا ۴۵ غیر از ۷، ۱۳، ۱۴، ۲۱، ۲۶، ۲۸، ۳۵، ۳۹ و ۴۲. پس باید از بین اعداد ۱ تا ۴۵ مضارب ۷ و ۱۳ را کنار بگذاریم. ابتدا همهٔ اعداد را به پیمانهٔ ۱۳ می‌نویسیم و سپس اعداد اضافی را کنار می‌گذاریم. پس در ابتدا همهٔ اعداد ۱ تا ۴۵ را در نظر می‌گیریم. از بین این اعداد $\frac{q-1}{2} = 3$ دسته جدا می‌کنیم. دستهٔ اول ۱ تا ۱۳، دستهٔ دوم ۱۴ تا ۲۶ و دستهٔ سوم ۲۷ تا ۳۹. می‌دانیم که عددهای ۱۳، ۲۶ و ۳۹ باید کنار گذاشته شوند. پس اعداد ۱ تا ۱۲ و اعداد ۱۴ تا ۲۵ و اعداد ۲۷ تا ۳۸ را داریم. تعداد این دسته‌ها برابر $\frac{q-1}{2}$ است و هر سه دسته به پیمانهٔ ۱۳ یکی هستند. پس $\frac{q-1}{2}$ بار اعداد ۱ تا $p - 1 = 12$ را داریم. اکنون اعداد ۴۰ تا ۴۵ نیز باقی مانده‌اند که به پیمانهٔ ۱۳ همان اعداد ۱ تا $\frac{p-1}{2} = 6$ هستند. پس حاصل ضرب اعداد معکوس‌پذیر به پیمانهٔ 7×13 برابر است با حاصل ضرب ۳ بار از اعداد ۱ تا ۱۲ همراه با یک بار اعداد ۱ تا ۶. فراموش نکرده‌ایم که باید مضارب q را که تعداد آنها ۶ تا بود کنار بگذاریم. خلاصه آن که حاصل ضرب اعداد معکوس‌پذیر به پیمانهٔ 7×13 که به پیمانهٔ ۱۳ محاسبه شده‌اند برابر

$$\frac{(1 \times 2 \times \ldots \times 12)^3 \times (1 \times 2 \times \ldots \times 6)}{7 \times 14 \times 21 \times 28 \times 35 \times 42}.$$

می‌باشد. (م)

محاسبه کنیم داریم

$$\prod_{\substack{۱\le x\le \frac{pq-۱}{۲}}}^{x \text{ معکوس‌پذیر}} x \equiv_q (-۱)^{\frac{p-۱}{۲}} \left(\frac{p}{q}\right).$$

بنابراین حاصل ضرب زوجهای (x,x) به پیمانهٔ (p,q) عبارت است از

$$\prod_{\substack{۱\le x\le \frac{pq-۱}{۲}}}^{x \text{ معکوس‌پذیر}} (x,x) \equiv_{(p,q)} \left((-۱)^{\frac{q-۱}{۲}}\left(\frac{q}{p}\right), (-۱)^{\frac{p-۱}{۲}}\left(\frac{p}{q}\right)\right) \qquad (۱)$$

تکمیل برهان

حال $\prod(x,x)$ را روی x های معکوس‌پذیر به روشی دیگر و صرفاً بر حسب توانهای ۱− ارزیابی می‌کنیم. با استفاده از قضیهٔ باقیماندهٔ چینی این حاصل ضرب را به عنوان حاصل ضربی از زوجهای (a,b) که a و b به طور مستقل روی فاصله‌هایی مناسب تغییر می‌کنند تلقی می‌کنیم.

به ازای هر x در فاصلهٔ $q \le x \le \frac{pq-۱}{۲}$ دقیقاً یکی از دو عدد $\{x,-x\}$ (به پیمانهٔ pq) در شرط $۱ \le x \le pq-۱$ صدق می‌کند. از این رو زوج باقیمانده‌های متناظر، یعنی

$$(a,b) = (x \text{ به پیمانه } q, x \text{ به پیمانه } p)$$

دقیقاً شامل یکی از دو عدد $\{(a,b),(-a,-b)\}$ می‌باشد. دقیقاً یکی از هر عضو را به پیمانهٔ (p,q) با شرط $۱ \le a \le p-۱$ و $q \le b \le \frac{q-۱}{۲}$ در نظر می‌گیریم. این کار علامت را نامشخص می‌سازد اما به هر حال داریم

$$\prod_{\substack{۱\le x\le \frac{pq-۱}{۲}}}^{x \text{ معکوس‌پذیر}} (x,x) \equiv_{(p,q)} \pm\left((p-۱)!^{\frac{q-۱}{۲}}, \left(\left(\frac{q-۱}{۲}\right)!\right)^{p-۱}\right) \qquad (۲)$$

چون هر مقدار a در $\frac{q-۱}{۲}$ زوج اتفاق می‌افتد و هر مقدار b در $p-۱$ زوج. با تشکر از قضیهٔ ویلسون می‌توانیم توان فاکتوریلها را در (۲) به صورت توانهایی از -۱ بیان کنیم.

چون $(p-۱)! \equiv_p -۱$، مؤلفهٔ اول، همنهشت با $(-۱)^{\frac{q-۱}{۲}}$ به پیمانهٔ p می‌باشد. برای یافتن $(\frac{q-۱}{۲})!$ به پیمانهٔ q همانند بخش ۵.٦ از $(q-۱)! \equiv_q -۱$ استفاده می‌کنیم:

$$\begin{aligned} -۱ &\equiv_q (q-۱)! \\ &\equiv_q ۱ \times ۲ \times \ldots \times (\frac{q-۱}{۲}) \times (-\frac{q-۱}{۲}) \times \ldots \times (-۲)(-۱) \\ &\equiv_q ((\frac{q-۱}{۲})!)^۲ (-۱)^{\frac{q-۱}{۲}}. \end{aligned}$$

بنابراین

$$((\frac{q-۱}{۲})!)^۲ \equiv_q (-۱)(-۱)^{\frac{q-۱}{۲}}.$$

اگر طرفین را به توان $\frac{p-۱}{۲}$ برسانیم، مؤلفهٔ دوم (۲) را به دست می‌آوریم

$$((\frac{q-۱}{۲})!)^{p-۱} \equiv_q (-۱)^{\frac{p-۱}{۲}}(-۱)^{\frac{p-۱}{۲}.\frac{q-۱}{۲}}.$$

لذا عبارت (۲) برای $\prod(x,x)$ به پیمانهٔ (p,q) به صورت

$$\prod_{\substack{۱\le x\le \frac{pq-۱}{۲} \\ x \text{ معکوس‌پذیر}}} (x,x) \equiv_{(p,q)} \pm((-۱)^{\frac{q-۱}{۲}}, (-۱)^{\frac{p-۱}{۲}}(-۱)^{\frac{p-۱}{۲}.\frac{q-۱}{۲}}) \qquad (۳)$$

تحویل می‌شود. با مساوی قرار دادن (۳) و (۱) داریم

$$\left(\frac{q}{p}\right) = ۱, \qquad \left(\frac{p}{q}\right) = (-۱)^{\frac{p-۱}{۲}.\frac{q-۱}{۲}}$$

یا

$$\left(\frac{q}{p}\right) = -۱, \qquad \left(\frac{p}{q}\right) = -(-۱)^{\frac{p-۱}{۲}.\frac{q-۱}{۲}}.$$

در هر حالت داریم

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-۱)^{\frac{p-۱}{۲}.\frac{q-۱}{۲}}. \square$$

تمرینها

به کمک تقابل مربعی می‌توانیم برای هر عدد اول فرد ثابت مانند p، اعداد اولی مانند q را بیابیم که برای آنها p یک مربع کامل به پیمانهٔ q باشد. این اعداد در تعدادی متناهی تصاعد حسابی قرار می‌گیرند (همان طور که قبلاً این مطلب را برای $p=-۱$ و $p=۲$ دیده‌ایم). در اینجا آنچه برای $p=۳$ اتفاق می‌افتد آمده است.

۱.۸.۹ شرح دهید که چرا هر عدد اول فرد مانند q به یکی از صورتهای $۱۲n+۱$، $۱۲n+۵$، $۱۲n+۷$ یا $۱۲n+۱۱$ می‌باشد.

۲.۸.۹ از تقابل مربعی با باقیمانده‌گیری (همانند بخش ۵.۹) استفاده کنید و نشان دهید که ۳ یک مربع کامل به پیمانهٔ q است فقط و فقط وقتی که q عدد اول فردی به صورت $۱۲n+۱$ یا $۱۲n+۱۱$ باشد.

با ضرب کردن مقادیر $\left(\frac{۳}{q}\right)$ (که در تمرین ۲.۸.۹ یافت شد) در مقادیر متناظر $\left(\frac{-۱}{q}\right)$ می‌توانیم مقادیر $\left(\frac{-۳}{q}\right)$ را نیز به دست آوریم:

۳.۸.۹ نشان دهید که -۱ یک مربع کامل به پیمانهٔ q است فقط و فقط وقتی که q عدد اول فردی به صورت $۱۲n+۱$ یا $۱۲n+۵$ باشد. نتیجه بگیرید که -۳ یک مربع کامل به پیمانهٔ q است فقط و فقط وقتی که q عدد اول فردی به صورت $۱۲n+۱$ یا $۱۲n+۷$ باشد.

به طور مشابه می‌توانیم مقادیر $\left(\frac{۵}{q}\right)$ و $\left(\frac{-۵}{q}\right)$ را نیز بیابیم:

۴۸.۹ نشان دهید اعداد اول فردی مانند q که برای آنها ۵ یک مربع کامل است دقیقاً عبارتند از آنهایی که به صورت $۲۰n + ۱$، $۲۰n + ۹$، $۲۰n + ۱۱$ یا $۲۰n + ۱۹$ هستند. با بررسی این مطلب که ۵ یک مربع کامل به پیمانهٔ ۴۱، ۲۹، ۱۱ و ۱۹ است این نتیجه را بیازمایید.

۵۸.۹ نشان دهید اعداد اول فردی مانند q که برای آنها ۵− یک مربع کامل است دقیقاً عبارتند از آنهایی که به صورت $۲۰n + ۱$، $۲۰n + ۳$، $۲۰n + ۷$ یا $۲۰n + ۹$ هستند. با بررسی این مطلب که ۵− یک مربع کامل به پیمانهٔ ۴۱، ۲۳، ۷ و ۲۹ است این نتیجه را بیازمایید.

۹.۹ بحث

همان طور که در چند فصل قبل متذکر شده‌ایم تقابل مربعی در مطالعهٔ اعداد اولِ نمایش داده شده توسط صورتهای مربعی از قبیل $x^۲ + y^۲$ و $x^۲ + ۲y^۲$ و $x^۲ + ۳y^۲$ پدیدار شده است. فرما اولین کسی بود که این سؤالات را مطرح کرد و به آنها پاسخ داد، اما روشهای وی ناشناخته مانده‌اند. تا آنجا که می‌دانیم اویلر اولین کسی بود که نقش تقابل مربعی را تشخیص داد و آن را در حالات خاص اثبات کرد.

اولین کسی که سعی در ارائهٔ اثباتی کلی داشت لژاندر (۱۷۸۵) بود. با این حال برهان وی وابسته به این فرض اثبات نشده بود که هر تصاعد حسابی مانند $an + b$ با شرط $\gcd(a, b) = ۱$ شامل بی‌نهایت عدد اول است. این فرض به سادگی در حالات خاص (از قبیل $۴n + ۱$ و $۴n + ۳$ که در تمرینهای بخش ۳.٦ و ۷.٦ آمده‌اند) اثبات می‌شود اما اثبات قضیهٔ کلی آن سخت‌تر از خود تقابل است. اولین برهان توسط دیریکله (۱۸۳۷) ارائه شد و روش تحلیلی عمیقی که وی برای اثبات آن ارائه کرد هنوز رهیافتی متعارف به اعداد اول در تصاعدهای حسابی است.

گاوس اولین برهان تقابل مربعی را در هجدهم آوریل ۱۷۹۶ (وقتی که حتی ۱۹ سال تمام نداشت) یافت. این برهانی طولانی و نازیباست و در آن زمان او آن را در رسالات حسابی خود (۱۸۰۱) منتشر کرد. وی دو برهان دیگر نیز یافته بود؛ یکی با استفاده از صورتهای مربعی و دیگری با استفاده از ریشه‌های واحد. تقابل مربعی قضیهٔ مورد علاقهٔ گاوس بود و روی هم رفته او هشت برهان برای آن ارائه داد. پس از آن ریاضیدانان بسیار دیگری برهانهایی را منتشر کردند. برخی از آنها شکلی دیگر یا ساده‌سازی برهان گاوس بود و بقیه ایده‌هایی جدید را معرفی می‌کردند.

شبیه قضیهٔ فیثاغورس در هندسه، تقابل مربعی قضیه‌ای هسته‌ای در نظریه اعداد است که نشان می‌دهد مهم نیست چگونه با معادله‌های دیوفانتی مربعی برخورد شود. دلیلی برای آن که چرا این قضیه برهانهای زیادی دارد این است که همهٔ راه‌ها به آن ختم می‌شود و هر راه، آن را از زاویه‌ای متفاوت نشان می‌دهد. تاریخچه‌ای جامع از تقابل مربعی، شامل یک جدول و رده‌بندی ۱۹۶ برهان (!) که تا سال ۲۰۰۰ ارائه شده است را می‌توان در لمرمیر[۱۵] (۲۰۰۰) یافت. یک کتاب جالب دیگر، پیپر[۱۶] (۱۹۷۸) است که ۱۴ برهان مختلف را با جزئیات مورد بحث قرار می‌دهد.

قانون تقابل مربعی به قانون تقابل مکعبی، دو مربعی و توانهای بالاتر تعمیم می‌یابد. درست همانند مشخصهٔ مربعی که مقادیر ± 1 (ریشه‌های دوم ۱) را می‌پذیرد، یک مشخصهٔ مکعبی[۱۷] با مقادیر ۱، ζ_3، ζ_3^2 (ریشه‌های سوم ۱) و یک مشخصهٔ دومربعی[۱۸] با مقادیر ± 1، $\pm i$ (ریشه‌های چهارم ۱) وجود دارد. این تعمیمها ساخته نشده‌اند به دلیل آن که ریاضیدانان از این که چیزی دربارهٔ صورتهای مربعی بگویند خسته شده بودند - و کاملاً برعکس آن؛ خود صورتهای مربعی، مطالعه در مورد صورتهای مکعبی و دومربعی را می‌طلبد. این

[۱۵] Lemmermeyer

[۱۶] Pieper

[۱۷] cubic character

[۱۸] biquadratic character

مطلب توسط اویلر کشف شد. وی به احکام زیر (که بعداً توسط گاوس اثبات شد) توجه کرد:

p یک عدد اول به صورت $x^۲ + ۲۷y^۲$ است فقط و فقط وقتی که $p = ۳n + ۱$ و نیز ۲ یک مکعب به پیمانهٔ p باشد؛

p یک عدد اول به صورت $x^۲ + ٦۴y^۲$ است فقط و فقط وقتی که $p = ۴n + ۱$ و نیز ۲ یک توان‌چهارم به پیمانهٔ p باشد.

قانون تقابل مکعبی توسط آیزنشتین (۱۸۴۴) یافت شد که نیازمند تحقیق در $\mathbb{Z}[\zeta_۳]$ است. به همین دلیل است که $\mathbb{Z}[\zeta_۳]$ را اعداد صحیح آیزنشتین می‌نامیم. (تقابل مکعبی قبلاً برای گاوس شناخته شده بود اما وی نتایج خود را منتشر نکرد.) به طور مشابه، تقابل دومربعی توسط گاوس کشف شد که موجب تحقیق در $\mathbb{Z}[i]$ گردید. این در حقیقت هدف گاوس (۱۸۳۲) بود که خواص مقدماتی $\mathbb{Z}[i]$ را برای اولین بار در آنجا منتشر کرد.

به طور مشابه یک قانون تقابل توان n ام با اعداد صحیح $\mathbb{Z}[\zeta_n]$ و همهٔ مشکلات مربوط به آن از قبیل شکست یکتایی تجزیه به اعداد اول که توسط کومر (۱۸۴۴) کشف شد سر و کار دارد. در مورد تقابل توان n ام (متفاوت با آنچه در مورد قضیهٔ آخر فرما اتفاق افتاد) کومر به طور کامل بر این مشکلات به وسیلهٔ نظریهٔ اعداد ایده‌آلی خود فائق آمد و یک قانون تقابل توان n ام را در ۱۸۵۰ منتشر کرد. آیزنشتین نیز با استفاده از نظریهٔ اعداد ایده‌آلی کومر نسخه‌ای متفاوت از تقابل توان n ام را در همان سال منتشر کرد. یک برهان مدرن برای قانون تقابل آیزنشتین را می‌توان در ایرلند[۱۹] و روسن[۲۰] (۱۹۸۲)، صفحات ۲۱۵ تا ۲۱۸ یافت و تاریخچهٔ همهٔ قانونهای تقابل تا سال ۱۸۵۰ را می‌توان در لمرمیر (۲۰۰۰) پیدا کرد.

---

[۱۹] Ireland
[۲۰] Rosen

۱۰

حلقه‌ها

پیش‌نگاه

این فصل بسیاری از ساختارهای جبری که در این کتاب با آنها مواجه شده‌ایم (از قبیل اعداد صحیح، اعداد صحیح به پیمانهٔ p، و انواع مختلف توسیع مفاهیم اعداد صحیح توسط گاوس، آیزنشتین و هرویتز) را در یک مفهوم مجرد به نام حلقه وحدت می‌بخشد.

با مفهوم کلی حلقه که توسط اصولی خاص برای $+$ و $\times$ معین می‌شود شروع می‌کنیم و مشاهده می‌کنیم که چگونه این اصول برای به دست آوردن مفاهیم کلی تقسیم‌پذیری، اعداد اول و یکه‌ها کافی است. مفهوم میدان (حلقه‌ای که در آن همهٔ عناصر غیر صفر یکه هستند) به طور خلاصه بحث شده است و مثالهای اصلی $\mathbb{Q}$، $\mathbb{R}$، $\mathbb{C}$ و $\frac{\mathbb{Z}}{p\mathbb{Z}}$ بازنگری گردیده‌اند.

سپس بحث خود را روی اعداد صحیح جبری و بالاخص اعداد صحیح مربعی متمرکز می‌کنیم. اعداد جبری و اعداد صحیح جبری را تعریف می‌کنیم و روش جبرخطی گونهٔ ددکیند را به کار می‌بریم تا نشان دهیم که اعداد صحیح جبری تحت $+$، $-$ و $\times$ بسته هستند و لذا یک حلقه را تشکیل می‌دهند.

حالت خاص حلقه‌های اعداد صحیح مربعی و میدانهای مربعی $\mathbb{Q}[\sqrt{d}]$ (که شامل آن است) با جزئیات بیشتر آزموده شده‌اند. توضیحی کلی در مورد پدیدهٔ اعداد صحیح مربعی مانند $\frac{-۱+\sqrt{-۳}}{۲}$ را که کسری به نظر می‌رسند با تعیین اعداد صحیح همهٔ میدانهایی مانند $\mathbb{Q}[\sqrt{d}]$ برای d یی صحیح ارائه می‌دهیم.

مفهوم نرم که قبلاً در حالتهای خاص دیده شد در تعریفی یکنواخت روی همهٔ میدانهای مربعی ارائه شده است. سرانجام میدانهای مربعی موهومی ($\mathbb{Q}[\sqrt{d}]$ برای d های صحیح منفی) را به طور خاص‌تر مورد بررسی قرار می‌دهیم. این میدانها واجد خواصی هستند که نسبت به $\mathbb{Q}[\sqrt{d}]$ برای d ی مثبت ساده‌تراند. مثلاً اعداد صحیح یک میدان مربعی موهومی فقط شامل تعدادی متناهی (حداکثر شش تا) یکه می‌باشد.

۱.۱۰ اصول حلقه

اعداد صحیح $\mathbb{Z}$ با اعمال $+$ و $\times$ اولین حلقه‌ای است که در ریاضیات مطالعه شده است. برخی خواص مقدماتی $\mathbb{Z}$ به عنوان خواص تعریف کنندهٔ (اصول موضوع) حلقه‌ها در حالت کلی در نظر گرفته شده‌اند. این خواص را به طور خلاصه در بخش ۳.۱ در مورد گروههای آبلی متذکر شدیم. برای هر سه عدد صحیح مانند a، b و c داریم

$$a+(b+c) = (a+b)+c \qquad \text{قانون شرکت‌پذیری}$$

$$a+b = b+a \qquad \text{قانون تعویض‌پذیری}$$

$$a+(-a) = 0 \qquad \text{خاصیت معکوس جمعی}$$

$$a+0 = a \qquad \text{خاصیت همانی ۰}$$

مجموعهٔ مشابهی از قواعد وجود دارد که رفتار $\times$ را توصیف می‌کند.

$$a\times(b\times c) = (a\times b)\times c \qquad \text{قانون شرکت‌پذیری}$$

قانون تعویض‌پذیری	$a \times b = b \times a$
خاصیت همانی ۱	$a \times ۱ = a$
خاصیت ۰	$a \times ۰ = ۰$

و سرانجام قاعده‌ای برای تأثیر متقابل $+$ و $\times$ وجود دارد:

قانون توزیع‌پذیری	$a \times (b + c) = a \times b + a \times c$

به بیان دقیق، اینها خواص تعریف کنندهٔ یک حلقهٔ تعویض‌پذیر هستند. گاهی با حلقه‌های غیر تعویض‌پذیر مانند چهارگانهای $\mathbb{H}$ نیز سر و کار داریم که در تمام اصول فوق غیر از قانون تعویض‌پذیری برای $\times$ صدق می‌کنند. با این حال چهارگانها از نظر داشتن نرم ضربی به حلقه‌های اعداد نزدیک‌ترند و در حالت کلی نظریهٔ حلقه‌های غیر تعویض‌پذیر طعمی نسبتاً متفاوت دارد.

منصفانه است اگر بگوییم که نظریهٔ حلقه‌ها اکثراً با اشیائی سر و کار دارد که رفتاری شبیه اعداد صحیح دارند و مثال $\mathbb{Z}$ به ما کمک می‌کند تا پیش‌بینی کنیم که چه مفاهیمی مناسب هستند و در مواجه شدن با اشیاء ناآشنا اما شبیه اعداد صحیح، مثالی مفید خواهد بود. در حقیقت قبلاً کلمهٔ صحیح را برای توسیعهایی از $\mathbb{Z}$ همچون $\mathbb{Z}[\mathbf{i}]$ (اعداد صحیح گاوسی)، $\mathbb{Z}[\zeta_۳]$ (اعداد صحیح آیزنشتین) و $\mathbb{Z}[\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲}, \mathbf{i}, \mathbf{j}, \mathbf{k}]$ (اعداد صحیح هرویتز) استفاده کرده‌ایم.

تقسیم‌پذیری و اعداد اول

در مثالهای اعداد صحیح تعمیم‌یافته، اهمیت مفاهیم تقسیم‌پذیری و اعداد اول در اعداد صحیح معمولی را دیده‌ایم. در یک حلقهٔ دلخواه، گوییم b عضو a را عاد می‌کند هرگاه عضوی مانند c موجود باشد به قسمی که

$$a = bc.$$

روش دیگر برای گفتن این مطلب این است که بگوییم a توسط b عاد می‌شود، b مقسوم‌علیهی از a است یا این که بگوییم a مضربی از b می‌باشد. عادپذیری، مفهومی جالب در $\mathbb{Z}$ است چرا که یک عدد صحیح دلخواه مانند a در حالت کلی توسط عدد صحیح دلخواه دیگر مانند b عاد نمی‌شود. در حقیقت به سختی می‌توان تصمیم گرفت که اصلاً a مقسوم‌علیهی غیر از ± 1 و $\pm a$ که بدیهی هستند دارد یا نه. یک عدد صحیح معمولی که هیچ مقسوم‌علیه غیر بدیهی ندارد اول نامیده می‌شود. در یک حلقهٔ دلخواه مانند R، مفهوم عدد اول همین است با این تفاوت که به جای ± 1 یکه‌های R قرار دارد؛ یعنی عناصری از R که ۱ را عاد می‌کنند (یا به طور معادل، عناصر معکوس‌پذیر R). لذا $a \in R$ را اول می‌نامیم اگر a فقط عدد توسط یکه‌ها و مضارب یکهٔ a (که شریکهای[۱] a نامیده می‌شوند) عاد شود.

حتی در $\mathbb{Z}$ اعداد اول الگوی روشنی را تشکیل نمی‌دهند و البته اعداد اول، بسیاری از مسائل حل نشدهٔ کلاسیک را در مورد $\mathbb{Z}$ به وجود می‌آورند. لذا گسترش نظریهٔ حلقه‌ها عمیقاً تحت نفوذ مسألهٔ درک اعداد اول است. تمایل بر این است که بهترین حلقه‌های درک شده همچون $\mathbb{Z}[i]$ آنهایی هستند که اعداد اولشان رفتاری مانند اعداد اول در $\mathbb{Z}$ دارند. در برخی حلقه‌ها که چنین نیست (به بیان مشخص، آنهایی که منحصر به فرد بودن تجزیه به اعداد اول با شکست مواجه می‌شود) دریافته‌اند که خلق ایده‌آلهای اول که بهتر از اعداد اول واقعی رفتار می‌کنند ارزشمند است. در فصلهای ۱۱ و ۱۲ داستان این ایده‌آلهای اول را تعریف می‌کنیم.

---
[۱] associates

تمرینها

از فصل ۸ یادآوری می‌کنیم که چهارگانهای $\mathbb{H}$ ماتریسهای ۲ × ۲ ی خاصی هستند. در حقیقت مفاهیم حلقه‌های (غیر تعویض‌پذیر) در این جهت بیشتر توسیع می‌یابند تا به حلقهٔ ماتریسهای $n \times n$ (برای عدد طبیعی ثابتی مانند n) برسیم.

برای لحظه‌ای همهٔ چنین ماتریسهایی با درایه‌های مختلط را همراه با ماتریس ۰ و ماتریس همانی ۱ در نظر می‌گیریم.

۱.۱.۱۰ بررسی کنید که اصول + برقرار است.

۲.۱.۱۰ بررسی کنید که اصول × غیر از قانون تعویض‌پذیری (در حالت ۲ ≤ n) برقرار است. نیازی نیست که از ضرب صریح برای اثبات قانون شرکت پذیری استفاده کنید. چرا؟

۳.۱.۱۰ بررسی کنید که قانون توزیع پذیری برقرار است.

۲.۱۰ حلقه‌ها و میدانها

مجموعه‌های $\mathbb{Q}$ (اعداد گویا)، $\mathbb{R}$ (اعداد حقیقی) و $\mathbb{C}$ (اعداد مختلط) نیز حلقه هستند زیرا به طور بدیهی خواص +، − و × را که در بخش قبل فهرست شده است دارند. این مطلب غافلگیر کننده نیست چون $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ همواره قصد دارند که مفهوم اعداد صحیح را با حفظ همهٔ خواص حلقه و چیزهایی اضافی توسیع دهند. چیزی که $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ دارند و $\mathbb{Z}$ ندارد وجود معکوس ضربی، یعنی a^{-1}، برای هر عنصر ناصفر مانند a است که دارای خاصیت $aa^{-1} = 1$ می‌باشد. یک حلقهٔ تعویض‌پذیر که در آن هر عنصر غیر صفر معکوس ضربی داشته باشد میدان نامیده می‌شود.

میدانها نمونهٔ واقعی حلقه‌ها نیستند و نظریهٔ آنها طعم کاملاً متفاوتی با نظریهٔ حلقه‌ها دارد. بالاخص، عادپذیری مفهومی جالب در یک میدان نیست زیرا یک عنصر ناصفر مانند b هر عنصر مانند a را (به وسیلهٔ خارج قسمت $\frac{a}{b} = ab^{-۱}$) عاد می‌کند. به طور مشابه، مفهوم یکه جالب نیست چون همهٔ عناصر غیر صفر یک میدان، یکه هستند. علی رغم این، میدانها نقشی مهم را در نظریهٔ حلقه‌ها ایفا می‌کنند. بسیاری از حلقه‌هایی که در فصلهای قبلی استفاده کردیم (همانند $\mathbb{Z}[\mathrm{i}]$، $\mathbb{Z}[\sqrt{-۲}]$ و $\mathbb{Z}[\zeta_۳]$) در میدان اعداد مختلط می‌نشینند. چون $\mathbb{C}$ همهٔ خواص حلقه (قانون شرکت پذیری، تعویض پذیری و غیره) را دارد، همین خواص برای هر زیرمجموعه مانند R از $\mathbb{C}$ که در آن $a+b$، $-a$ و $a \times b$ (که در اصول حلقه ذکر می‌شوند) مفهوم داشته باشد برقرار است. یعنی یک مجموعه مانند $R \subseteq \mathbb{C}$ یک حلقه است مشروط بر آن که R تحت $+$، $-$ و $\times$ بسته باشد. این بدان معنی است که برای هر $a, b \in R$ داشته باشیم $a+b, a-b, a \times b \in R$.

حلقه‌هایی که هم‌اکنون گفته شد فرآیند بسته کردن یک مجموعه تحت اعمال $+$، $-$ و $\times$ را با مثال می‌فهماند. در این مثالها عددی مانند a را که در $\mathbb{Z}$ نیست در نظر می‌گیریم و $\mathbb{Z} \cup \{a\}$ را با تشکیل همهٔ جمعها، تفاضلها و حاصل ضربهای ممکنی که a و اعداد صحیح در آنها ظاهر شده است، بسته می‌سازیم. ماحصل این کار، حلقهٔ $\mathbb{Z}[a]$ نامیده می‌شود.

سپس اگر عنصری مانند b را بگیریم که در $\mathbb{Z}[a]$ نیست و فرآیند بسته کردن تحت $+$، $-$ و $\times$ را تکرار کنیم، حلقهٔ حاصل $\mathbb{Z}[a,b]$ نامیده می‌شود؛ و به همین ترتیب. این مطلب با نمادهایی که قبلاً برای حلقه‌های $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ و $\mathbb{Z}[\frac{۱+\mathbf{i}+\mathbf{j}+\mathbf{k}}{۲}, \mathbf{i},\mathbf{j},\mathbf{k}]$ از چهارگانهای صحیح به کار بردیم جور در می‌آید. هر زیرمجموعه از چهارگانها که تحت $+$، $-$ و $\times$ بسته باشد یک حلقه است، گرچه در حالت کلی تعویض‌پذیر نیست. (در حقیقت، بدیهی است که هر زیرحلقه از $\mathbb{H}$ که شامل مضارب ناصفر بیش از یکی از $\mathbf{i}$، $\mathbf{j}$، $\mathbf{k}$ باشد غیر تعویض‌پذیر است.)

هنگامی که حلقهٔ ما زیرمجموعه‌ای از $\mathbb{C}$ باشد می‌توانیم بستار آن تحت

تقسیم بر عناصر ناصفر را تشکیل دهیم و یک میدان به دست آوریم. اگر عنصری مانند a که در چنین میدانی مانند F نیست را بگیریم و مجدداً تحت $+$، $-$، $\times$ و $\div$ (بر عناصر غیر صفر) بسته سازیم آنگاه ماحصل را با $F(a)$ نمایش می‌دهیم. گهگاه این نماد پرانتز را برای میدانهایی چون $\mathbb{Q}(\sqrt{۲})$ به کار می‌بریم، گرچه در حقیقت در اینجا داریم $\mathbb{Q}(\sqrt{۲})= Q[\sqrt{۲}]$.

حلقه‌های متناهی و میدانها

حلقه‌های متناهی صریحاً در بخش ۲.۳ آمد که در آنجا نماد $\frac{\mathbb{Z}}{n\mathbb{Z}}$ را برای مجموعهٔ رده‌های همنهشتی به پیمانهٔ n تحت اعمال $+$ و $\times$ معرفی کردیم. در آن زمان هیچ توضیحی برای این مطلب ندادیم اما به سادگی دیده می‌شود که $\frac{\mathbb{Z}}{n\mathbb{Z}}$ یک حلقه است. خواص حلقه‌ای آن از والدش، یعنی حلقهٔ $\mathbb{Z}$ به ارث می‌رسد. مثلاً عمل $+$ روی رده‌های همنهشتی تعویض‌پذیر است چون

$$\begin{aligned}(n\mathbb{Z}+a)+(n\mathbb{Z}+b) &= n\mathbb{Z}+(a+b)\\ &= n\mathbb{Z}+(b+a)\\ &= (n\mathbb{Z}+b)+(n\mathbb{Z}+b).\end{aligned}$$

همچنین در بخش ۳.۳ نشان دادیم هرگاه p اول باشد، آنگاه هر عنصر ناصفر $\frac{\mathbb{Z}}{p\mathbb{Z}}$ معکوس ضربی دارد. لذا حلقهٔ متناهی $\frac{\mathbb{Z}}{p\mathbb{Z}}$ یک میدان است.

یکه‌های حلقهٔ $\frac{\mathbb{Z}}{n\mathbb{Z}}$ به طور ویژه‌ای جالب هستند، چون گروه $(\frac{\mathbb{Z}}{n\mathbb{Z}})^{\times}$ را تشکیل می‌دهند که می‌تواند کاملاً پیچیده باشد. به سادگی دیده می‌شود (تمرین) که یکه‌های هر حلقه یک گروه تشکیل می‌دهند. اگر حلقه غیر تعویض‌پذیر باشد آنگاه ممکن است گروه یکه‌ها غیر تعویض‌پذیر باشد، همان طور که در حالت اعداد صحیح هرویتز در تمرینهای بخش ۵.۸ دیدیم.

همچنین دیدیم که ممکن است گروهی نامتناهی از یکه‌ها داشته باشیم (مثلاً در $\mathbb{Z}[\sqrt{۲}]$). این مطلب در بخش ۴.۵ تصریح شده است.

تمرینها

۱.۲.۱۰ نشان دهید که حاصل ضرب دو یکه در R، یکه‌ای در R است.

۲.۲.۱۰ همچنین نشان دهید که معکوس ضربی یک یکه، عنصری یکه است. از این رو یکه‌های هر حلقه، یک گروه تشکیل می‌دهند.

حلقهٔ $\frac{\mathbb{Z}}{n\mathbb{Z}}$ برای n ی غیر اول از نظر داشتن مقسوم‌علیه صفر (عناصر غیر صفر که حاصل ضرب آنها صفر است) با $\mathbb{Z}$ فرق دارد.

۳.۲.۱۰ مثالی از یک مقسوم‌علیه صفر در $\frac{\mathbb{Z}}{۴\mathbb{Z}}$ ارائه دهید.

۴.۲.۱۰ توضیح دهید که چرا برای هر n غیر اول، $\frac{\mathbb{Z}}{n\mathbb{Z}}$ مقسوم‌علیه صفر دارد.

مقسوم‌علیه‌های صفر، ما را از توسیع $\frac{\mathbb{Z}}{n\mathbb{Z}}$ به یک میدان توسط الحاق کسرها (به گونه‌ای که مثلاً $\mathbb{Z}$ را به $\mathbb{Q}$ توسیع دادیم) باز می‌دارد.

۵.۲.۱۰ اگر a یک مقسوم‌علیه صفر در $\frac{\mathbb{Z}}{n\mathbb{Z}}$ باشد، نشان دهید که نمی‌توانیم به طور مستحکم عنصری چون $a^{-۱}$ را به آن ملحق کنیم که $aa^{-۱} = ۱$ در $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

۳.۱۰ اعداد صحیح جبری

اعداد جبری

بسیاری از مفاهیم نظریهٔ حلقه‌ها از نظریهٔ اعداد صحیح جبری ددکیند سرچشمه می‌گیرد. ددکیند ایدهٔ نشاندن اعداد صحیح معمولی در میدان اعداد گویا را توسط نشاندن حلقه‌های متنوعی از اعداد صحیح جبری در میدان اعداد جبری تعمیم داد.

تعریف. یک عدد مانند $\alpha \in \mathbb{C}$ جبری است هرگاه

$$a_m\alpha^m + a_{m-۱}\alpha^{m-۱} + \ldots + a_۱\alpha + a_۰ = ۰$$

که در آن $a_۰, a_۱, \ldots, a_m \in \mathbb{Z}$. این عدد از درجهٔ m است اگر در هیچ معادله‌ای به این شکل از درجهٔ کمتر صدق نکند.

مثالها عبارتند از

- اعداد گویا، که اعداد جبری از درجهٔ ۱ هستند،
- $\sqrt{۲}$، که از درجهٔ ۲ است چون در معادلهٔ $x^۲ - ۲ = ۰$ صدق می‌کند اما در هیچ معادله‌ای از درجهٔ کمتر صدق نمی‌کند (چون $\sqrt{۲}$ اصم است).

مجموعهٔ همهٔ اعداد جبری (همانند اعداد گویا) یک میدان است، گرچه این مطلب بدیهی نیست. حتی واضح نیست که اعداد جبری تحت + بسته هستند. مثلاً

$\sqrt[۳]{۲}$ در $x^۳ - ۲ = ۰$ صدق می‌کند و از این رو جبری است،
$\sqrt[۵]{۳}$ در $x^۵ - ۳ = ۰$ صدق می‌کند و از این رو جبری است،
اما معادله‌ای که $\sqrt[۳]{۲} + \sqrt[۵]{۳}$ در آن صدق می‌کند کدام است؟

در اینجا اثبات نمی‌کنیم که اعداد جبری یک میدان تشکیل می‌دهند اما می‌توانیم نشان دهیم که $\sqrt[3]{۲}+\sqrt[5]{۳}$ در یک معادلهٔ چندجمله‌ای با ضرایب صحیح صدق می‌کند. این مطلب از آنچه می‌خواهیم در مورد اعداد صحیح جبری اثبات کنیم نتیجه می‌شود که تعریف آن را از بخش ۴.۷ یادآوری می‌کنیم.

تعریف. یک عدد مانند $\alpha\in\mathbb{C}$ یک عدد صحیح جبری است هرگاه در یک معادلهٔ چندجمله‌ای تکین با ضرایب صحیح، یعنی

$$\alpha^m + a_{m-۱}\alpha^{m-۱} + \ldots + a_۱\alpha + a_۰ = ۰$$

که در آن $a_۰, a_۱, \ldots, a_{m-۱}\in\mathbb{Z}$ صدق کند.

مثالها عبارتند از

- اعداد صحیح معمولی، که اعداد صحیح جبری از درجهٔ ۱ هستند،
- $\sqrt[3]{۲}$ و $\sqrt[5]{۳}$، زیرا به ترتیب در چندجمله‌ایهای تکین $x^۲-۲=۰$ و $x^۵-۳=۰$ صدق می‌کنند،
- $\frac{-۱+\sqrt{-۳}}{۲}$، زیرا در $x^۲+x+۱=۰$ صدق می‌کند.

از طرف دیگر همان طور که در بخش ۴.۷ اثبات شد، تنها اعداد صحیح جبری گویا، اعداد صحیح معمولی هستند.

حلقه اعداد صحیح جبری

اعداد صحیح جبری در حلقهٔ $\mathbb{C}$ قرار دارند. از این رو برای آن که نشان دهیم این اعداد یک حلقه تشکیل می‌دهند کافی است اثبات کنیم که تحت $+$، $-$ و $\times$ بسته هستند. این مطلب اولین بار توسط آیزنشتین اثبات شد، اما برهانی مدرن‌تر که توسط ددکیند اثبات شده است را پی می‌گیریم.

خواص بسته بودن اعداد صحیح جبری. اگر α و β اعداد صحیح جبری باشند آنگاه $\alpha+\beta$، $\alpha-\beta$ و $\alpha\beta$ نیز چنین هستند.

برهان. بنابر فرض α و β در معادلات

$$\begin{aligned}\alpha^m + a_{m-1}\alpha^{m-1} + \ldots + a_1\alpha + a_0 &= 0\\ \beta^n + b_{n-1}\beta^{n-1} + \ldots + b_1\beta + b_0 &= 0,\end{aligned}$$

که در آن $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}$ و $b_0, b_1, \ldots, b_{n-1} \in \mathbb{Z}$ صدق می‌کنند.

این معادلات نشان می‌دهند که:

- $\alpha^m = -a_0 - a_1\alpha - \ldots - a_{m-1}\alpha^{m-1}$ ترکیبی خطی از ۱، α، ...، α^{m-1} با ضرایب صحیح است.
- $\alpha^{m+1} = -a_0\alpha - a_1\alpha^2 - \ldots - a_{m-1}\alpha^m$ ترکیبی خطی از ۱، α، ...، α^{m-1} با ضرایب صحیح است (چون α^m را می‌توان بر حسب ۱، α، ...، α^{m-1} نوشت).
- به طور مشابه هر توان α ترکیبی خطی از ۱، α، ...، α^{m-1} با ضرایب صحیح است.
- همچنین به طور مشابه هر توان β ترکیبی خطی از ۱، β، ...، β^{n-1} با ضرایب صحیح است.
- بنابراین هر چندجمله‌ای از α و β، ترکیبی خطی از جملاتی مانند $\alpha^i\beta^j$ است که $0 \le i \le m-1$ و $0 \le j \le n-1$.

لذا اگر همهٔ mn حاصل ضرب $\alpha^i\beta^j$ را با ω_1، ω_2، ...، ω_{mn} نمایش دهیم می‌توانیم هر چندجمله‌ای مانند ω از α و β با ضرایب صحیح را به صورت ترکیبی خطی از ω_1، ω_2، ...، ω_{mn} با ضرایب صحیح بنویسیم. بالاخص، اگر ω هر یک از $\alpha+\beta$، $\alpha-\beta$ یا $\alpha\beta$ باشد، داریم

$$\omega = k_1\omega_1 + \ldots + k_{mn}\omega_{mn} \qquad (*)$$

برای k_1، k_2، ...، k_{mn} ی در $\mathbb{Z}$ از این عبارت، mn معادله با mn مجهول ω_1، ω_2، ...، ω_{mn} توسط ضرب کردن (*) در ω_1، ω_2، ...، ω_{mn} و دوباره‌نویسی هر جملهٔ طرف راست به صورت ترکیبی خطی از ω_1، ω_2، ...، ω_{mn} با ضرایب صحیح مانند $k_s^{(t)}$ به دست می‌آید:

$$\begin{aligned}
\omega\omega_1 &= k'_1\omega_1 + \ldots + k'_{mn}\omega_{mn} \\
\omega\omega_2 &= k''_1\omega_1 + \ldots + k''_{mn}\omega_{mn} \\
&\vdots \\
\omega\omega_{mn} &= k_1^{(mn)}\omega_1 + \ldots + k_{mn}^{(mn)}\omega_{mn}
\end{aligned}$$

این معادلات بر حسب ω_1، ω_2، ...، ω_{mn} معادلاتی همگن با جوابی ناصفر می‌باشند. از این رو دترمینان ضرایب آن باید صفر باشد. یعنی

$$\begin{vmatrix}
k'_1 - \omega & k'_2 & \ldots & k'_{mn} \\
k''_1 & k''_2 - \omega & \ldots & k''_{mn} \\
\vdots & \vdots & \vdots & \vdots \\
k_1^{(mn)} & k_2^{(mn)} & \ldots & k_{mn}^{(mn)} - \omega
\end{vmatrix} = 0.$$

این دترمینان یک چندجمله‌ای بر حسب ω با ضرایب در $\mathbb{Z}$ است و ضریب ω^{mn} آن برابر ± 1 می‌باشد. از این رو $\omega = \alpha + \beta, \alpha - \beta$ یا $\alpha\beta$ یک عدد صحیح جبری است. □

تمرینها

بنابر تعریف، در میان اعداد صحیح جبری، یکه‌ها باید ۱ را عاد کنند و از این رو این اعداد، اعدادی صحیح و جبری مانند α هستند که α^{-1} نیز یک عدد صحیح جبری است.

۱.۳.۱۰ نتیجه بگیرید که α یک عدد صحیح جبری یکه است فقط و فقط وقتی که α در یک معادلهٔ چندجمله‌ای تکین با ضرایب صحیح و جملهٔ ثابت ± 1 صدق کند.

۲.۳.۱۰ تحقیق کنید که برای یکه‌های $\pm\zeta_3$ و $\pm\zeta_3^2$ از $\mathbb{Z}[\zeta_3]$ چنین چندجمله‌ایهایی وجود دارند.

۴.۱۰ میدانهای مربعی و اعداد صحیح آنها

حلقهٔ همهٔ اعداد صحیح جبری خواص ناجوری دارد. مثلاً ریشهٔ دوم هر عدد صحیح جبری مانند α نیز یک عدد صحیح جبری است و لذا α دارای تجزیهٔ $\alpha = \sqrt{\alpha}\sqrt{\alpha}$ می‌باشد. این مطلب نشان می‌دهد که هیچ عدد اولی در حلقهٔ اعداد صحیح وجود ندارد. بدین دلیل، اغلب در یک حلقهٔ اعداد صحیح با درجهٔ کراندار (از قبیل حلقه‌های $\mathbb{Z}[i]$ و $\mathbb{Z}[\sqrt{-2}]$ که قبلاً استفاده کردیم) کار می‌کنیم. حال مثالهای قبلی را به حلقهٔ اعداد صحیح یک میدان مربعی تعمیم می‌دهیم.

هر میدان مربعی را می‌توان به صورت $\mathbb{Q}(\sqrt{d})$ نوشت که $d \in \mathbb{Z}$ و $\mathbb{Q}(\sqrt{d})$ کوچک‌ترین میدان شامل $\mathbb{Q}$ و $\sqrt{d}$ است. یا به عبارت دیگر ماحصل بسته کردن $\mathbb{Q}\cup\{\sqrt{d}\}$ تحت اعمال $+$، $-$، $\times$ و $\div$ (بر عناصر ناصفر) می‌باشد. این بسته کردن تحت $\div$ است که میدان تولید می‌کند و از نماد پرانتز برای تمایز مجموعهٔ حاصله از بسته کردن تحت $+$، $-$ و $\times$ به تنهایی که حلقه (و نه لزوماً میدان) تولید می‌کند استفاده می‌کنیم. (مثلاً $\mathbb{Z}[i]$ بستار $\mathbb{Z}\cup\{i\}$ تحت $+$، $-$ و $\times$ است و یک میدان نمی‌باشد.)

نماد پرانتز در این حالت زائد است چون در حقیقت $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$.

مشخص سازی $\mathbb{Q}(\sqrt{d})$. داریم

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}.$$

برهان. هر عدد مانند $a+b\sqrt{d}$ که $a,b\in\mathbb{Q}$ مطمئناً از $\sqrt{d}$ و اعداد a و b در $\mathbb{Q}$ توسط $+$ و $\times$ حاصل می‌شود. از این رو

$$\{a+b\sqrt{d} : a,b\in\mathbb{Q}\}\subseteq\mathbb{Q}[\sqrt{d}]\subseteq\mathbb{Q}(\sqrt{d}).$$

بالعکس، می‌توانیم نشان دهیم که $\{a+b\sqrt{d} : a,b\in\mathbb{Q}\}$ تحت اعمال $+$، $-$ و $\times$ بسته است و لذا $\{a+b\sqrt{d} : a,b\in\mathbb{Q}\}\supseteq\mathbb{Q}[\sqrt{d}]$.

مجموعهٔ $\{a+b\sqrt{d} : a,b\in\mathbb{Q}\}$ به طور بدیهی تحت $+$ و $-$ بسته است. این مجموعه تحت $\times$ بسته است زیرا

$$(a_1+b_1\sqrt{d})(a_2+b_2\sqrt{d})=a_1a_2+b_1b_2d+(a_1b_2+a_2b_1)\sqrt{d}.$$

و تحت $\div$ (بر عناصر ناصفر) بسته است زیرا

$$\begin{aligned}\frac{1}{a+b\sqrt{d}} &= \frac{a-b\sqrt{d}}{(a+b\sqrt{d})(a-b\sqrt{d})}\\ &= \frac{a-b\sqrt{d}}{a^2-b^2d}\\ &= \frac{a}{a^2-b^2d}-\frac{b}{a^2-b^2d}\sqrt{d}. \ \square\end{aligned}$$

اعداد صحیح $\mathbb{Q}(\sqrt{d})$ شامل $\pm\sqrt{d}$ است (چون $\pm\sqrt{d}$ در معادلهٔ تکین $x^2-d=0$ صدق می‌کند) و از این رو این اعداد شامل همهٔ اعضای $\mathbb{Z}[\sqrt{d}]$ (بنابر بسته بودن اعداد صحیح جبری تحت $+$) می‌باشد. اما گاهی اوقات این مجموعه شامل اعدادی بیش از این است که بدین دلیل مجبوریم از عبارت طولانی اعداد صحیح $\mathbb{Q}(\sqrt{d})$ به جای $\mathbb{Z}[\sqrt{d}]$ استفاده کنیم. مثلاً $\mathbb{Q}(\sqrt{-3})$ شامل $\frac{-1+\sqrt{-3}}{2}$ است و این عدد یک عدد صحیح جبری است چون در معادلهٔ $x^2+x+1=0$ صدق می‌کند.

این وضعیت به طور دقیق در قضیهٔ بعد توصیف شده است. قبل از آن که قضیه را بیان کنیم و برهان آن را شروع کنیم توجه می‌کنیم که عدد صحیح d در $\mathbb{Q}(\sqrt{d})$ را می‌توان خالی از مربع فرض کرد یعنی توسط هیچ مربعی بزرگ‌تر از ۱ عاد نمی‌شود. این مطلب بدان دلیل است که اگر $d = n^۲c$ برای n و c یی در $\mathbb{Z}$، آنگاه $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(n\sqrt{c})$ که بنابر بسته کردن تحت $\times$ و $\div$ برابر $\mathbb{Q}(\sqrt{c})$ می‌باشد. چیز دیگری که باید یادآوری شود این است که هر مربعی همنهشت با ۰ یا ۱ به پیمانهٔ ۴ است.

اعداد صحیح $\mathbb{Q}(\sqrt{d})$. وقتی $d \not\equiv_۴ ۱$، اعداد صحیح $\mathbb{Q}(\sqrt{d})$ عبارتند از $a + b\sqrt{d}$ هایی که $a, b \in \mathbb{Z}$. وقتی $d \equiv_۴ ۱$، اعداد صحیح $\mathbb{Q}(\sqrt{d})$ عبارتند از $a + b\sqrt{d}$ هایی که $a, b \in \mathbb{Z}$ یا $a + \frac{۱}{۲}, b + \frac{۱}{۲} \in \mathbb{Z}$.

برهان. اگر $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ یک عدد صحیح جبری و لذا جوابی برای معادله‌ای مانند $x^۲ + Ax + B = ۰$ با شرط $A, B \in \mathbb{Z}$ باشد، آنگاه از فرمول مجذور نتیجه می‌شود که جواب دیگر $a - b\sqrt{d}$ است. از این رو

$$x^۲ + Ax + B = (x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})).$$

با مساوی قرار دادن ضرایب داریم

$$A = -۲a, \qquad B = a^۲ - db^۲,$$

که نشان می‌دهد $۲a$ و $a^۲ - db^۲$ اعداد صحیح معمولی هستند.

بالاخص $a \in \mathbb{Z}$ یا $a + \frac{۱}{۲} \in \mathbb{Z}$. در حالت اول ($۲a$ زوج)،

$$\begin{aligned} a \in \mathbb{Z} &\implies a^۲ \in \mathbb{Z} \\ &\implies db^۲ \in \mathbb{Z} \\ &\implies b^۲ \in \mathbb{Z} \\ &\implies b \in \mathbb{Z}. \end{aligned}$$

حالت $a+\frac{1}{2}\in\mathbb{Z}$ هنگامی رخ می‌دهد که $2a$ فرد باشد ودر نتیجه $(2a)^2\equiv_4 1$.
در این صورت

$$\begin{aligned} a^2-db^2\in\mathbb{Z} &\implies (2a)^2-d(2b)^2\equiv_4 0\\ &\implies d(2b)^2\equiv_4(2a)^2\equiv_4 1\\ &\implies d\equiv_4 1,\quad (2b)^2\equiv_4 1\\ &\implies d\equiv_4 1,\quad 2b\equiv_2 1\\ &\implies d\equiv_4 1,\quad b+\frac{1}{2}\in\mathbb{Z}. \end{aligned}$$

نهایتاً برای آن که ببینیم هر عدد به صورت $a+b\sqrt{d}$ با شرط $a+\frac{1}{2},b+\frac{1}{2}\in\mathbb{Z}$ وقتی $d=4m+1$، عدد صحیحی از $\mathbb{Q}(\sqrt{d})$ است کافی است ضرایب معادله‌ای را که در آن صدق می‌کند (یعنی $(x^2-2ax+(a^2-db^2)=0$ بررسی کنیم. به سادگی می‌توان نشان داد که این اعداد صحیح هستند. □

تمرینها

۱.۴.۱۰ نشان دهید هر عضو $\mathbb{Q}(\sqrt{d})$ عدد صحیحی از $\mathbb{Q}(\sqrt{d})$ است که بر یک عدد صحیح معمولی تقسیم شده باشد.

جواب دوم (مانند α') از معادلهٔ مربعی تکین با ضرایب صحیح که عددی صحیح و مربعی مانند α در آن صدق می‌کند مزدوج α نامیده می‌شود. این مطلب مفهوم مزدوج مختلط در $\mathbb{Z}[i]$ و مفهوم مزدوج گنگ از جبر دبیرستانی را تعمیم می‌دهد.

۲.۴.۱۰ اگر α گویا باشد، α' چیست؟

۳.۴.۱۰ تحقیق کنید که مزدوجگیری، یک خودریختی حلقه‌ها از $\mathbb{Q}[\sqrt{d}]$ است، یعنی

- نگاشت $\alpha \mapsto \alpha'$ یک به یک و برو است.
- $(\alpha+\beta)' = \alpha' + \beta'$ و $(\alpha\beta)' = \alpha'\beta'$.

۵.۱۰ نرم و یکه‌های میدانهای مربعی

نرم روی $\mathbb{Q}(\sqrt{d})$ تابعی است که به صورت

$$\text{نرم}\,(a+b\sqrt{d}) = a^{۲} - db^{۲}$$

تعریف می‌شود. نتیجه می‌شود که یک عدد صحیح مانند $a+b\sqrt{d}$ از $\mathbb{Q}(\sqrt{d})$ دارای نرم صحیح (معمولی) می‌باشد چرا که برهان قضیهٔ اخیر از بخش قبل، نشان داد که در این حالت $a^{۲} - db^{۲}$ یک عدد صحیح معمولی است. این نرم شامل نرمهای قبلی تعریف شده برای $d = -۱$، $d = -۲$ و $d = n$ است و مشابه آنها ضربی می‌باشد:

$$\text{برای هر } x_۱, x_۲ \in \mathbb{Q}(\sqrt{d}) \qquad \text{نرم}\,(x_۱ x_۲) = \text{نرم}\,(x_۱)\ \text{نرم}\,(x_۲),$$

این مطلب را می‌توان با فرض $x_۱ = a_۱ + b_۱\sqrt{d}$، $x_۲ = a_۲ + b_۲\sqrt{d}$ و کار کردن روی دو طرف بررسی کرد. همچنین می‌توان اتحاد

$$(a_۱a_۲ + db_۱b_۲)^{۲} - d(a_۱b_۲ + a_۲b_۱)^{۲} = (a_۱^{۲} - db_۱^{۲})(a_۲^{۲} - db_۲^{۲})$$

را که اتحاد براهماگوپتا از بخش ۴.۵ (برای $d > ۰$) و اتحاد دیوفانتوس از بخش ۸.۱ (برای $d = -۱$) است به دست آورد. این خواص نرم ایجاب می‌کند که اگر $x_۱$ عدد $x_۲$ را در اعداد صحیح $\mathbb{Q}(\sqrt{d})$ عاد کند آنگاه نرم $(x_۱)$ نیز نرم $(x_۲)$ را در اعداد صحیح معمولی عاد خواهد کرد.

یکه‌ها (همانند هر حلقه‌ای) در میان اعداد صحیح $\mathbb{Q}(\sqrt{d})$ عبارتند از عناصری که ۱ را عاد می‌کنند. بنابر تبصرهٔ قبل نتیجه می‌شود که یکه‌های $\mathbb{Q}(\sqrt{d})$ اعداد صحیحی با نرم ۱± هستند. بالعکس، اعداد صحیح با نرم ۱± یکه هستند زیرا اگر $a+b\sqrt{d}$ عدد صحیحی (با شرط $a,b\in\mathbb{Z}$ یا $a+\frac{۱}{۲},b+\frac{۱}{۲}\in\mathbb{Z}$) باشد که نرم آن ۱± است آنگاه

$$\pm ۱ = a^{۲}-db^{۲} = (a-b\sqrt{d})(a+b\sqrt{d}).$$

و این نشان می‌دهد که $a+b\sqrt{d}$ عدد ۱ را عاد می‌کند. وقتی $d>۱$ بی‌نهایت یکه در بین اعداد صحیح $\mathbb{Q}(\sqrt{d})$ متناظر با بی‌نهایت جواب معادلهٔ پل $x^{۲}-dy^{۲}=۱$ وجود دارد. مثلاً جوابهای $x^{۲}-۲y^{۲}=۱$ زوجهای (x,y) یی هستند که برای آنها $x+y\sqrt{۲}$ یکه‌ای از $\mathbb{Q}(\sqrt{۲})$ است. این جوابها را در بخش ۲.۵ یافتیم که یکه‌های $\pm(۳+۲\sqrt{۲})^{n}$ را برای $n\in\mathbb{Z}$ به دست می‌دهد.

از طرف دیگر اگر $d<۰$ آنگاه فقط تعدادی متناهی عدد صحیح یا نیم‌صحیح a و b با شرط $a^{۲}-db^{۲}=۱$ وجود دارد و از این رو فقط تعدادی متناهی یکه داریم. بالاخص:

- یکه‌های $\mathbb{Z}[i]$ عبارتند از ۱±، $\pm\mathbf{i}$،
- یکه‌های $\mathbb{Z}[\sqrt{-۲}]$ عبارتند از ۱±،
- یکه‌های $\mathbb{Z}[\zeta_{۳}]$ که در آن $\zeta_{۳}=\frac{-۱+\sqrt{-۳}}{۲}$ عبارتند از ۱±، $\pm\zeta_{۳}$، $\pm\zeta_{۳}^{۲}$.

بنابر قضیهٔ بخش قبل، $\mathbb{Z}[\zeta_{۳}]$ حلقهٔ اعداد صحیح میدان $\mathbb{Q}(\sqrt{-۳})$ است و در حقیقت بیشترین یکه را در بین هر حلقه‌ای از اعداد صحیح $\mathbb{Q}(\sqrt{d})$ با شرط $d<۰$ دارد.

میدانهای $\mathbb{Q}(\sqrt{d})$ با شرط $d<۰$ میدانهای مربعی موهومی نامیده می‌شوند و مخصوصاً نظریهٔ پایه‌ای آنها زیباست. مزیتی که این میدانها نسبت به میدانهای مربعی حقیقی دارند این است که وقتی $d<۰$، مقدار

$a^۲ - db^۲ =$ نرم $(a+b\sqrt{d})$ همان مربع فاصلهٔ $a+b\sqrt{d}$ تا ۰ در صفحهٔ مختلط است. این مطلب، خواصی مشخص مانند خواص تقسیم برای $\mathbb{Z}[i]$ را که در بخش ۴.٦ یافت شد به طور هندسی روشن می‌سازد. مثال دیگر قضیهٔ زیر است.

یکه‌های میدانهای مربعی موهومی. تنها یکه‌های میدانهای مربعی موهومی عبارتند از ۱±، $\pm i$، $\pm\zeta_۳$ و $\pm\zeta_۳^۲$.

برهان. چون یکه‌ها نرم ۱ دارند، یکه‌های میدان مربعی $\mathbb{Q}(\sqrt{d})$ در فاصلهٔ ۱ از ۰ در صفحهٔ مختلط قرار دارند. اما همچنین می‌دانیم که اعداد صحیح $\mathbb{Q}(\sqrt{d})$ به صورت $a+b\sqrt{d}$ هستند که در آن $a,b \in\mathbb{Z}$ یا $a+\frac{۱}{۲}, b+\frac{۱}{۲} \in\mathbb{Z}$. اگر $|d| \geq ۵$ آنگاه همهٔ چنین اعداد صحیحی غیر از ۰ و ۱± در فاصلهٔ بیشتر از ۱ نسبت به ۰ قرار دارند. لذا تنها یکه‌های غیر از ۱± همانهایی هستند که در بالا فهرست شده‌اند و در $\mathbb{Q}(i)$ و $\mathbb{Q}(\sqrt{-۳})$ اتفاق می‌افتند. □

میدانهای مربعی موهومی نسبت به میدانهای حقیقی بهتر درک می‌شوند. مثلاً گاوس (۱۸۰۱) دریافت که اعداد صحیح $\mathbb{Q}(\sqrt{d})$ برای

$$d = -۱, -۲, -۳, -۷, -۱۱, -۱۹, -۴۳, -٦۷, -۱٦۳$$

واجد یکتایی تجزیه به اعداد اول هستند و در سال ۱۹٦۷ بیکر[۲] و استارک[۳] نشان دادند که اینها تنها میدانهای مربعی موهومی با یکتایی تجزیه به اعداد اول می‌باشند. میدانهای مربعی حقیقی با یکتایی تجزیه به اعداد اول هنوز شناخته نشده‌اند و حتی هنوز نمی‌دانیم که آیا بی‌نهایت از آنها وجود دارد یا نه.

---

[۲] Baker
[۳] Stark

تمرینها

یک روش معادل برای تعریف نرم که به میدانهای اعداد جبری دلخواه از درجهٔ متناهی تعمیم می‌یابد بر حسب مزدوجها است.

۱.۵.۱۰ نشان دهید $\alpha\alpha' = $ نرم (α).

۲.۵.۱۰ اگر α گویا باشد، نرم (α) چیست؟

۳.۵.۱۰ از این رو خاصیت ضربی نرم را از خاصیت ضربی مزدوجگیری نتیجه بگیرید.

۶.۱۰ بحث

حلقه‌های $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ قبل از آن که مفهوم حلقه، نامی به خود بگیرد شناخته شده بودند. شروع توسعهٔ حلقه‌ها در اواسط قرن نوزدهم بود که کومر حلقه‌های دایره‌بُر $\mathbb{Z}[\zeta_n]$ را مطالعه کرد و ددکیند در جست و جوی یک نظریهٔ عمومی در مورد اعداد صحیح جبری بود. اولین ارائهٔ ددکیند از نظریه‌اش به عنوان مکملی بر درسهایی از نظریه اعداد دیریکله در سال ۱۸۷۱ ظاهر شد. در آن زمان همهٔ مثالهای مورد علاقه ددکیند، حلقه‌های اعداد جبری بودند. در سال ۱۸۷۱ می‌شد یک حلقه را (که هنوز نام نگرفته بود) به عنوان زیرمجموعه‌ای بسته تحت $+$، $-$ و $\times$ تعریف کرد.

نیاز به تعریف توسط اصول موضوعه[۴] به جای خواص بسته بودن به تدریج به شکل مجموعه‌های دیگری با اعمال $+$، $-$ و $\times$ شدیداً احساس شد. ردهٔ همنهشتی حلقه‌های $\frac{\mathbb{Z}}{n\mathbb{Z}}$ (که اساساً به روش مدرن ددکیند (۱۸۵۷) با رده‌های همنهشتی به عنوان اشیائی که می‌توانند جمع و ضرب شوند تعریف

[۴] axioms

می‌گردد) رده‌ای از مثالها بود. دیگری، ردهٔ حلقهٔ ماتریسها بود که توسط کیلی (۱۸۵۸) نشان داده شد. این حلقه شامل چهارگانها است و پیرس[5] (۱۸۸۱) اثبات کرد که شامل بسیاری ساختارهای دیگر می‌باشد.

گرچه حلقه‌های ماتریسی در حالت کلی غیر تعویض‌پذیر هستند، شامل حلقه‌های جابجایی جالب بسیاری می‌باشند. در بخش ۱.۸ دیدیم که چگونه $\mathbb{C}$ را می‌توان توسط ماتریسهای ۲×۲ با درایه‌های حقیقی نمایش داد. همچنین می‌توان $\mathbb{Z}[\alpha]$ را برای هر عدد صحیح از درجهٔ n مانند α توسط ماتریسهای صحیح $n \times n$ و نیز $\mathbb{Q}(\alpha)$ را توسط ماتریسهای گویای $n \times n$ نمایش داد. به طور خلاصه ایدهٔ آن به صورت زیر است.

اگر معادلهٔ تکینی که α در آن صدق می‌کند عبارت باشد از

$$\alpha^n + a_{n-۱}\alpha^{n-۱} + \ldots + a_۱\alpha + a_۰ = ۰, \qquad a_۰, \ldots, a_{n-۱} \in \mathbb{Z}$$

آنگاه $\alpha^n = -a_{n-۱}\alpha^{n-۱} - \ldots - a_۱\alpha - a_۰$. از این رو همهٔ توانهای α^n، $\alpha^{n+۱}$، ... ترکیب خطی گویایی از ۱، α، $\alpha^۲$، ...، $\alpha^{n-۱}$ هستند. این مطلب به ما امکان می‌دهد که $\mathbb{Q}(\alpha)$ را به صورت فضای برداری روی $\mathbb{Q}$ با پایهٔ $\{۱, \alpha, \alpha^۲, \ldots, \alpha^{n-۱}\}$ تلقی کنیم. ضرب کردن در α نگاشتی خطی از این فضای برداری با نمایش ماتریسی

$$M_\alpha = \begin{pmatrix} ۰ & ۰ & \ldots & ۰ & -a_۰ \\ ۱ & ۰ & \ldots & ۰ & -a_۱ \\ ۰ & ۱ & \ldots & ۰ & -a_۲ \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ ۰ & ۰ & \ldots & ۰ & -a_{n-۱} \end{pmatrix}$$

را القا می‌کند زیرا ضرب کردن بردار سطری $(۱\ \alpha\ \alpha^۲\ \ldots\ \alpha^{n-۲}\ \alpha^{n-۱})$ در M_α از سمت راست، ضرب کردن آن در α، یعنی

$$(\alpha\ \alpha^۲\ \alpha^۳\ \ldots\ -a_{n-۱}\alpha^{n-۱} - \ldots - a_۱\alpha - a_۰)$$

---

[5] Peirce

را به دست می‌دهد. نتیجه می‌شود که چندجمله‌ایهای ماتریسی بر حسب M_α با ضرایب گویا، رفتاری همانند چندجمله‌ایهای متناظر بر حسب α، یعنی همانند عناصر $\mathbb{Q}(\alpha)$ دارند.

همهٔ این مثالها نهایتاً تحت مفهوم مجرد حلقه که توسط فرانکل (۱۹۱۴) به صورت اصل موضوعی تعریف شده و توسط امی نوتر[۶] و دانشجویانش در حدود سالهای ۱۹۲۰ گسترش یافت، وحدت پیدا کرد. نوتر همیشه می‌گفت: "این مطلب قبلاً در ددکیند بوده است" و دانشجویانش را وادار می‌کرد که همهٔ کارهای ددکیند در مورد اعداد صحیح جبری را بخوانند. این کارها شامل سه نسخهٔ متفاوت از مکمل آخر وی بر درسهای دیریکله در ۱۸۷۱، ۱۸۷۹ و ۱۸۹۴ و نیز کاری که به طور مجزا منتشر شده است و اکنون به صورت ترجمهٔ انگلیسی با عنوان ددکیند (۱۸۷۷) در دسترس است بود. این آخری احتمالاً ساده‌ترین نوع معرفی کارهای ددکیند برای خواننده‌ای امروزی می‌باشد.

در میان چیزهای دیگر، ددکیند (۱۸۷۷) مفهوم نرم را به میدان اعداد جبری دلخواهی مانند $\mathbb{Q}(\alpha)$ تعمیم می‌دهد. وی مزدوجهای α'، α''، ... را برای α به عنوان جوابهای دیگر معادلهٔ تکین با درجهٔ کمین که α در آن صدق می‌کند تعریف کرد و نرم (α) را به صورت $\alpha\alpha'\alpha''\ldots$ معرفی نمود. در این صورت می‌توان نشان داد که وقتی α عدد صحیحی از $\mathbb{Q}(\alpha)$ باشد، نرم (α) یک عدد صحیح معمولی است و می‌توان نشان داد که نرم (β) نرم (α) = نرم $(\alpha\beta)$. برهانها سخت نیستند اما این آخری مفاهیم دیگری (مربوط به یکریختی میدانها) را از کتاب مکمل این کتاب، یعنی کتاب اصول جبر می‌طلبد. می‌توان گفت که نظریهٔ جبری اعداد جایی است که آغاز برهم‌کنشِ مفاهیم نظریهٔ معادلات جبری (گروهها و میدانها) با مفاهیم نظریهٔ معادلات دیوفانتی (حلقه‌ها) است.

[۶] Emmy Noether

۱۱

ایده‌آلها

پیش‌نگاه

فصل حاضر این ایده را تعقیب می‌کند که یک عدد توسط مجموعهٔ مضاربش شناخته می‌شود. در نتیجه، یک عدد ایده‌آلی توسط مجموعه‌ای که شبیه مجموعهٔ مضارب رفتار می‌کند شناخته می‌شود. چنین مجموعه‌ای مانند I در یک حلقه مانند R را یک ایده‌آل می‌نامیم که توسط دو خاصیت بسته بودن تحت جمع (یعنی $a, b \in I \Rightarrow a+b \in I$) و بسته بودن تحت ضرب در همهٔ عناصر حلقه (یعنی $a \in I, r \in R \Rightarrow ar \in I$) تعریف می‌گردد.

مجموعهٔ $(a) = \{ar : r \in R\}$ متشکل از همهٔ مضارب $a \in R$، یک ایده‌آل است که ایده‌آل اصلی تولید شده توسط a[1] نامیده می‌شود. لذا هر ایده‌آل غیر اصلی مانند I برابر مجموعهٔ مضارب هیچ عضوی از R نیست – چنین ایده‌آلی یک عدد ایده‌آلی R را نمایش می‌دهد.

در $\mathbb{Z}$ هر ایده‌آل، اصلی است و خواص ایده‌آلها، ویژگیهای شناخته شدهٔ اعداد صحیح را باز می‌تاباند. بالاخص:

[1] principal ideal generated by a

a عنصر b را عاد می‌کند فقط و فقط وقتی که (a) شامل (b) باشد.
$(\gcd(a,b)) = \{am + bn : m, n \in \mathbb{Z}\}$ که همان ایده‌آل تولید شده توسط a و b است.
p اول است فقط و فقط وقتی که (p) بیشین[۲] باشد.

در حلقه‌هایی که یکتایی تجزیه به اعداد اول با شکست مواجه می‌شود (مانند $\mathbb{Z}[\sqrt{-5}]$)، ایده‌آلهای غیر اصلی وجود دارد. می‌بینیم که چنین ایده‌آلی به عنوان ب.م.م. ایده‌آلیِ[۳] ۲ و $1 + \sqrt{-5}$ است (یعنی به صورت $\{2m + (1 + \sqrt{-5})n : m, n \in \mathbb{Z}\}$) و غیر اصلی بودن آن را با مشاهدهٔ شکلش در صفحه تأیید می‌کنیم.

ایده‌آل $\{2m + (1 + \sqrt{-5})n : m, n \in \mathbb{Z}\}$ ایده‌آل اصلی (2) را عاد می‌کند زیرا شامل آن است و اول است چون بیشین می‌باشد. اما اگر یک ایده‌آل مانند I ایده‌آلی مانند J را عاد کند آنگاه باید حاصل ضرب دو ایده‌آل I و K (یعنی IK) برابر J باشد.

امیدواریم (2) به چنین حاصل ضربی بشکنند چرا که این امر باعث برطرف شدن عدم یکتایی تجزیه به اعداد اول در $\mathbb{Z}[\sqrt{-5}]$ (که به صورت $(1 - \sqrt{-5})(1 + \sqrt{-5}) = 3 \times 2$ اتفاق می‌افتد) خواهد شد.

لذا گام نهایی این است که حاصل ضرب ایده‌آلها را تعریف کنیم. بدین ترتیب، همان گونه که انتظارش را داشتیم، نتیجه می‌شود که این دو حاصل ضرب متمایز در $\mathbb{Z}[\sqrt{-5}]$ برابر ۶ می‌گردند که به حاصل ضرب یکسانی از ایده‌آلهای اول می‌شکنند.

---
[۲] maximal
[۳] gcd ideal

۱.۱۱ ایده‌آلها و ب.م.م.

در بخش ۴.۷ هنگامی که دریافتیم ۴ دارای دو تجزیهٔ متفاوت در $\mathbb{Z}[\sqrt{-۳}]$ به صورت

$$۴ = ۲ \times ۲ = (۱ + \sqrt{-۳})(۱ - \sqrt{-۳})$$

است، نگاهی اجمالی به شکست یکتایی تجزیه به اعداد اول داشتیم.

این مسأله را می‌توان با وسعت دادن $\mathbb{Z}[\sqrt{-۳}]$ به $\mathbb{Z}[\frac{-۱+\sqrt{-۳}}{۲}]$ برطرف نمود. بدین ترتیب تجزیه‌های ۲×۲ و $(۱ + \sqrt{-۳})(۱ - \sqrt{-۳})$ تا حد عوامل یکه واقعاً یکی هستند. این مطلب بدان جهت است که $\mathbb{Z}[\frac{-۱+\sqrt{-۳}}{۲}]$ شامل یکه‌های $\frac{۱+\sqrt{-۳}}{۲}$ و $\frac{۱-\sqrt{-۳}}{۲}$ است که حاصل ضرب آنها برابر ۱ می‌باشد و لذا

$$۲ \times ۲ = ۲(\frac{۱ + \sqrt{-۳}}{۲})۲(\frac{۱ - \sqrt{-۳}}{۲}) = (۱ + \sqrt{-۳})(۱ - \sqrt{-۳}).$$

با این حال این اتفاق، به مفهومی، فراری خوش‌اقبالانه است اما مشکلی جدی‌تر در $\mathbb{Z}[\sqrt{-۵}]$ رخ می‌دهد که در آن ٦ دو تجزیهٔ متفاوت

$$٦ = ۲ \times ۳ = (۱ + \sqrt{-۵})(۱ - \sqrt{-۵})$$

را دارد.

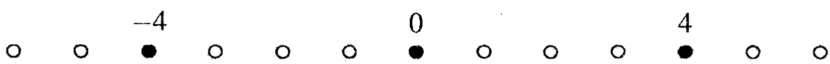
با استفاده از نرم یک عنصر دلخواه مانند $a + b\sqrt{-۵} \in \mathbb{Z}[\sqrt{-۵}]$ که برابر $a^۲ + ۵b^۲$ است می‌توان بررسی کرد که هیچ یک از این عوامل، حاصل ضرب عناصر با نرم کوچک‌تر نیست. هیچ یک از یکه‌های ±۱ از $\mathbb{Z}[\sqrt{-۵}]$ نمی‌توانند اختلاف بین این تجزیه‌ها را توجیه کنند. لذا ٦ دو تجزیهٔ متفاوت در $\mathbb{Z}[\sqrt{-۵}]$ دارد. و لذا نمی‌توانیم به سادگی قبل، با وسعت بخشیدن به این حلقه (همانند توسیع $\mathbb{Z}[\sqrt{-۳}]$ به $\mathbb{Z}[\frac{-۱+\sqrt{-۳}}{۲}]$) بر این مشکل فائق شویم چرا که $\mathbb{Z}[\sqrt{-۵}]$ از قبل شامل همهٔ اعداد صحیح $\mathbb{Q}(\sqrt{-۵})$ است.

در چنین وضعیتهایی بود که کومر و ددکیند با توسیع مفهوم حاصل ضرب و تقسیم‌پذیری، قادر به احراز یکتایی تجزیه به اعداد اول شدند. این چیزی بود

که کومر آن را اعداد ایده‌آلی نامید و ددکیند ایده‌آل. اولین عدد ایده‌آلی را با جست و جوی ب.م.م. ۲ و $\sqrt{-5}+1$ در $\mathbb{Z}[\sqrt{-5}]$ می‌یابیم که مبتنی بر نگرشی جدید به ب.م.م. در $\mathbb{Z}$ است.

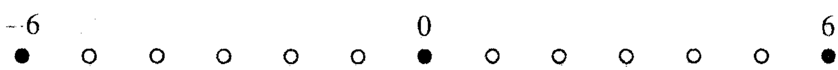
ملاقات مجدد ب.م.م. در اعداد صحیح

ایدهٔ اصلی کومر و ددکیند این است که یک عدد توسط مجموعهٔ مضاربش شناخته می‌شود. توسط محاسبهٔ $\gcd(4,6)$ این ایده و کاربرد آن را برای یافتن ب.م.م. روشن می‌سازیم. شکل ۱.۱۱ مجموعهٔ مضارب ۴ را نشان می‌دهد که آن را با (۴) نمایش می‌دهیم و توسط دایره‌های توپر در بین اعداد صحیح آمده‌اند:



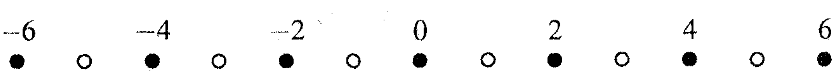
شکل ۱.۱۱: مضارب ۴

شکل ۲.۱۱ به طور مشابه مجموعهٔ (٦) متشکل از مضارب ٦ را نشان می‌دهد:



شکل ۲.۱۱: مضارب ٦

سرانجام شکل ۳.۱۱ همهٔ حاصل جمعهای عناصر (۴) و عناصر (٦) را نشان می‌دهد. مجموعهٔ چنین حاصل جمعهایی را با (٦) + (۴) نمایش می‌دهیم:



شکل ۳.۱۱: حاصل جمعهای عناصر (۴) و عناصر (٦)

روشن است که $(۲) = (٦) + (۴)$ و $\gcd(۴, ٦) = ۲$. لذا مضارب $\gcd(۴, ٦)$ را می‌توان با جمع کردن همهٔ مضارب ۴ و همهٔ مضارب ٦ به دست آورد. به طور کلی، فرض کنیم که (k) مجموعهٔ $\{kn : n \in \mathbb{Z}\}$ برای k یی در $\mathbb{Z}$ باشد. در این صورت داریم: مجموعهٔ $(a) + (b) = \{am + bn : m, n \in \mathbb{Z}\}$ برابر مجموعهٔ $(\gcd(a, b))$ متشکل از همهٔ مضارب $\gcd(a, b)$ است.

این قضیه را در بخش بعد اثبات می‌کنیم. این قضیه صورت دیگری از الگوریتم اقلیدسی را برای یافتن ب.م.م. به دست می‌دهد؛ با این مزیت که در هر حلقه مانند R قابل کاربرد است. این کار توسط جایگزینی مجموعه‌های (k) (که در بالا آمد) با مفهوم کلی‌تری که در زیر می‌آید انجام خواهد شد.

تعریف. یک ایده‌آل در یک حلقه مانند R، زیرمجموعه‌ای مانند I از R است که

- $a \in I$ و $b \in I$ نتیجه دهد که $a + b \in I$،
- $a \in I$ و $r \in R$ نتیجه دهد که $ar \in I$.

به بیان دیگر، I تحت جمع و تحت ضرب کردن در عناصر R بسته است. این مطلب نتیجه می‌دهد که I تحت تفریق نیز بسته است زیرا $b \in I$ نتیجه می‌دهد که $-b \in I$ (با توجه به ضرب کردن در $-۱ \in R$) و به علاوه داریم $a - b = a + (-b)$.

همچنین می‌دانیم که اگر I و J ایده‌آل باشند آنگاه

$$I + J = \{i + j : i \in I, j \in J\}$$

نیز چنین است. مجموعهٔ اخیر چیزی است که آن را $\gcd(I, J)$ می‌نامیم و از آن در بخش ۵.۱۱ برای یافتن ب.م.م. ۲ و $۱ + \sqrt{-۵}$ در $\mathbb{Z}[\sqrt{-۵}]$ استفاده می‌کنیم. اما در ابتدا مفهوم ایده‌آل را در حلقهٔ آشنای $\mathbb{Z}$ مورد مطالعه قرار می‌دهیم.

تمرینها

قضیه‌ای را که می‌گوید $(a)+(b)=(\gcd(a,b))$ می‌توان در $\mathbb{Z}$ به طور مستقیم اثبات کرد، و این کار برای کمک به اثبات آن در بخش بعد با استفاده از نظریهٔ ایده‌آلها ارزشمند خواهد بود.

۱.۱.۱۱ نشان دهید که همهٔ اعضای $(a)+(b)=\{am+bn : m,n\in\mathbb{Z}\}$ مضارب $\gcd(a,b)$ هستند.

۲.۱.۱۱ نشان دهید که $\{am+bn : m,n\in\mathbb{Z}\}$ تحت تفاضل بسته است و نتیجه بگیرید که همهٔ اعضای این مجموعه، مضرب کوچک‌ترین عضو مثبت آن (مثلاً c) هستند.

۳.۱.۱۱ نتیجه بگیرید که $c=\gcd(a,b)$. بنابراین $(a)+(b)=(\gcd(a,b))$.

۲.۱۱ ایده‌آلها و تقسیم پذیری در اعداد صحیح

ساده‌ترین مثالهای ایده‌آلها در $\mathbb{Z}$ اتفاق می‌افتد. مثلاً $(۲)=\{۲n : n\in\mathbb{Z}\}$ و $(٦)=\{٦n : n\in\mathbb{Z}\}$ ایده‌آل هستند. در حقیقت برای هر $a\in\mathbb{Z}$، مجموعهٔ

$$(a)=\{an : n\in\mathbb{Z}\}$$

یک ایده‌آل است که آن را ایده‌آل اصلی تولید شده توسط a می‌نامیم. تقسیم‌پذیری در $\mathbb{Z}$ متناظر با شمولِ[۴] ایده‌آلهای اصلی است. مثلاً

۲ عدد ٦ را عاد می‌کند، (۲) شامل (٦) است،

و به طور کلی

[۴] containment

a عدد b را عاد می‌کند فقط و فقط وقتی که (a) شامل (b) باشد.

ایدهٔ ددکیند این بود که تقسیم‌پذیری ایده‌آلها را در یک حلقه، با استفاده از

I ایده‌آل J را عاد می‌کند فقط و فقط وقتی که I شامل J باشد

تعریف کند. (کلمات عاد می‌کند و تعریف کند را از آن جهت با حروف متفاوت نوشته‌ایم که باید نشان دهیم این مفهوم با مفهوم متداول تقسیم پذیری سازگار است: I ایده‌آل J را عاد می‌کند فقط و فقط وقتی که برای ایده‌آلی مانند K داشته باشیم $J = IK$. هنگامی که ضرب ایده‌آلها را در بخش ۷.۱۱ تعریف کنیم، مفهوم اخیر مرتبط با مفهوم بالا از آب در می‌آید.)

تعریف ددکیند، حالت تقسیم‌پذیری برای دو عضو $s, t \in R$ را شامل می‌شود زیرا می‌توانیم ایده‌آلهای اصلی را در هر حلقه به صورت

$$(s) = \{sr : r \in R\}, \qquad (t) = \{tr : r \in R\}$$

تعریف کنیم و نشان دهیم که

s عضو t را عاد می‌کند فقط و فقط وقتی که (s) شامل (t) باشد.

اما تقسیم‌پذیری ایده‌آلها به طور کلی مفهوم تقسیم‌پذیری عناصر را توسیع می‌دهد چرا که چنین نیست که هر ایده‌آلی اصلی باشد.

بالاخص می‌بینیم که ایده‌آلهای غیر اصلی نیز در $\mathbb{Z}[\sqrt{-5}]$ وجود دارد و شامل ایده‌آلهای اول هستند که باعث حصول یکتایی تجزیه به اعداد اول می‌گردد. اما قبل از این که چنین کنیم مفید است از دیدگاه ایده‌آلها، نگاهی نزدیک‌تر به $\mathbb{Z}$ داشته باشیم. این کار به ما امکان می‌دهد که ببینیم چگونه نظریهٔ مقدماتی ایده‌آلها به برازندگی شامل نظریهٔ سنتی تقسیم‌پذیری، مقسوم‌علیه مشترک، و اعداد اول است.

نظریه ایده‌آلها در اعداد صحیح

نظریهٔ مقدماتی تقسیم‌پذیری در $\mathbb{Z}$ متشکل از سه قضیه در مورد ایده‌آلها است. اولین آنها همتایی برای خاصیت تقسیم است.

خاصیت ایده‌آل اصلی $\mathbb{Z}$. همهٔ ایده‌آلهای $\mathbb{Z}$ اصلی هستند.

برهان. فرض کنیم I ایده‌آلی از $\mathbb{Z}$ غیر از (0) باشد. در این صورت I دارای کوچک‌ترین عضو مثبت است که مثلاً آن را a می‌نامیم[5]. چون I تحت ضرب کردن در عناصر $\mathbb{Z}$ بسته است پس باید شامل همهٔ عناصر

$$(a) = \{an : n \in \mathbb{Z}\}$$

باشد. اما این عناصر تنها اعضای I هستند زیرا اگر b مضربی از a نباشد آنگاه

$$b - (\text{بزرگ‌ترین مضرب } a \text{ که کمتر از } b \text{ است})$$

نیز عضو مثبتی از I است که کمتر از a می‌باشد. و این با فرض ما در تناقض است. □

قضیهٔ دوم ب.م.م. را بدون الگوریتم اقلیدسی به دست می‌دهد که مثال بخش قبل را تعمیم می‌دهد.

ایده‌آل ب.م.م. مجموعهٔ $(a) + (b) = \{am + bn : m, n \in \mathbb{Z}\}$ برابر $(\gcd(a, b))$ است.

برهان. چون $\gcd(a, b)$ هم a و هم b را عاد می‌کند باید همهٔ اعداد $am + bn$ را نیز عاد کند. لذا $\{am + bn : m, n \in \mathbb{Z}\}$ فقط شامل مضارب $\gcd(a, b)$ است.

اکنون واضح است که $\{am + bn : m, n \in \mathbb{Z}\}$ یک ایده‌آل است. از این رو بنابر قضیهٔ قبل، باید شامل مضارب کوچک‌ترین عضو مثبتش (که آن را با c نمایش می‌دهیم) باشد. چون a و b اعدادی به صورت $am + bn$ هستند بنابراین

[5] بدیهی است که I شامل حداقل یک عضو مثبت است و بنابر خوشترتیب بودن اعداد طبیعی، a وجود دارد. (م)

آنها نیز مضرب c می‌باشند. از این رو c مقسوم‌علیه مشترکی از a و b است. اما از قبل می‌دانیم که c مضرب $\gcd(a,b)$ است. لذا $c = \gcd(a,b)$. بنابراین ایده‌آل $\{am + bn : m, n \in \mathbb{Z}\}$ متشکل از مضارب c دقیقاً شامل مضارب $\gcd(a,b)$ است. □

سرانجام، می‌توانیم خاصیت مقسوم‌علیه اول را بر حسب ایده‌آلها بیان کنیم. برهان این مطلب به برهانی که اولین بار برای خاصیت مقسوم‌علیه اول (در بخش ۴.۲) ارائه شد نزدیک است. از آنجایی که برای ایده‌آلها عاد کردن به معنای شامل بودن است، تنها ایده‌آلهایی که مشمول ایده‌آلی مانند (p) (برای عددی اول مانند p) هستند عبارتند از خود (p) و ایده‌آل $\mathbb{Z} = (۱)$.

خاصیت ایده‌آل اول. اگر p اول باشد و ایده‌آل (p) شامل (ab) باشد آنگاه (p) شامل (a) یا شامل (b) است.

برهان. فرض کنیم $(p) \not\supseteq (a)$. بنابراین باید اثبات کنیم که $(p) \supseteq (b)$.

چون ایده‌آل $\{am + pn : m, n \in \mathbb{Z}\}$ هم شامل (p) و هم شامل (a) است و $(p) \not\supseteq (a)$ پس $\{am + bn : m, n \in \mathbb{Z}\}$ فقط می‌تواند برابر (۱) باشد.

این بدان معنی است که برای m و n ی صحیح داریم $am + pn = ۱$. لذا

$$\begin{aligned} ۱ = am + pn \quad &\Longrightarrow \quad b = abm + pbn \\ &\Longrightarrow \quad b \in (p) \\ &\Longrightarrow \quad (b) \subseteq (p). \ \square \end{aligned}$$

همان طور که می‌دانیم خاصیت مقسوم‌علیه اول اساس یکتایی تجزیه به اعداد اول است. اما هنوز هم نمی‌توانیم در مورد تجزیهٔ ایده‌آلها در حالت کلی صحبت کنیم چرا که هنوز ضرب ایده‌آلها را تعریف نکرده‌ایم. به طور مشابه، هنوز نمی‌توانیم مفهوم کلی ایده‌آل اول را تعریف کنیم، گرچه خاصیت ایده‌آل اول برای $\mathbb{Z}$ پیشنهاد می‌کند که پس از تعریف ضرب ایده‌آلها چگونه باید این کار را انجام داد.

تمرینها

درست همان طور که $\gcd(a,b)$ از اعمالی ساده بر (a) و (b) حاصل می‌شود، $\operatorname{lcm}(a,b)$ نیز چنین است. به علاوه این اعمال روی هر ایده‌آلی معنی دارند و لذا تعریف کلی ک.م.م. را در هر حلقه‌ای به دست می‌دهند.

۱.۲.۱۱ نشان دهید که $\operatorname{lcm}(a,b) = (a) \cap (b)$.

۲.۲.۱۱ ثابت کنید به ازای هر دو ایده‌آل مانند I و J در هر حلقه مانند R، مجموعهٔ $I \cap J$ یک ایده‌آل است.

۳.۱۱ حوزه‌های با ایده‌آل اصلی

$\mathbb{Z}$ مثالی از یک حوزهٔ با ایده‌آل اصلی[۶] است، یعنی حلقه‌ای که در آن هر ایده‌آل به شکل $(a) = \{ar : r \in R\}$ می‌باشد.

مثالهای دیگر، حلقه‌های دارای الگوریتمی اقلیدسی، از قبیل $\mathbb{Z}[i]$، $\mathbb{Z}[\sqrt{-۲}]$ و $\mathbb{Z}[\zeta_۳]$ هستند. همان طور که می‌دانیم، یک حلقه مانند R دارای الگوریتمی اقلیدسی است فقط و فقط وقتی که R دارای خاصیت تقسیم باشد که می‌توانیم آن را به صورت زیر بیان کنیم.

تعریف. R یک حلقهٔ اقلیدسی[۷] است هرگاه تابعی نامنفی و صحیح مقدار مانند $|r|$ روی R موجود باشد به قسمی که $|r| = ۰$ فقط وقتی که $r = ۰$، و برای هر $a, b \in R$ با شرط $|b| > ۰$ عناصری مانند $q, r \in R$ موجود باشند به قسمی که $a = qb + r$ با شرط $۰ \leq |r| < |b|$.

برای حلقه‌هایی که در بالا ذکر شد، تابع $|r|$ همان تابع قدرمطلق است. برای مثالهای خاصی که در آنها نرم می‌تواند منفی باشد (مثل $\mathbb{Z}[\sqrt{۲}]$) مجذور

[۶] principal ideal domain
[۷] Euclidean ring

قدرمطلق نرم را می‌توان به جای $|r|$ اختیار کرد. (بنابراین تمرین ۶.۱.۹ برهانی برای این مطلب است که $\mathbb{Z}[\sqrt{2}]$ یک حلقهٔ اقلیدسی می‌باشد.)

قضایای مربوط به $\mathbb{Z}$ که در بخش قبل آمد به قضایای زیر در مورد حلقه‌های با ایده‌آل اصلی تعمیم می‌یابد. از آنجایی که برهانها شبیه هم هستند آنها را اندکی خلاصه می‌کنیم.

خاصیت ایده‌آل اصلی برای حلقه‌های اقلیدسی. هر حلقهٔ اقلیدسی یک حوزهٔ با ایده‌آل صحیح است.

برهان. اگر $I \neq (0)$ ایده‌آلی از R باشد آنگاه $b \in I$ را عنصری با نرم مثبت مینیمم در نظر می‌گیریم[8]. چون I یک ایده‌آل است، شامل همهٔ br هایی که $r \in R$ می‌باشد.

بالعکس، اگر $a \in I$ مضربی از b نباشد آنگاه داریم $a = qb + r$ که $0 < |r| < |b|$. و این مطلب که $r = a - qb$ عضوی از R است در تناقض با مینیمم بودن نرم b می‌باشد.

لذا $I = (b)$ $\square$

خاصیت مقسوم‌علیه اول برای حوزه‌های با ایده‌آل اصلی. اگر p عنصری اول در یک حوزهٔ با ایده‌آل اصلی باشد که ab را عاد می‌کند، آنگاه p باید a یا b را عاد کند.

برهان. فرض کنیم p عنصری اول باشد که ab را عاد می‌کند اما a را عاد نمی‌کند. بنابراین باید نشان دهیم که b را عاد می‌کند.

R یک حوزه با ایده‌آل اصلی باشد

$\Longrightarrow$ $t \in R$ یی موجود است که $\{ar + ps : r, s \in R\} = (t)$

$\Longrightarrow$ $(t) \supseteq (a), \qquad (t) \supseteq (p)$

$\Longrightarrow$ t عناصر a و p را عاد می‌کند

[8] چون نرم مثبت طبیعی مقدار است، بنابر خوشترتیب بودن اعداد طبیعی، b وجود دارد. (م)

$\implies$ $t = ۱$ چون p اوّل است

$\implies$ $۱ = ar + ps$ که $r, s \in R$ ی موجودند

$\implies$ $b = abr + pbs$

$\implies$ p عنصر b را عاد می‌کند $\square$

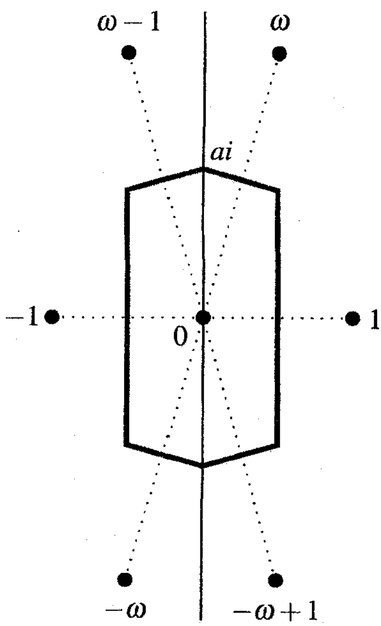
این قضایا دلیل برقراری خاصیت مقسوم‌علیه اول (و در نتیجه دلیل برقراری یکتایی تجزیه به اعداد اول) را در حلقه‌های $\mathbb{Z}$، $\mathbb{Z}[\mathrm{i}]$، $\mathbb{Z}[\sqrt{-۲}]$ و $\mathbb{Z}[\zeta_۳]$ به طور همزمان شرح می‌دهند (این حلقه‌ها اقلیدسی هستند و لذا حوزهٔ با ایده‌آل اصلی می‌باشند).

خاصیت ایده‌آل اصلی $\mathbb{Z}[\mathrm{i}]$ تعبیر هندسی جالبی دارد. همان طور که در بخش ۴.٦ مشاهده کردیم ایده‌آل اصلی (β) متشکل از همهٔ مضارب $\beta \neq ۰$ در $\mathbb{Z}[\mathrm{i}]$، شبکه‌ای با همان شکل $\mathbb{Z}[\mathrm{i}]$ را تشکیل می‌دهد (که توسط $|\beta|$ بزرگ شده است). بنابراین از آنجایی که همهٔ ایده‌آلهای $\mathbb{Z}[\mathrm{i}]$ اصلی هستند نتیجه می‌شود که هر ایده‌آل ناصفر در $\mathbb{Z}[\mathrm{i}]$ به همان شکل $\mathbb{Z}[\mathrm{i}]$ است. همین مطلب (همان گونه که در بخشهای ۲.۷ و ۴.۷ دیدیم) در مورد $\mathbb{Z}[\sqrt{-۲}]$ و $\mathbb{Z}[\zeta_۳]$ نیز درست است. (گوییم دو مجموعه در صفحه یک شکل هستند هرگاه یکی از آنها را بتوان توسط تابعی که فواصل را در عددی ثابت ضرب می‌کند به روی دیگری تصویر کرد.)

بالعکس، ایده‌آلهای غیر اصلی فقط در صورتی موجودند که یکتایی تجزیه با شکست مواجه شود. لذا ایده‌آلهای با شکل متفاوت فقط در صورتی وجود دارند که یکتایی تجزیه با شکست مواجه شود. خواهیم دید که چنین ایده‌آلهایی در $\mathbb{Z}[\sqrt{-۳}]$ و $\mathbb{Z}[\sqrt{-۵}]$ واقعاً اتفاق می‌افتند.

تمرینها

جریان از این قرار است که تنها میدانهای مربعی موهومی مانند $\mathbb{Q}(\sqrt{d})$ که عناصر صحیح آن حلقه‌ای اقلیدسی تشکیل می‌دهند عبارتند از حالتهای $d = -۱, -۲, -۳, -۷, -۱۱$. تنها دو تا از اینها هستند که قبلاً آنها را مورد مطالعه قرار نداده‌ایم. این دو تا عبارتند از $\mathbb{Q}(\sqrt{-۷})$ و $\mathbb{Q}(\sqrt{-۱۱})$ که حلقه‌های عناصر صحیح آنها به ترتیب عبارتند از $\mathbb{Z}[\frac{۱+\sqrt{-۷}}{۲}]$ و $\mathbb{Z}[\frac{۱+\sqrt{-۱۱}}{۲}]$ (زیرا در این حالات داریم $d \equiv_۴ ۱$). فرض می‌کنیم $\omega = \frac{۱+\sqrt{-۷}}{۲}$ یا $\omega = \frac{۱+\sqrt{-۱۱}}{۲}$ و نقاط $\mathbb{Z}[\omega]$ را در صفحهٔ اعداد مختلط در نظر می‌گیریم.



شکل ۴.۱۱: ناحیهٔ نقاطی که به صفر نزدیک‌ترند تا همسایه‌های آن

مطابق معمول، خاصیت تقسیم توسط این گزاره نتیجه می‌شود که هر نقطه از صفحه در فاصله‌ای کمتر از ۱ از نزدیک‌ترین نقطهٔ $\mathbb{Z}[\omega]$ قرار داشته باشد (فصل ۷ را ببینید). این مطلب را به کمک شکل ۴.۱۱ که ۰ و شش همسایهٔ آن یعنی ±۱، $\pm\omega$ و $\pm(\omega - ۱)$ را نشان می‌دهد اثبات می‌کنیم. ناحیهٔ شش ضلعی اطراف

۰ توسط نیمسازهای متعامد خطوط بین ۰ و همسایه‌هایش احاطه شده است و از این رو نقاط داخل آن، نقاطی هستند که به ۰ نزدیک‌ترین‌اند تا هر همسایهٔ دیگر. از آنجایی که هر نقطهٔ $\mathbb{Z}[\omega]$ شبیه ۰ به نظر می‌رسد، کافی است اثبات کنیم نقطه‌ای روی شش ضلعی که از صفر دورتر است (یعنی $a\mathrm{i}$) در فاصله‌ای کمتر از ۱ قرار دارد.

۱.۳.۱۱ نقطهٔ $a\mathrm{i}$ از ۰ و ω به یک فاصله است (چرا؟). نتیجه بگیرید که

$$|a\mathrm{i}| = |a\mathrm{i} - \omega| = |-\frac{۱}{۲} + \frac{۲a - \sqrt{|d|}}{۲}\mathrm{i}|.$$

۲.۳.۱۱ از تمرین ۱.۳.۱۱ نتیجه بگیرید که $a = \frac{۱+|d|}{۴\sqrt{|d|}}$.

۳.۳.۱۱ از تمرین ۲.۳.۱۱ نتیجه بگیرید که برای $d = -۷, -۱۱$ داریم $a < ۱$ و لذا $\mathbb{Z}[\frac{۱+\sqrt{d}}{۲}]$ در این حالات واجد خاصیت تقسیم است.

لذا $\mathbb{Z}[\frac{۱+\sqrt{-۷}}{۲}]$ و $\mathbb{Z}[\frac{۱+\sqrt{-۱۱}}{۲}]$ دارای یکتایی تجزیه به اعداد اول هستند. می‌توانیم از این مطلب برای حل معادله‌های $y^۳ = x^۲ + ۷$ و $y^۳ = x^۲ + ۱۱$ کمک بگیریم و آن را همانند معادله‌های $y^۳ = x^۲ + ۱$، $y^۳ = x^۲ + ۲$ و $y^۳ = x^۲ + ۴$ که در فصل ۷ و تمرینهای آن بررسی کردیم، حل کنیم. بالاخص معادلهٔ $y^۳ = x^۲ + ۱۱$ جالب است چون یکی از جوابهای آن به اندازهٔ کافی بزرگ است و بدیهی نمی‌باشد.

۴.۳.۱۱ اگر $y^۳ = x^۲ + ۱۱ = (x + \sqrt{-۱۱})(x - \sqrt{-۱۱})$ آنگاه از یکتایی تجزیه در $\mathbb{Z}[\frac{۱+\sqrt{-۱۱}}{۲}]$ استفاده کنید و نشان دهید که

$$x + \sqrt{-۱۱} = (a^۳ - ۳۳ab^۲) + (۳a^۲b - ۱۱b^۳)\sqrt{-۱۱},$$

که در آن a و b هر دو صحیح هستند یا هر دو نیم‌صحیحی هستند که صحیح نمی‌باشند.

۵.۳.۱۱ به وسیلهٔ یافتن جوابی صحیح برای معادلهٔ $۱ = b(۳a^۲ - ۱۱b^۲)$، جوابی صحیح برای $y^۳ = x^۲ + ۱۱$ بیابید.

۶.۳.۱۱ به وسیلهٔ یافتن جوابی نیم‌صحیح برای معادلهٔ $۱ = b(۳a^۲ - ۱۱b^۲)$، جواب صحیح دیگری برای $y^۳ = x^۲ + ۱۱$ بیابید و نشان دهید که این جواب تنها جواب دیگر x و y (تا حد علامت x) برای این معادله است.

۴.۱۱ یک ایده‌آل غیر اصلی

می‌توانیم یکتا نبودن تجزیهٔ ۴ به اعداد اول در $\mathbb{Z}[\sqrt{-۳}]$ را که به صورتهای

$$۴ = ۲ \times ۲ = (۱ + \sqrt{-۳})(۱ - \sqrt{-۳})$$

تجزیه می‌شود با مشاهدهٔ مقسوم‌علیه‌های مشترک ایده‌آلی ۲ و $۱ + \sqrt{-۳}$ برای تجزیه به عوامل دریابیم. با استفاده از ایدهٔ بخش ۱.۱۱ ایده‌آل $(۲) + (۱ + \sqrt{-۳})$ را با افزودن همهٔ مضارب ۲ به همهٔ مضارب $۱ + \sqrt{-۳}$ تشکیل می‌دهیم.

یک عنصر دلخواه از $(۲) + (۱ + \sqrt{-۳})$ عبارت است از

$$۲(a + b\sqrt{-۳}) + (۱ + \sqrt{-۳})(c + d\sqrt{-۳})$$

برای a، b، c و d یی در $\mathbb{Z}$ و این برابر است با

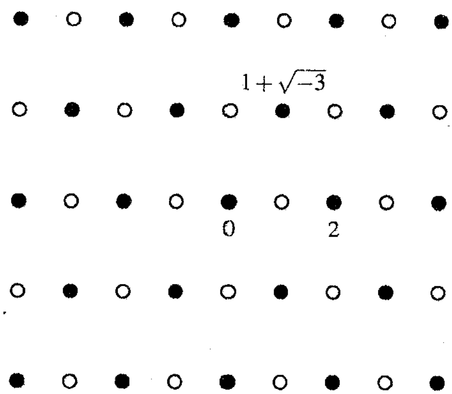
$$۲(a - b - ۲d) + (۱ + \sqrt{-۳})(۲b + c + d)$$

که برابر $۲m + (۱ + \sqrt{-۳})n$ برای m و n ی در $\mathbb{Z}$ می‌باشد.

بالعکس، برای هر $m, n \in \mathbb{Z}$ داریم $۲m + (۱ + \sqrt{-۳})n \in (۲) + (۱ + \sqrt{-۳})$ و در نتیجه

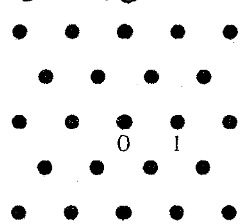
$$(۲) + (۱ + \sqrt{-۳}) = \{۲m + (۱ + \sqrt{-۳})n : m, n \in \mathbb{Z}\}.$$

شکل ۵.۱۱ عناصر این ایده‌آل را نشان می‌دهد که با دایره‌های سیاه در بین اعضای $\mathbb{Z}[\sqrt{-۳}]$ مشخص شده‌اند. واضح است که $(۲) + (۱ + \sqrt{-۳})$ متشکل از مثلثهایی متساوی‌الاضلاع است و از این رو به همان شکل $\mathbb{Z}[\sqrt{-۳}]$ نمی‌باشد. (مثلاً هیچ نقطه‌ای از این ایده‌آل همسایه‌ای در جهتهای متعامد ندارد.)



شکل ۵.۱۱: ایده‌آل $(۲) + (۱ + \sqrt{-۳})$ در $\mathbb{Z}[\sqrt{-۳}]$

لذا $(۲) + (۱ + \sqrt{-۳})$ یک ایده‌آل غیر اصلی است: این ایده‌آل متشکل از همهٔ مضارب عنصری از $\mathbb{Z}[\sqrt{-۳}]$ نیست. اما می‌توانیم این رویا را در سر داشته باشیم که $(۲) + (۱ + \sqrt{-۳})$ متشکل از مضارب عددی ایده‌آلی (چیزی بیرون $\mathbb{Z}[\sqrt{-۳}]$) است و این رویا به سادگی به تحقق می‌پیوندد.



شکل ۶.۱۱: ایده‌آل اصلی $\mathbb{Z}[\frac{۱+\sqrt{-۳}}{۲}] = (\frac{۱+\sqrt{-۳}}{۲})$

شکل $(۲) + (۱ + \sqrt{-۳})$ دقیقاً مثل شکل $\mathbb{Z}[\frac{۱+\sqrt{-۳}}{۲}]$ است که مجموعهٔ مضارب $\frac{۱+\sqrt{-۳}}{۲}$ می‌باشد (شکل ۶.۱۱). لذا $\frac{۱+\sqrt{-۳}}{۲}$ همان عدد ایده‌آلی مطلوب است. عدد $\frac{۱+\sqrt{-۳}}{۲}$ در $\mathbb{Z}[\frac{۱+\sqrt{-۳}}{۲}]$ هم ۲ را عاد می‌کند و هم $۱ + \sqrt{-۳}$ را، و نرمش نیز برابر ۱ است. از این رو $\frac{۱+\sqrt{-۳}}{۲}$ همان ب.م.م. ۲ و $۱ + \sqrt{-۳}$ است.

لذا در این حالت، این عدد ایده‌آلی که مضارب آن ایده‌آل غیر اصلی ما را تشکیل می‌دهد واقعاً وجود دارد اما در جایی خارج از حلقهٔ مورد بحث.

تمرینها

گونهٔ جالب دیگری از این پدیده در $\mathbb{Z}[\sqrt{-۷}]$ اتفاق می‌افتد که در آن ایده‌آل $(۲) + (۱ + \sqrt{-۷})$ غیر اصلی است. شکل این ایده‌آل در حقیقت با ایده‌آل اصلی مضارب $\frac{۱+\sqrt{-۷}}{۲}$ در $\mathbb{Z}[\frac{۱+\sqrt{-۷}}{۲}]$ یکی است، گرچه به سادگی دیده نمی‌شود که چنین باشد.

۱.۴.۱۱ نشان دهید که

$$(۲) + (۱ + \sqrt{-۷}) = \{۲m + (۱ + \sqrt{-۷})n : m, n \in \mathbb{Z}\}.$$

۲.۴.۱۱ با استفاده از تقریب ۲/۶ برای $\sqrt{۷}$ طرحی از شکل $\mathbb{Z}[\sqrt{-۷}]$ را ارائه دهید و اعضای $(۲) + (۱ + \sqrt{-۷})$ را در آن مشخص سازید.

۳.۴.۱۱ نشان دهید که شکل $(۲) + (۱ + \sqrt{-۷})$ با $\mathbb{Z}[\sqrt{-۷}]$ یکی نیست و از این رو یک ایده‌آل اصلی نمی‌باشد.

۴.۴.۱۱ نشان دهید که در $\mathbb{Z}[\frac{۱+\sqrt{-۷}}{۲}]$ داریم

$$\gcd(۲, ۱ + \sqrt{-۷}) = \frac{۱ + \sqrt{-۷}}{۲}$$

و طرحی از ایده‌آل اصلی $(\frac{۱+\sqrt{-۷}}{۲})$ را در $\mathbb{Z}[\frac{۱+\sqrt{-۷}}{۲}]$ ارائه دهید.

۵.۴.۱۱ با محاسبهٔ طول اضلاع یک مثلث از این ایده‌آل اصلی، نشان دهید که شکل آن با $(۲) + (۱ + \sqrt{-۷})$ در $\mathbb{Z}[\sqrt{-۷}]$ یکی است.

۶.۴.۱۱ نشان دهید که ۸ در $\mathbb{Z}[\sqrt{-۷}]$ تجزیه‌های متفاوتی دارد اما همهٔ این تجزیه‌ها در $\mathbb{Z}[\frac{۱+\sqrt{-۷}}{۲}]$ یکی هستند.

۵.۱۱ یک ایده‌آل غیر اصلی دیگر

شبیه $\mathbb{Z}[\sqrt{-۳}]$ همان طور که دو تجزیهٔ

$$۲ \times ۳ = (۱ + \sqrt{-۵})(۱ - \sqrt{-۵})$$

نشان می‌دهد، خاصیت مقسوم‌علیه اول در $\mathbb{Z}[\sqrt{-۵}]$ نیز با شکست مواجه می‌شود.

نرم اعداد ۲، ۳، $۱ + \sqrt{-۵}$ و $۱ - \sqrt{-۵}$ به ترتیب برابر ۴، ۹، ٦ و ٦ است که مقسوم‌علیه‌های ۲ و ۳ از آنها برابر نرم $a^۲ + ۵b^۲$ از هیچ عنصری مانند $a + b\sqrt{-۵}$ از $\mathbb{Z}[\sqrt{-۵}]$ نیست. از این رو هیچ یک از اعداد ۲، ۳، $۱ + \sqrt{-۵}$ و $۱ - \sqrt{-۵}$ حاصل ضرب اعدادی با نرم کوچک‌تر نیستند و لذا در $\mathbb{Z}[\sqrt{-۵}]$ اولند.

برای درک این عدم یکتایی تجزیه، ابتدا ب.م.م. ایده‌آلی ۲ و $۱ + \sqrt{-۵}$ را می‌سازیم: مجموعهٔ $(۲) + (۱ + \sqrt{-۵})$ متشکل از مجموع مضارب ۲ و مضارب $۱ + \sqrt{-۵}$. محاسباتی مشابه آنچه در بخش قبل داشتیم نشان می‌دهد که هر عضو

$$۲(a + b\sqrt{-۵}) + (۱ + \sqrt{-۵})(c + d\sqrt{-۵}) \in (۲) + (۱ + \sqrt{-۵})$$

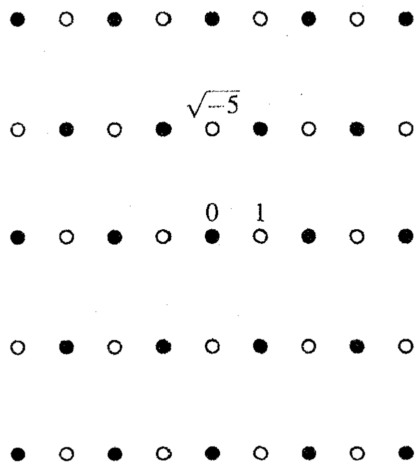
واقعاً به شکل $۲m + (۱ + \sqrt{-۵})n$ برای m و n ی در $\mathbb{Z}$ است (تمرین).

بالعکس، هر چنین عددی به شکل $۲m + (۱ + \sqrt{-۵})n$ در $(۲) + (۱ + \sqrt{-۵})$ است و لذا

$$(۲) + (۱ + \sqrt{-۵}) = \{۲m + (۱ + \sqrt{-۵})n : m, n \in \mathbb{Z}\}.$$

شکل ۷.۱۱ اعضای این ایده‌آل را به صورت دایره‌های سیاه در شکلی از $\mathbb{Z}[\sqrt{-۵}]$ نشان می‌دهد. از این شکل واضح است که هیچ نقطهٔ سیاهی همسایه‌ای در جهت‌های متعامد ندارد و لذا این ایده‌آل به شکل $\mathbb{Z}[\sqrt{-۵}]$

نیست. بالاخص این ایده‌آل یک ایده‌آل اصلی به شکل (β) نیست چرا که (β) همان $\mathbb{Z}[\sqrt{-۵}]$ است که در β ضرب شده است و در نتیجه، فواصل همگی در $|\beta|$ ضرب می‌شوند و از این رو همان طور که در بخش **۱.۸** دیدیم مجموعه‌ای با همان شکل $\mathbb{Z}[\sqrt{-۵}]$ به دست می‌آید. لذا $(۲)+(۱+\sqrt{-۵})$ غیر اصلی است.



شکل ۷.۱۱: ایده‌آل غیر اصلی $(۲)+(۱+\sqrt{-۵})$ در $\mathbb{Z}[\sqrt{-۵}]$

علاقه‌مندیم که اعضای $(۲)+(۱+\sqrt{-۵})$ را به عنوان مضارب عددی ایده‌آلی در بیرون $\mathbb{Z}[\sqrt{-۵}]$ بنگریم. اما $\mathbb{Z}[\sqrt{-۵}]$ از قبل شامل همهٔ اعداد صحیح $\mathbb{Z}[\sqrt{-۵}]$ است. لذا واضح نیست که این عدد ایده‌آلی را کجا می‌توان یافت. در عوض، روش ددکیند (۱۸۷۱) را پی می‌گیریم و بدون عدد ایده‌آلی، مستقیماً با خود ایده‌آل کار می‌کنیم.

همان گونه که دیدیم، یک ایده‌آل اصلی مانند (β) همانند β رفتار می‌کند، بدین معنی که

(β) شامل (γ) است فقط و فقط وقتی که β عنصر γ را عاد کند.

بدین مفهوم، ایده‌آل غیر اصلی $(۲)+(۱+\sqrt{-۵})$ رفتاری شبیه عددی که هم ۲ و هم $۱+\sqrt{-۵}$ را عاد می‌کند دارد، زیرا

$(۲) + (۱ + \sqrt{-۵})$ شامل (۲) و شامل $(۱ + \sqrt{-۵})$ است.

و در حقیقت می‌بینیم که $(۲) + (۱ + \sqrt{-۵})$ شایستگی آن را دارد که بزرگ‌ترین مقسوم‌علیه مشترک ۲ و $۱ + \sqrt{-۵}$ باشد زیرا ایده‌آل نظیر آن در $\mathbb{Z}$ (یعنی $(a) + (b) = \{am + bn : m, n \in \mathbb{Z}\}$ که $\gcd(a, b)$ است) نیز همان طور که در بخش ۱.۱۱ دیدیم چنین است.

نه فقط این، بلکه $(۲) + (۱ + \sqrt{-۵})$ لیاقت اول تلقی شدن را نیز دارد. در بخش ۲.۱۱ دیدیم که یک ایده‌آل اصلی اول مانند (p)، بیشین است بدین مفهوم که (۱) و (p) تنها ایده‌آلهای شامل آن هستند. به طور مشابه، تنها ایده‌آلهای شامل $(۲) + (۱ + \sqrt{-۵})$ عبارتند از (۱) و خود $(۲) + (۱ + \sqrt{-۵})$. این مطلب بدان دلیل است که

$$(۲) + (۱ + \sqrt{-۵}) = \{۲m + (۱ + \sqrt{-۵})n : m, n \in \mathbb{Z}\}$$

متشکل از اعدادی به شکل یک عدد زوج به علاوهٔ $(۱ + \sqrt{-۵})n$ است. از این رو هر عضو $\mathbb{Z}[\sqrt{-۵}]$ که در $(۲) + (۱ + \sqrt{-۵})$ نباشد باید به شکل عددی فرد به علاوهٔ $(۱ + \sqrt{-۵})n$ باشد. اما ایده‌آلی که شامل همهٔ اعضای به شکل یک عدد زوج به علاوهٔ $(۱ + \sqrt{-۵})n$ و حداقل یک عضو به شکل یک عدد فرد به علاوهٔ $(۱ + \sqrt{-۵})n'$ باشد به وضوح شامل ۱ است و از این رو همهٔ $\mathbb{Z}[\sqrt{-۵}]$ را (با توجه به بسته بودن تحت ضرب در اعضای $\mathbb{Z}[\sqrt{-۵}]$) در خود دارد. لذا $(۲) + (۱ + \sqrt{-۵})$ یک ایده‌آل بیشین است. همین که ضرب ایده‌آلها تعریف شود، خواهیم دید که ایده‌آلهای بیشین، اول هستند.

همچنین برای تأیید این حقیقت که $(۲) + (۱ + \sqrt{-۵})$ ایده‌آل (۲) را (به مفهومی متعارف در نظریهٔ حلقه‌ها) عاد می‌کند (یعنی برای ایده‌آلی مانند I داریم $I \times ((۲) + (۱ + \sqrt{-۵})) = (۲)$) احتیاج داریم که ضرب ایده‌آلها را تعریف کنیم. این کار را در بخش ۷.۱۱ انجام خواهیم داد و راز عامل I را در بخش ۸.۱۱ می‌گشاییم.

تمرینها

۱.۵.۱۱ بررسی کنید که وقتی a، b، c و d اعدادی صحیح باشند $۲(a+b\sqrt{-۵})+(۱+\sqrt{-۵})(c+d\sqrt{-۵})$ به شکل $۲m+(۱+\sqrt{-۵})n$ برای m و n ی صحیح است.

همچنین مهم است توجه شود که برای تلفیق دو تجزیهٔ ۶ در $\mathbb{Z}[\sqrt{-۵}]$ به ایده‌آل ۳ و $۱+\sqrt{-۵}$ می‌رسیم که اعضای آن به شکل

$$۳(a+b\sqrt{-۵})+(۱+\sqrt{-۵})(c+d\sqrt{-۵})$$

برای a، b، c و d یی در $\mathbb{Z}$ می‌باشند.

۲.۵.۱۱ بررسی کنید که $۳(a+b\sqrt{-۵})+(۱+\sqrt{-۵})(c+d\sqrt{-۵})$ به شکل $۳m+(۱+\sqrt{-۵})n$ برای m و n ی در $\mathbb{Z}$ می‌باشد.

۳.۵.۱۱ از تمرین ۲.۵.۱۱ نتیجه بگیرید که

$$(۳)+(۱+\sqrt{-۵})=\{۳m+(۱+\sqrt{-۵})n : m,n\in\mathbb{Z}\}.$$

۶.۱۱ ایده‌آلهای میدانهای مربعی موهومی به عنوان شبکه

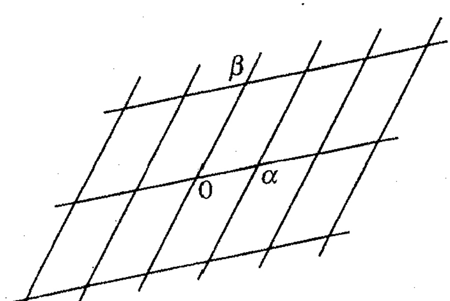
گرچه ایده‌آلهای حلقه‌های اعداد صحیح مربعی همیشه اصلی نیستند، با این حال می‌توانیم چیزی شبیه این قضیه را که $\mathbb{Z}$ یک حوزهٔ با ایده‌آل اصلی است اثبات کنیم. هر یک از ایده‌آلهای $\mathbb{Z}$ دارای یک مولد هستند، بدین مفهوم که هر یک از آنها متشکل از مضارب عددی صحیح مانند a است. خود $\mathbb{Z}$ ایده‌آلی

است که توسط ۱ تولید می‌شود. قضیهٔ مشابه (با برهانی مشابه) برای ایده‌آلهای مشمول در اعداد صحیح $\mathbb{Q}(\sqrt{d})$ بیان می‌دارد که چنین ایده‌آلهایی دارای دو مولد هستند؛ همان طور که خود اعداد صحیح $\mathbb{Q}(\sqrt{d})$ نیز چنین است.

توصیف اعداد صحیح $\mathbb{Q}(\sqrt{d})$ در بخش ۴.۱۰ نشان داد که آنها شامل $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ یا $\mathbb{Z}[\sqrt{d}]$ هستند. در هر یک از حالات، اعداد صحیح $\mathbb{Q}(\sqrt{d})$ زیرگروهی مانند L از $\mathbb{C}$ را با دو مولد تشکیل می‌دهد: ۱ و $\frac{1+\sqrt{d}}{2}$ برای $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ و نیز ۱ و $\sqrt{d}$ برای $\mathbb{Z}[\sqrt{d}]$. وقتی $d < 0$، مولدهای L را می‌توان به طور هندسی به عنوان دو عنصر غیر صفری که به ۰ نزدیک‌ترند اما روی خطی یکسان که از ۰ می‌گذرد قرار ندارند توصیف کرد. و گروهی که این دو عضو تولید می‌کنند یک شبکه نامیده می‌شود.

در حالت کلی، یک شبکه مانند L در $\mathbb{C}$، مجموعهٔ $\{\alpha m + \beta n : m, n \in \mathbb{Z}\}$ است که در آن α و β اعداد غیر صفر مختلطی هستند که روی خطی یکسان که از ۰ می‌گذرد قرار ندارند. زوج α و β از مولدها را یک پایهٔ صحیح برای L می‌نامیم. عناصر L روی تقاطع دو خانواده از خطوط موازی قرار دارند که شبکه‌ای را به مفهوم واقعی کلمهٔ شبکه به وجود می‌آورند (شکل ۸.۱۱). خاصیتی مهم از شبکهٔ اعداد صحیح در $\mathbb{Z}(\sqrt{d})$ این است که هر زیرگروه آن (و از این رو هر ایده‌آل آن) نیز یک شبکه است.

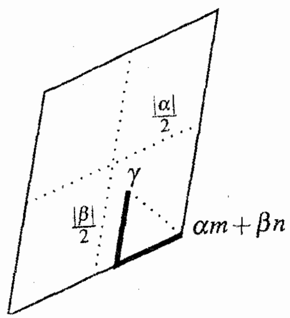
خاصیت شبکه‌ای ایده‌آلها. وقتی $d < 0$، هر ایده‌آل غیر صفر در اعداد صحیح $\mathbb{Q}(\sqrt{d})$ یک شبکه است.



شکل ۸.۱۱: یک شبکه در $\mathbb{C}$

برهان. فرض کنیم I ایده‌آلی در اعداد صحیح $\mathbb{Q}(\sqrt{d})$ باشد. نیز فرض کنیم α عنصری غیر صفر از I باشد که نزدیک‌ترین نقطه به ۰ است[۹]. چون I تحت جمع و تحت ضرب در ۱− بسته است، شامل مضارب صحیح معمولی α نیز می‌باشد. اما این همهٔ I نیست چون I، عدد $\alpha\sqrt{d}$ را نیز در بر دارد که در جهتی عمود بر جهت خط واصل بین α و ۰ قرار دارد (چون $d < 0$).

حال فرض کنیم $\beta \in I$ تا جایی که می‌تواند به ۰ نزدیک باشد اما نه در جهتی که مضارب صحیح α قرار گرفته‌اند. ادعا می‌کنیم که شبکهٔ $\{\alpha m + \beta n : m, n \in \mathbb{Z}\}$ برابر I است.



شکل ۹.۱۱: نقطهٔ $\alpha m + \beta n$ از شبکه که نزدیک‌ترین نقطه به γ است

اگر چنین نباشد، γ را عضوی از I می‌گیریم که در $\{\alpha m + \beta n : m, n \in \mathbb{Z}\}$ نباشد و متوازی‌الاضلاعی از شبکه را که شامل γ است در نظر می‌گیریم (شکل ۹.۱۱). اکنون γ لزوماً در یک چهارم متوازی‌الاضلاع قرار دارد که در این حالت بنابر نامساوی مثلث، فاصله‌اش از نزدیک‌ترین گوشه یعنی $\alpha m + \beta n$ کمتر از $\frac{|\alpha|}{۲} + \frac{|\beta|}{۲}$ و لذا کمتر از $\max(|\alpha|, |\beta|)$ است که برابر ضلع بزرگ‌تر متوازی‌الاضلاع می‌باشد. اما در این صورت عنصر $\gamma - (\alpha m + \beta n)$ از I در فاصلهٔ کمتر از $\max(|\alpha|, |\beta|)$ از ۰ قرار دارد که متناقض با انتخاب α و β می‌باشد. □

برهان فوق فرض نمی‌کند که I یک ایده‌آل باشد بلکه فقط فرض می‌کند که تحت + و − بسته باشد (و از این رو یک گروه باشد). با فرض آن که

[۹] با توجه به طبیعی بودن فاصله‌ها این نقطه وجود دارد. (م)

$I = \{\alpha m + \beta n : m, n \in \mathbb{Z}\}$ ایده‌آل باشد به نتیجهٔ قوی‌تر $I = (\alpha) + (\beta)$ می‌رسیم؛ مجموعی از دو ایده‌آل اصلی که توسط α و β تولید می‌شود.

همواره داریم

$$I = \{\alpha m + \beta n : m, n \in \mathbb{Z}\} \subseteq (\alpha) + (\beta)$$

چون $\alpha m \in (\alpha)$ و $\beta n \in (\beta)$. بالعکس، $\{\alpha m + \beta n : m, n \in \mathbb{Z}\}$ لزوماً شامل α است. از این رو اگر I یک ایده‌آل باشد آنگاه شامل همهٔ اعضای (α) می‌باشد چرا که I تحت مضارب α از حلقه بسته است. به طور مشابه I شامل همهٔ اعضای (β) است. لذا $(\alpha) + (\beta) \supseteq I$، چون I تحت جمع بسته است.

تمرینها

باید تاکید کرد که گرچه یک ایده‌آل مانند $\{\alpha m + \beta n : m, n \in \mathbb{Z}\}$ لزوماً برابر ایده‌آل مجموع $(\alpha) + (\beta)$ است با این حال عکس این مطلب لزوماً درست نیست. مسلماً همان طور که در بالا دیدیم $(\alpha) + (\beta) \supseteq \{\alpha m + \beta n : m, n \in \mathbb{Z}\}$، اما $(\alpha) + (\beta)$ ممکن است شامل اعضایی باشد که به شکل $\alpha m + \beta n$ برای m و n ی در $\mathbb{Z}$ نباشند. در این حالت زوج α و β پایه‌ای صحیح برای $(\alpha) + (\beta)$ نیست.

۱.۶.۱۱ نشان دهید که $(۵) + (۱ + \sqrt{-۵})$ در $\mathbb{Z}[\sqrt{-۵}]$ شامل $\sqrt{-۵}$ است.

۲.۶.۱۱ نشان دهید که به ازای هر $m, n \in \mathbb{Z}$ داریم

$$\sqrt{-۵} \neq ۵m + (۱ + \sqrt{-۵})n.$$

لذا $(۵) + (۱ + \sqrt{-۵}) \neq \{۵m + (۱ + \sqrt{-۵})n : m, n \in \mathbb{Z}\}$ و بنابراین ۵ و $۱ + \sqrt{-۵}$ پایه‌ای صحیح برای $(۵) + (۱ + \sqrt{-۵})$ نیست. با این حال بنابر

خاصیت شبکه‌ای ایده‌آلها که در بالا اثبات کردیم می‌دانیم که $(۵) + (۱ + \sqrt{-۵})$ پایه‌ای صحیح مانند α و β دارد.

۳.۶.۱۱ α و β یی در $\mathbb{Z}[\sqrt{-۵}]$ بیابید که

$$(۵) + (۱ + \sqrt{-۵}) = \{\alpha m + \beta n : m, n \in \mathbb{Z}\}.$$

۷.۱۱ حاصل ضرب ایده‌آلها و ایده‌آلهای اول

از آنجایی که می‌خواهیم ایده‌آل (s) از یک حلقه مانند R شبیه عنصر s از R رفتار کند، حاصل ضرب $(s)(t)$ از ایده‌آلهای اصلی (s) و (t) نیز باید برابر (st) باشد. این بدان معنی است که حاصل ضرب هر عنصر به صورت rs از (s) و هر عنصر به صورت $r't$ از (t) عنصری به صورت $rr'st$ از $(s)(t)$ است. و از این رو چنین نتیجه‌ای باید برای مجموع هر دو چنین حاصل ضربی نیز برقرار باشد. از این ایده برای تعریف حاصل ضرب دو ایده‌آل در حالت کلی استفاده می‌کنیم.

تعریف. حاصل ضرب AB از دو ایده‌آل A و B در یک حلقه مانند R عبارت است از

$$AB = \{a_۱b_۱ + a_۲b_۲ + \ldots + a_kb_k : a_i \in A, b_i \in B\}.$$

واضح است که AB تحت جمع و ضرب در عناصر R بسته است و از این رو یک ایده‌آل می‌باشد. اکنون ایده‌آلهای اول را به عنوان ایده‌آلهایی که خاصیت مقسوم‌علیه اول نسبت به حاصل ضرب ایده‌آلها دارند تعریف می‌کنیم.

تعریف. یک ایده‌آل مانند P اول است هرگاه از این که P شامل حاصل ضرب AB باشد (یعنی AB را عاد کند) نتیجه بگیریم که P شامل A یا شامل B است.

روشی کوتاه‌تر برای بیان تعریف ایده‌آل اول این است:

$$AB \subseteq P \Longrightarrow A \subseteq P \quad \text{یا} \quad B \subseteq P \qquad (۱)$$

تعریفی که به جای شمول با عضویت سر و کار داشته باشد عبارت است از:

$$ab \in P \Longrightarrow a \in P \quad \text{یا} \quad b \in P \qquad (۲)$$

و این دو صورت بنابر قضیهٔ زیر معادلند.

تعاریف معادل ایده‌آل اول. خواص زیر برای یک ایده‌آل مانند P معادلند:

(۱) اگر $AB \subseteq P$ آنگاه $A \subseteq P$ یا $B \subseteq P$،

(۲) اگر $ab \in P$ آنگاه $a \in P$ یا $b \in P$.

برهان. $(۲) \Rightarrow (۱)$:

$$\begin{aligned} ab \in P \quad &\Longrightarrow \quad (ab) \subseteq P \quad && \text{بنابر بسته بودن } P \\ &\Longrightarrow \quad (a)(b) \subseteq P && \text{بنابر تعریف } (a)(b) \\ &\Longrightarrow \quad (a) \subseteq P \text{ یا } (b) \subseteq P && \text{بنابر خاصیت } (۱) \\ &\Longrightarrow \quad a \in P \text{ یا } b \in P, && \text{چون } a \in (a) \text{ و } b \in (b) \end{aligned}$$

$(۱) \Rightarrow (۲)$:

فرض کنیم $AB \subseteq P$ ولی $A \not\subseteq P$. لذا باید نشان دهیم که $B \subseteq P$. چون $A \not\subseteq P$، عضوی از A مانند a موجود است که $a \notin P$. بنابراین برای هر $b \in B$ داریم

$$\begin{aligned} AB \subseteq P \quad &\Longrightarrow \quad ab \in P && \text{بنابر تعریف } AB \\ &\Longrightarrow \quad a \in P \text{ یا } b \in P && \text{بنابر خاصیت } (۲) \\ &\Longrightarrow \quad b \in P && \text{چون } a \notin P \\ &\Longrightarrow \quad B \subseteq P. \square \end{aligned}$$

همان طور که در بخش ۲.۱۱ گفتیم، ایده‌آلهای اصلی اول، بیشین هستند بدین مفهوم که تنها ایده‌آلی که به طور محض شامل آنها است کل حلقه می‌باشد. اما اول و بیشین در حالت کلی یکی نیستند لذا به تعریفی مجزا برای ایده‌آل بیشین نیاز داریم.

تعریف. یک ایده‌آل مانند M در یک حلقه مانند R بیشین است هرگاه $M \neq R$ اما تنها ایده‌آلهای شامل M عبارت باشند از R و خود M.

اکنون می‌توانیم ارتباطی بین ایده‌آلهای اول و بیشین را در یک جهت اثبات کنیم:

اول بودن ایده‌آلهای بیشین. هر ایده‌آل بیشین اول است.

برهان. فرض کنیم که M ایده‌آلی بیشین باشد، $ab \in M$ ولی $a \notin M$. لذا (با استفاده از تعریف دوم ایده‌آل اول) باید نشان دهیم که $b \in M$.

چون M بیشین است و $a \notin M$، پس ایده‌آل

$$M[a] = \{ar + ms : r, s \in R, m \in M\},$$

که هم شامل M و هم شامل a است باید برابر کل R باشد. بالاخص این بدان معنی است که ۱ به صورت $ar + ms$ است. اکنون می‌توانیم از حقه‌ای معروف استفاده کنیم:

$$\begin{aligned} ۱ = ar + ms \quad &\Longrightarrow \quad b = abr + mbs \\ &\Longrightarrow \quad b \in M, \quad \text{چون } ab \in M \text{ و } m \in M \quad \square \end{aligned}$$

مثالهایی از ایده‌آل اول

• در بخش ۵.۱۱ دریافتیم که ایده‌آل غیر اصلی $(۲) + (۱ + \sqrt{-۵})$ بیشین است. از این رو بنابر قضیهٔ فوق ایده‌آلی اول می‌باشد.

• مثالی دیگر $(۳) + (۱ + \sqrt{-۵}) = \{۳m + (۱ + \sqrt{-۵})n : m, n \in \mathbb{Z}\}$ است که بنابه دلیل زیر بیشین می‌باشد. عناصری که در آن نیستند به شکل $۳m' + ۱ + (۱ + \sqrt{-۵})n'$ یا $۳m' + ۲ + (۱ + \sqrt{-۵})n'$ هستند. اکنون هر ایده‌آلی که شامل $(۳) + (۱ + \sqrt{-۵})$ و عددی به شکل $۳m' + ۱ + (۱ + \sqrt{-۵})n'$ باشد شامل ۱ است و لذا برابر کل $\mathbb{Z}[\sqrt{-۵}]$ می‌باشد. همچنین هر ایده‌آلی که شامل $(۳) + (۱ + \sqrt{-۵})$ و عددی به شکل $۳m' + ۲ + (۱ + \sqrt{-۵})n'$ باشد شامل ۲ است و لذا شامل $۱ = ۳ - ۲$ نیز می‌باشد و در نتیجه این ایده‌آل نیز برابر کل $\mathbb{Z}[\sqrt{-۵}]$ است.

• با استدلالی مشابه، ایده‌آل $(۳) + (۱ - \sqrt{-۵})$ بیشین و لذا اول است. این ایده‌آل، مزدوج $(۳) + (۱ + \sqrt{-۵})$ نامیده می‌شود چون اعضای آن مزدوج اعضای $(۳) + (۱ + \sqrt{-۵})$ هستند.

شبیه $(۲) + (۱ + \sqrt{-۵})$، ایده‌آل $(۳) + (۱ + \sqrt{-۵})$ و مزدوج آن نیز در $\mathbb{Z}[\sqrt{-۵}]$ غیر اصلی هستند. این مطلب را می‌توان با ساختن تصویری از $(۳) + (۱ + \sqrt{-۵})$ و مشاهدهٔ این نکته که هیچ عضوی از آن دارای همسایه‌هایی در جهتهای متعامد نیست و از این رو شکل آن با $\mathbb{Z}[\sqrt{-۵}]$ یکی نیست مورد تحقیق قرار داد. نکتهٔ نسبتاً تعجب‌آور این است که شکل آن با $(۲) + (۱ + \sqrt{-۵})$ یکی است (تمرین).

تمرینها

در مطالعهٔ شکل شبکه‌ها، حقیقت کلیدی که باعث آگاهی می‌شود این است که اگر α و β اعدادی مختلط در جهتهایی متفاوت از ۰ باشند آنگاه نسبت فواصل آنها از ۰ برابر $|\frac{\alpha}{\beta}|$ است و زاویهٔ بین جهتهایشان برابر $\arg\frac{\alpha}{\beta}$ می‌باشد. لذا شکل متوازی‌الاضلاع مشخص شده به وسیلهٔ ۰، α و β توسط خارج قسمت $\frac{\alpha}{\beta}$ تعیین می‌گردد.

۱.۷.۱۱ طرحی از شکل $(3) + (1 + \sqrt{-5})$ را تا حدی دقیق ارائه دهید که برای اثبات متفاوت بودن شکل آن با $\mathbb{Z}[\sqrt{-5}]$ کافی باشد.

۲.۷.۱۱ توضیح دهید که چرا شبکه‌های $(3) + (1 + \sqrt{-5})$ و $(3) + (1 - \sqrt{-5})$ شکلی یکسان دارند.

۳.۷.۱۱ با درنظر گرفتن خارج قسمتهای $\frac{2}{1+\sqrt{-5}}$ و $\frac{1-\sqrt{-5}}{3}$ نشان دهید که شبکه‌های $(2) + (1 + \sqrt{-5})$ و $(3) + (1 - \sqrt{-5})$ یک شکل هستند.

همهٔ ایده‌آلهای غیر اصلی $\mathbb{Z}[\sqrt{-5}]$ با $(2) + (1 + \sqrt{-5})$ یک شکل هستند (تمرین ۷.۱۲ را ببینید). لذا دقیقاً دو شکل برای ایده‌آلهای $\mathbb{Z}[\sqrt{-5}]$ اتفاق می‌افتد. بیان این مطلب به شیوهٔ کلاسیک چنین است: عدد رده‌ای[۱۰] $\mathbb{Z}[\sqrt{-5}]$ برابر ۲ است.

۸.۱۱ تجزیه به ایده‌آلهای اول

اکنون که تعریفی از حاصل ضرب ایده‌آلها داریم می‌توانیم تقسیم‌پذیری را برای آنها تعریف کنیم؛ همان گونه که قبلاً نیز در مورد هر حاصل ضرب تعویض‌پذیری این کار را انجام دادیم: B ایده‌آل A را عاد می‌کند یعنی ایده‌آلی

[۱۰] class number

مانند C وجود دارد به قسمی که $A = BC$. اما قبلاً پیشنهاد کرده بودیم که عاد کردن برای ایده‌آلها باید به معنای شامل بودن باشد. لذا اکنون این بخت را داریم که شایستگی شمول را برای مفهوم تقسیم‌پذیری بیازماییم.

مثالهای ما ایده‌آلهایی غیر اصلی در $\mathbb{Z}[\sqrt{-۵}]$ از قبیل $(۲) + (۱ + \sqrt{-۵})$ هستند. برای آن که خواندن حاصل ضربها ساده‌تر باشد، ایده‌آل با پایهٔ صحیح α و β را به صورت (α, β) می‌نویسیم؛ مثلاً $(۲, ۱ + \sqrt{-۵}) = (۲) + (۱ + \sqrt{-۵})$ (این نماد با نمادی که برای زوج مرتب به کار می‌رود اشتباه می‌شود اما در اینجا هیچ زوج مرتبی نداریم تا ابهام ایجاد کند.)

اولین مثال، ایده‌آل اول $(۲, ۱ + \sqrt{-۵})$ است که شامل ایده‌آل (۲) می‌باشد. آیا ایده‌آلی مانند C که

$$(۲) = (۲, ۱ + \sqrt{-۵})C$$

وجود دارد؟ خوشبختانه پاسخ مثبت است و در حقیقت حکم زیر را داریم.

تجزیهٔ (۲) به ایده‌آلهای اول. $(۲, ۱ + \sqrt{-۵})^۲ = (۲)$.

برهان. از تعریف حاصل ضرب ایده‌آلها نتیجه می‌شود که

$$۴ = ۲ \times ۲ \in (۲, ۱ + \sqrt{-۵})^۲,$$
$$۲ + ۲\sqrt{-۵} = ۲ \times (۱ + \sqrt{-۵}) \in (۲, ۱ + \sqrt{-۵})^۲,$$
$$-۴ + ۲\sqrt{-۵} = (۱ + \sqrt{-۵})^۲ \in (۲, ۱ + \sqrt{-۵})^۲.$$

و

$$۴, ۲ + ۲\sqrt{-۵}, -۴ + ۲\sqrt{-۵} \in (۲, ۱ + \sqrt{-۵})^۲$$

$$\Longrightarrow \quad ۲ \in (۲, ۱ + \sqrt{-۵})^۲ \qquad \text{بنابر بسته بودن تحت } + \text{ و } -$$

$$\Longrightarrow \quad (۲) \subseteq (۲, ۱ + \sqrt{-۵})^۲.$$

بالعکس، هر عنصر $(۲, ۱ + \sqrt{-۵})^۲$ مجموعی از حاصل ضربهای جملات $۲m$ و $(۱ + \sqrt{-۵})n$ است. هر حاصل ضربی که $۲m$ در آن ظاهر شده باشد مضرب

۲ است و هر حاصل ضربی که $(۱+\sqrt{-۵})^۲ = -۴ + ۲\sqrt{-۵}$ داشته باشد نیز چنین است. بنابراین هر عنصر $(۲, ۱+\sqrt{-۵})^۲$ مضربی از ۲ است و از این رو $(۲) \subseteq (۲, ۱+\sqrt{-۵})^۲$. □

به طور مشابه، ایده‌آلهای اول $(۳, ۱+\sqrt{-۵})$ و $(۳, ۱-\sqrt{-۵})$ شامل (۳) هستند و در حقیقت عوامل اول (۳) می‌باشند.

تجزیهٔ (۳) به ایده‌آلهای اول. $(۳, ۱+\sqrt{-۵})(۳, ۱-\sqrt{-۵}) = (۳)$.

برهان. از تعریف حاصل ضرب ایده‌آلها نتیجه می‌شود که

$$۹ = ۳ \times ۳ \in (۳, ۱+\sqrt{-۵})(۳, ۱-\sqrt{-۵}),$$
$$٦ = (۱+\sqrt{-۵})(۱-\sqrt{-۵}) \in (۳, ۱+\sqrt{-۵})(۳, ۱-\sqrt{-۵}).$$

و

$$\begin{aligned} & ۹, ٦ \in (۳, ۱+\sqrt{-۵})(۳, ۱-\sqrt{-۵}) \\ \Longrightarrow\ & ۳ \in (۳, ۱+\sqrt{-۵})(۳, ۱-\sqrt{-۵}) \qquad \text{بنابر بسته بودن تحت } - \\ \Longrightarrow\ & (۳) \subseteq (۳, ۱+\sqrt{-۵})(۳, ۱-\sqrt{-۵}). \end{aligned}$$

بالعکس، هر عنصر $(۳, ۱+\sqrt{-۵})(۳, ۱-\sqrt{-۵})$ مجموعی از حاصل ضربهای جملات $۳m$ و $n(۱ \pm \sqrt{-۵})$ است. هر حاصل ضربی که $۳m$ در آن ظاهر شده باشد مضرب ۳ است و هر حاصل ضربی که $(۱+\sqrt{-۵})(۱-\sqrt{-۵}) = ٦$ داشته باشد نیز چنین است. بنابراین هر عنصر $(۳, ۱+\sqrt{-۵})(۳, ۱-\sqrt{-۵})$ مضربی از ۳ است و از این رو $(۳) \subseteq (۳, ۱+\sqrt{-۵})(۳, ۱-\sqrt{-۵})$. □

این دو تجزیه ایجاب می‌کنند که تجزیهٔ ۲ × ۳ از ٦ در $\mathbb{Z}[\sqrt{-۵}]$ را بتوان بیشتر شکست و به تجزیه به ایده‌آلهای اولی به صورت

$$٦ = (۲, ۱+\sqrt{-۵})^۲(۳, ۱+\sqrt{-۵})(۳, ۱-\sqrt{-۵})$$

رسید (در حقیقت به جای (۲) و (۳) تجزیهٔ آنها به ایده‌آلهای اول را قرار داده‌ایم). حتی حیرت‌آورتر این که این عوامل ایده‌آلی را می‌توان با ترتیبی دیگر

در یکدیگر ادغام کرد تا تجزیهٔ دیگر ٦ به صورت $(۱ + \sqrt{-۵})(۱ - \sqrt{-۵})$ حاصل شود (که در آن $(۱ + \sqrt{-۵})$ و $(۱ - \sqrt{-۵})$ به عنوان ایده‌آلهای اصلی آمده‌اند). دلیل این امر چنین است

$$\begin{aligned}(۱ + \sqrt{-۵}) &= (۲, ۱ + \sqrt{-۵})(۳, ۱ + \sqrt{-۵}),\\ (۱ - \sqrt{-۵}) &= (۲, ۱ + \sqrt{-۵})(۳, ۱ - \sqrt{-۵}).\end{aligned}$$

تجزیه‌های اخیر را می‌توانیم به همان روشی که برای (۲) و (۳) انجام دادیم بررسی کنیم (تمرین).

لذا دو تجزیهٔ ۳×۲ و $(۱ - \sqrt{-۵})(۱ + \sqrt{-۵})$ برای ٦ در حقیقت دسته‌بندیهای متفاوتی از تجزیه‌ای یکسان به ایده‌آلهای اول هستند. مسلماً این حقیقت اثبات نمی‌کند که تجزیه به ایده‌آلهای اول در $\mathbb{Z}[\sqrt{-۵}]$ یکتاست اما نشان می‌دهد که چگونه ممکن است یکتایی امکان پذیر باشد. و فصل بعد شرح می‌دهد که چرا این مطلب در حقیقت درست است.

تمرینها

۱.۸.۱۱ نشان دهید که $۱ + \sqrt{-۵} \in (۲, ۱ + \sqrt{-۵})(۳, ۱ + \sqrt{-۵})$ و در نتیجه

$$(۱ + \sqrt{-۵}) \subseteq (۲, ۱ + \sqrt{-۵})(۳, ۱ + \sqrt{-۵}).$$

۲.۸.۱۱ نشان دهید که $۱ + \sqrt{-۵}$ هر یک از اعضای

$$(۲, ۱ + \sqrt{-۵})(۳, ۱ + \sqrt{-۵})$$

را عاد می‌کند. از این رو از تمرین ۱.۸.۱۱ نتیجه بگیرید که

$$(۱ + \sqrt{-۵}) = (۲, ۱ + \sqrt{-۵})(۳, ۱ + \sqrt{-۵}).$$

۳۸.۱۱ به طور مشابه نشان دهید که

$$(۱ - \sqrt{-۵}) = (۲, ۱ - \sqrt{-۵})(۳, ۱ - \sqrt{-۵}).$$

۹.۱۱ بحث

شکست یکتایی تجزیه به اعداد اول مسأله‌ای عمیقاً مخفی بود که حدود دو قرن پس از اولین تأثیرگذاریش کشف نشده باقی مانده بود. اولین بازتاب آن در رفتار نامعمول صورت $x^۲ + ۵y^۲$ به چشم خورد که توسط فرما در سال ۱۶۵۴ مورد توجه قرار گرفت. همان طور که می‌دانیم فرما توانسته بود قبل از آن به طور موفقیت‌آمیزی اعداد اول به صورت $x^۲ + y^۲$، $x^۲ + ۲y^۲$ و $x^۲ + ۳y^۲$ را رده‌بندی کند. و در فصلهای ۷ و ۹ دیدیم که رده‌بندی او چگونه می‌تواند به کمک یکتایی تجزیه، به ترتیب در $\mathbb{Z}[\sqrt{-۱}]$، $\mathbb{Z}[\sqrt{-۲}]$ و $\mathbb{Z}[\frac{-۱+\sqrt{-۳}}{۲}]$ شرح داده شود. فرما احتمالاً چنین تصوری از مسأله نداشت، در غیر این صورت او می‌بایست در مورد $x^۲ + ۵y^۲$ با مشکل مواجه می‌شد، چرا که یکتایی تجزیه در $\mathbb{Z}[\sqrt{-۵}]$ با شکست مواجه می‌شود.

او در حقیقت با مشکل مواجه شد اما به دلایلی نامعلوم او تنها این حدس را در مورد حاصل ضربهای اعداد اول به صورت $x^۲ + ۵y^۲$ باقی گذاشت: اگر $p_۱$ و $p_۲$ اعداد اولی به صورت $۲۰n + ۳$ یا $۲۰n + ۷$ باشند آنگاه $p_۱p_۲ = x^۲ + ۵y^۲$.

این حکمی قوی است زیرا اعدادی اول به صورت $x^۲ + ۵y^۲$ وجود دارند (مثلاً $۲۹ = ۳^۲ + ۵ \times ۲^۲$) و کاربردی ساده از همنهشتی به پیمانهٔ ۲۰ نشان می‌دهد که هر عدد اول مانند $p = x^۲ + ۵y^۲$ باید به صورت $۲۰n + ۱$ یا $۲۰n + ۹$ باشد. اویلر (۱۷۴۴) به طور بدیهی چنین چیزی را درک کرده بود و حدس زد که عکس این مطلب نیز درست است. لذا:

$$p = x^۲ + ۵y^۲ \Longleftrightarrow p = ۲۰n + ۱ \quad \text{یا} \quad ۲۰n + ۹.$$

با کنار هم گذاشتن حدسهای فرما و اویلر این حدس را داریم که $x^۲ + ۵y^۲$ باید به صورتهای زیر باشد:

- اعداد اول به صورت $۲۰n + ۱$ یا $۲۰n + ۹$،
- حاصل ضرب دو عدد اول به صورت $۲۰n + ۳$ یا $۲۰n + ۷$.

اولین کسی که متوجه این دوگانگی در رفتار $x^۲ + ۵y^۲$ گردید لاگرانژ (۱۷۷۳) بود که کشف کرد $x^۲ + ۵y^۲$ معاشری مستور دارد (صورت مربعی $۲x^۲ + ۲xy + ۳y^۲$) که مقادیر اول آن به صورت $۲۰n + ۳$ یا $۲۰n + ۷$ هستند. لاگرانژ این اکتشاف را در خلال نظریه‌اش در مورد معادل بودن صورتهای مربعی مهیا کرد که ما آن را در بخش ۶.۵ معرفی کردیم. او کشف کرد که صورتهای معادل، دترمینان یکسان دارند و:

همهٔ صورتهای با دترمینان ۱ معادل $x^۲ + y^۲$ هستند.
همهٔ صورتهای با دترمینان ۲ معادل $x^۲ + ۲y^۲$ هستند.
همهٔ صورتهای با دترمینان ۳ معادل $x^۲ + ۳y^۲$ هستند.

در حالی که:

برای دترمینان ۵ دو صورت غیر معادل وجود دارد:
$x^۲ + ۵y^۲$ و $۲x^۲ + ۲xy + ۳y^۲$.

این کشفیات پرتویی جدید بر رفتار منظم $x^۲+y^۲$، $x^۲+۲y^۲$ و $x^۲+۳y^۲$ می‌افکند و نیز دلیل نامنظم بودن $x^۲+۵y^۲$ را به ذهن القا می‌کند. هر یک از دترمینانهای ۱، ۲ و ۳ فقط یک ردهٔ هم‌ارزی از صورتها دارند یا به عبارت دیگر عدد رده‌ای آنها برابر ۱ است که ساده‌ترین وضعیت ممکن را دارد (اکنون این مطلب به عنوان صورت معادلی برای یکتایی تجزیه به اعداد اول در حلقهٔ نظیر آن شناخته می‌شود). دترمینان ۵ دو ردهٔ هم‌ارزی دارد یا عدد رده‌ای آن برابر ۲ است و پیچیده‌تر است چون این دو صورت بر یکدیگر اثر می‌گذارند: لاگرانژ مشاهده کرد که حاصل ضرب دو عدد به صورت $۲x^۲+۲xy+۳y^۲$ به صورت $x^۲+۵y^۲$ است، زیرا

$$(۲x_۱^۲+۲x_۱y_۱+۳y_۱^۲)(۲x_۲^۲+۲x_۲y_۲+۳y_۲^۲)=X^۲+۵Y^۲,$$

که در آن $X=۲x_۱x_۲+x_۱y_۲+x_۲y_۱-۲y_۱y_۲$ و $Y=x_۱y_۲+x_۲y_۱+y_۱y_۲$.
وی همچنین مشاهده کرد که عددی به صورت $x^۲+۵y^۲$ ضربدر عددی به صورت $۲x^۲+۲xy+۳y^۲$ مجدداً به صورت $۲x^۲+۲xy+۳y^۲$ است زیرا

$$(x_۱^۲+۵y_۱^۲)(۲x_۲^۲+۲x_۲y_۲+۳y_۲^۲)=۲X^۲+۲XY+۳Y^۲,$$

که در آن $X=x_۱x_۲-y_۱x_۲-۳y_۱y_۲$ و $Y=x_۱y_۲+۲y_۱x_۲+y_۱y_۲$.

این شاهکارهای درخشان جبر دبیرستانی را می‌توان به روشی هنرمندانه‌تر با استفاده از تجزیه در $\mathbb{Q}(\sqrt{-۵})$ و تلفیق جملات برای رسیدن به عوامل مزدوج یکدیگر به دست آورد. مثلاً چون

$$\begin{aligned} x^۲+۵y^۲ &= (x+y\sqrt{-۵})(x-y\sqrt{-۵}), \\ ۲x^۲+۲xy+۳y^۲ &= ۲[x+\frac{y}{۲}(۱+\sqrt{-۵})][x+\frac{y}{۲}(۱-\sqrt{-۵})] \end{aligned}$$

داریم

$$(x_۱^۲+۵y_۱^۲)(۲x_۲^۲+۲x_۲y_۲+۳y_۲^۲)$$

$$\begin{aligned}
&= (x_1 + y_1\sqrt{-5})(x_1 - y_1\sqrt{-5}) \\
&\quad \times 2[x_2 + \frac{y_2}{2}(1 + \sqrt{-5})][x_2 + \frac{y_2}{2}(1 - \sqrt{-5})] \\
&= 2(x_1 + y_1\sqrt{-5})[x_2 + \frac{y_2}{2}(1 + \sqrt{-5})] \\
&\quad \times (x_1 - y_1\sqrt{-5})[x_2 + \frac{y_2}{2}(1 - \sqrt{-5})] \\
&= 2[x_1x_2 - y_1x_2 - 3y_1y_2 + \frac{x_1y_2 + 2y_1x_2 + y_1y_2}{2}(1 + \sqrt{-5})] \\
&\quad \times \text{مزدوج آن} \\
&= 2X^2 + 2XY + 3Y^2,
\end{aligned}$$

که در آن $X = x_1x_2 - y_1x_2 - 3y_1y_2$ و $Y = x_1y_2 + 2y_1x_2 + y_1y_2$.

اما آیا چیزی مشابه در مورد هر دترمینانی اتفاق می‌افتد؟

نتیجهٔ لاگرانژ در مورد دو صورت غیر معادل با دترمینان ۵ از اولین گامها در نظریه‌ای بود که بعدها به عنوان ترکیب صورتهای مربعی شناخته شد. اولین قدمهای آن اتحاد دیوفانتوس و تعمیم براهماگوپتا از آن است:

$$(x_1^2 - ny_1^2)(x_2^2 - ny_2^2) = X^2 - nY^2,$$

که در آن $X = x_1x_2 + ny_1y_2$ و $Y = x_1y_2 + y_1x_2$. اتحاد براهماگوپتا بیان می‌دارد که اگر صورت $x^2 - ny^2$ با خودش ترکیب شود، خودش را به دست می‌دهد. اگر صورت $x^2 + 5y^2$ را با A و صورت $2x^2 + 2xy + 3y^2$ را با B نمایش دهیم آنگاه نتیجهٔ لاگرانژ (همراه با نتیجهٔ براهماگوپتا) بیان می‌دارد که ترکیب A و B جدول ضربی به صورت زیر دارد:

$$A^2 = A, \quad AB = BA = B, \quad B^2 = A.$$

در می‌یابیم که این جدول ضرب همان جدول گروه دو عضوی با عنصر همانی A است. امروزه آن را گروه رده‌ای[11] برای $\mathbb{Q}(\sqrt{-5})$ می‌نامیم و به روشی کاملاً متفاوت با استفاده از ایده‌آلها تعریف می‌شود.

---

[11] class group

رده‌های A و B از صورتهای غیر معادل $x^۲ + ۵y^۲$ و $۲x^۲ + ۲xy + ۳y^۲$ متناظر با دو رده از ایده‌آلهای $\mathbb{Z}[\sqrt{-۵}]$ هستند: ردهٔ A^* متشکل از ایده‌آلهای اصلی و ردهٔ B^* متشکل از ایده‌آلهای غیر اصلی (در این حلقه، همهٔ ایده‌آلهای غیر اصلی به این مفهوم که شکل یکسان دارند با هم معادلند). حاصل ضرب ایده‌آلهایی که در بخش قبل محاسبه شد نشان می‌دهد که رده‌های ایده‌آلی A^* و B^* جدول ضربی یکسان دارند، همان طور که شکلهای A و B چنین هستند.

گمان می‌رود بتوان توافق کرد که ضرب کردن ایده‌آلها از ترکیب کردن شکلها ساده‌تر است اما نمی‌توان به سادگی دید که چرا واقعاً این دو، یک چیز هستند. از این رو، جایگزین کردن شکلها به وسیلهٔ ایده‌آلها تغییر جهتی خطیر برای نظریه اعداد است. اولین کار در سمت و سوی ایده‌آلها (از قبیل استفادهٔ اویلر از اعداد صحیح مربعی) هنگامی که ظاهراً گاوس دریافت که یکتایی تجزیه به اعداد اول می‌تواند با شکست مواجه شود، رو به خاموشی نهاد. روش وی برای عبور از این مانع، توسعهٔ نظریهٔ لاگرانژ در مورد صورتهای مربعی به دترمینانهای دلخواه بود که این مهم را با پیچیدگی بهت‌آوری در رسالات (۱۸۰۱) به انجام رساند.

گاوس با برهان خود در مورد یکتایی تجزیه در $\mathbb{Z}[\mathrm{i}]$ که در سال ۱۸۳۲ آن را به چاپ رساند، گامی کوچک به سمت نظریهٔ سخت اعداد صحیح مربعی برداشت. این کار به طور مؤثری نظریهٔ صورت $x^۲ + y^۲$ را منسوخ ساخت. با این حال، تنها در سالهای ۱۸۴۰ و ۱۸۵۰ بود که دیریکله، کومر، کرونکر و ددکیند گسترش گونه‌های کلی دیگری را برای ترکیب کردن صورتها آغاز کردند. همان طور که قبلاً متذکر شدیم، کومر ایدهٔ اعداد ایده‌آلی را داشت و از آن به شکلی موفقیت‌آمیز در نظریهٔ اعداد صحیح دایره‌بُر (که هیچ گونهٔ ماندگاری از آن وجود نداشت) استفاده کرد. پس از آن، نظریهٔ ساده‌تر اعداد صحیح مربعی پدیدار نشد، شاید بدین دلیل که دیریکله و ددکیند زمان زیادی را صرف ساده‌سازی نظریه‌ای برای ترکیب صورتها کرده بودند.

ترکیب کردن صورتها فقط در سالهای ۱۸۷۰ رو به خاموشی نهاد؛ هنگامی

که ددکیند نظریهٔ ایده‌آلها را برای اعداد صحیح جبری با درجهٔ دلخواه گسترش داد. او در سال ۱۸۷۷ توصیفی دقیق از مثال $\mathbb{Z}[\sqrt{-5}]$ را ارائه داد تا نظریهٔ کلی‌اش را در مورد ایده‌آلهای اعداد صحیح جبری برانگیزد. مطالعهٔ کتاب کوچک بسیار خواندنی او (که ترجمهٔ انگلیسی آن با عنوان ددکیند (۱۸۷۷) است) به دلیل بصیرتی که برای تلاش ددکیند به منظور واقعی ساختن اعداد ایده‌آلی به دست می‌دهد توصیه می‌گردد. همچنین مقدمهٔ مترجم آن نیز توصیه می‌شود چرا که این مقدمه گامهایی تاریخی را از صورتهای مربعی گرفته تا اعداد صحیح مربعی، با جزییاتی بیش از آنچه در اینجا امکان دارد به بحث می‌کشد.

۱۲

ایده‌آلهای اول

پیش‌نگاه

در این فصل نهایی، یکتایی تجزیه به اعداد اول در حلقه‌هایی از قبیل $\mathbb{Z}[\sqrt{-5}]$ را توسط ایده‌آلهای اول به جای اعداد اول به دست می‌آوریم.

در ابتدا به مفهوم جبری محض ایده‌آلها در یک حلقه مانند R توجه می‌کنیم: ایده‌آلها زیر مجموعه‌هایی مانند I هستند که برای آنها مفهوم همنهشتی به پیمانهٔ I معنی پیدا می‌کند. این مطلب ایدهٔ همنهشتی به پیمانهٔ n در $\mathbb{Z}$ را تعمیم می‌دهد. تعمیم متناظری برای حلقهٔ $\frac{\mathbb{Z}}{n\mathbb{Z}}$ یعنی حلقهٔ خارج قسمتی[1] $\frac{R}{I}$ وجود دارد.

خواص ایده‌آل I (بالاخص، اول یا بیشین بودن) درخواص حلقهٔ خارج قسمتی $\frac{R}{I}$ بازتاب پیدا می‌کند (که آن را به ترتیب به حوزهٔ صحیح[2] یا میدان مبدل می‌سازد). برای اعداد صحیح یک میدان مربعی موهومی، اول بودن با بیشین بودن معادل از آب در می‌آید که به ما کمک می‌کند تا خاصیت کلیدی ایده‌آلها را اثبات کنیم: این که شامل بودن یعنی عاد کردن. به عبارت دیگر

[1] quotient ring
[2] integral domain

$A \supseteq B$ نتیجه می‌دهد که $A = BC$ برای ایده‌آلی مانند C.

گام اول این است که مزدوج $\bar{A}$ برای ایده‌آلی مانند A را معرفی کنیم و اثبات کنیم که $A\bar{A}$ ایده‌آلی اصلی است. این مطلب برای تعمیم نتایج مربوط به ایده‌آلهای اصلی (که به دلیل شباهت رفتار آنها با اعداد، ساده هستند) به نتایجی در مورد ایده‌آلهای کلی به کار می‌رود.

از این ترفند برای اثبات این که شامل بودن به مفهوم عاد کردن می‌باشد و برای به دست آوردن تجزیهٔ یکتای ایده‌آلها به ایده‌آلهای اول بهره می‌بریم.

نهایتاً با بازگشت به حالت خاص $\mathbb{Z}[\sqrt{-۵}]$ نگاهی اجمالی به مفهوم رده‌های ایده‌آلی داریم تا نشان دهیم که همهٔ ایده‌آلهای غیر اصلی $\mathbb{Z}[\sqrt{-۵}]$ شکلی یکسان دارند. این نتیجه را برای به انجام رساندن کار ناتماممان با $\mathbb{Z}[\sqrt{-۵}]$ (یعنی رده‌بندی اعداد اول به صورت $x^۲ + ۵y^۲$) احتیاج داریم.

۱.۱۲ ایده‌آلها و همنهشتی

اکنون می‌دانیم که ایده‌آلها را می‌توان به عنوان اعداد ایده‌آلی در وضعیتی که اعداد واقعی ناقص به نظر می‌رسند به کارگرفت؛ مثلاً در $\mathbb{Z}[\sqrt{-۵}]$ که در آن ۲ و $۱ + \sqrt{-۵}$ باید بزرگ‌ترین مقسوم‌علیه مشترکی غیر از ۱ داشته باشند ولی چنین نیست. اما ایده‌آلها نیز یک تابع مجرد طبیعی دارند: یک ایده‌آل مانند I در یک حلقه مانند R زیر مجموعه‌ای از R است که برای آن همنهشتی به پیمانهٔ I معنی پیدا می کند.

برای یک ایده‌آل داده شده مانند I ، همنهشتی به پیمانهٔ I را به صورت

$$a \equiv_p b \iff a - b \in I$$

تعریف می‌کنیم. در این صورت خواص هم ارزی $\equiv$ از خواص بسته بودن I نتیجه می‌شود:

- $a \equiv_I a$.

زیرا $-a \in I \Longrightarrow a \in I$، چون هر عضو I ضربدار ۱−، عضوی از I است که بنابر بسته بودن I تحت + نتیجه می‌دهد $a + (-a) = 0 \in I$.

- $a \equiv_I b \Longrightarrow b \equiv_I a$.

زیرا $b - a \in I \Longrightarrow a - b \in I$ ، مجدداً به این دلیل که I تحت ضرب کردن در ۱− بسته است.

- $(a \equiv_I b$ و $b \equiv_I c) \Longrightarrow a \equiv_I c$.

زیرا $a - b \in I$ و $b - c \in I$ بنابر بسته‌بودن I تحت + نتیجه می‌دهد که $a - c \in I$.

نتیجه می‌شود که R به رده‌های همنهشتی $I + a$ که در آن

$$I + a = \{i + a : i \in I\}$$

افراز می‌شود.

به علاوه جمع و ضرب کردن رده‌ها تحت قواعد

$$\begin{aligned}(I + a) + (I + b) &= I + (a + b),\\ (I + a)(I + b) &= I + ab\end{aligned}$$

معنی خواهد داشت. این مطلب را می‌توان دقیقاً به روش بخش ۲.۳ برای رده‌های همنهشتی $n\mathbb{Z}+a$ و $n\mathbb{Z}+b$ در $\mathbb{Z}$ اثبات کرد.

هر عضو $I + a$ به صورت $k + a$ برای k یی در I می‌باشد. بنابراین اگر آن را به عضو دلخواهی مانند $\ell + b$ از $I + b$ که $\ell \in I$ بیفزاییم به

$$(k + \ell) + (a + b)$$

می‌رسیم که در $I + (a + b)$ است چون $k + \ell = i \in I$ (بنابر بسته بودن I تحت جمع).

اگر عضو $k+a \in I+a$ را در $\ell+b \in I+b$ ضرب کنیم به

$$k\ell + kb + \ell a + ab$$

می‌رسیم که در $I+ab$ است چون

$$\begin{aligned} & k, \ell \in I \\ \Longrightarrow\ & k\ell, kb, \ell b \in I, \quad \text{ضرب عناصر } R \text{ در عناصر } I \text{ در } I \text{ است چون حاصل} \\ \Longrightarrow\ & k\ell + kb + \ell a \in I \quad \text{بنابر بسته بودن } I \text{ تحت جمع} \end{aligned}$$

(باید در اینجا متذکر شد که فرض کرده‌ایم R (همانند حلقه‌های اعداد معمولی که ما به آنها علاقه‌مند هستیم) تعویض‌پذیر می‌باشد. برای حلقه‌های غیر تعویض پذیر می‌توان بین ایده‌آلهای چپ و راست تمایز قائل شد.)

نهایتاً مجموعهٔ $\frac{R}{I}$ متشکل از رده‌های همنهشتی تحت اعمال $+$ و $\times$ که هم‌اکنون تعریف شد، خواص حلقه را از R به ارث می‌برد. مثلا ضرب در $\frac{R}{I}$ تعویض‌پذیر است چون در R چنین است:

$$\begin{aligned} (I+a)(I+b) &= I+ab \\ &= I+ba \\ &= (I+b)(I+a) \end{aligned}$$

خواص دیگر را می‌توان به طور مشابه بررسی کرد و لذا $\frac{R}{I}$ یک حلقه است که حلقهٔ خارج قسمتی R توسط ایده‌آل I نامیده می‌شود.

پس اگر بخواهیم با الگوگیری از $\frac{\mathbb{Z}}{n\mathbb{Z}}$ در فصل ۳، خواص $\frac{R}{I}$ را مطالعه کنیم، آنگاه سؤال بعدی این است: برای چه ایده‌آلهایی مانند I، حلقهٔ $\frac{R}{I}$ یک میدان است؟ در $\mathbb{Z}$ این مطلب هنگامی اتفاق افتاد که n اول بود اما در حلقه‌های کلی پاسخ به این سادگی نیست. در بخش بعد به این سؤال خواهیم پرداخت.

تمرینها

۱.۱.۱۲ چه رده‌های همنهشتی نقش ۱ و ۰ را در $\frac{R}{I}$ ایفا می‌کنند؟

۲.۱.۱۲ دیگر خواص حلقه‌ای $\frac{R}{I}$ را بررسی کنید.
مفید است که رده‌های همنهشتی برخی ایده‌آلهای واقعی I را مثلاً در $\mathbb{Z}[\sqrt{-5}]$ تجسم کنید.

۳.۱.۱۲ رده‌های همنهشتی $I = (3) + (1 + \sqrt{-5})$ در $\mathbb{Z}[\sqrt{-5}]$ را بیابید و نشان دهید که سه ردهٔ همنهشتی دارد.

۲.۱۲ ایده‌آلهای اول و بیشین

در بخش ۷.۱۱ دیدیم که ایده‌آلهای بیشین اول هستند. اما ایده‌آلهای اول همیشه بیشین نیستند و تفاوت بین این دو به زیبایی توسط خواص حلقهٔ خارج قسمتی $\frac{R}{I}$ به دست می‌آید.

مشخص سازی ایده‌آلهای اول. I یک ایده‌آل اول از حلقهٔ R است $\iff$ $\frac{R}{I}$ مقسوم علیه صفر نداشته باشد. (مقسوم علیه‌های صفر، رده‌های همنهشتی غیر صفر مانند $I+a$ و $I+b$ هستند که حاصل ضرب آنها یعنی $I+ab$ در I برابر ردهٔ ۰ باشد.)

برهان. $(\Rightarrow)$ فرض کنیم I اول باشد، بنابراین باید اثبات کنیم که $\frac{R}{I}$ مقسوم علیه صفر ندارد.

$I+ab$ رده ۰ باشد $\implies ab \in I$

چون I اول است $\implies a \in I$ یا $b \in I$

$$\Longrightarrow \quad I+a=I \quad \text{یا} \quad I+b=I$$

$$\Longrightarrow \quad \frac{R}{I} \text{ مقسوم علیه صفر ندارد}$$

($\Longleftarrow$) فرض کنیم $\frac{R}{I}$ مقسوم علیه صفر نداشته باشد. لذا باید اثبات کنیم که I یک ایده‌آل اول است.

$$ab \in I$$

$$\Longrightarrow \quad I+ab=I$$

$$\Longrightarrow \quad (I+a)(I+b)=I \qquad \text{بنابر تعریف ضرب رده‌های همنهشتی}$$

$$\Longrightarrow \quad I+a=I \quad \text{یا} \quad I+b=I \qquad \text{چون } \frac{R}{I} \text{ مقسوم علیه صفر ندارد}$$

$$\Longrightarrow \quad a \in I \quad \text{یا} \quad b \in I$$

$$\Longrightarrow \quad I \text{ یک ایده‌آل اول است} \quad \square$$

مشخص سازی ایده‌آلهای بیشین. I یک ایده‌آل بیشین حلقهٔ R است اگر و فقط اگر $\frac{R}{I}$ یک میدان باشد. (یعنی هر عنصر غیر صفر $\frac{R}{I}$ یک معکوس ضربی داشته باشد.)

برهان. ($\Longrightarrow$) فرض کنیم I بیشین باشد. لذا باید اثبات کنیم که $\frac{R}{I}$ یک میدان است.

$$I+a \text{ یک رده همنهشتی غیر صفر است}$$

$$\Longrightarrow \quad a \notin I$$

$$\Longrightarrow \quad \{ir+as : r,s \in R, i \in I\} = R, \quad \text{با توجه به بیشین بودن } I$$

$$\Longrightarrow \quad 1 = ir+as, \quad r,s \in R, i \in I \text{ برای}$$

$$\Longrightarrow \quad I+as = I+1$$

$$\Longrightarrow \quad \text{است } I+s \text{ دارای معکوس } I+a$$
$$\Longrightarrow \quad \text{یک میدان است } \frac{R}{I}$$

($\Longleftarrow$) فرض کنیم هر ردهٔ همنهشتی غیر صفر مانند $I+a$ دارای معکوسی مانند $I+s$ باشد. پس باید اثبات کنیم که I بیشین است، یعنی تنها ایده‌آل شامل I و عنصری مانند a که در I نیست برابر R می‌باشد.

$a \notin I \implies$ $I+a$ یک رده همنهشتی غیر صفر است

$\implies I+as=I+۱,$ که $I+s$ معکوس $I+a$ است

$\implies ۱=ir+as, \quad r\in R, i\in I$ برای

$\implies$ هر ایده‌آل شامل I و a شامل ۱ است و لذا برابر R می‌باشد

$\implies$ I بیشین است. $\square$

تبصره. حلقه‌ای که مقسوم علیه صفر نداشته باشد حوزهٔ صحیح نامیده می‌شود. هر میدان، یک حوزهٔ صحیح است اما یک حوزهٔ صحیح لزوماً میدان نیست. مثلاً $\mathbb{Z}$ یک حوزهٔ صحیح است ولی میدان نیست. اما یک حوزهٔ صحیح همیشه یک خاصیت مشترک با میدان دارد. این خاصیت مشترک قاعدهٔ حذف[۳] یعنی

$$(ab=ac, a\neq ۰) \Longrightarrow b=c$$

است، چون

$ab=ac \implies ab-ac=۰$

$\implies a(b-c)=۰$

$\implies b-c=۰$ چون $a\neq ۰$ و مقسوم علیه صفر نداریم

$\implies b=c.$

---

[۳] cancellation law

تمرینها

به سادگی یک ایده‌آل غیر بیشین اول در $\mathbb{Z}[\sqrt{-5}]$ پیدا می‌شود. مثلاً ایده‌آل (۲).

۱.۲.۱۲ سه عنصر غیر صفر $\frac{\mathbb{Z}[\sqrt{-5}]}{(2)}$ را بیابید و نشان دهید که مقسوم علیه صفر نیستند و لذا (۲) یک ایده‌آل اول است.

۲.۲.۱۲ چرا (۲) در $\mathbb{Z}[\sqrt{-5}]$ بیشین نیست؟

۳.۱۲ ایده‌آلهای اول میدانهای مربعی موهومی

در حالت کلی تفاوت بزرگی بین حوزه‌های صحیح و میدانها و به طور متناظر، تمایز زیادی بین ایده‌آلهای اول و بیشین وجود دارد. با این‌حال یک حالت مهم وجود دارد که در آن حوزه‌های صحیح همیشه میدان هستند، یعنی حالتی که متناهی باشند.

لم. هر حوزهٔ صحیح متناهی یک میدان است.

برهان. فرض کنیم a عنصر غیر صفری از حوزهٔ صحیح متناهی D باشد. a^2، a^3، a^4، ... را در نظر می‌گیریم. چون D متناهی است، مقداری مانند a^m از این دنباله با مقدار دیگری بعد از آن مانند a^{m+n} برابر است. لذا $a^{m+n} = a^m$ و از این رو بنابر قاعدهٔ حذف داریم $a^n = 1$.

اما این بدان معنی است که $aa^{n-1} = 1$. لذا a دارای معکوس ضربی a^{n-1} است و از این رو D یک میدان می‌باشد. □

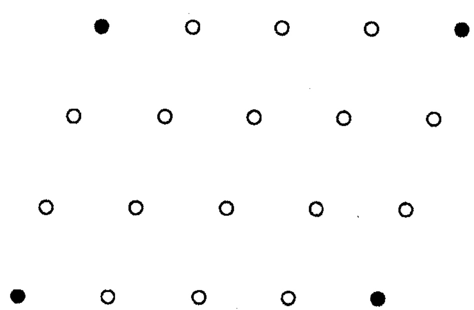
در پرتو این لم و مشخص سازی ایده‌آلهای اول و بیشین در بخش ۲.۱۲، یک ایده‌آل اول در یک حلقه مانند R بیشین خواهد بود هرگاه $\frac{R}{I}$ متناهی باشد.

این مطلب به قضیهٔ زیر منجر می‌شود.

بیشین بودن ایده‌آلهای اول در میدانهای مربعی موهومی. یک ایده‌آل اول در اعداد صحیح یک میدان مربعی موهومی، بیشین است.

برهان. فرض کنیم R حلقهٔ اعداد صحیح میدان مربعی و I ایده‌آلی اول باشد. بنابر نتیجهٔ فوق کافی است نشان دهیم که $\frac{R}{I}$ متناهی است؛ به بیان دیگر باید نشان دهیم که تعدادی متناهی ردهٔ همنهشتی مانند $I+r$ (وقتی r در R تغییر می‌کند) وجود دارد. اما این مطلب بنابر خاصیت شبکهٔ ایده‌آلها در بخش ۶.۱۱ واضح است. رده‌های همنهشتی $I+r$ بوسیلهٔ r هایی که در یک متوازی الاضلاع شبکهٔ I (شکل ۱.۱۲) قرار دارد نمایش داده می‌شوند زیرا هریک از متوازی الاضلاعهای دیگر I همنهشت (به پیمانهٔ I) با چنین r ی هستند.

لذا فقط تعدادی متناهی ردهٔ همنهشتی $I+r$ وجود دارد. □



شکل ۱.۱۲: یک متوازی الاضلاع از شبکهٔ I.

تمرینها

ما توجه خود را بر میدانهای مربعی موهومی محدود کردیم زیرا اعداد صحیح آنها برای تجسم کردن آسان هستند و اکثر مثالهای برانگیزانندهٔ ما به آنها منجر می‌شوند. یک حلقه از اعداد صحیح مربعی حقیقی، مانند $\mathbb{Z}[\sqrt{-۲}]$، به مفهوم

واقعی شبکه نیست زیرا در محور اعداد حقیقی چگال است. با این حال بدیهی است که $\mathbb{Z}[\sqrt{-۲}]$ پایهٔ صحیح ۱ و $\sqrt{-۲}$ دارد و می‌توانیم اثبات کنیم که ایده‌آلهای آن نیز پایهٔ صحیح دارند.

ایده این است که عناصر $a+b\sqrt{۲}$ از $\mathbb{Z}[\sqrt{۲}]$ را به نقاط $a+bi\sqrt{۲}$ از $\mathbb{C}$ بنگاریم. سپس می‌توانیم استدلالهای هندسی را برای نقاط تصویر به کار بریم.

۱.۳.۱۲ نشان دهید که هر زیرمجموعه مانند I از $\mathbb{Z}[\sqrt{۲}]$ که تحت $+$ و $-$ بسته باشد، به زیر مجموعه‌ای مانند I^* از $\mathbb{C}$ با حفظ جمع و تفریق تصویر می‌شود. نشان دهید که اگر I یک ایده‌آل باشد آنگاه I^* در یک خط قرار نمی‌گیرد.

۲.۳.۱۲ نشان دهید که نگاشت $a+b\sqrt{-۲} \mapsto a+bi\sqrt{-۲}$ همردهٔ I را به همردهٔ I^* می‌فرستد و نتیجه بگیرید که $\frac{\mathbb{Z}[\sqrt{۲}]}{I}$ متناهی است. (و به طور مشابه برای اعداد صحیح هر میدان مربعی حقیقی.)

۴.۱۲ مزدوج ایده‌آلها

کلید موفقیت تجزیهٔ ایده‌آل اول در میدانهای مربعی این حقیقت است (که در زیر اثبات شده است) که هر ایده‌آل، یک ایده‌آل اصلی را عاد می‌کند. این مطلب به ما امکان می‌دهد که سؤالات درمورد عوامل ایده‌آل را با سؤالات ساده‌تری در مورد عوامل ایده‌آل اصلی عوض کنیم. ترفند این است که یک ایده‌آل مانند A را در $\bar{A}$ یعنی مجموعهٔ همهٔ مزدوجهای عناصر A ضرب کنیم. درست همان‌طور که حاصل ضرب مزدوج اعداد صحیح مربعی، یک عدد صحیح معمولی مانند k است، حاصل ضرب دو ایده‌آل مزدوج یکدیگر، ایده‌آلی مانند (k) متشکل از مضارب یک عدد صحیح معمولی از آب در می‌آید.

حاصل ضرب ایده‌آلهای مزدوج. اگر R حلقهٔ اعداد صحیح یک میدان مربعی موهومی باشد و A ایده‌آلی از R، آنگاه $k \in \mathbb{Z}$ یی هست که $A\bar{A}=(k)$.

برهان. از بخش ۶.۱۱ می‌دانیم که برای دو عدد صحیح α و β از R داریم $A = \{\alpha m + \beta n : m, n \in \mathbb{Z}\}$. از این رو $\bar{A} = \{\bar{\alpha} m + \bar{\beta} n : m, n \in \mathbb{Z}\}$ و بنابر تعریف حاصل ضرب ایده‌آلها،

$$A\bar{A} = \{s\alpha\bar{\alpha} + t\beta\bar{\beta} + u\bar{\alpha}\beta + v\alpha\bar{\beta} : s, t, u, v \in \mathbb{Z}\}.$$

حال $\alpha\bar{\alpha}$، $\beta\bar{\beta}$ و $\bar{\alpha}\beta + \alpha\bar{\beta}$ خود مزدوج هستند و لذا حقیقی می‌باشند. ابتدا یک عدد صحیح معمولی مانند R می‌یابیم که آنها را عاد کند و سپس می‌بینیم چه پیش می‌آید:

$\alpha\bar{\alpha}$، $\beta\bar{\beta}$ و $\bar{\alpha}\beta + \alpha\bar{\beta}$ اعداد حقیقی R هستند

$$\Longrightarrow \quad \alpha\bar{\alpha}, \beta\bar{\beta}, \bar{\alpha}\beta + \alpha\bar{\beta} \in \mathbb{Z}$$

$$\Longrightarrow \quad \gcd(\alpha\bar{\alpha}, \beta\bar{\beta}, \bar{\alpha}\beta + \alpha\bar{\beta}) = k \in \mathbb{Z}$$

$$\Longrightarrow \quad k = p\alpha\bar{\alpha} + q\beta\bar{\beta} + r(\bar{\alpha}\beta + \alpha\bar{\beta}), \quad \text{برای } p, q, r \in \mathbb{Z}$$

$$\Longrightarrow \quad k \in A\bar{A}$$

$$\Longrightarrow \quad (k) \subseteq A\bar{A}.$$

بالعکس، برای آن که نشان دهیم $(k) \supseteq A\bar{A}$ کافی است نشان دهیم که k چهار مولد $\alpha\bar{\alpha}$، $\beta\bar{\beta}$، $\bar{\alpha}\beta$ و $\alpha\bar{\beta}$ از $A\bar{A}$ را عاد می‌کند. k، عناصر $\alpha\bar{\alpha}$ و $\beta\bar{\beta}$ را بنابر ساختارش عاد می‌کند و $\bar{\alpha}\beta$ و $\alpha\bar{\beta}$ را عاد می‌کند مشروط بر آن که $\frac{\alpha\bar{\beta}}{k}$ و $\frac{\bar{\alpha}\beta}{k}$ متعلق به R باشند. این اعداد آخری ریشه‌های

$$(x - \frac{\alpha\bar{\beta}}{k})(x - \frac{\bar{\alpha}\beta}{k}) = x^{۲} - \frac{\alpha\bar{\beta} + \bar{\alpha}\beta}{k}x + \frac{\alpha\bar{\alpha}}{k} \cdot \frac{\beta\bar{\beta}}{k} = ۰$$

هستند. از این رو $\frac{\alpha\bar{\beta}}{k}$ و $\frac{\bar{\alpha}\beta}{k}$ اعداد صحیح مربعی و لذا عضو R می‌باشند. □

تمرینها

برهان فوق خاصیت شبکهٔ ایده‌آلها یا این مطلب را که هر ایده‌آل، پایهٔ صحیحی مانند α، β دارد فرض می‌کند و بنابر مجموعهٔ تمرینهای قبل می‌دانیم که این مطلب برای حلقهٔ اعداد صحیح میدانهای مربعی حقیقی نیز درست است.

۱.۴.۱۲ بررسی کنید که برهان فوق برای میدانهای مربعی حقیقی نیز کار می‌کند که در آن عمل مزدوج‌گیری $a + b\sqrt{d} \mapsto a - b\sqrt{d}$ است.

حاصل ضرب ایده‌آلهای مزدوج به ما کمک می‌کند که وجود گروه ردهٔ ایده‌آلی[۴] را اثبات کنیم زیرا این مطلب وجود معکوس را نشان می‌دهد. ردهٔ همانی این گروه ردهٔ ایده‌آلهای اصلی است، لذا این قضیه بیان می‌دارد که هر (ردهٔ) ایده‌آل ضربدر (ردهٔ) مزدوج آن برابر ردهٔ همانی است، از این رو رده‌های مزدوج ایده‌آلها معکوس یکدیگر هستند.

۲.۴.۱۲ با یادآوری این مطلب که ایده‌آلهای معادل، شکل یکسان دارند نشان دهید که ایده‌آل $(۲, ۱ + \sqrt{-۵})$ خود مزدوج و لذا خود معکوس است.

۳.۴.۱۲ از قبل می‌دانیم که $(۲, ۱ + \sqrt{-۵})$ خود معکوس است. چرا؟

۵.۱۲ عادپذیری و شمول

حال تقریباً آماده‌ایم اثبات کنیم که برای همهٔ ایده‌آلهای حلقهٔ اعداد صحیح یک میدان مربعی موهومی شمول یعنی عاد کردن. می‌دانیم که این مطلب برای ایده‌آلهای اصلی درست است و تنها حکم دیگری که احتیاج داریم قاعدهٔ حذف زیر است.

قاعدهٔ حذف ایده‌آلها. اگر A ، B و C ایده‌آلهای غیر صفری از R باشند و $AB \supseteq AC$ ، آنگاه $B \supseteq C$.

---
[۴] ideal class group

برهان. در حالت خاص که $A = (\alpha)$ اصلی باشد

$$AB \supseteq AC \implies (\alpha)B \supseteq (\alpha)C$$
$$\implies \alpha B \supseteq \alpha C$$
$$\implies B \supseteq C$$ طرفین را در α^{-1} ضرب می‌کنیم

در حالت کلی،

$$AB \supseteq AC \implies \bar{A}AB \supseteq \bar{A}AC$$ با ضرب کردن طرفین در $\bar{A}$
$$\implies (k)B \supseteq (k)C$$ بنابر بخش ۴.۱۲ برای یک k
$$\implies B \supseteq C$$ بنابر حالت خاص

این اولین کاربرد ترفند بخش ۴.۱۲ است (ضرب کردن ایده‌آل در مزدوجش برای تخفیف دادن به حالت ساده‌تر ایده‌آل اصلی). اکنون حذف کردن به ما اجازه می‌دهد که این ترفند را بیشتر تعمیم دهیم: می‌توانیم یک ایده‌آل را در مزدوجش ضرب کنیم تا به حالت خاص و (سادهٔ) ایده‌آلی اصلی تحویل یابد و به حالت عادی برگردیم. بدین ترتیب اثبات می‌کنیم که چگونه شمول یعنی عاد کردن .

شمول یعنی عاد کردن. اگر A و B ایده‌آلهایی از R باشند و $B \supseteq A$ آنگاه B ایده‌آل A را عاد می‌کند؛ یعنی $A = BC$ برای ایده‌آلی مانند C.

برهان. در حالت خاص که $B = (\beta)$ ایده‌آلی اصلی باشد، داریم

$$B \supseteq A \implies (\beta) \supseteq A$$
$$\implies$$ β هر عضو A را عاد می‌کند
$$\implies A = (\beta)\{\frac{\alpha}{\beta} : \alpha \in A\}$$
$$\implies A = BC$$

که در آن B ایده‌آل (β) است و $C = \{\frac{\alpha}{\beta} : \alpha \in A\}$ نیز ایده‌آلی از R است. عناصر $\frac{\alpha}{\beta} \in C$ متعلق به R هستند چون هر α توسط β عاد می شود، و این عناصر تحت $+$ و ضرب کردن در عناصر R بسته‌اند (چون α ها در A چنین می‌باشند).

در حالت کلی،

$$
\begin{aligned}
B \supseteq A &\implies B\bar{B} \supseteq A\bar{B} &&\text{با ضرب کردن طرفین در } \bar{B} \\
&\implies (k) \supseteq A\bar{B} &&\text{بنابر بخش ۴.۱۲} \\
&\implies A\bar{B} = (k)C &&\text{بنابر حالت خاص برای ایده‌آلی مانند } C \\
&\implies A\bar{B} = \bar{B}BC &&\text{چون } (k) = \bar{B}B \\
&\implies A = BC &&\text{بنابر حذف ایده‌آل } \bar{B} \quad \square
\end{aligned}
$$

۶.۱۲ تجزیهٔ ایده‌آلها

حال آماده‌ایم که وجود و یکتایی تجزیه به ایده‌آلهای اول را در حلقهٔ R از اعداد صحیح یک میدان مربعی موهومی اثبات کنیم. چون ایده‌آلهای اول در این حالت بیشین هستند، فرآیند معمولی یافتن عوامل کوچک‌تر و کوچک‌تر توسط فرآیند یافتن ایده‌آلهای بزرگ‌تر و بزرگ‌تر جایگزین می گردد.

وجود. هر ایده‌آل غیر صفر و متمایز با R مانند A، حاصل ضربی از ایده‌آلهای اول است.

برهان. اگر A اول نباشد، بنابر بخش ۷.۱۱، بیشین نیست. از این رو ایده‌آلی مانند B که $A \subset B$ و $B \neq R$ وجود دارد. چون شمول یعنی عاد کردن، نتیجه می‌شود که $A = BC$ برای ایده‌آلی مانند C. اگر B یا C اول نباشد به طور

مشابه آن را تجزیه می کنیم و به همین ترتیب. این فرآیند در تعداد متناهی گام پایان می‌پذیرد (که تجزیه به عوامل اول را به دست می‌دهد) چون هر ایده‌آل غیر صفر مانند I فقط تعدادی متناهی ردهٔ همنهشتی چون $I + r$ دارد (بخش ۳.۱۲) و هر توسیع به ایده‌آلی بزرگ‌تر حداقل یکی از این رده‌ها را جذب می‌کند. □

یکتایی. تجزیهٔ یک ایده‌آل غیر صفر به ایده‌آلهای اول تا حد ترتیب عوامل، منحصر به فرد است.

برهان. همچون همیشه، یکتایی از وجود و یک خاصیت مقسوم‌علیه اول نتیجه می‌شود. در اینجا این خاصیت این گونه بیان می‌شود: اگر ایده‌آلی اول مانند P حاصل ضرب دو ایده‌آل مانند AB را عاد کند آنگاه P، ایده‌آل A یا ایده‌آل B را عاد خواهد کرد.

بنابر تعریف (بخش ۷.۱۱) یک ایده‌آل اول مانند P دارای این خاصیت است که اگر $AB \supseteq P$ آنگاه $A \supseteq P$ یا $B \supseteq P$. حال خاصیت مقسوم‌علیه اول نتیجه می‌شود زیرا شمول یعنی عاد کردن. □

تمرینها

بنابر تجزیه به ایده‌آلهای اول، دو تجزیهٔ متفاوت به اعداد اول باید به تجزیهٔ یکسانی از ایده‌آلهای اول تبدیل شود. دیدیم که این مطلب در بخش ۸.۱۱ برای دو تجزیهٔ ۶ در $\mathbb{Z}[\sqrt{-۵}]$ اتفاق افتاد. مثال دیگری در $\mathbb{Z}[\sqrt{-۵}]$ عبارت است از

$$۹ = ۳ \times ۳ = (۲ + \sqrt{-۵})(۲ - \sqrt{-۵}).$$

۱.۶.۱۲ از نرم استفاده کنید و نشان دهید که ۳ ، $۲ + \sqrt{-۵}$ و $۲ - \sqrt{-۵}$ اعداد اولی از $\mathbb{Z}[\sqrt{-۵}]$ هستند.

حال از بخش ۸.۱۱ می‌دانیم که $(۳, ۱ + \sqrt{-۵})(۳, ۱ - \sqrt{-۵}) = (۳)$. لذا این عوامل ایده‌آل اول ۳ باید عوامل ایده‌آلی $۲ + \sqrt{-۵}$ و $۲ - \sqrt{-۵}$ نیز باشند.

۲.۶.۱۲ نشان دهید که $۲ - \sqrt{-۵} \in (۳, ۱ + \sqrt{-۵})^۲$ لذا

$$(۲ - \sqrt{-۵}) \subseteq (۳, ۱ + \sqrt{-۵})^۲.$$

۳.۶.۱۲ بالعکس، نشان دهید که $۲ - \sqrt{-۵}$ عناصر ۹، $۳ + ۳\sqrt{-۵}$ و $-۴ + ۲\sqrt{-۵}$ را که مولد $(۳, ۱ + \sqrt{-۵})^۲$ هستند عاد می‌کند. لذا $(۲ - \sqrt{-۵}) \subseteq (۳, ۱ + \sqrt{-۵})^۲$.

لذا عامل $۲ - \sqrt{-۵}$ از ۹، دارای تجزیهٔ $(۳, ۱ + \sqrt{-۵})^۲$ است. پس باقی می‌ماند که نشان دهیم عامل دیگر یعنی $۲ + \sqrt{-۵}$، دارای تجزیهٔ $(۳, ۱ - \sqrt{-۵})^۲$ است.

۴.۶.۱۲ از $۲ - \sqrt{-۵} = (۳, ۱ + \sqrt{-۵})^۲$ نتیجه می‌شود که

$$۲ + \sqrt{-۵} = (۳, ۱ - \sqrt{-۵})^۲.$$

۷.۱۲ رده‌های ایده‌آلی

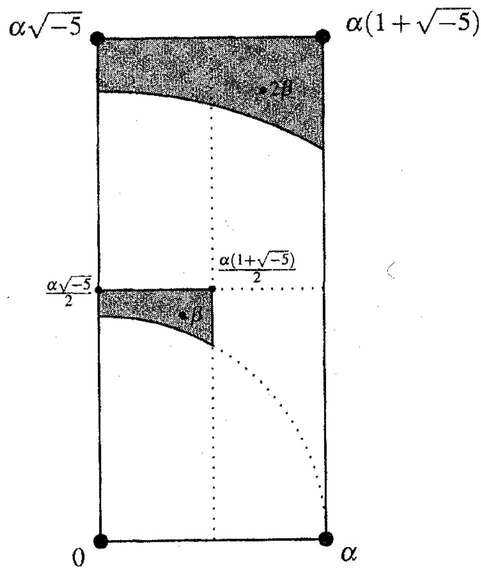
به عنوان کاربردی از تجزیه به ایده‌آلهای اول، اعداد اول به صورت $x^۲ + ۵y^۲$ را مشخص می‌سازیم. لذا مسأله‌ای که فرما و اویلر را سردرگم کرده بود حل می‌شود. برای انجام این کار احتیاج داریم اندکی بیشتر در مورد ایده‌آلهای $\mathbb{Z}[\sqrt{-۵}]$ بدانیم، یعنی این که این ایده‌آلها در دو رده قرار می‌گیرند: ایده‌آلهای اول و همهٔ آنهایی که به صورت

$(۲, ۱+\sqrt{-۵}) = \{۲m + (۱+\sqrt{-۵})n : m, n \in Z\}$ هستند. در حالت کلی، تعداد شکلهای ایده‌آلها در حلقهٔ اعداد صحیح یک میدان مربعی موهومی، عدد رده‌ای آن نامیده می‌شود.

عدد رده‌ای $\mathbb{Z}[\sqrt{-۵}]$. عدد رده‌ای $\mathbb{Z}[\sqrt{-۵}]$ برابر ۲ است.

برهان. فرض کنیم I ایده‌آلی غیر اصلی از $\mathbb{Z}[\sqrt{-۵}]$ باشد و α و β پایه‌ای صحیح برای I (که همانند برهان خاصیت شبکهٔ ایده‌آلها در بخش ۶.۱۱ ساخته شد. یعنی α عنصر غیر صفری با کمترین فاصله از ۰ در بین همهٔ عناصر I که روی خط واصل α تا ۰ نیستند می‌باشد).

چون I یک ایده‌آل است، شامل مضارب $\alpha\sqrt{-۵}$ و $\alpha(۱+\sqrt{-۵})$ از α و نیز عنصر ۰ می‌باشد. این چهار نقطه همراه با هم مستطیلی را که در شکل ۲.۱۲ نشان داده شده است تشکیل می‌دهند که نمونه‌ای از ایده‌آل اصلی تولید شده توسط α است. (محض ساده شدن، خط واصل ۰ و α در شکل، افقی نشان داده شده است اما این خط افقی لزوماً محور حقیقی نیست.)



شکل ۲.۱۲: یک مستطیل از مضارب α

چون I ایده‌آل اصلی (α) نیست، عناصر دیگری از I داخل مستطیل است و از

این رو حداقل یک عضو در یکی از یک چهارمهای مشخص شده دارد. بدون کاستن از کلیت می‌توانیم فرض کنیم که β در یک چهارم پایین سمت چپ است (اگر لازم باشد، می‌توانیم با تفاضل گرفتن بین عنصری از I در جای دیگری از مستطیل و نزدیک‌ترین گوشه یا تعویض α با $-\alpha$ کاری کنیم تا این شرط برقرار گردد). نهایتاً، بنابر ساختار پایهٔ صحیح در بخش ۶.۱۱، چون β از α نزدیک‌تر به ۰ نیست، در ناحیهٔ هاشور خوردهٔ یک چهارم پایین سمت چپ قرار دارد.

اما در این صورت ۲β در قسمت هاشور خوردهٔ نیمهٔ بالایی مستطیل قرار دارد که هر نقطه از این ناحیه به وضوح در فاصلهٔ کمتر از $|\alpha|$ از $\alpha(۱+\sqrt{-۵})$ یا $\alpha\sqrt{-۵}$ واقع است. این ایجاب می‌کند که عناصر $۲\beta - \alpha(۱+\sqrt{-۵})$ یا $\beta - \alpha\sqrt{-۵}$ از I قدرمطلقی کمتر از $|\alpha|$ داشته باشند که با انتخاب α در تناقض است مگر

$$\beta = \alpha\frac{۱+\sqrt{-۵}}{۲} \qquad \text{یا} \qquad \beta = \alpha\frac{\sqrt{-۵}}{۲}.$$

در حالت اول، I همان شکل ایده‌آل $(۲, ۱+\sqrt{-۵})$ را دارد و از این رو متعلق به همان رده است. حالت دوم غیر ممکن است چون

$$\alpha\frac{\sqrt{-۵}}{۲} \in I \implies -\frac{۵\alpha}{۲} \in I \quad \text{با ضرب کردن در } \sqrt{-۵}$$
$$\implies \frac{\alpha}{۲} \in I \quad \text{با افزودن } ۳\alpha$$

که متناقض با انتخاب α به عنوان عنصری با کمترین قدرمطلق می‌باشد. □

تمرینها

استدلال استفاده شده در بالا را می توان برای $\mathbb{Z}[\sqrt{-۶}]$ نیز به کار برد، اما پیامد جالبی دارد. اولین امکان برای β یک ایده‌آل غیر اصلی به وجود نخواهد آورد اما امکان دوم به وجود می‌آورد، لذا $\mathbb{Z}[\sqrt{-۶}]$ عدد رده‌ای ۲ دارد.

۱.۷.۱۲ نشان دهید که

$$I = (۲, ۱ + \sqrt{-٦}) = \{۲m + (۱ + \sqrt{-٦})n : m, n \in Z\}$$

شامل ۱ است و لذا برابر $\mathbb{Z}[\sqrt{-٦}]$ می‌باشد اما

$$J = (۲, \sqrt{-٦}) = \{۲m + \sqrt{-٦}n : m, n \in Z\}$$

ایده‌آلی غیر اصلی است.

۲.۷.۱۲ با بازگشت به استدلال فوق شرح دهید که چرا اکنون فقط امکان دوم برای β، ایده‌آلی غیر اصلی به وجود می‌آورد. لذا نشان دهید که عدد رده‌ای $\mathbb{Z}[\sqrt{-٦}]$ برابر ۲ است و همه ایده‌آلهای غیر اصلی $\mathbb{Z}[\sqrt{-٦}]$ به شکل $(\alpha, \alpha\frac{\sqrt{-٦}}{۲})$ می‌باشند.

اجازه دهید به $\mathbb{Z}[\sqrt{-۵}]$ بازگردیم. می‌دانیم که ایده‌آل غیر اصلی $(۳, ۱ + \sqrt{-۵})$ در همان رده‌ای است که $(۲, ۱ + \sqrt{-۵})$ قرار دارد زیرا در تمرین بخش ۷.۱۱ بررسی کردیم که همان شکل را دارد. اما پایهٔ صحیح ۳ و $۱ + \sqrt{-۵}$ از این ایده‌آل به شکل α و $\frac{\alpha(۱+\sqrt{-۵})}{۲}$ نیست.

۳.۷.۱۲ چه پایه‌های صحیحی از $(۳, ۱ + \sqrt{-۵})$ توسط فرآیند برهان فوق بدست می‌آید؟

۸.۱۲ اعداد اول به صورت $x^{۲} + ۵y^{۲}$

اکنون به اندازهٔ کافی در مورد $\mathbb{Z}[\sqrt{-۵}]$ می‌دانیم که بتوانیم با صورت مربعی $x^{۲} + ۵y^{۲}$ و اعداد اولی که نمایش می‌دهد سر و کار داشته باشیم. در ابتدا مشاهده می‌کنیم که توسط ابزارهای کلاسیک (همنهشتی و تقابل مربعی) چه کارهایی می‌توانیم انجام دهیم.

- کسب تجربه با صورتهای $x^2 + ny^2$ برای $n = 1, 2, 3, \ldots$ (بخش ۱.۹) ما را به در نظر گرفتن مقادیر $x^2 + 5y^2$ به پیمانهٔ ۲۰ راهنمایی می‌کند. مقادیر ممکن x^2 به پیمانهٔ ۲۰ عبارتند از ۱، ۴، ۹، ۱۶، ۵ و ۰. از این رو مقادیر ممکن $5y^2$ به پیمانهٔ ۲۰ عبارتند از ۵ و ۰. مقادیر اول $x^2 + 5y^2$ فرد هستند و مضرب ۵ نمی‌باشند لذا مقادیر اول ممکن $x^2 + 5y^2$ به پیمانهٔ ۲۰ اعداد ۱ و ۹ هستند. یعنی، اعداد اول به صورت $x^2 + 5y^2$ به صورت $20n + 1$ و $20n + 9$ هستند.

- برای کارکردن با $x^2 + 5y^2$ به طور مشابه توقع داریم به مشخصهٔ مربعی ۵− نیاز داشته باشیم. وقتی p به صورت $20n + 1$ یا $20n + 9$ باشد، داریم

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = 1 \times \left(\frac{p}{5}\right) \qquad \text{بنابر تقابل مربعی}$$

چون $1^2 \equiv_5 1 \equiv_5 20n + 1$ و $2^2 \equiv_5 4 \equiv_5 20n + 9$. از اینرو ۵− یک مربع به پیمانهٔ p است وقتی p به صورت $20n + 1$ یا $20n + 9$ باشد.

برای اثبات عکس مشاهدهٔ اول یعنی این که هر عدد اول به صورت $20n + 1$ یا $20n + 9$ به صورت $x^2 + 5y^2$ است به تجزیه به ایده‌آلهای اول احتیاج داریم. جدا از ظاهر شدن ایده‌آلهای غیر اصلی، برهان شبیه برهان $x^2 + y^2$ در فصل ٦ می‌باشد.

اعداد اول به صورت $x^2 + 5y^2$. اعداد اول به صورت $x^2 + 5y^2$ دقیقاً همانهایی هستند که به صورت $20n + 1$ یا $20n + 9$ هستند.

برهان. باقی می‌ماند که نشان دهیم که اعداد اول به صورت $20n + 1$ یا $20n + 9$، به صورت $x^2 + 5y^2$ هستند.

مشاهدهٔ دوم فوق نشان می‌دهد که ۵− به پیمانهٔ p برای p هایی که به صورت $20n + 1$ یا $20n + 9$ باشد یک مربع است. به بیان دیگر برای هر چنین p یی $m \in Z$ ی هست که

عدد p $(m - \sqrt{-۵})(m + \sqrt{-۵}) = m^۲ + ۵$ را عاد می‌کند.

اما p هیچ یک از عوامل $m + \sqrt{-۵}$ یا $m - \sqrt{-۵}$ در $\mathbb{Z}[\sqrt{-۵}]$ را عاد نمی‌کند، چون $\mathbb{Z}[\sqrt{-۵}] \not\ni \frac{\sqrt{-۵}}{p} \pm \frac{m}{p}$. از یکتایی تجزیه به ایدآلهای اول در $\mathbb{Z}[\sqrt{-۵}]$، نتیجه می‌شود که (p) ایده‌آل اولی از $\mathbb{Z}[\sqrt{-۵}]$ نیست و از این رو تجزیه‌ای غیر بدیهی دارد.

حالت ساده این است که یک عامل ایده‌آل اصلی مثلاً $(a + b\sqrt{-۵})$ باشد. در اینجا می‌توانیم همانند آنچه در $\mathbb{Z}[\mathrm{i}]$ در بخش ۳.۶ انجام شد استدلال کنیم:

$$\text{برای ایده‌آلی غیر بدیهی مانند } C \qquad (p) = (a + b\sqrt{-۵})C$$

از این رو با مزدوج‌گیری داریم

$$\text{چون } \bar{p} = p \qquad (p) = (a - b\sqrt{-۵})\bar{C}$$

ضرب کردن دو معادله آخری در یکدیگر (همراه با محاسبهٔ حاصل ضرب $C\bar{C}$ از ایده‌آلهای مزدوج در بخش ۴.۱۲) نتیجه می‌دهد که برای k یی در $\mathbb{Z}$ داریم

$$(p^۲) = (a^۲ + ۵b^۲)C\bar{C} = (a^۲ + ۵b^۲)(k).$$

اما در این صورت $p^۲ = (a^۲ + ۵b^۲)k$ یک تجزیهٔ غیر بدیهی در $\mathbb{Z}$ است، و بنابراین $p = a^۲ + ۵b^۲$.

حالت سخت‌تر این است که همهٔ عوامل اول (p) ایده‌آلهای غیر اصلی و لذا بنابر بخش قبل به شکل $(\alpha, \frac{\alpha(۱+\sqrt{-۵})}{۲})$ برای $\alpha \in \mathbb{Z}[\sqrt{-۵}]$ یی باشند. فرض کنیم

$$(p) = (\alpha, \frac{\alpha(۱ + \sqrt{-۵})}{۲})C.$$

مجدداً با مزدوج‌گیری داریم

$$(p) = (\bar{\alpha}, \frac{\bar{\alpha}(۱ - \sqrt{-۵})}{۲})\bar{C}.$$

و با ضرب کردن این دو معادلهٔ آخر در یکدیگر داریم

$$(p^{۲}) = (\alpha, \frac{\alpha(۱+\sqrt{-۵})}{۲})(\bar{\alpha}, \frac{\bar{\alpha}(۱-\sqrt{-۵})}{۲})C\bar{C}.$$

حال $(\alpha\bar{\alpha}) = (\alpha, \frac{\alpha(۱+\sqrt{-۵})}{۲})(\bar{\alpha}, \frac{\bar{\alpha}(۱-\sqrt{-۵})}{۲})$ چون مولدهای آن $\alpha\bar{\alpha}$ و $\frac{۳\alpha\bar{\alpha}}{۲}$ می‌باشد. و همانند قبل $C\bar{C} = (k)$، لذا داریم

$$۲p^{۲} = \alpha\bar{\alpha}\cdot k = (a^{۲} + ۵b^{۲})k \qquad \text{برای } a, b, k \text{ یی در } \mathbb{Z}$$

نتیجه می‌شود که $p = a^{۲} + b^{۲}$ یا $۲p = a^{۲} + ۵b^{۲}$ برای a و b یی در $\mathbb{Z}$.

امکان آخر توسط همنهشتی به پیمانهٔ ۲۰ رد می‌شود. از مقادیر $x^{۲}$ و $۵y^{۲}$ به پیمانهٔ ۲۰ که در بالا یافتیم می‌بینیم که مقادیر زوج ممکن $a^{۲} + ۵b^{۲}$ به پیمانهٔ ۲۰ عبارتند از ۴،۶،۱۰،۱۴و۱۶. هیچ یک از اینها با مقدار $۲p$ یعنی $۴۰n + ۲$ یا $۴۰n + ۱۸$ جور نیست. از این رو در همهٔ حالات، عدد اول به صورت $۲۰n + ۱$ یا $۲۰n + ۹$، به صورت $x^{۲} + ۵y^{۲}$ می‌باشد. □

تمرینها

اکنون اعداد اول به صورت $x^{۲} + y^{۲}$، $x^{۲} + ۲y^{۲}$، $x^{۲} + ۳y^{۲}$ و $x^{۲} + ۵y^{۲}$ را رده بندی کرده‌ایم. چرا از صورت $x^{۲} + ۴y^{۲}$ صرف نظر کرده‌ایم؟

۱۸.۱۲ نشان دهید که اعداد اول به صورت $x^{۲} + ۴y^{۲}$ با یک استثنا دقیقاً همانند اعداد اول به صورت $x^{۲} + y^{۲}$ هستند.

اعداد اول به صورت $x^{۲} + ۶y^{۲}$ را می‌توان به همان روش اعداد به صورت $x^{۲} + ۵y^{۲}$ یافت. برای گام سخت (که درآن عوامل ایده‌آل (p) همه غیر اصلی هستند) از تعیین ایده‌آلهای غیر اصلی $\mathbb{Z}[\sqrt{-۶}]$ که در مجموعه تمرینهای قبلی آمده است استفاده می‌کنیم.

۲۸.۱۲ از همنهشتی به پیمانهٔ ۲۴ استفاده کنید تا نشان دهید که هر عدد اول به صورت $x^{۲} + ٦y^{۲}$ به صورت $۲۴n + ۱$ یا $۲۴n + ۷$ است.

۳۸.۱۲ از تقابل مربعی استفاده کنید و نشان دهید که برای هر عدد اول به صورت $۲۴n + ۱$ یا $۲۴n + ۷$ عدد -٦ به پیمانهٔ p مربع کامل است.

۴۸.۱۲ از تمرین ۳.۸.۱۲ نتیجه بگیرید که وقتی p عدد اولی به صورت $۲۴n + ۱$ یا $۲۴n + ۷$ باشد، (p) ایده‌آل اولی از $\mathbb{Z}[\sqrt{-٦}]$ نیست.

۵۸.۱۲ هنگامی که (p) عامل ایده‌آل اولی به صورت $(a + b\sqrt{-٦})$ داشته باشد نشان دهید $p = a^{۲} + ٦b^{۲}$.

۶۸.۱۲ نشان دهید که وقتی همهٔ عوامل ایده‌آل اول (p) غیر اصلی (و لذا بنابر تمرین ۲.۷.۱۲ به شکل $(\alpha, \frac{\alpha\sqrt{-٦}}{۲})$) باشند، آنگاه (p) نیز به صورت $x^{۲} + ٦y^{۲}$ است.

۹.۱۲ بحث

بررسی حلقه‌ها، ایده‌آلها و حلقه‌های خارج قسمتی در ابتدای این فصل احتمالاً کمترین چیز لازم برای کاربردهایی برجسته در نظریه اعداد می‌باشد. علاوه بر آن مقداری از نظریهٔ گروهها و نظریهٔ میدانها، که در اصول جبر از قبیل هک[۵] (۱۹۸۱) یافت می‌شود باید زمینهٔ جبری کافی برای خواندن جنبه‌های نظریهٔ جبری اعداد را به دست دهد. در آن کتاب، قضیهٔ یکتایی تجزیه به اعداد اول برای ایده‌آلهای یک میدان عددی دلخواه مانند $\mathbb{Q}(\theta)$ (که θ یک عدد جبری است) و متناهی بودن عدد رده‌ای یافت خواهد شد. این دو قضیه اولین بار توسط ددکیند (۱۸۷۱) اثبات شد و تفسیر وی از آنها در ددکیند (۱۸۷۷) هنوز هم ارزش خواندن دارد گرچه کاملاً به شکل مدرن نیست. بالاخص متناهی

[۵] Hecke

بودن عدد رده‌ای، امروزه معمولا به کمک هندسهٔ مینکوفسکی اعداد[6] اثبات می‌شود. عدد رده‌ای تاریخچه‌ای طولانی دارد که با ایدهٔ لاگرانژ (۱۷۷۳) از تحویل صورتهای مربعی دودویی شروع می‌شود. در حالت دترمینان مثبت، لاگرانژ الگوریتمی ارائه داد که ساده‌ترین معادل یک صورت داده شده را پیدا می‌کند و به طور همزمان فهرست کاملی از صورتهای غیر معادل را نیز می‌یابد. لذا این الگوریتم تعداد صورتهای غیر معادل با دترمینان D داده شده، و به بیان دیگر عدد رده‌ای D را تعیین می‌کند.

گاوس (۱۸۰۱) الگوریتم لاگرانژ را به صورتهای مربعی دودویی با دترمینان منفی به وسیلهٔ استخراج تناوب ذاتی چنین صورتهایی که در فصل ۵ مشاهده کردیم تعمیم داد. یافتن فرمولی برای عدد رده‌ای بسیار سخت‌تر بود و هنگامی که دیریکله (۱۸۳۹) موفق شد به نقطهٔ بازگشتی در تاریخ نظریه اعداد تبدیل گردید. روش وی از L–سریها که تعمیم ماهرانه‌ای از تابع ζ توسط اویلر است (و در بخش ۹.۲ متذکر گردید) استفاده می‌کند. هیچ رهیافت ذاتاً ساده‌تری تاکنون یافت نشده است و در حقیقت به نظر می‌رسد L–سریها دقیقاً ابزاری برای این کار هستند. دیریکله نیز از آنها برای اثبات قضیه‌اش در مورد اعداد اول تصاعدهای حسابی استفاده کرد (بخش ۹.۹ را برای زمینه‌ای در مورد این قضیه ببینید). هم فرمول عدد رده‌ای و هم قضیهٔ اعداد اول را می‌توان در درسهای دیریکله در نظریه اعداد (۱۸۶۳) که ترجمهٔ انگلیسی آن در دسترس است، یافت.

رهیافتهای دیگر با عدد رده‌ای نیز با ریاضیات ماهرانه‌ای همچون توابع پیمانه‌ای[7] درگیر است. تابع پیمانه‌ای کلاسیک $j(z)$ تابعی است که بر نیمهٔ بالایی صفحهٔ $\mathbb{C}$ با تناوبی که در شکل ۳.۱۲ مشخص شده است و مفروش پیمانه‌ای[8] نامیده می‌شود، تعریف می‌گردد.

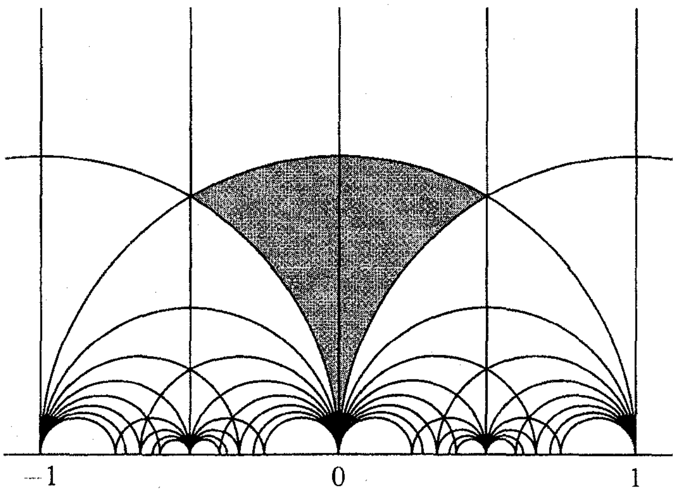
تابع j ناحیهٔ هاشور خورده را به طور یک به یک به روی $\mathbb{C}$ می‌نگارد (یک

---

[6] Minkowski's geometry of numbers
[7] modular functions
[8] modular tessellation

نیمه به روی نیم‌صفحهٔ بالایی و نیمهٔ دیگر به روی نیم‌صفحهٔ پایینی)، و مقدارش را در هر ناحیهٔ دیگرِ مفروش تکرار می‌کند. روش دقیق بیان مطلب این است که اگر $a, b, c, d \in\mathbb{Z}$ و $ad - bc = \pm ۱$ آنگاه

$$j\left(\frac{az+b}{cz+d}\right) = j(z).$$



شکل ۳.۱۲: مفروش پیمانه‌ای

این خاصیت تناوبی امکان می‌دهد که j را به صورت تابعی از شکل شبکه همان طور که اکنون شرح می‌دهیم تلقی کنیم.

یک شبکهٔ تولید شده توسط $\omega_۱, \omega_۲ \in\mathbb{C}$ دارای شکلِ داده شده به وسیلهٔ عدد مختلط $\frac{\omega_۱}{\omega_۲}$ است زیرا $|\frac{\omega_۱}{\omega_۲}| = \left|\frac{\omega_۱}{\omega_۲}\right|$ نسبت طول ضلع یک متوازی الاضلاع تولید شده است در حالی که $\arg(\frac{\omega_۱}{\omega_۲})$ زاویهٔ بین اضلاع می‌باشد. اما همین شبکه توسط $a\omega_۱ + b\omega_۲$ و $c\omega_۱ + d\omega_۲$ برای $a, b, c, d \in\mathbb{Z}$ با شرط $ad - bc + \pm ۱$ تولید می‌گردد و از این رو شکل آن به همان صورت، توسط عدد $\frac{a\omega_۱+b\omega_۲}{c\omega_۱+d\omega_۲} = \frac{a\frac{\omega_۱}{\omega_۲}+b}{c\frac{\omega_۱}{\omega_۲}+d}$ نمایش داده می‌شود. ناحیهٔ هاشور خوردهٔ مفروش پیمانه‌ای، دقیقاً شامل یک

نماینده از هر شکل شبکه است. لذا j به هر شکل، مقداری متفاوت می‌دهد اما (بنابر تناوب) j همان مقدار را در هر نماینده از یک شکل شبکه می‌گیرد.

بدین دلیل، j می‌تواند چیزی برای گفتن در مورد عدد رده‌ای میدانهای مربعی موهومی داشته باشد که (همان‌طور که در بخش ۱.۱۷ دیدیم) برابر تعداد شکلهای ایده‌آلهای آن میدان است. کرونکر (۱۸۵۷) کشف کرد که چنین است: عدد رده‌ای $\mathbb{Q}(\sqrt{d})$ درجهٔ $j(\sqrt{d})$ است. مثلاً با $d-۱$ عدد صحیح معمولی

$$j(i) = ۱۷۲۸$$

را داریم که از درجهٔ ۱ است و با این مطلب که اعداد صحیح گاوسی عدد رده‌ای ۱ دارند (یعنی همهٔ ایده‌آلهای آن اصلی است) تطابق دارد. به طور مشابه

$$j\left(\frac{(۱+\sqrt{-۱۵})}{۲}\right) = \frac{(-۱۹۱۰۲۵+۸۵۹۹۵\sqrt{۵})}{۲}$$

را داریم که از درجهٔ ۲ است و نشان می‌دهد که $\mathbb{Q}(\sqrt{-۱۵})$ عدد رده‌ای ۲ دارد. برای برهان قضیهٔ حیرت‌آور کرونکر، مک‌کین[۹] و مل[۱۰] (۱۹۹۷) یا کاکس[۱۱] (۱۹۸۹) را ببینید.

کتاب کاکس در حقیقت حسن ختامی زیبا بر این مبحث است زیرا رده‌بندی کامل اعداد اول به صورت $x^۲+ny^۲$ را توصیف می‌کند. این کتاب نه تنها با جبری پیچیده‌تر (نظریهٔ ردهٔ میدانها) بلکه با توابع پیمانه‌ای و مباحث مرتبط با آن از آنالیز نیز سر و کار دارد. کتاب دیگری که ارزش معرفی شدن دارد اسکارلا[۱۲] و اپلکا[۱۳] (۱۹۸۵) با عنوان از فرما تا مینکوفکسی[۱۴] می‌باشد. همان طور که عنوان آن بیان می‌دارد، این کتاب توسعهٔ نظریهٔ اعداد از فرما تا

---

[۹] McKean
[۱۰] Moll
[۱۱] Cox
[۱۲] Scharlau
[۱۳] Opolka
[۱۴] From Fermat to Minkowski

مینکوفسکی را با تأکید ویژه بر صورتهای مربعی پوشش می‌دهد. به گونه‌ای، این کتاب مکملی بر کتاب اولی که معرفی شد می‌باشد، چرا که مقدار کمی در مورد نظریهٔ ایده‌آلها می‌گوید اما در مورد آنالیز و هندسه اعداد، قوی است. مباحث اخیر برای هر کس که بخواهد بر نظریه اعدادی که در ورای **اصول** پوشش داده شده در اینجا قرار دارد مسلط شود، اساسی است.

کتابنامه

Argand, J. R. (1806). *Essai sur un manière de représenter les quantités imaginaires dans les constructions géométriques.* Paris.

Artmann, B. (1999). *Euclid-the Creation of Mathematics.* Springer-Verlag, New York.

Baker, A. (1984). *A Concise Introduction to the Theory of Numbers.* Cambridge University Press, Cambridge.

Brouncker, W. (1657). Letter to Wallis, 3/13 October 1657. Translation in Fermat *Oueuvres* 3: 419-420.

Cayley, A. (1858). A memoir on the theory of matrices. *Phil. Trans. Roy. Soc. London,* **148**, 17-37. In his *Collected Mathematical Papers* 2: 475-496.

Conway, J. H. (1997). *The Sensual (Quadratic) Form.* Mathematical Association of America, Washington, DC. With the assistance of Francis Y. C. Fung.

Cox, D. A. (1989). *Primes of the Form* $x^2 + ny^2$. John Wiley & Sons Inc., New York.

Coxeter, H. S. M. (1948). *Regular Polytopes.* Methuen & Co. Ltd., London.

Davenport, H. (1960). *The Higher Arithmetic: An Introduction to the Theory of Numbers.* Harper & Brothers, New York.

Dedekind, R. (1857). Abriss einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus. *J. reine angew. Math.,* **54**, 1-26. In his *Werke* I: 40-67.

Dedekind, R. (1871). Supplement X. In Dirichlet's *Vorlesungen über Zahlentheorie,* 2nd ed., Vieweg 1871.

Dedekind, R. (1877). *Theory of Algebraic Integers.* Cambridge University Press, Cambridge. Translated from the 1877 French original and with and an introduction by John Stillwell, 1996.

Dedekind, R. (1888). *Was sind and was sollen die Zahlen?* Braunschweig. English translation in *Essays on the Theory of Numbers,* Open Court, Chicago, 1901.

Dedekind, R. (1894). Supplement XI. In 4th edition of Dirichlet's *Vorlesungen über Zahlentheorie.*

Diffie, W. and Hellman, M. E. (1976). New directions in cryptography. *IEEE Trans. Information Theory,* **IT-22**(6), 644-654.

Dirichlet, P. G. L. (1837). Beweis des Satzes, dass jede unbegrentze arithmetische Progression, deren erstes Glied and Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendliche viele Primzahlen enthält. *Abh. Akad. Wiss. Berlin,* pages 45-81. In his *Werke* 1: 315-342.

Dirichlet, P. G. L. (1839). Recherches sur diverses applications de l'analyse infinitésimal à la théorie des nombres. *J. reine anger. Math.,* **19**, 324-369. In his Werke 1:41 1-496.

Dirichlet, P. G. L. (1863). *Vorlesungen über Zahlentheorie.* F. Vieweg und Sohn, Braunschweig. English translation *Lectures on Number Theory,* with Supplements by R. Dedekind, translated from the German and with an introduction by John Stillwell, American Mathematical Society, Providence, **RI**, 1999.

Ebbinghaus, H. D., Hermes, H., Hirzebruch, F., Koecher, M., Mainzer, K., Neukirch, J., Prestel, A., and Remmert, R. (1991). *Numbers.* Springer-Verlag, New York. With an introduction by K. Lamotke, Translated from the second 1988 German edition by H. L. S. Orde, Translation edited and with a preface by J. H. Ewing, Readings in Mathematics.

Eisenstein. F. G. (1844). Beweis des Reciprocitätssatzees für die cubischen Reste in der Theorie der Theorie der aus dritten Wurzel der Einheit zusammengesetzten complexen Zahlen . *J. reine angew. Math.,* **27**, 289-310. Also in his *Mathematische Werke* 1: 59-80.

Euler, L. (1744). Theoremata circa divisores numerorum in hac forma $paa \pm qbb$ contentorum. *Comm. acad. sci. Petrop.,* **14**, 151-181. Also in his *Opera Omnia* ser. 1, vol.2, 194-222.

Euler, L. (1747). Letter to Goldbach, 6 May, 1747. In Fuss (1968), 1.413-420.

Euler, L. (I 748a). *Introductio in analysin infinitornm, I.* Volume 8 of his *Opera Omnia,* series 1. English translation, *Introduction to the Analysis of the Infinite. Book I,* Springer-Verlag, 1988.

Euler, L. (I 748b). Letter to Goldbach, 4 May 1748. In Fuss (1968), I, 450-455.

Euler, L. (1755). Demonstratio theorematis Fermatiani omnem numerum primum formae $4n+1$ esse summam duorum quadratorum. *Novi comm. acad. sci. Petrop.,* **5**, 13-58. Also in his *Opera Omnia* ser. 1, vol. 2, 338-372.

Euler, L. (1756). Solutio generalis quorundam problematum diophanteorum quae vulgo nonnisi solutiones speciales admittere videntur. *Novi. comm. acad. sci. Petrop.,* **6**, 155-184. Also in his *Opera Omnia* ser. 1, vol. 2, 428-458.

Euler, L. (1770). *Elements of Algebra.* Translated from the German by John Hewlett. Reprint of the 1840 edition, with an introduction by C. Truesdell, Springer-Verlag, New York, 1984.

Fibonacci (1202). *Fihonacci's Liber Abaci.* Springer-Verlag. English translation by Laurence Sigler, 2002.

Fraenkel, A. (1914). Über die Teiler der Null and die Zerlegung von Ringen. *J. reine angew. Math.,* **145**, 139-176.

Fuss, P.-H. (1968). *Correspondance mathématique et physique de quelques célèbres géomètres du XVIIIème siècle. Tomes I, II.* Johnson Reprint Corp., New York. Reprint of the Euler correspondence originally published by l'Académie Impériale des Sciences de Saint-Pétersbourg. The Sources of Science , No. 35.

Gauss, C. F. (1801). *Disquisitiones arithmeticae.* Translated and with a preface by Arthur A. Clarke. Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse, Springer-Verlag, New York, 1986.

Gauss, C. F. (1832). Theoria residuorum biquadraticorum. *Comm. Soc. Reg. Sci. Gött. Rec.,* **4**. Also in his *Werke* 2: 67-148.

Genocchi, A. (1876). Généralisation du théorème de Lamé sur l'impossibilité de l'équation $x^7 + y^7 + z^7 = 0$. *C. R. Acad. Sci. Paris,* **82**, 910-913.

Graham, R. L., Knuth, D. E., and Patashnik, O. (1994). *Concrete Mathematics.* Addison-Wesley Publishing Company, Reading, MA, second edition.

Grassmann, H. (1861). Stücke aus dem Lehrbuche der Arithmetik. *Hermann Grassmann's Mathematische and Physikalische Werke,* **II/I**, 295-349.

Grosswald, E. (1966). *Topics from the Theory of Numbers.* The Macmillan Co., New York.

Hardy, G. H. (1937). The Indian Mathematician Ramanujan. *Amer. Math. Monthly,* **44**, 137-155.

Hardy, G. H. and Wright, E. M. (1979). *An Introduction to the Theory of Numhers.* The Clarendon Press Oxford University Press Oxford University Press, New York, fifth edition.

Hasse, H. (1923). Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen. *J. reine angew. Math.,* **152**, 129-148.

Hecke, E. (1981). *Lectures on the Theory of Algebraic Numhers.* Springer-Verlag, New York. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen.

Ireland, K. F. and Rosen, M. I. (1982). *A Classical introduction to Modern Number Theory.* Springer-Verlag, New York.

Kronecker, L. (1857). Über die elliptischen Functionen für welche complexe Multiplication stattfindet. In his *Werke* 4: 179-183.

Kummer, E. E. (1844). De numeris complexis, qui radicibus unitatis et numeris realibus constant. *Gratulationschrift der Univ. Breslau zur Juhelf'ier der Univ. Königsberg.* Also in his *Collected Papers* 1: 165-192.

Lagrange, J. L. (1768). Solution d'un problème d'arithmétique. *Miscellanea Taurinensia,* **4**, 19ff. In his *Oeuvres* 1: 671-731.

Lagrange. J. L. (1770). Demonstration d'un théorème d'arithmétique. *Noun. Mém. Acad. Berlin.* In his *Oeuvres* 3: 189-201.

Lagrange, J. L. (1773). Recherches d'arithmétique. *Nouv. mḿ. de l'acad. sci. Berlin,* page 265ff. Also in his *Oeuvres* 3: 695-795.

Lamé. G. (1847). Démonstration général du théorème de Fermat. *C. R. Acad. Sci. Paris,* **24**, 310-315.

Lebesgue, V. A. (1840). Démonstration de l'impossibilité de résoudre l'équation $x^7 + y^7 + z^7 = 0$ en nombres entiers. *J. Math. Pures Appl.,* **5**, 276-279.

Legendre, A. M. (1785). Recherches d'analyse indéterminée. *Hist. de l'Acad. Roy. des Sci.,* pages 465-559.

Lemmermeyer, F. (2000). *Reciprocity Laws. From Euler to Eisenstein.* Springer-Verlag, Berlin.

Lenstra, Jr., H. W. (2002). Solving the Pell equation. *Notices Amer. Math. Soc.,* **9**(2), 182-192.

McKean, H. and Moll, V. (1997). *Elliptic Curves.* Cambridge University Press, Cambridge.

Mordell, L. J. (1969). *Diophantine Equations.* Academic Press, London.

Nagell, T. (1951). *Introduction to Number Theory.* John Wiley & Sons Inc., New York.

Peirce, B. (1881). Linear associative algebra. *Amer. J. Math.,* **4**, 97-229.

Pieper, H. (1978). *Variationen fiber ein zahlentheoreti.sches Thema von Carl Friedrich Gauß.* Birkhäuser Verlag, Basel. With a foreword by Hans Reichardt.

Rademacher, H. (1983). *Higher Mathematics from an Elementary Point of View.* Birkhäuser Boston, Mass. Edited by D. Goldfeld, With notes by G. Crane.

Redmond, D. (1996). *Number Theory.* Marcel Dekker Inc., New York.

Ribenboim, P. (1999). *Fermat's Last Theorem for Amateurs.* Springer-Verlag. New York.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM,* **21**(2), 120-126. Rousseau, G. (1991). On the quadratic reciprocity law. *J. Austral. Math. Soc. Ser. A,* **51**(3), 423-425.

Samuel, P. (1970). *Algebraic Theory of Numbers.* Houghton Mifflin Co., Boston, MA.

Scharlau, W. and Opolka, H. (1985). *From Fermat to Minkowski.* Springer-Verlag, New York. Translated from the German by Walter Kauffmann-Bühler and Gary Cornell.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994),* pages 124-134. IEEE Comput. Soc. Press, Los Alamitos, CA.

Silverman, J. H. and Tate, J. (1992). *Rational Points on Elliptic Curves*. Springer-Verlag, New York.

Smith, D. E. (1959). *A Source Book in Mathematics*. Dover Publications Inc., New York. 2 vols.

Stillwell, J. (1994). *Elements of Algebra*. Springer-Verlag, New York.

Stillwell, J. (1998). *Numbers and Geometry*. Springer-Verlag, New York.

Viète, F. (1593). Variorum de rebus mathematicis responsorum libri octo. In his *Opera*, 347-435.

Weil, A. (1984). *Number Theory. An Approach through History, from Hamnuurapi to Legendre*. Birkhäuser Boston Inc., Boston, MA.

Wessel, C. (1797). Om Directionens analytiske Betegning, et Forsøg anvendt fornemmelig til plane og sphæriske Polygoners Opløsning. *Danske Selsk. Skr. N. Samml.*, **5**. English translation in Smith (1959), vol. I. 55-66.

Yan, S. Y. (2000). *Number Theory, for Computing*. Springer-Verlag. Berlin.

فهرست الفبایی