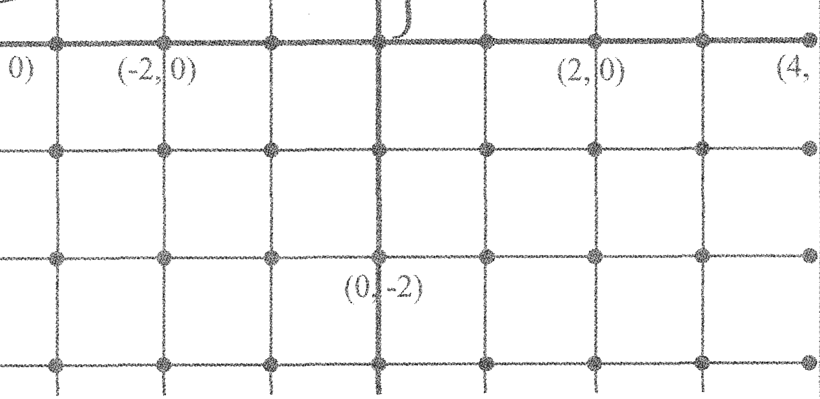
گروه‌خوانی
کتاب ریاضی
کتابخانهٔ کلاغ‌ها، ۴

هندسهٔ اعداد

سی. دی. اولدز، آنلی لکس، جولیانا داویدف

مترجمان:
امیرحسین اصغری
بهزاد اسلامی مسلّم
عرفان صلواتی
نیوشا مدبّرنیا
بردیا حسام

انتشارات فاطمی



گروه‌خوانی
کتاب ریاضی
کتابخانهٔ کلاغ‌ها،۴

هندسه اعداد

سی. دی. اولدز، آنلی لکس، جولیانا داویدف

مترجمان:

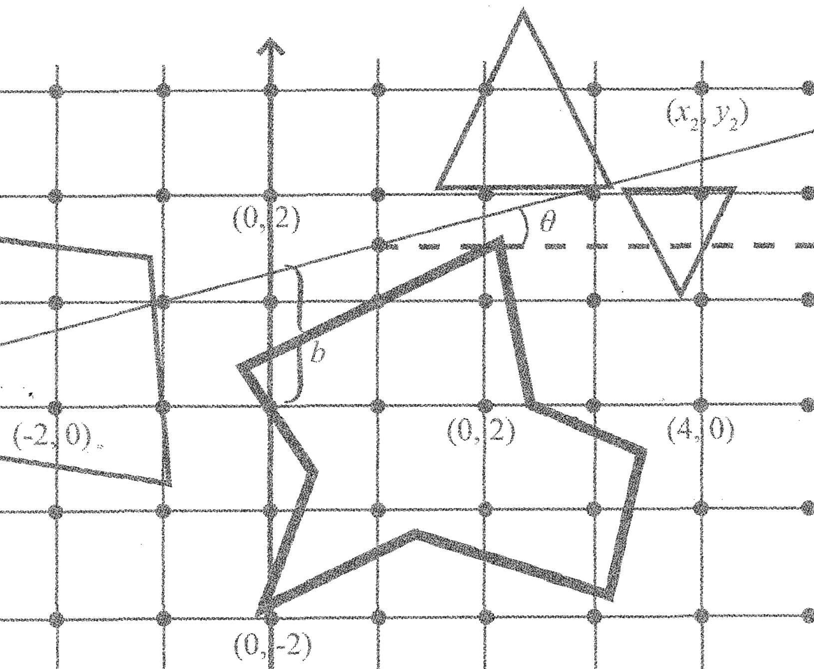
امیرحسین اصغری

بهزاد اسلامی مسلّم

عرفان صلواتی

نیوشا مدبّرنیا

بردیا حسام



انتشارات فاطمی

فهرست

به‌نام خدا

پیشگفتار

معرفی مسابقهٔ کلاغ‌ها

مسابقهٔ «کلاغ‌ها» (گروه‌خوانی کتاب ریاضی) که به‌طور سنتی معمولاً در بلندترینِ شب سال برگزار می‌گردد رقابتی شاداب برای تشویق و تمرین کار گروهی و ریاضی‌خوانی مستقل است که با هدف بالا بردن فرهنگ ریاضی‌خوانی، افزایش تعداد ریاضی‌خوانان و نزدیک کردن ریاضیدانان آینده به یکدیگر برگزار می‌شود. تمام سؤال‌هایی که در جریان مسابقه مطرح می‌شوند مبتنی بر کتابی ریاضی است که چند هفته قبل از برگزاری مسابقه در اختیار شرکت‌کنندگان قرار می‌گیرد. مسابقهٔ کلاغ‌ها گروهی و هر گروه متشکل از سه دانشجو است؛ اعضای هر تیم با هم کتاب را می‌خوانند و در طول مسابقه با هم‌فکری یکدیگر به سؤال‌ها پاسخ می‌دهند.

اما چرا «کلاغ‌ها»؟ مسابقهٔ کلاغ‌ها:
گروهی است؛
در اواخر پاییز، یا اوایل زمستان است؛
پر سروصدا است؛
و . . .

پس چه نامی بهتر از «مسابقهٔ کلاغ‌ها» برای توصیف مسابقه‌ای که هر سال صدای کلاغ‌ها در پاییز ما را به آن فرا می‌خواند.

معرفی کتاب

بنابر مادهٔ ۳ از آیین‌نامه مسابقهٔ «کلاغ‌ها»، تمام سؤال‌هایی که در جریان مسابقه مطرح می‌شوند مبتنی بر کتابی ریاضی با معیارهای زیر است:

۱. «قابل استفاده» برای طیف وسیعی از دانشجویان است؛
۲. دارای جذابیت موضوعی است؛

۳. سلیقه‌های مختلف را پوشش می‌دهد؛

۴. از کتاب‌های درسی رایج دورهٔ کارشناسی نیست.

کتاب "The Geometry of Numbers" کتابی فوق‌العاده و دارای همهٔ معیارهای مذکور است. آنچه پیش رو دارید ترجمهٔ این کتاب است که برای چهارمین دورهٔ مسابقهٔ کلاغ‌ها آماده شده است.

ترجمهٔ کتاب حاضر

داستان ترجمهٔ این کتاب، همچون تألیف آن، داستان همهٔ افرادی است که از ریاضیات لذت می‌برند و مایلند این لذت را با دیگران سهیم شوند. نام بردن از این افراد کمترین کار و درواقع در مورد این ترجمه، تنها کاری است که در تشکر از همراهی ایشان می‌توان انجام داد. در زیر اسامی مترجمان به‌ترتیب حروف الفبا می‌آید:

بهزاد اسلامی مسلّم (دانشجوی دکترای ریاضی، دانشگاه شهید بهشتی)

امیرحسین اصغری (هیأت علمی گروه ریاضی، دانشگاه شهید بهشتی)

بردیا حسام (دانش‌آموختهٔ کارشناسی ارشد ریاضی، دانشگاه صنعتی شریف)

عرفان صلواتی (دانشجوی دکترای ریاضی، دانشگاه صنعتی شریف)

نیوشا مدبّرنیا (دانشجوی کارشناسی ارشد ریاضی، دانشگاه شهید بهشتی)

مؤسسهٔ انتشارات فاطمی، حروفچینی اولیهٔ کار را در زمانی اندک به انجام رساند. با وجود دقت مثال‌زدنی نسخهٔ اولیه، بهزاد اسلامی مسلّم، امیرحسین اصغری و نیوشا مدبرنیا به همراه فرید حسینی و طه عزتی (دانشجویان کارشناسی ریاضی، دانشگاه شهید بهشتی) و حنیف رشتیان (دانشجوی کارشناسی ارشد ریاضی، دانشگاه صنعتی شریف) هر یک بخشی از متن حروف‌چینی شده را با کتاب و دست‌نوشته‌ها مقابله کردند. مانی رضایی (دانشجوی دکترای ریاضی، دانشگاه شهید بهشتی) همهٔ متن ترجمه‌ها را خواند و آنها را از لحاظ ساختاری به هم نزدیک کرد. در نهایت، کتاب توسط امیرحسین اصغری مورد بازبینی مجدد قرار گرفت.

این همه، به معنی بی‌نقص بودن کار نیست. درواقع، علاوه بر کاستی‌های احتمالی ترجمهٔ حاضر، اگر تصحیح متن را به موسسهٔ فرهنگی فاطمی واگذار می‌کردیم کاری به مراتب حرفه‌ای‌تر می‌داشتیم. اما با در اختیار داشتن وقتی کمتر از یک ماه از شروع ترجمه تا آماده‌سازی کتاب برای مسابقه، فرید مصلحی، مدیر فنی محترم مؤسسهٔ فاطمی، پذیرفت که بخشی از کار را به چشمان ناآزمودهٔ ما واگذار کند. امیدواریم که او و همکاران ایشان را از اعتماد به ما پشیمان نکرده باشیم.

در پایان، امید است که محصول نهایی شایستهٔ شما و همهٔ آنانی که به مسابقهٔ گروه‌خوانی کتاب ریاضی باور دارند، باشد.

بخش برگزاری چهارمین مسابقهٔ «کلاغ‌ها» ـ پاییز ۱۳۸۹

مقدمه

هندسهٔ اعداد شاخه‌ای از نظریهٔ اعداد است که با انتشار کار دوران‌ساز مینکوفسکی در ۱۸۹۶ آغاز شد و درنهایت جای خود را به‌عنوان یک حوزهٔ مهم مطالعه باز کرد. تمرکز اصلی این حوزه بر تبدیل مسائل حساب به مسائل هندسه است چنانکه بعضی از مسائل بسیار سخت حساب را می‌توان با ساختارهای نسبتاً بدیهی هندسه حل کرد. یک مسئلهٔ اساسی، تعریف شرایطی است که تحت آنها یک ناحیهٔ داده‌شده شامل یک نقطهٔ مشبکه است، یعنی نقطهٔ (p, q) با مختصات صحیح. یک مسئلهٔ اساسی دیگر، مشخص کردن ناحیه‌هایی مانند R است که هر نقطه در آن را می‌توان با یک انتقال صحیح بر نقطهٔ دیگری در آن منطبق کرد؛ به‌عبارت دیگر، پیدا کردن شرایطی برای R است که تحت آنها برای هر نقطهٔ P در R، نقطهٔ Q در R چنان وجود دارد که $P - Q$ یک نقطهٔ مشبکه است.

اگرچه در نگاه اول چنین سؤال‌هایی مجرد و بدون کاربرد به نظر می‌رسند، درواقع آنها نقشی اساسی در تکنولوژی و کاربردهای علم مدرن ایفا می‌کنند. مسائل نقاط مشبکه نه‌تنها با این سؤال که آیا فلان معادله دارای جواب‌های صحیح است، بلکه با تعیین چگال‌ترین بسته‌بندی کروی، یا پرکردن فضا با کره‌ها به فشرده‌ترینِ شکل ممکن، در ارتباط است. تحقیقات گستردهٔ اخیر برای پاسخ‌گویی به این مسائل، منجر به پیشرفت‌های زیادی در حوزه‌های مختلف، از جمله بلورشناسی، نظریهٔ ابر ریسمان‌ها وکدگذاری شده است. در حالی که انتقالِ با سیم و بی‌سیم داده‌ها و اطلاعات دیجیتالی جهانی راکه ما در آن زندگی و کار می‌کنیم دستخوش تغییر کرده است، به سختی می‌توان کاربردی مهم‌تر از تشخیص و تصحیح کدهایی که با آنها اطلاعات ذخیره، برای انتقال فشرده و بالاخره، دریافت می‌شوند، پیدا کرد.

چگونه می‌توان مسائل حساب را به زبان هندسه بیان کرد؟ به‌عنوان یک مثال ساده، این مسئله را در نظر بگیرید که کدام اعداد صحیح را می‌توان به شکل مجموع دو مربع نوشت، یعنی، برای چه nهایی در $\mathbb{Z}$، می‌توان اعداد صحیح p و q را چنان پیدا کرد که $n = p^2 + q^2$. نسخهٔ هندسی این

مسئله این است که آیا می‌توان هیچ نقطهٔ مشبکه‌ای در دایره‌ای به مرکز $(0, 0)$ و به شعاع $\sqrt{n}$، یعنی دایرهٔ $x^2 + y^2 = n$، پیدا کرد. با همین روال، می‌توان مسئله وجود جواب‌های صحیح یک معادلهٔ خطی با ضرایب صحیح را به این مسئلهٔ هندسی تبدیل کرد که آیا در صفحه، هیچ نقطهٔ مشبکه‌ای روی خط متناظر با معادلهٔ مذکور قرار دارد یا نه.

این زمینهٔ آخری، خود منجر به بسیاری از سؤال‌های جالب سوای سؤال اول ما می‌شود: خط ما باید دارای چه خاصیتی باشد تا بتوان نقاط مشبکه‌ای را پیدا کرد که به اندازه دلخواه به آن نزدیک باشند؟ آیا می‌توان دو خط موازی را چنان پیدا کرد که نوار محدود به آنها شامل هیچ نقطهٔ مشبکه‌ای نباشد؟

قسمت اول. مسائلی شبیه آنچه در بالا ذکر شد انگیزه بخش فصل ۱ کتاب هستند، در حالی که فصل‌های ۲ و ۳ تحقیق ما را به نقاط مشبکهٔ درون و یا روی چندضلعی‌ها گسترش می‌دهند. فصل ۴، جنبه‌های مختلفی از مسئلهٔ دایره را بررسی خواهد کرد. این چهار فصل، بخش اول این کتاب را شکل می‌دهند که تم اصلی آن بررسی مسائل نظریهٔ اعدادی با استفاده از نقاط مشبکه است.

قسمت دوم. در قسمت دوم، معرفی رسمی ما از هندسهٔ اعداد آغاز می‌شود. اگرچه همهٔ تعاریف و نتایجی را که مطرح می‌شود می‌توان به‌راحتی به n بعد تعمیم داد، ما خود را تقریباً به‌طور کامل به صفحهٔ دوبعدی که بیشتر آشنا و به‌راحتی قابل تصور است محدود خواهیم کرد. در فصل ۵، قضیهٔ بنیادی مینکوفسکی معرفی و با ذکر انگیزه‌های آن، اثبات می‌شود. در فصل ۶، بعضی دیگر از قضیه‌های او مطرح و اثبات خواهند شد. روش‌های مینکوفسکی منجر به تقریب‌های بسیار خوبی برای اعداد گنگ به‌وسیلهٔ اعداد گویا می‌شود؛ برخی از کاربردهای روش او برای این «تقریب‌های دیوفانتی» نیز در فصل ۶ توصیف می‌شود.

با کمی تغییر جهت، در فصل ۷ تبدیلات خطی را بررسی خواهیم کرد و نشان خواهیم داد چگونه می‌توان به کمک آنها، از مشبکه‌های اصلی از نقاط صحیح به مشبکه‌های کلی‌تری که بر پایهٔ دو بردار دلخواه قرار دارند رسید. با سود بردن از این زمینهٔ کلی‌تر، فصل ۸ یکی از مسئله‌های اساسی هندسهٔ اعداد را بررسی خواهد کرد: پیدا کردن مقدار مینیمم فرم‌های درجهٔ دوم با دو متغیر یا بیشتر. مینکوفسکی، و بعد از او، بلیکفلت و دیگران کران‌های بالایی برای این مینیمم به‌دست دادند؛ دو کاربرد از نتایج آنها را خواهیم دید: اول، تقریبی بهتر برای گنگ‌ها به‌وسیلهٔ گویاها؛ دوم، اثباتی ساده برای قضیهٔ لاگرانژ در مورد نمایش یک عدد صحیح به شکل مجموع چهار مربع.

فصل‌های ۹ و ۱۰ به کارهای بلیکفلت اختصاص داده شده‌اند. او نه‌تنها روش‌های مینکوفسکی را توسعه داد، بلکه با ارائه بینشی نوآورانه و توانمند پایه‌های پیشرفت‌های بعدی در هندسهٔ اعداد را بنا نهاد. فصل ۹، بعضی از روش‌های جدید بلیکفلت را معرفی می‌کند و بر اساس آنها اثبات دیگری برای قضیهٔ بنیادی مینکوفسکی می‌دهد، فصل ۱۰، اثباتی از بلیکفلت را برای قضیه‌ای از چبیشف ارائه می‌دهد؛ نتیجه‌ای که بعداً توسط مینکوفسکی قوی‌تر شد. قضیهٔ آخر، نمونه‌ای از مسئلهٔ معروف به

مسئلهٔ ناهمگن در هندسهٔ اعداد است که همچون روش مینکوفسکی تقریب‌های خوبی برای اعداد گنگ توسط اعداد گویا به‌دست می‌دهد، اما این یکی دارای این خاصیت اضافی است که می‌توان صورت و مخرج را از یک دنبالهٔ حسابی داده‌شده به‌دست آورد. مطالب دو فصل آخر نسبت به فصل‌های قبل کار بیشتری از خواننده می‌طلبد، بخصوص اثبات ارائه‌شده در فصل ۱۰ که خواندن آن «اختیاری» است. در واقع، اگرچه استدلال داده‌شده پیچیده است، برای فهمیدن آن به هیچ ابزاری بیشتر از بعضی از نتایج هندسه تحلیلی فضایی نیاز نیست.

پیوست‌ها. وقتی نقاط مشبکهٔ (p, q) را به‌عنوان اعداد صحیح گاوسی $p + qi$ در نظر بگیریم، می‌توان علاوه بر ساختار جمعی مورد استفاده در بدنهٔ اصلی کتاب آنها را به ساختار ضربی نیز مجهز کرد. در پیوست الف، پیتر لکس با بررسی این ساختار حسابی اضافی، اثباتی زیبا از این واقعیت که اعداد صحیح گاوسی یک دامنهٔ اقلیدسی هستند ارائه می‌دهد، اعداد اول گاوسی را مشخص می‌کند و بالاخره ثابت می‌کند که تجزیه یکتا در اینجا نیز برقرار است. در حین ارائه این مطالب، او دوباره خواننده را به مباحث فصل ۴ کتاب برمی‌گرداند و دوباره توانایی‌های روش‌های هندسی در حل مسائل نظریهٔ اعدادی را به نمایش می‌گذارد. پیوست ب، نگاهی کوتاه به مسئله بسته‌بندی کروی دارد و خواننده را با آخرین دست‌آوردهای این حوزه آشنا می‌کند. خوانندهٔ علاقه‌مند می‌تواند خلاصه‌ای از زندگی‌نامه‌های هرمان مینکوفسکی و هانس فردریک بلیکفلت را در پیوست ج مطالعه کند.

توصیه به خواننده. کتاب حاضر، متن نوشته‌شده توسط اولدز و منابع آن را به روزکرده و توسعه داده است تا حوزهٔ غنی و معاصر هندسهٔ اعداد را به طیف وسیعی از خوانندگان غیرحرفه‌ای ولی علاقه‌مند معرف کند. با نگاهی کوتاه به کتابنامه می‌توان دید که هنوز بسیاری از کارهای اصلی این حوزه از زبان آلمانی ترجمه نشده‌اند. بیشتر کتاب‌های بسیار خوبی که در هندسهٔ اعداد نوشته شده‌اند «پیشرفته‌اند»، به این معنی که ریاضیات مورد نیاز آنها، ریاضیات سال‌های آخر دوره‌های کارشناسی ریاضی است. همچنان که دکتر اولدز وقتی این کتاب را شروع کرد پیش‌بینی می‌کرد، اثری از این نوع می‌تواند بدون جزییاتی خاص و پیچیده شما را با این حوزهٔ بینهایت مهم آشنا کند.

مانند هر متن ریاضی دیگری، در هنگام خواندن این کتاب نیز به قلم و کاغذ نیاز دارید. اگر بخشی از یک اثبات را متوجه نمی‌شوید، بعداً دوباره به آن برگردید و اگر لازم شد این کار را تکرار کنید تا کاملاً بر آن مسلط شوید. همهٔ مسائل را حل کنید چرا که این اساسی‌ترین آزمونی است که نشان می‌دهد که آیا شما آنچه را که خوانده‌اید یاد گرفته‌اید یا نه. (بجز برای مسائل خیلی آسان، جواب یا راهنمایی همهٔ مسائل دیگر در انتهای کتاب آمده است.) متأسفانه، تعداد مسائل مقدماتی که می‌شد در این کتاب مطرح کرد چندان زیاد نیست چرا که به محض اینکه خود را کمی از کتاب جدا می‌کنیم با مسائل تحقیقی کوچک و بزرگی روبرو می‌شویم که نیازمند مطالعات بسیار بیشتری است.

۱ نقاط مشبکه‌ای و خطوط راست

۱.۱ مشبکهٔ اصلی

موضوع این کتاب، هندسهٔ اعداد است؛ شاخه‌ای از نظریهٔ اعداد که هرمان مینکوفسکی (۱۹۰۹-۱۸۶۴) آن را کشف کرد. مینکوفسکی با نبوغ خود، به مسائلی از نوعی خاص، رویکردی هندسی داشت، حال آنکه ریاضی‌دانان دیگر به آنها به‌طور جبری حمله می‌کردند. او با استفاده از نظم آشکار ساختارهای هندسی، توانست روابط عددی را کشف کند و بکاود.

ما اکتشافات مینکوفسکی را در بخش دوم از این کتاب پی خواهیم گرفت. در اینجا، در ابتدا با تعریف دو مفهوم ابتدایی که همهٔ هندسهٔ اعداد بر آن بنا شده است. شروع می‌کنیم: دستگاه مشبکهٔ اصلی L و مشبکهٔ نقطه‌ای اصلی Λ که L مشخصش می‌کند.

وقتی دربارهٔ دستگاه مشبکه‌ای صحبت می‌کنیم، مشبکه‌ای از نقاط را در فضا تصور می‌کنیم که مانند داربست به هم وصل شده‌اند. می‌توانیم با استفاده از دستگاه مختصات معمول و با رسم خطوط راست، مشبکه‌ای در صفحه بسازیم. ابتدا خطوط راستی موازی با محور yها از نقاط

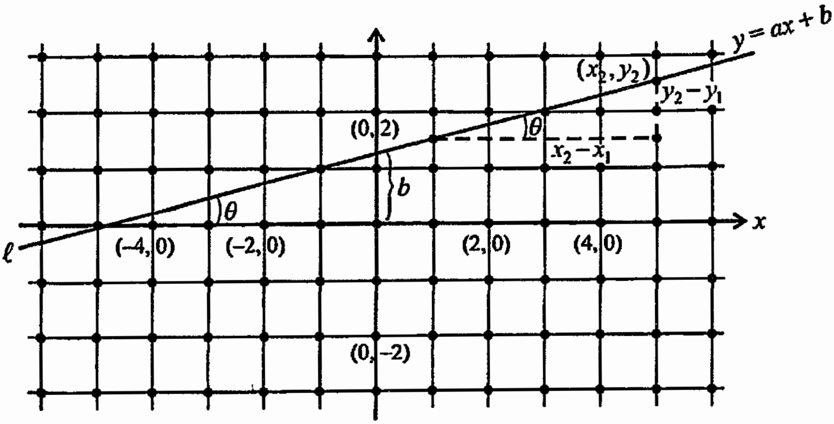
$$\ldots, (-۲, ۰), (-۱, ۰), (۰, ۰), (۱, ۰), (۲, ۰), (۳, ۰), \ldots,$$

بگذرانیم و سپس خطوطی موازی محور xها رسم کنیم که از نقاط

$$\ldots, (۰, -۲), (۰, -۱), (۰, ۰), (۰, ۱), (۰, ۲), \ldots$$

بگذرند. این خطوط، مشبکهٔ اصلی L را تشکیل می‌دهند.

نقاطی را که این خطوط به یکدیگر برمی‌خورند، نقطه‌های مشبکه‌ای می‌نامیم. این نقاط رأس‌های مربع‌هایی‌اند که ایجاد می‌شوند. در مثال ما، نقاط مشبکه‌ای نقاطی هستند با مختصاتی مانند (x, y) که در آن هم طول عددی صحیح است و هم عرض، همان‌طور که در شکل ۱.۱ می‌بینید. برای اینکه بین نقاط



شکل ۱.۱ مشبکهٔ اصلی L و خط l

مشبکه‌ای و نقاط دیگر مثل (x, y) تمایز قائل شویم، نقاط مشبکه‌ای را از این پس با (p, q) نشان می‌دهیم که در آن p و q عددهایی صحیح‌اند.

نقاط مشبکه‌ای، مشبکهٔ نقطه‌ای اصلی Λ را مشخص می‌کنند. فعلاً، فقط مشبکه‌های صفحه را در نظر می‌گیریم، و نوع nبعدی را به بخش ۲ می‌سپاریم.

در نظر اول، نقطه‌های مشبکه‌ای چندان جالب به نظر نمی‌رسند؛ نقاطی که به فاصلهٔ مساوی روی خطوط موازی محورهای x و y قرار دارند. در سال ۱۸۳۷، کارل فریدریش گاوس (۱۸۵۵-۱۷۷۷) [۱] مقاله‌ای مهم دربارهٔ تعداد نقاط مشبکه‌ای در داخل و روی دایره به شعاع r نوشت. از آن زمان، ریاضی‌دانان، چندین مسئلهٔ شگفت‌انگیز مرتبط با این مسئله، ارائه دادند. اکنون بسیاری از این مسئله‌ها حل شده‌اند؛ بعضی فقط تا قسمتی حل شده‌اند؛ و بعضی ــ از جمله شکل بهینهٔ مسئلهٔ اصلی گاوس ــ هنوز حل نشده‌اند. برای اینکه خودمان را برای آزمودن چنین مسئله‌هایی آماده کنیم، باید ابتدا بعضی روابط بین خطوط راست و نقاط مشبکه‌ای را بررسی کنیم.

۲.۱ خطوط در دستگاه‌های مشبکه‌ای

در دستگاه مشبکه‌ای، خط

$$l : y = ax + b \qquad (۱.۱)$$

را با شیب a و عرض از مبدأ b رسم می‌کنیم. وقتی $x = ۰$، $y = b$ و در نتیجه، l از نقطهٔ $(۰, b)$ روی محور yها می‌گذرد (شکل ۱.۱ را ببینید). فرض کنید که $(x_۱, y_۱)$ و $(x_۲, y_۲)$ مختصات دو

نقطه روی خط l باشند. در این صورت شیب l برابر است با

$$a = \tan\theta = \frac{y_۲ - y_۱}{x_۲ - x_۱}$$

که θ زاویه‌ای است که l با محور xها می‌سازد، به‌ازای $x_۲ \neq x_۱$.

آشکار است که اگر $x_۲ = x_۱$، شیب a تعریف نشده است، زیرا مخرج صفر می‌شود. چنین خطوطی معادله‌ای به شکل $x = c$ دارند، که در اینجا c عددی ثابت است؛ این خطوط با محور yها موازی‌اند. مشابهاً، اگر $y_۲ = y_۱$ و $x_۲ \neq x_۱$، خطوط با محور xها موازی‌اند. چنین خطوطی معادله‌ای به شکل $y = c$ دارند، و بنابر تعریف، شیب آنها برابر صفر است.

شیب خط l که همان‌طور که گفته شد، به صورت $a = \tan\theta$ تعریف می‌شود، عددی حقیقی است، پس یا گنگ است یا گویا. وقتی شیب a عددی گویاست، آن را می‌توان به شکل نسبت دو عدد صحیح مانند m و n نوشت که این دو عدد نسبت به هم اول‌اند و $n \neq ۰$. وقتی بزرگ‌ترین مقسوم‌علیه مشترک دو عدد برابر ۱ باشد (یعنی وقتی $\gcd(m,n) = ۱$[1])، می‌گوییم دو عدد نسبت به هم اول‌اند. پس اگر شیب l گویا باشد، آن را می‌توان به شکل

$$a = \frac{m}{n} \quad \text{که} \quad \gcd(m,n) = ۱ \quad \text{و} \quad n \neq ۰$$

نشان داد و اگر شیب a گویا نباشد، عددی گنگ است مانند $\sqrt{۲}$ یا $\sqrt{۳} + ۱$ یا π. چنین عددهایی را نمی‌توان به شکل نسبت دو عدد صحیح نشان داد. برای دانستن جزئیات بیشتر در مورد اعداد گویا و گنگ، به نوشتهٔ مقدماتی ایوان نیون در [۲] و نوشتهٔ عمیق‌ترش در [۳] مراجعه کنید.

با توجه به اینکه شیب خط می‌تواند گویا یا گنگ باشد، این پرسش را می‌پرسیم:

خط $y = ax + b$ از چند نقطهٔ مشبکه‌ای می‌گذرد؟

معلوم خواهد شد که پاسخ، بسیار به شیب بستگی دارد. همان‌طور که خواهیم دید، هر خطی یکی از این پنج نوع است:

۱. خطوط با شیب گویا که نقطهٔ مشبکه‌ای ندارند.

۲. خطوط با شیب گویا که نامتناهی نقطهٔ مشبکه‌ای دارند.

۳. خطوط با شیب گنگ که هیچ نقطهٔ مشبکه‌ای ندارند.

1. greatest common divisor

۴. خطوط با شیب گنگ که دقیقاً یک نقطهٔ مشبکه‌ای دارند.

۵. خطوط موازی محور yها (به شکل $x = k$) با شیب تعریف نشده که یا نامتناهی نقطه مشبکه‌ای دارند یا هیچ نقطهٔ مشبکه‌ای ندارند، بسته به اینکه k عددی صحیح باشد یا نه.

توجه کنید که هر خط موازی محور xها (به شکل $y = k$) در یکی از دسته‌های ۱ و ۲ جای می‌گیرد. ملاحظات مربوط به نقاط مشبکه‌ای خطوط به شکل $x = k$ و $y = k$ به‌قدری واضح‌اند که از این پس، در بیشتر موارد به آنها توجه نمی‌کنیم.

اگر دربارهٔ این حالات مختلف فکر کنید، کم‌کم پرسش‌های جالبی می‌یابید. مثلاً فرض کنید خطی دارای نامتناهی نقطهٔ مشبکه‌ای باشد: این نقاط چگونه روی خط پخش شده‌اند؟ یا فرض کنید خطی از هیچ نقطهٔ مشبکه‌ای نگذرد، یا فقط از یک نقطهٔ مشبکه‌ای بگذرد: آیا می‌توان نقطه‌ای مشبکه‌ای به‌قدر دلخواه نزدیک به آن بیابیم؟ اینها بعضی از پرسش‌هایی‌اند که وقتی دربارهٔ پنج نوع خطوط در دستگاه مشبکه‌ای بحث می‌کنیم، به آنها پاسخ می‌دهیم.

۳.۱ خطوط با شیب گویا

ابتدا دو نوع از خطوط را که شیب گویا دارند، در دستگاه مشبکه‌ای بررسی می‌کنیم. هر خطی از این نوع، یا نامتناهی نقطهٔ مشبکه‌ای دارد یا هیچ نقطهٔ مشبکه‌ای ندارد. خط

$$y = \frac{m}{n}x + b \quad \text{که} \quad \gcd(m,n) = ۱ \quad \text{و} \quad n \neq ۰ \tag{۲.۱}$$

را در نظر بگیرید که شیب آن عدد گویای $a = \frac{m}{n}$ است. به یاد بیاورید که $\gcd(m,n) = ۱$ یعنی m و n نسبت به هم اول‌اند. این پرسش طبیعی است:

> شرط‌های لازم و کافی برای اینکه خط (۲.۱) از نقطه‌ای مشبکه‌ای به شکل $(x,y) = (p,q)$ بگذرد، چیست؟

اول فرض کنید که نقطه (p,q) روی خط (۲.۱) قرار داشته باشند. آن‌گاه p و q در معادلهٔ

$$q = \frac{m}{n}p + b$$

صدق می‌کنند. با ضرب دو طرف در عدد ناصفر n به‌دست می‌آوریم $nq = mp + nb$ و در نتیجه، $b = \frac{nq-mp}{n}$. پس b نسبت دو عدد صحیح است و در نتیجه، گویاست. بنابراین، می‌توانیم b را به

شکل $b = \frac{r}{s}$ که $\gcd(r,s) = ۱$ و $s \neq ۰$ بنویسیم. حالا می‌بینیم که خط (۲.۱) به شکل

$$y = \frac{m}{n}x + \frac{r}{s} \quad \text{که} \quad \gcd(m,n) = \gcd(r,s) = ۱ \tag{۳.۱}$$

است. پس می‌بینیم که شرط لازم برای اینکه خطی با شیب گویا از نقطه‌ای مشبکه‌ای بگذرد این است که عرض از مبدأ گویا داشته باشد، یعنی به شکل (۳.۱) باشد.

حالا بیایید به شرط‌های کافی توجه کنیم.

آیا هر خطی به شکل (۳.۱) از نقطه‌ای مشبکه‌ای می‌گذرد؟

مثلاً خط

$$y = \frac{۳}{۴}x - \frac{۱}{۵} \tag{۴.۱}$$

را در نظر بگیرید که از این نوع است، زیرا $\gcd(۳,۴) = \gcd(۱,۵) = ۱$. اگر $(x,y) = (p,q)$ نقطه‌ای مشبکه‌ای روی خط (۴.۱) باشد، آنگاه مختصات (p,q) در تساوی

$$q = \frac{۳}{۴}p - \frac{۱}{۵}$$

صدق می‌کند. بنابراین $۵(۳p - ۴q) = ۴$. اما از این تساوی نتیجه می‌گیریم که ۴ بر ۵ بخش‌پذیر است، که نادرست است. پس هیچ نقطهٔ مشبکه‌ای روی خط (۴.۱) قرار ندارد. از اینجا می‌فهمیم که چنین نیست که هر خطی که به شکل (۳.۱) باشد از نقطه‌ای مشبکه‌ای می‌گذرد. آیا می‌توانیم مشخص کنیم کدام‌ها می‌گذرند؟

بیایید شرط موردنظر را دقیق‌تر بیان کنیم. برای این کار، دو نماد نیاز داریم:

۱. نماد $s \mid n$ یعنی s عاملی از n است، یا اینکه n دقیقاً بر s بخش‌پذیر است. از این رابطه نتیجه می‌شود که $n = ks$، که k عددی صحیح است.

۲. $s \nmid n$ یعنی s عدد n را نمی‌شمارد.

در ادامه، به چند حکم دربارهٔ خواص بخش‌پذیری اعداد صحیح نیاز داریم. به همین دلیل، آنها را در اینجا ذکر می‌کنیم.

لم مقدماتی. فرض کنید m و n دو عدد صحیح باشند و بزرگ‌ترین مقسوم‌علیه مشترک آنها $d_۰$ باشد، یعنی $\gcd(m,n) = d_۰$. در این‌صورت، اعدادی صحیح مانند $s_۰$ و $t_۰$ وجود دارند به‌طوری که $ms_۰ + nt_۰ = d_۰$.

اثبات. مجموعهٔ $S = \{ms + nt = d \mid s, t \in \mathbb{Z}\}$ را در نظر بگیرید. وقتی $t = ۰$ و $s = \pm ۱$ می‌بینیم که $|m| \in S$، پس S دست‌کم یک عضو صحیح و مثبت دارد و در نتیجه، زیرمجموعه‌ای ناتهی از مجموعهٔ اعداد طبیعی مانند S' دارد. فرض کنید کوچک‌ترین عضو S'، عددی مانند $d = ms_۰ + nt_۰$ باشد. ممکن است جفت‌های زیادی از اعداد مانند S و t موجود باشند که همان مقدار d را بدهند؛ در حقیقت، وجود هم دارند. یکی از این جفت‌ها را انتخاب کنید و فرض کنید که این جفت همان $s_۰$ و $t_۰$ای باشد که ما در نظر گرفتیم. حالا ادعا می‌کنیم که این کوچک‌ترین d در S'، بزرگ‌ترین مقسوم‌علیه مشترک m و n است؛ به عبارت دیگر، $d = d_۰$.

ابتدا باید ثابت کنیم که اگر عدد دیگری مانند $d_۱$ هر دوی m و n را بشمارد، آنگاه $d_۱ \mid d$. این حکم درست است، زیرا اگر $m = d_۱k$ و $n = d_۱r$ آنگاه

$$
\begin{aligned}
d &= d_۱ks_۰ + d_۱rt_۰ \\
&= d_۱(ks_۰ + rt_۰) \\
&= d_۱k'
\end{aligned}
$$

باید ثابت کنیم که $d \mid m$ و $d \mid n$. حالا، با داشتن m و d، می‌دانیم که $q, r \in \mathbb{Z}$ وجود دارند، طوری که

$$
\begin{aligned}
m &= dq + r \\
&= (ms_۰ + nt_۰)q + r
\end{aligned}
$$

که $۰ \leq r < d$

اما در این‌صورت، می‌توانیم بنویسیم

$$
\begin{aligned}
r &= m - (ms_۰ + nt_۰)q \\
&= m(۱ - s_۰q) + n(-t_۰q) \\
&= ms_۱ + nt_۱
\end{aligned}
$$

که از آن نتیجه می‌شود که اگر $r \neq ۰$، آنگاه $r \in S'$. اما می‌دانیم که این نمی‌تواند درست باشد چرا که در این‌صورت S' دارای عدد صحیح مثبتی کوچک‌تر از d خواهد بود که با انتخاب ما از d در تناقض است. پس باید $r = ۰$ و در نتیجه، $d \mid m$. با همین روش نتیجه می‌گیریم که $d \mid n$. پس $d = d_۰$.

قضیهٔ اساسی حساب. اگر عددی صحیح مانند c حاصل‌ضرب دو عدد صحیح مانند a و b را بشمارد و $\gcd(c, a) = ۱$ آنگاه $c \mid b$.

اثبات. چون بزرگ‌ترین مقسوم‌علیه مشترک c و a برابر ۱ است، می‌توانیم عددهایی صحیح مانند

s و t بیابیم به‌طوری که $cs + at = ۱$. دو طرف را در b ضرب می‌کنیم و به $cbs + abt = b$ می‌رسیم. اما می‌دانیم که $c \mid cbs$ و $c \mid abt$. پس $c \mid (cbs + abt)$، که یعنی $c \mid b$.

حالا اگر (p, q) نقطه‌ای مشبکه‌ای روی خط (۳.۱) باشد، آنگاه

$$q = \frac{m}{n}p + \frac{r}{s} \quad \text{که} \quad \gcd(m, n) = \gcd(r, s) = ۱$$

که با ساده کردن آن، به تساوی

$$s(nq - mp) = nr$$

می‌رسیم، که یعنی $s \mid nr$. نتیجه می‌گیریم $s \mid n$، زیرا $\gcd(r, s) = ۱$.

اکنون می‌توانیم ثابت کنیم که اگر نقطه‌ای مشبکه‌ای مانند (p, q) روی خط (۲.۱) باشد، آنگاه b عددی گویا به شکل $b = \frac{r}{s}$ است، به‌طوری که $\gcd(r, s) = ۱$ و $s \mid n$. در نتیجه، اکنون تقریباً به آسانی می‌توانیم معادلاتی از نوع (۱) را نمایش دهیم که شیب آنها گویاست و هیچ نقطهٔ مشبکه‌ای ندارند. کافی است که معادله‌ها را به شکل (۳.۱) بنویسیم و توجه کنیم که $s \nmid n$. معادلهٔ (۴.۱) چنین خطوطی را به‌دست می‌دهد.

حالا خطوط نوع (۲) را در نظر بگیرید. ثابت می‌کنیم که اگر فقط یک نقطهٔ مشبکه‌ای مانند $(x, y) = (p_۰, q_۰)$ روی خطی با معادلهٔ

$$y = \frac{m}{n}x + \frac{r}{s} \quad \text{که در آن} \quad \gcd(m, n) = \gcd(r, s) = ۱ \quad \text{و} \quad s \mid n \qquad (۵.۱)$$

باشد، آنگاه معادلهٔ

$$p_k = p_۰ + kn$$

$$q_k = q_۰ + km$$

به‌ازای $k = ۰, \pm ۱, \pm ۲, \ldots$، نه‌تنها نقطهٔ $(p_۰, q_۰)$ را ــ که به‌ازای $k = ۰$ تولید می‌شود ــ می‌دهد، بلکه تعداد نامتناهی نقطهٔ مشبکه‌ای دیگر مانند (p_k, q_k) روی خط (۵.۱) وجود دارد که در آنها $k = \pm ۱, \pm ۲, \ldots$. این حکم را به این صورت ثابت می‌کنیم. فرض کنید که با روشی فهمیده‌ایم که نقطهٔ $(p_۰, q_۰)$، نقطه‌ای مشبکه‌ای روی خط (۵.۱) است. در این‌صورت

$$q_۰ = \frac{m}{n}p_۰ + \frac{r}{s} \quad \text{که در آن} \quad \gcd(m, n) = \gcd(r, s) = ۱ \qquad (۶.۱)$$

ما هنوز نمی‌دانیم که آیا خط (۵.۱) نقطهٔ مشبکه‌ای دیگری هم دارد یا نه. اما فعلاً فرض می‌کنیم که نقطهٔ مشبکه‌ای دیگری هم مانند (p,q) داشته باشد، طوری که

$$q = \frac{m}{n}p + \frac{r}{s} \tag{۷.۱}$$

با کم کردن (۶.۱) از (۷.۱) به تساوی

$$n(q - q_\circ) = m(p - p_\circ) \tag{۸.۱}$$

می‌رسیم که از آن نتیجه می‌شود $n \mid m(p-p_\circ)$. چون $\gcd(m,n) = ۱$، پس $n \nmid m$ و در نتیجه، باید $n \mid (p-p_\circ)$. بنابراین $p - p_\circ = kn$ که یعنی $p = p_\circ + kn$ که در آن k عددی صحیح است. با جایگذاری $p - p_\circ = kn$ در معادلهٔ (۸.۱) به تساوی

$$n(q - q_\circ) = m(kn)$$

می‌رسیم که از آن به آسانی نتیجه می‌شود

$$q = q_\circ + mk$$

تا اینجا ثابت کرده‌ایم که اگر $(p_\circ, q_\circ)$ نقطه‌ای مشبکه‌ای روی خط (۵.۱) باشد، آنگاه اگر نقطهٔ مشبکه‌ای دیگری مانند $(p,q) = (p_k, q_k)$ روی همان خط باشد، آنگاه به‌ازای عددی صحیح مانند k، تساوی

$$\begin{aligned} p &= p_k = p_\circ + kn \\ q &= q_k = q_\circ + km \end{aligned} \tag{۹.۱}$$

برقرار است. چون p و q به عدد k وابسته است، می‌توانیم نمادگذاریمان را از (p,q) به (p_k, q_k) تغییر دهیم.

حالا به‌سادگی می‌توانیم عکس حکم را بررسی کنیم: اگر $(p_\circ, q_\circ)$ نقطه‌ای مشبکه‌ای روی خط (۵.۱) باشد، آنگاه معادلهٔ (۹.۱) به‌ازای $k = \circ, \pm۱, \pm۲, \ldots$ به‌طور خودکار تعداد نامتناهی نقطهٔ مشبکه‌ای دیگر روی این خط تولید می‌کند. برای اثبات این حکم، کافی است که از (۹.۱)، $x = p_k$ و $y = q_k$ را در (۵.۱) جایگذاری کنیم تا به

$$q_\circ + km = \frac{m}{n}(p_\circ + kn) + \frac{r}{s}$$

برسیم، که یعنی

$$q_\circ = \frac{m}{n}p_\circ + \frac{r}{s} + (mk - mk)$$

که به‌ازای $k = \circ, \pm ۱, \pm ۲, \ldots$، به

$$q_\circ = \frac{m}{n}p_\circ + \frac{r}{s}$$

تبدیل می‌شود. این تساوی درست است، زیرا فرض کرده‌ایم که $(p_\circ, q_\circ)$ نقطه‌ای مشبکه‌ای روی خط (۵.۱) است.

یادداشت. بحث ما تا اینجا به این رسیده است که «اگر $(p_\circ, q_\circ)$ نقطه‌ای مشبکه‌ای روی خط (۵.۱) باشد آنگاه ...». اما آیا مطمئنیم که چنین نقطهٔ مشبکه‌ای واقعاً وجود دارد؟ با شرایطی که در (۵.۱) بیان شد، می‌توان با استفاده از الگوریتم اقلیدس [۵]، یا با استفاده از کسرهای مسلسل [۴، صص. ۴۸-۴۶]ثابت کرد که جوابی مانند $(p_\circ, q_\circ)$ همیشه وجود دارد. با حدس‌زدن هم ممکن است بتوان اولین جواب (۵.۱) را یافت.

به این ترتیب، اثبات اینکه خطی با شیب گویا، نامتناهی نقطه‌ای مشبکه‌ای دارد اگر و تنها اگر شرایط (۵.۱) برقرار باشد، به پایان رسیده است. مشخصاً اگر شرط آخر برقرار نباشد (یعنی اگر $s \nmid n$) آنگاه خط با شیب گویا، هیچ نقطهٔ مشبکه‌ای ندارد.

۴.۱ خطوط با شیب گنگ

حالا در فهرستمان که ارتباط بین خطوط راست و نقاط مشبکه‌ای را برقرار می‌کرد، دسته‌های (۳) و (۴) از خطوط را بررسی می‌کنیم. می‌خواهیم ثابت کنیم که خط

$$y = ax + b \qquad (۱۰.۱)$$

با شیب گنگ، یا هیچ نقطهٔ مشبکه‌ای ندارد، یا فقط یکی دارد.

بیایید خلاف این حکم را در نظر بگیریم:

> اگر دو نقطهٔ مشبکه‌ای مختلف، مانند $(p_۱, q_۱)$ و $(p_۲, q_۲)$ روی خط (۱۰.۱) باشند، چه اتفاقی می‌افتد؟

در این‌صورت، با توجه به دستور شیب، می‌توانیم بنویسیم

$$a = \tan\theta = \frac{q_۲ - q_۱}{p_۲ - p_۱}$$

که در آن $q_۲ - q_۱$ و $p_۲ - p_۱$ هر دو مخالف صفرند و اعدادی صحیح‌اند. بنابراین، شیب a باید عددی گویا باشد، که با فرضمان در تناقض است. بنابراین، چنین خطی باید یا یک نقطهٔ مشبکه‌ای داشته باشد، یا هیچ نقطهٔ مشبکه‌ای نداشته باشد.

می‌توانیم به آسانی معادلهٔ خطوطی را بنویسیم که این دو حالت را داشته باشند. مثلاً خط $y - q = a(x - p)$ که در آن a گنگ است، از نقطهٔ مشبکه‌ای (p, q) می‌گذرد، اما هیچ نقطهٔ مشبکه‌ای دیگری ندارد. واضح است که خط $x = c$ که در آن c عددی صحیح نیست، هیچ نقطهٔ مشبکه‌ای ندارد.

در حالت کلی‌تر، در معادلهٔ (۱۰.۱) عددی b را عددی گویا ولی غیرصحیح انتخاب کنید. در این‌صورت

$$y = ax + b \quad \text{و در نتیجه} \quad b = y - ax$$

اگر این خط نقطه‌ای مشبکه‌ای مانند $(x, y) = (p, q)$ داشته باشد که در آن $x = p \neq ۰$، آنگاه $b = q - ap$ و در نتیجه، b عددی گنگ خواهد بود، زیرا a گنگ است و p و q صحیح‌اند. اما فرض کرده‌ایم که b عددی گویا است. اگر $x = ۰$، هیچ نقطهٔ مشبکه‌ای روی این خط قرار ندارد، زیرا اگر نقطهٔ $(x, y) = (۰, q)$ روی خط باشد، نتیجه می‌شود $b = q$ پس b عددی صحیح است. پس خطی با شیب گنگ و با عرض از مبدأ گویای غیرصحیح، هیچ نقطهٔ مشبکه‌ای ندارد.

یادداشت. از معادلهٔ خطی با شیب گنگ، سؤالی جالب طرح می‌شود: به‌ازای چه مقادیری از θ، شیب a (که با دستور $a = \tan\theta$ به‌دست می‌آید) عددی گنگ است؟ می‌توان ثابت کرد [۳] که اگر θ برحسب رادیان عددی گویا و ناصفر باشد، $\tan\theta$ گنگ است. ضمناً اگر θ برحسب درجه، عددی گویا و ناصفر بجز $۴۵ + ۹۰n$ باشد (که $n = ۰, \pm۱, \pm۲, \ldots$) آنگاه $\tan\theta$ عددی گنگ است.

بنابراین، خطی با شیب گنگ نمی‌تواند از بیش از یک نقطهٔ مشبکه‌ای بگذرد: یا از هیچ نقطهٔ مشبکه‌ای نمی‌گذرد یا فقط از یکی از آنها می‌گذرد. سؤال جالبی در این‌باره می‌توان طرح کرد:

> بین نقطه‌های مشبکه‌ای که خطی با شیب گنگ از آنها نمی‌گذرد، کدام با آن خط کمترین فاصله را دارد؟

پاسخ این سؤال با قضیهٔ بعد داده می‌شود، که بنابر آن، خط می‌تواند از هیچ نقطهٔ مشبکه‌ای عبور نکند، اما تا حد دلخواه به تعداد نامتناهی از آنها نزدیک می‌شود؛ یعنی اگر فاصله‌ای مشخص داده شود، هر قدر هم که کوچک باشد، باز تعداد نامتناهی از نقاط مشبکه‌ای، از خط در فاصله‌ای نزدیک‌تر از فاصلهٔ داده شده قرار دارند. قضیه را می‌توانیم به‌طور دقیق بیان کنیم:

قضیهٔ ۱.۱ خطی به شکل $y = ax + b$ را که در آن a گنگ است و b عدد حقیقی دلخواهی است در نظر بگیرید. فرض کنید ϵ عددی مثبت باشد. در این‌صورت، در هر یک از دو طرف خط، نامتناهی نقطهٔ مشبکه‌ای با فاصله‌ای کمتر از ϵ از خط قرار دارند، حتی اگر ϵ بسیار کوچک باشد.

برای اثبات قضیهٔ ۱.۱، به قضیهٔ مقدماتی یا لمی نیاز داریم:

لم ۱.۱ فرض کنید a عددی گنگ c عددی حقیقی و مثبت و ϵ عددی مثبت و به‌قدر دلخواه کوچک باشد. در این‌صورت می‌توانیم جفتی از اعداد صحیح مانند $(p_۱, q_۱)$ بیابیم به‌طوری که

$$c < p_۱a - q_۱ < c + \epsilon \tag{۱۱.۱}$$

یعنی

$$\circ < p_۱a - q_۱ - c < \epsilon \tag{۱۱'.۱}$$

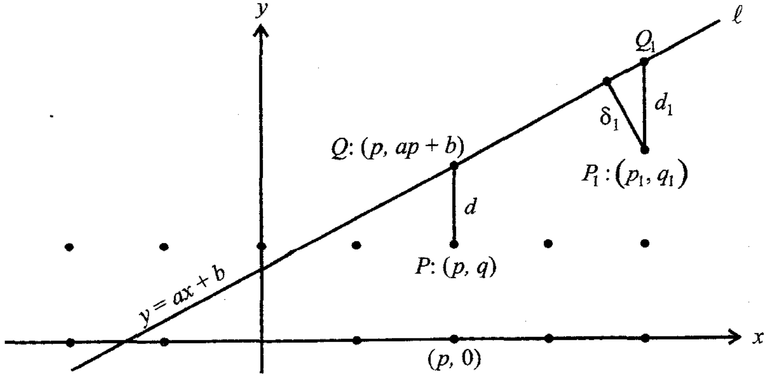
مشابهاً می‌توانیم جفتی از اعداد صحیح مانند $(p_۲, q_۲)$ بیابیم به‌طوری که

$$c - \epsilon < p_۲a - q_۲ < c \tag{۱۲.۱}$$

یعنی

$$-\epsilon < p_۲a - q_۲ - c < \circ \tag{۱۲'.۱}$$

اثبات قضیهٔ ۱.۱. به شکل ۲.۱ توجه کنید.



شکل ۲.۱ یافتن نقاط مشبکه‌ای نزدیک به خط.

فرض کنید که عددی مثبت مانند $\epsilon_۱$ داده شده است. اگر $b > ۰$، بنابر لم ۱.۱ قرار دهید $c = -b$ و در این‌صورت نقطه‌ای مشبکه‌ای مانند $P_۱ : (p_۱, q_۱)$ می‌یابیم، طوری که $۰ < ap_۱ - q_۱ + b < \epsilon_۱$. بنابراین،

$$۰ < d_۱ = y - q_۱ = ap_۱ + b - q_۱ < \epsilon_۱$$

و چون $d_۱ > ۰$، نقطهٔ $P_۱$ زیر خط قرار می‌گیرد.

فاصلهٔ واقعی بین $P_۱$ و l فاصلهٔ عمودی $\delta_۱$ است که از $d_۱$ کمتر است. بنابراین، $۰ < \delta_۱ < \epsilon_۱$. از طرف دیگر، اگر $b > ۰$ آنگاه می‌توانیم عددی طبیعی مانند n را طوری بیابیم که $b - n < ۰$ و می‌توانیم قرار دهیم $c = -(b - n)$. در نتیجه، باز هم بنابر لم ۱.۱ می‌توانیم نقطه‌ای مانند $P_۱ : (p_۱, q_۱)$ را طوری بیابیم که

$$۰ < ap_۱ - q_۱ + (b - n) < \epsilon$$

و بنابراین،

$$\begin{aligned} ۰ < d_۱ &= ap_۱ + b - (q_۱ + n) \\ &= y - (q_۱ + n) < \epsilon_۱ \end{aligned}$$

پس باز هم $P_۱ : (p_۱, q_۱ + n)$ زیر خط قرار می‌گیرد و $\delta_۱$ در شرط $۰ < \delta_۱ < \epsilon_۱$ صدق می‌کند.

از لم می‌توانیم نتیجه بگیریم که به‌ازای هر عدد مثبت مانند ϵ، جفتی از اعداد صحیح مانند p و q وجود دارند که در نابرابری (۱۱'.۱) صدق کنند. پس با انتخاب دنباله‌ای نزولی از اعداد مانند $\epsilon_۱ > \epsilon_۲ > \cdots > ۰$ می‌توانیم دنباله‌ای نامتناهی از نقاط مشبکه‌ای مانند $P_۱, P_۲, P_۳, \ldots$ بسازیم که همه زیر l قرار دارند و هر P_i در فاصلهٔ عمودی کمتر از ϵ_i از l قرار دارد.

برای اینکه وجود نامتناهی نقطهٔ مشبکه‌ای در بالای l را هم ثابت کنیم، استدلال بالا را تکرار می‌کنیم. اما در این حالت، نقاط، بالای l قرار می‌گیرند. پس $q > y = ap + b$. پس $ap - q + b < ۰$ و در نتیجه باید از نابرابری (۱۲'.۱) استفاده کنیم. بدین‌ترتیب اثبات قضیهٔ ۱.۱ به پایان می‌رسد، بجز اینکه باید لم را هم ثابت کنیم.

یادداشت. می‌توانید در اولین باری که متن را می‌خوانید، اثبات لم ۱.۱ را نخوانید.

اثبات لم ۱.۱. کافی است لم را در حالت خاصی که $a = \alpha$ و $c = \gamma$ عددهای بین ۰ و ۱ هستند، ثابت کنیم، زیرا فرض کنید a عددی گویا باشد و c عددی حقیقی باشد. می‌توانیم هر یک را به شکل زیر بنویسیم.

چون a گنگ است، می‌توانیم آن را به شکل $a = [a] + \alpha$ بنویسیم، که در آن $۰ < \alpha < ۱$. تابعی

که با $[x]$ نمایش داده می‌شود، به‌ازای هر عدد حقیقی مانند x به صورت بزرگ‌ترین عدد صحیحی که از x بزرگ‌تر نیست تعریف می‌شود. این تابع مهم را در فصل ۲ بررسی می‌کنیم.

مشابهاً، چون c عددی حقیقی است، می‌توانیم آن را به شکل $c = [c] + \gamma$ بنویسیم که در آن $۰ \leq \gamma < ۱$. بنابراین، اگر بتوانیم عددهای صحیح مانند $p_۱$ و q را طوری بیابیم که

$$\gamma < p_۱\alpha - q$$
$$< \gamma + \epsilon$$

آنگاه می‌توانیم با جایگذاری $\alpha = a - [a]$ و $\gamma = c - [c]$ به نابرابری‌های

$$c - [c] < p_۱(a - [a]) - q$$
$$< c - [c] + \epsilon$$

برسیم. با جمع‌کردن عدد صحیح $[c]$ به دو طرف این نابرابری‌ها به نابرابری‌های

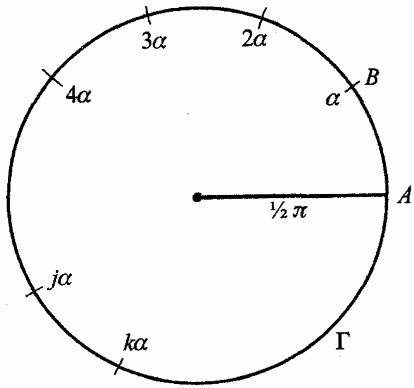
$$c < p_۱ a - p_۱[a] - q + [c]$$
$$< c + \epsilon$$

می‌رسیم. اکنون می‌توانیم عدد صحیح $p_۱[a] + q - [c]$ را $q_۱$ بنامیم و نابرابری مطلوب (۱۱.۱) را به‌دست بیاوریم:

$$c < p_۱ a - q_۱$$
$$< c + \epsilon$$

حالا لم را به‌ازای عددی گنگ مانند α که $۰ < \alpha < ۱$، و به‌ازای عددی مانند γ که $۰ \leq \gamma < ۱$ ثابت می‌کنیم. دایره‌ای مانند Γ به شعاع $۱/(۲\pi)$ (یعنی با محیط ۱) رسم می‌کنیم و نقطه‌ای روی محیطش مانند A انتخاب می‌کنیم. با شروع از A و حرکت روی محیط، طول‌های α، ۲α، ۳α و ... را علامت می‌زنیم. مثلاً در شکل ۳.۱، طول کمان AB برابر α است. حالا فرض کنید که با شروع از نقطهٔ A و حرکت روی دایرهٔ Γ به نقطهٔ $j\alpha$ رسیده‌ایم، که j عددی صحیح است. در این حرکت ممکن است چند دفعه، محیط دایره را به‌طور کامل طی کرده باشیم. تعداد دفعات را می‌توانیم با $n_۱$ نمایش دهیم، که $n_۱ = [j\alpha]$. ضمناً مسافتی اضافه بر $n_۱$ هم طی کرده‌ایم، که می‌توانیم آن را $\alpha_۱$ نمایش دهیم که $۰ < \alpha_۱ < ۱$. بنابراین می‌توانیم نقطهٔ جدیدمان را به‌صورت

$$j\alpha = n_۱ + \alpha_۱ \quad \text{که} \quad ۰ < \alpha_۱ < ۱ \qquad (۱۳.۱)$$



شکل ۳.۱ مضارب صحیح طول α روی Γ علامت خورده‌اند.

نمایش دهیم، که در آن j و n_1 اعدادی صحیح‌اند. به‌طور مشابه، نقاط دیگر را هم که با $k\alpha$ مشخص شده‌اند (که k عددی صحیح است و $k \neq j$) می‌توان به شکل

$$k\alpha = n_2 + \alpha_2 \quad \text{که} \quad 0 < \alpha_2 < 1 \tag{۱۴.۱}$$

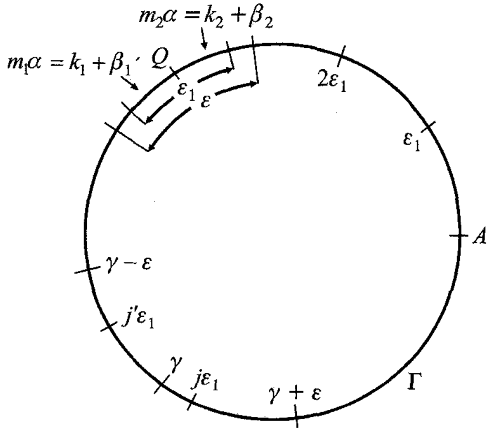
نمایش داد، که n_2 عددی صحیح است و $n_2 = [k\alpha]$. چون α گنگ است، هیچ دو نقطه‌ای مانند $j\alpha$ و $k\alpha$ منطبق نیستند، زیرا اگر منطبق می‌بودند، آنگاه $\alpha_2 = \alpha_1$ و با کم کردن (۱۴.۱) از (۱۳.۱) به‌دست می‌آوردیم $(j-k)\alpha = n_1 - n_2$ که یعنی

$$\alpha = \frac{n_1 - n_2}{j-k} \quad \text{که} \quad j \neq k$$

و نتیجه می‌شد که α گویاست، که با فرضمان در تناقض است.

به‌طور شهودی چه می‌فهمیم؟ وقتی دور Γ می‌چرخیم و به ترتیب، نامتناهی نقطهٔ α، 2α، 3α و ... را مشخص می‌کنیم، هیچ دو نقطه‌ای منطبق نمی‌شوند. بنابراین، در همسایگی دست‌کم یکی از نقاط روی Γ، تعداد نامتناهی از این نقطه‌ها «انباشته می‌شوند». یکی از این نقاط انباشتگی را Q بنامید. بنابراین، هر قدر هم که کمانی که در نزدیک Q روی محیط دایره انتخاب می‌کنیم، کوچک باشد، باز هم می‌توانیم نامتناهی نقطهٔ به شکل $n\alpha$ روی کمان بیابیم.

یادداشت. اگر بخواهید می‌توانید این استدلال شهودی را با استفاده از قضیه‌ای مهم در آنالیز به نام قضیهٔ بولتسانو ـ وایرشتراس دقیق کنید. بنابراین قضیه هر مجموعهٔ نامتناهی کران‌دار از نقاط، دست‌کم یک نقطهٔ حدی (انباشتگی) دارد. برای بحث و اثبات، می‌توانید به هر کتاب درسی حسابان پیشرفته‌ای مراجعه کنید.



شکل ۴.۱ Q، γ و نقاط $n\epsilon_۱$ روی Γ.

باز هم مانند شکل ۴.۱، نقطهٔ انباشتگی روی دایرهٔ Γ را Q بنامید. در بین نقاطی که حول Q انباشته شده‌اند، باید دست‌کم دوتا باشند مانند

$$m_۱\alpha = k_۱ + \beta_۱$$

$$m_۲\alpha = k_۲ + \beta_۲$$

که در آنها $\beta_۱ \neq \beta_۲$ و فاصلهٔ آنها روی Γ کمتر از طول کمان است که ϵ فرض شده است، و هر قدر هم که ϵ کوچک انتخاب شود، این دو نقطه وجود خواهند داشت. به بیان دیگر، فاصلهٔ این دو نقطه که روی محیط دایره اندازه گرفته می‌شود [و طول پاره‌خط واصلشان نیست] عددی است مانند $\epsilon_۱$ که $\epsilon > \epsilon_۱ > ۰$. حالا زیرنویس‌ها را طوری مرتب می‌کنیم که $\beta_۱ > \beta_۲$. حالا چون این دو نقطه منطبق نیستند، می‌توانیم بنویسیم

$$\epsilon_۱ = \beta_۱ - \beta_۲ = (m_۱\alpha - k_۱) - (m_۲\alpha - k_۲) = m\alpha - k \qquad (۱۵.۱)$$

که در آن اگر تعریف کنیم $m = m_۱ - m_۲$ و $k = k_۱ - k_۲$، آنگاه m و k عددهایی صحیح‌اند.

بیایید لحظه‌ای توقف کنیم و ببینیم کجای کار هستیم. روی Γ مجموعه‌ای نامتناهی از نقاط را با فاصلهٔ $n\alpha$ از A علامت زده‌ایم، که در اینجا $n = ۱, ۲, ۳, \ldots$. این نقاط حول نقطه‌ای مانند Q انباشته می‌شوند. کمانی به طول مثبتی مانند ϵ حول Q را تثبیت کرده‌ایم و دو نقطه مانند $m_۱\alpha$ و $m_۲\alpha$ روی کمان یافته‌ایم که فاصله‌شان از یکدیگر برابر $\epsilon_۱$ است که $\epsilon > \epsilon_۱$. حالا می‌توانیم این مجموعه از نقاط $n\alpha$ را به کناری بگذاریم و مجموعه‌ای دیگر بسازیم.

برای ادامه، دوباره از A روی رونوشتی از دایرهٔ Γ که علامت نخورده است شروع کنید و نقاطی که فاصله‌شان از A بر روی محیط دایره برابر عدد دوم ما یعنی γ است، علامت بزنید. در اینجا $۱ \le \gamma \le ۰$ و به یاد بیاورید که γ عددی است که در عبارت لم ۱.۱ به جای c می‌نشیند. همچنین نقطه‌های با فاصله‌های $\epsilon_۱$، $۲\epsilon_۱$، $۳\epsilon_۱$، ... از A را علامت بزنید. در این‌صورت، کوچک‌ترین عددی مانند j را در نظر بگیرید که به‌ازای آن، γ بر روی کمانی بین $(j-۱)\epsilon_۱$ و $j\epsilon_۱$ قرار می‌گیرد. یعنی

$$(j-۱)\epsilon_۱ \le \gamma < j\epsilon_۱ \qquad (۱۶.۱)$$

فاصلهٔ بین دو نقطهٔ متوالی در این مجموعه برابر $\epsilon_۱$ است که $\epsilon_۱ < \epsilon$. بنابراین در شکل ۴.۱، هر یک از دو کمان، از نقطهٔ $\gamma - \epsilon$ تا نقطهٔ γ و از نقطهٔ γ تا نقطهٔ $\gamma + \epsilon$، شامل نقطه‌ای از مجموعهٔ $n\epsilon_۱$ هستند.

اکنون می‌دانیم که به دلیل انتخاب j در (۱۶.۱)، کمان دوم، شامل $j\epsilon_۱$ است. اگر γ مضربی صحیح از $\epsilon_۱$ نباشد، کمان اول شامل نقطهٔ $(j-۱)\epsilon_۱$ است؛ در غیر این‌صورت شامل نقطهٔ $(j-۲)\epsilon_۱$ است. بنابراین همیشه می‌توانیم اعدادی صحیح مانند j و j' بیابیم طوری که

$$\gamma < j\epsilon_۱ < \gamma + \epsilon$$
$$\gamma - \epsilon < j'\epsilon_۱ < \gamma$$

ضمناً چون بنابر (۱۵.۱) می‌دانیم که $\epsilon_۱ = m\alpha - k$، می‌توانیم اعدادی صحیح مانند j و j' بیابیم طوری که

$$\gamma < jm\alpha - jk < \gamma + \epsilon$$
$$\gamma - \epsilon < j'm\alpha - j'k < \gamma$$

یعنی اعدادی صحیح مانند $p_۱ = jm$، $q_۱ = jk$، $p_۲ = j'm$ و $q_۲ = j'k$ یافته‌ایم، طوری که

$$\gamma < p_۱\alpha - q_۱ < \gamma + \epsilon$$
$$\gamma - \epsilon < p_۲\alpha - q_۲ < \gamma$$

و به این ترتیب، اثبات لم ۱.۱ به پایان می‌رسد.

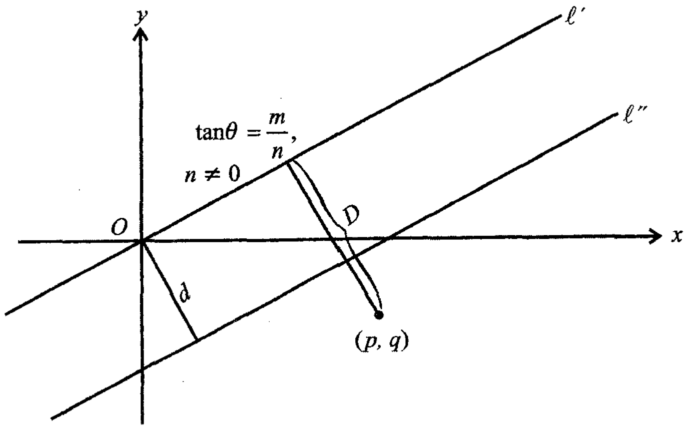
۵.۱ عریض‌ترین مسیرهای بدون نقاط مشبکه‌ای

دیدیم که خطوطی وجود دارند که هیچ نقطهٔ مشبکه‌ای ندارند. این سؤال پیش می‌آید که

آیا نوارها یا مسیرهایی نامتناهی بین دو خط موازی وجود دارند که آنها هم نقطهٔ مشبکه‌ای نداشته باشند؟

بنابر قضیهٔ ۱.۱، اگر دو خط موازی شیب گنگ داشته باشند، پاسخ منفی است. اما در حالتی که نوار بین خطوطی با شیب گویا تعریف شده باشند، پاسخ سؤال مثبت است. در این قسمت به دنبال عریض‌ترین مسیرهای مربوط به این خط‌ها می‌گردیم که نقطهٔ مشبکه‌ای ندارند.

از مبدأ $(\circ,\circ)$ در مشبکهٔ نقطه‌ای اصلی Λ، خط l' را با زاویهٔ θ از محور xها رسم می‌کنیم. بدون کاسته شدن از کلیت، می‌توانیم فرض کنیم که $\circ \leq \theta \leq \frac{\pi}{۲}$ (زیرا اگر $\frac{\pi}{۲} < \theta < \pi$، می‌توانیم با تصویر آینه‌ای l' نسبت به محور yها کار کنیم و نتایج یکسان خواهند بود). سپس مانند شکل ۵.۱، خط دیگری مانند l'' بالا (یا پایین) l' و موازی با و در فاصلهٔ d از آن رسم می‌کنیم.



شکل ۵.۱ مسیری با عرض d.

ناحیهٔ بین l' و l'' را مسیری با عرض d در جهت θ می‌نامیم. در دو حالتی که $\theta = \circ$ و $\theta = \frac{\pi}{۲}$ [یعنی وقتی خطوط عمودی یا افقی هستند]، واضح است که مسیر دارای عرضی برابر ۱ است. سؤال ما این است:

عریض‌ترین مسیر در جهت θ که هیچ نقطهٔ مشبکه‌ای در درونش وجود ندارد، چیست؟

وقتی θ طوری است که $\tan\theta$ گنگ است، بنابر قضیهٔ ۱.۱ هر مسیری با عرض متناهی d در جهت θ، نامتناهی نقطهٔ مشبکه‌ای در درونش دارد.

اما اگر $\tan\theta$ گویا باشد چطور؟ (یعنی اگر $\tan\theta = \frac{m}{n}$ که m و n اعدادی صحیح‌اند و نسبت به هم اول‌اند و $n \neq \circ$) در این حالت، مسیرهایی با عرض مثبتی برابر w وجود دارند که هیچ نقطهٔ مشبکه‌ای ندارند. قضیهٔ بعد توصیفی دقیق از این موقعیت است.

قضیهٔ ۲.۱ اگر $\tan\theta = m/n$ که $gcd(m,n) = ۱$ و $n \neq \circ$ آنگاه مسیری از عرض

$d = ۱/\sqrt{m^۲ + n^۲}$ در جهت θ وجود دارد که شامل هیچ نقطهٔ مشبکه‌ای در درونش نیست. ضمناً هر مسیر با عرض بیشتر از d بالا، نقاط مشبکه‌ای دارد.

اثبات. فرض کنید D فاصلهٔ عمودی نقطه‌ای مشبکه‌ای مانند (p, q) از l' باشد، این فاصله را می‌توان با دستوری از هندسهٔ تحلیلی به صورت

$$D = \frac{| mp - nq|}{\sqrt{m^۲ + n^۲}} \tag{۱۷.۱}$$

یافت (این دستور معمول، با نوشتن معادلهٔ خط $y = (m/n)x$ به شکل

$$\frac{(mx - ny)}{\sqrt{m^۲ + n^۲}} = ۰$$

به‌دست می‌آید. به‌ازای نقطه‌ای مانند (p, q) در صفحه، با عبارت

$$\frac{|mp - nq|}{\sqrt{m^۲ + n^۲}}$$

فاصلهٔ (p, q) از l' به‌دست می‌آید.)

اگر بتوانیم ثابت کنیم که فاصلهٔ l' از نزدیک‌ترین نقطهٔ مشبکه‌ای که واقعاً روی l' نیست، برابر است با $۱/\sqrt{m^۲ + n^۲}$، قضیه اثبات خواهد شد.

ابتدا به صورت کسر (۱۷.۱) دقت می‌کنیم. چون $\gcd(m, n) = ۱$، همیشه می‌توانیم دو عدد صحیح مانند $p = p_۱$ و $q = q_۱$ بیابیم و در نتیجه، نقطه‌ای مشبکه‌ای بیابیم طوری که $mp_۱ - nq_۱ = \pm ۱$ [۴، صص. ۴۲-۳۶]. می‌توانیم بنویسیم

$$|mp_۱ - nq_۱| = ۱$$

این کوچک‌ترین مقدار ناصفر ممکن در صورت دستور (۱۷.۱) است، چون اگر صورت برابر صفر باشد، آنگاه (p, q) نقطه‌ای مشبکه‌ای روی l' خواهد بود.

مخرج در (۱۷.۱) برابر $\sqrt{m^۲ + n^۲}$ است که وقتی شیب خط l' داده شود، مقداری ثابت است. بنابراین، فاصلهٔ l' تا نزدیک‌ترین نقطهٔ مشبکه‌ای $(p_۱, q_۱)$ با عبارت

$$d = \frac{۱}{\sqrt{m^۲ + n^۲}}$$

به‌دست می‌آید.

عرض بین خطوط l' و l'' را w بنامید. اگر w از d کمتر باشد یا با آن مساوی باشد، مسیر هیچ نقطهٔ مشبکه‌ای ندارد؛ اما اگر $w > d$، خواهد داشت. پس با $d = \frac{۱}{\sqrt{m^۲+n^۲}}$، مسیر با بیشترین عرض در جهت θ که درونش هیچ نقطهٔ مشبکه‌ای وجود ندارد، مشخص می‌شود و قضیهٔ ۲.۱ به اثبات می‌رسد.

۶.۱ مستطیل‌ها روی مسیرهای بدون نقطهٔ مشبکه‌ای

جالب است که مساحت مستطیلی را که وقتی l' و l'' مرزهای مسیری بدون نقطهٔ مشبکه‌ای با عرض بیشینه‌اند، بیابیم.

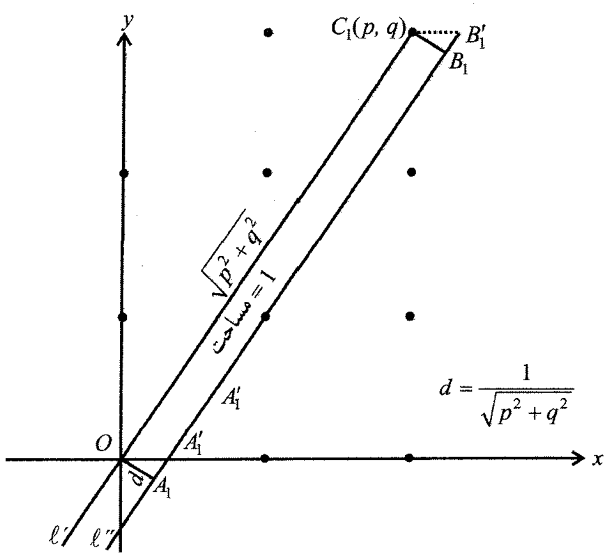
فرض کنید یکی از مرزها ــ مثلاً l' ــ از مبدأ یعنی $O : (۰, ۰)$ و نقطهٔ مشبکه‌ای دیگری مانند $C_۱ : (p, q)$ بگذرد طوری که p و q نسبت به هم اول باشند. همان‌طور که در شکل ۶.۱ می‌بینیم، می‌توان مستطیلی با $OA_۱B_۱C_۱$ تشکیل داد، که در آن

$$|\overline{OA_۱}| = |\overline{C_۱B_۱}| = d$$

و

$$d = \frac{۱}{\sqrt{p^۲ + q^۲}}$$

این مستطیل دارای مساحت واحد است.



شکل ۶.۱ مستطیل واحد در مسیری بدون نقطهٔ مشبکه‌ای.

اثبات تقریباً واضح است، می‌بینیم که $|\overline{OC_1}| = \sqrt{p^2+q^2}$. می‌دانیم که $d = 1/\sqrt{p^2+q^2}$ (d همان عرض مسیر است)، و مساحت مستطیل برابر ضرب این دو عدد است.

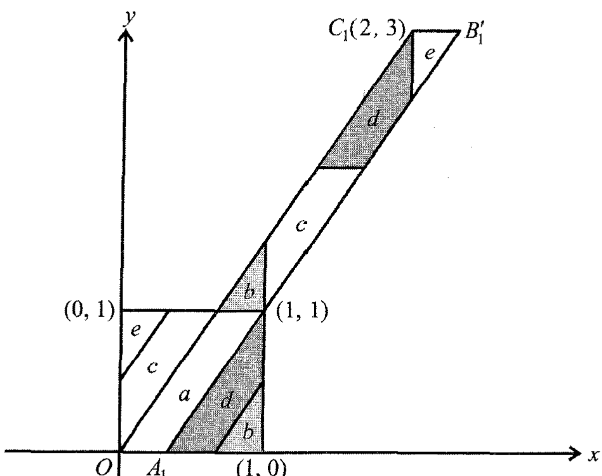
این حکم دربارهٔ مساحت واحد را می‌توان با استفاده از حالتی خاص، به‌طور هندسی هم نتیجه گرفت. ابتدا توجه کنید که در شکل ۶.۱ مساحت مستطیل $OA_1B_1C_1$ برابر است با مساحت متوازی‌الاضلاع $OA'_1B'_1C_1$. اکنون می‌توان این امر را با شکل ۷.۱ مقایسه کرد، که در آن l' خطی با شیب $\tan\theta = m/n = ۳/۲$ است و $\gcd(۳,۲) = ۱$. این خط از $O = (۰,۰)$ و از نقطهٔ مشبکه‌ای $C : (۲,۳)$ می‌گذرد.

کدام نقطهٔ مشبکه‌ای، از همه به l' نزدیک‌تر است؟ نقطهٔ (۱.۱)، زیرا بنابر دستور فاصله (۱۷.۱)، فاصلهٔ $(۱,۱)$ تا l' برابر است با

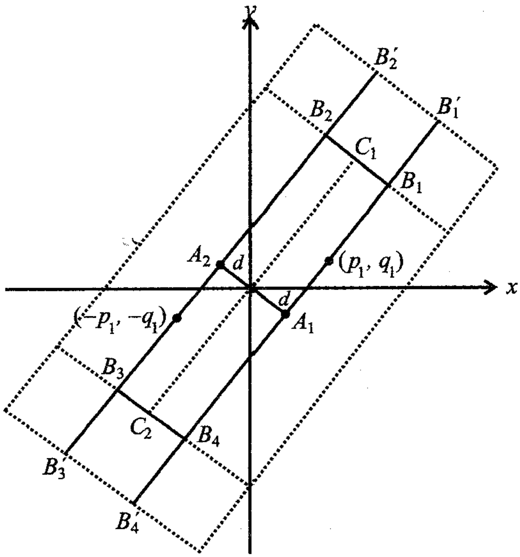
$$D = \frac{|۳\cdot ۱ - ۲\cdot ۱|}{\sqrt{۳^۲+۲^۲}} = \frac{۱}{\sqrt{۱۳}}$$

بنابراین، اگر بتوانیم خط l'' را از $(۱,۱)$ موازی با l' رسم کنیم، هیچ نقطهٔ مشبکه‌ای نمی‌تواند داخل متوازی‌الاضلاع $OA'_1B'_1C_1$ باشد که مساحت آن از قسمت‌هایی تشکیل می‌شود که با a تا e مشخص شده است.

حالا قسمت‌های شکل ۷.۱ را دوباره مرتب می‌کنیم تا مربعی واحد بسازیم. قسمت a را همانجا که هست باقی می‌گذاریم، و قسمت‌های b و c را به موازات محور yها به سمت پایین حرکت می‌دهیم.



شکل ۷.۱ تشکیل مستطیل واحد.



شکل ۸.۱ گسترش دادن مستطیل

سپس قسمت b را در جای جدیدش در نزدیک $(۱,۰)$ باقی می‌گذاریم و قسمت c را به موازات محور xها حرکت می‌دهیم تا به جای جدیدش در سمت چپ قسمت a، و قسمت e را در سمت چپ قسمت c می‌گذاریم. مربع واحد اکنون کاملاً پر شده است، همان‌طور که در شکل ۷.۱ می‌بینید. مستطیل $OA_۱B_۱C_۱$ با مساحت ۱ در شکل ۶.۱، در شکل ۸.۱ گسترش یافته است. مستطیل گسترش یافتهٔ $B_۱B_۲B_۳B_۴$ از چهار مستطیل تشکیل شده که همگی با $OA_۱B_۱C_۱$ همنهشت‌اند. بنابراین مساحت این مستطیل برابر ۴ است. ضمناً این مستطیل نسبت به مبدأ متقارن است؛ یعنی اگر نقطه‌ای به شکل (a,b) که عضو شکل باشد، نقطهٔ $(-a,-b)$ هم عضو شکل است.

هیچ نقطهٔ مشبکه‌ای درون $OA_۱B_۱C_۱$ نیست، و نیز چون p و q نسبت به هم اول‌اند، هیچ نقطهٔ مشبکه‌ای بین $(۰,۰)$ و (p,q) وجود ندارند. بنابراین، مبدأ تنها نقطهٔ مشبکه‌ای درون $B_۱B_۲B_۳B_۴$ است. دست‌کم دو نقطهٔ مشبکه‌ای روی مرز قرار دارند، یعنی $C_۱ : (p,q)$ و $C_۲ : (-p,-q)$. اما باید دست‌کم یک نقطهٔ مشبکه‌ای مانند $(p_۱,q_۱)$ روی ضلع $A_۱B_۱$ قرار داشته باشد و بنابر تقارن، نقطهٔ مشبکه‌ای دیگری نیز مانند $(-p_۱,-q_۱)$ روی ضلع $B_۳A_۲$ قرار دارد. بنابراین می‌توانیم دست‌کم چهار نقطهٔ مشبکه‌ای روی مرز $B_۱B_۲B_۳B_۴$ بیابیم. چه می‌شود اگر مستطیل را با حفظ تقارن گسترش دهیم؟ مثلاً بیایید از ضلع‌های $B_۱B_۲$ و $B_۳B_۴$ فراتر رویم و به ضلع‌های $B'_۱B'_۲$ و $B'_۳B'_۴$ برسیم، همان‌طور که در شکل ۸.۱ با خط‌چین مشخص شده است. مساحت مستطیل جدید از ۴ بیشتر است، و درونش علاوه‌بر $(۰,۰)$، دست‌کم دو نقطهٔ مشبکه‌ای دارد، یعنی (p,q) و $(-p,-q)$

در حقیقت تا جایی که تقارن را حفظ کنیم، هر قدر هم که مستطیل را با حرکت جفت ضلع‌هایش کشیده‌تر کنیم تا مستطیلی با مساحتی بیشتر از ۴ به‌دست آوریم، مرز جدید همچنان علاوه‌بر $(\circ, \circ)$ دست‌کم دو نقطهٔ مشبکه‌ای دیگر هم دارد.

از این بحث ترغیب می‌شویم که بگوییم هر مستطیلی که حول مبدأ متقارن باشد و مساحتش بیش از ۴ باشد، دست‌کم دو نقطهٔ مشبکه‌ای بجز مبدأ دارد.

بی‌درنگ، سؤالاتی دیگر به ذهن می‌رسند. آیا این گزاره در مورد هر بیضی‌ای که مرکزش در مبدأ باشد درست است؟ حکم چقدر عمومی است؟ فرض کنید مستطیلی با ضلع‌های a و b جایی از مشبکه‌ای نقطه‌ای اصلی Λ گذاشته شده باشد. a و b چقدر باشند تا مطمئن باشیم که مستطیل دست‌کم یک نقطهٔ مشبکه‌ای درونش یا روی مرزش دارد؟ می‌توان در سطحی ابتدایی به سمت پاسخ بعضی سؤالات شبیه اینها حرکت کرد. ما این کار را در فصل‌های بعدی می‌کنیم.

مجموعهٔ مسائل فصل ۱

راهنمایی‌ها برای مسائل آسان و راه‌حل‌های کامل مسائل دشوارتر در پایان کتاب آمده‌اند.

۱. سه مثال از l با شیب گویا بیاورید که

الف) هیچ نقطهٔ مشبکه‌ای نداشته باشند.

ب) نامتناهی نقطهٔ مشبکه‌ای داشته باشند.

۲. ثابت کنید که نقطه‌های مشبکه‌ای (p_k, q_k) که از معادلهٔ (۹.۱) به‌ازای عددی صحیح مانند k که $k = \circ, \pm ۱, \pm ۲, \ldots$ به‌دست می‌آیند، روی خط (۵.۱) با فاصله‌های برابر پخش شده‌اند.

۳. خطی با معادلهٔ $y = mx + b$ از نقطه‌های مشبکه‌ای $(p_۱, q_۱)$ و $(p_۲, q_۲)$ گذشته است. ثابت کنید که از نقطه‌های مشبکه‌ای (p_k, q_k) هم که با دستورهای $p_k = p_۱ + k(p_۲ - p_۱)$ و $q_k = q_۱ + k(q_۲ - q_۱)$ تعریف می‌شوند، می‌گذرد. در اینجا k عددی صحیح است.

۴. خطی با معادلهٔ $y = (m/n)x$ که در آن m و n اعدادی صحیح و نسبت به هم اول‌اند، از نقطهٔ مشبکه‌ای (p, q) می‌گذرد که p و q نسبت به هم اول‌اند. ثابت کنید که هیچ نقطهٔ مشبکه‌ای دیگری در بین $(\circ, \circ)$ و (p, q) روی این خط قرار ندارد.

۵. خط با معادلهٔ $y = \sqrt{۲}x$ را در نظر بگیرید. آیا این خط از هیچ نقطهٔ مشبکه‌ای می‌گذرد؟ توضیح دهید که چرا آری یا چرا نه.

۶. به‌ازای هر عدد مثبت ϵ که در پایین داده شده است، نقطه‌های مشبکه‌ای مانند (p, q) بیابید که فاصله‌اش از خط $y = \sqrt{۲}x$ کمتر از ϵ باشد:

الف) $\epsilon = \frac{۱}{۲}$

ب) $\epsilon = \frac{۱}{۵}$

ج) $\epsilon = \frac{۱}{۱۰}$

۷. ثابت کنید هر مثلثی با سه رأس غیر هم‌خط روی نقاط مشبکه‌ای، که نقطهٔ مشبکه‌ای دیگری روی مرزش و درونش ندارد، مساحتش برابر $\frac{۱}{۲}$ است.

مراجع

1. C. F. Gauss, *Werke*, Vol. 2 (Göttingen: Gesellschaft der Wissenschaften, 1876).

2. Ivan Niven, *Numbers: Rational and Irrational*, New Mathematical Library Series, Vol. 1 (New York and Toronto: Random House, 1961).

3. ________, "Simple Irrationalities," Chapter 2, Section 2, in *Irrational Numbers,* Carus Mathematical Monographs, No. 11 (New York: Wiley, 1956), 16-21.

4. Carl D. Olds, *Continued Fractions,* New Mathematical Library Series, Vol. 9 (New York and Toronto: Random House, 1963).

5. J. V. Uspensky and M. A. Heaslet, *Elementary Number Theory* (New York: McGraw-Hill, 1939).

۲ شمارش نقاط مشبکه‌ای

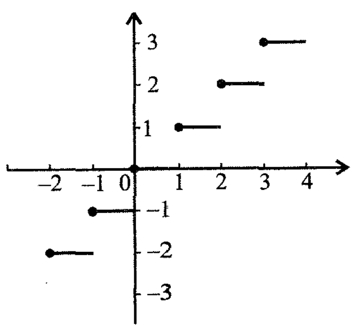
۱.۲ تابع جزء صحیح، $[x]$

معمولاً برایمان این سؤال پیش می‌آید که چند نقطهٔ مشبکه‌ای روی پاره‌خط‌ها یا درون مستطیل‌ها یا در قسمت‌های مختلف مقاطع مخروطی و مانند آن قرار دارند. اساساً آنچه می‌خواهیم بدانیم این است که: چگونه نقاط مشبکه‌ای را می‌شماریم، یا دست‌کم تعدادشان را تخمین می‌زنیم؟ در این فصل، چند ایده معرفی می‌شوند.

دوباره از تابع حسابی $[x]$ استفاده خواهیم کرد که به‌ازای هر عدد حقیقی مانند x، به‌صورت بزرگ‌ترین عدد صحیحی که از x بزرگ‌تر نیست تعریف می‌شود.

$$[x] = \text{بزرگ‌ترین عدد صحیح} \leq x$$

این عدد صحیح را جزء صحیح x می‌نامیم. برای مثال، جزء صحیح ۳/۶ که آن را با [۳/۶] نمایش می‌دهیم، برابر ۳ است، زیرا ۳ بزرگ‌ترین عدد صحیحی است که از ۳/۶ کوچک‌تر یا با آن برابر است. مشابهاً ۶ = [۶]، ۲− = [۲−] و ۳− = [۲/۵−]. معادلهٔ $y = [x]$ در شکل ۱.۲ رسم شده است.



شکل ۱.۲ نمودار $y = [x]$.

وقتی به x روی محور اعداد فکر می‌کنیم، چگونه می‌توانیم ارتباطش را با اعداد صحیح مجاور بیان کنیم؟ بنابر تعریف، عدد صحیح $[x]$ در نابرابرای $[x] \leq x < [x] + ۱$ صدق می‌کند. در نتیجه، می‌توانیم بنویسیم

$$x = [x] + \zeta \quad \text{که در آن} \quad ۰ \leq \zeta < ۱$$

ما ζ را جزء اعشاری x می‌نامیم، همان‌طور که در شکل ۲.۲ دیده می‌شود.

شکل ۲.۲ جزء اعشاری x.

تابع $[x]$ ویژگی‌های مفید بسیاری دارد، که چهارتایشان را در پایین برشمرده‌ایم. هر یک را با مثال‌های عددی امتحان کنید.

۱. اگر n عددی صحیح باشد، $[x + n] = [x] + n$.

۲. اگر x عددی صحیح باشد، $[x] + [-x] = ۰$.
اگر x عددی صحیح نباشد، $[x] + [-x] = -۱$.

۳. $[x] + [y] \leq [x + y] \leq [x] + [y] + ۱$.

۴. اگر n عددی طبیعی باشد، $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$.

اثباتی که از ویژگی (۳) در پی می‌آید، فکرهای اصلی را برای اثبات بقیهٔ ویژگی‌ها روشن می‌کند.

اثبات ویژگی ۳. می‌خواهیم ثابت کنیم که $[x + y] \geq [x] + [y]$. قرار دهید

$$x = [x] + \zeta_۱ \quad \text{که} \quad ۰ \leq \zeta_۱ < ۱$$

و

$$y = [y] + \zeta_۲ \quad \text{که} \quad ۰ \leq \zeta_۲ < ۱$$

حاصل‌جمع این دو برابر است با

$$x + y = [x] + [y] + (\zeta_۱ + \zeta_۲)$$

پس

$$[x + y] = [(\zeta_۱ + \zeta_۲) + ([x] + [y])]$$

چون $[x]+[y]$ عددی صحیح است، می‌توانیم با استفاده از ویژگی (۱)، بنویسیم

$$[x+y]=[\zeta_1+\zeta_2]+[x]+[y]$$

شرط‌های ما $1>\zeta_1\geq 0$ و $1>\zeta_2\geq 0$ بودند. پس $2>\zeta_1+\zeta_2\geq 0$. بنابراین، بسته به اینکه $1>\zeta_1+\zeta_2\geq 0$ یا $2>\zeta_1+\zeta_2\geq 1$، می‌توانیم نتیجه بگیریم که $[\zeta_1+\zeta_2]$ برابر با ۰ یا ۱ است.

متناظراً

$$[x+y]=\begin{cases}[x]+[y] & \text{اگر } [\zeta_1+\zeta_2]=0،\\ [x]+[y]+1 & \text{اگر } [\zeta_1+\zeta_2]=1،\end{cases}$$

پس ثابت کرده‌ایم که $[x+y]\geq[x]+[y]$ که همان ویژگی (۳) است.

مجموعهٔ مسائل قسمت ۱.۲

۱. با آوردن مثال نقض، ثابت کنید هیچ‌یک از گزاره‌های زیر به‌ازای همهٔ x و yها برقرار نیست.

الف) $[x+y]=[x]+[y]$

ب) $\left[\frac{x}{y}\right]=\frac{[x]}{[y]}$

ج) $[xy]=[x]\cdot[y]$

۲. ویژگی (۱) را ثابت کنید.

۳. ویژگی (۲) را ثابت کنید.

۴. تلاش کنید که ویژگی (۴) را در مورد $[x]$ ثابت کنید. ابتدا مثال‌های عددی را بررسی کنید. (اگر مجبور شدید که به راه‌حل‌های آخر کتاب نگاه کنید، دلسرد نشوید.)

۵. ثابت کنید که $[2x]+[2y]\geq[x]+[y]+[x+y]$.

۶. ثابت کنید اگر a و b اعدادی طبیعی باشند، آنگاه تعداد مضرب‌های b که از a بیشتر نیستند، برابر است با $[a/b]$.

۷. ثابت کنید $-[-x]$ کوچک‌ترین عدد صحیحی است که با x برابر است یا از آن بزرگ‌تر است.

۸. ثابت کنید که $\left[x+\frac{1}{2}\right]$ نزدیک‌ترین عدد صحیح به x است. اگر x در وسط دو عدد صحیح باشد، $\left[x+\frac{1}{2}\right]$ عدد بزرگ‌تر را می‌دهد.

۹. مانند مسئلهٔ ۸، گزاره‌هایی مشابه دربارهٔ $\left[-x+\frac{۱}{۲}\right]-$ بسازید و ثابت کنید.

۱۰. این حکم در همهٔ کتاب‌های درسی نظریهٔ اعداد ثابت می‌شود: اگر n عددی طبیعی باشد، نمای بزرگ‌ترین توان عدد اولی مانند p که $n! = ۱\cdot۲\cdot۳\cdot\ldots n$ را می‌شمارد برابر است با

$$E(p,n)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^{۲}}\right]+\left[\frac{n}{p^{۳}}\right]+\cdots,$$

که مجموعی است که در آن، فقط تعداد متناهی جملهٔ ناصفر وجود دارند. از این دستور استفاده کنید تا ثابت کنید $E(۷,۱۰۰۰)=۱۶۴$؛ یعنی $۷^{۱۶۴}$ بزرگ‌ترین توان ۷ در $۱۰۰۰!$ است.

۲.۲ جواب‌های طبیعی معادلهٔ $ax+by=n$

فرض کنید معادلهٔ خط l به شکل

$$l: ax+by=n \qquad (۱.۲)$$

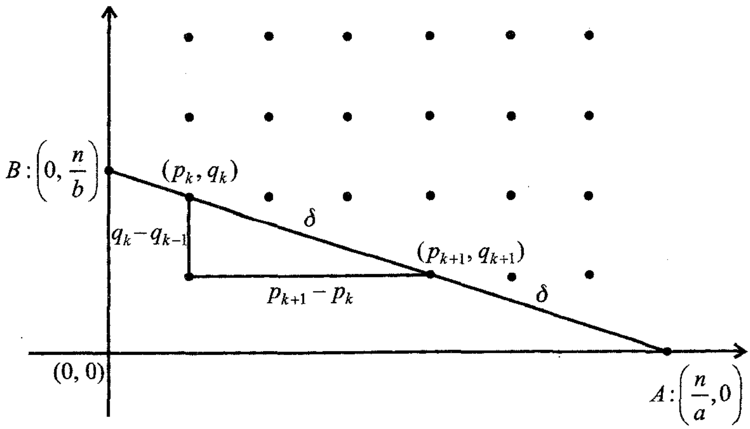
باشد که در آن، a و b نسبت به هم اول‌اند و a، b و n اعدادی طبیعی‌اند. می‌خواهیم این معادله را به دید معادله‌ای دیوفانتی نگاه کنیم؛ یعنی ضرایب آنها اعدادی صحیح‌اند و ما به دنبال جواب‌های صحیح x و y هستیم. در فصل ۱ ثابت کردیم که معادلهٔ $ax+by=n$ در (۱.۲) دارای نامتناهی جواب به شکل $x=p_k$ و $y=q_k$ است که p_k و q_k هر دو اعداد صحیح‌اند. بنابراین خط (۱.۲) از نامتناهی نقطهٔ مشبکه‌ای (p_k,q_k) از Λ می‌گذرد. فرض کنید $(p_\circ,q_\circ)$ یکی از نقطه‌های مشبکه‌ای آن باشد. در این‌صورت همهٔ نقطه‌های مشبکه‌ای دیگر مانند (p_k,q_k) روی l را می‌توان از معادله‌های

$$\begin{aligned} p_k &= p_\circ + kb \\ q_k &= q_\circ - ka \end{aligned} \qquad (۲.۲)$$

به‌ازای $k=\circ,\pm۱,\pm۲,\ldots$ حساب کرد. (شاید این نوع معادله‌ها را بشناسید. در قسمت ۳.۱ دربارهٔ معادله‌هایی دیگر از همین نوع بحث کردیم، گرچه شرط نکرده بودیم که ضرایب در معادلهٔ (۵.۱) باید مثبت باشند.)

خط l در (۱.۲) محور xها را در نقطهٔ $A:(n/a,\circ)$ و محور yها را در نقطهٔ $B:(\circ,n/b)$ قطع می‌کند. این الگو سؤال زیر را ایجاد می‌کند:

آیا دستوری برای یافتن نقاط مشبکه‌ای روی l بین نقاط A و B وجود دارند؟



شکل ۳.۲ فاصلهٔ بین نقاط مشبکه‌ای متوالی روی l.

به بیان دیگر، معادلهٔ (۱.۲) چند جواب صحیح دارد؟

ما برای رسیدن به پاسخ این سؤال، به شکل ۳.۲ توجه می‌کنیم، که در آن مثلث قائم‌الزاویهٔ OAB ساق‌هایی با طول‌های n/a و n/b دارد. بنابر دستور طول وتر $\overline{AB}$ می‌توانیم بنویسیم

$$c = \sqrt{\left(\frac{n}{a}\right)^۲ + \left(\frac{n}{b}\right)^۲} = \frac{n}{ab}\sqrt{a^۲ + b^۲}$$

اگر در (۲.۲)، k را با $k + ۱$ عوض کنیم تا نقطهٔ مشبکه‌ای بعدی را مشخص کنیم، می‌بینیم که

$$p_{k+۱} = p_۰ + (k + ۱)b = p_k + b$$
$$q_{k+۱} = q_۰ - (k + ۱)a = q_k - a$$

از اینجا می‌توانیم فاصلهٔ بین دو نقطهٔ مشبکه‌ای متوالی $P_k : (p_k, q_k)$ و $P_{k+۱} : (p_{k+۱}, q_{k+۱})$ روی l را که با δ نشان می‌دهیم، به‌صورت

$$\delta = \sqrt{(p_{k+۱} - p_k)^۲ + (q_{k+۱} - q_k)^۲} = \sqrt{a^۲ + b^۲}$$

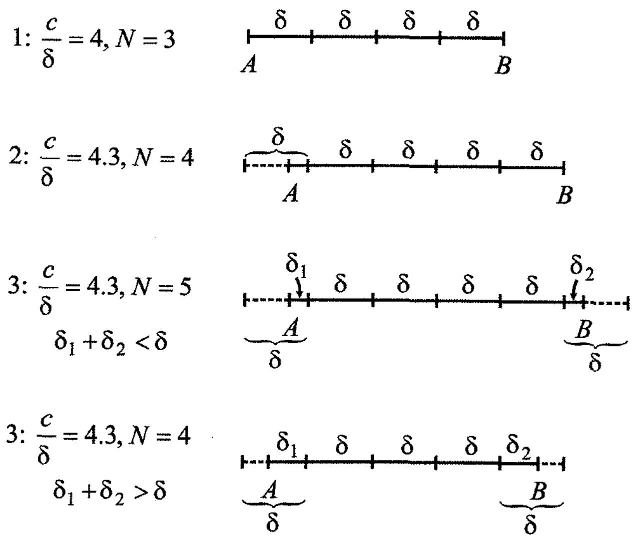
بیابیم.

اکنون آماده‌ایم که تعداد نقاط مشبکه‌ای روی $\overline{AB}$ را که با N نمایش می‌دهیم تخمین بزنیم. ابتدا طول پاره‌خط $c = |\overline{AB}|$ را به طول‌های δ که برابر است با $|\overline{P_kP_{k+۱}}|$ تقسیم‌بندی می‌کنیم تا به‌دست بیاوریم $c/\delta = n/ab$. در این‌صورت از

$$\left[\frac{c}{\delta}\right] = \left[\frac{n}{ab}\right]$$

می‌توان تعداد بازه‌هایی به طول δ را که می‌توانیم به‌طورکامل روی $\overline{AB}$ علامت بزنیم، مشخص کرد. در پایان، چون نقاط انتهایی هر بازه نقطه‌های مشبکه‌ای‌اند، می‌توانیم تخمین بزنیم که چند نقطهٔ مشبکه‌ای روی $\overline{AB}$ قرار دارند.

اما در اینجا پیچیدگی‌ای وجود دارد. چون kتا بازهٔ کنار هم به طول‌های δ روی $\overline{AB}$ با $k - ۱$ زیر تقسیم نقطه‌های مشبکه‌ای جدا شده‌اند، و چون c/δ ممکن است صحیح نباشد، باید حالت‌های زیر را جداگانه در نظر بگیریم که هر یک در شکل ۴.۲ نمایش داده شده‌اند.



شکل ۴.۲ بازه‌های به طول δ، کامل یا کسری. حالت‌های ۱، ۲ و ۳.

حالت ۱. هر دوی A و B نقاط مشبکه‌اند.

نتیجه می‌شود که هر دوی n/b و n/a اعدادی صحیح‌اند، یا به عبارت دیگر $a \mid n$ و $b \mid n$، که $\gcd(a, b) = ۱$. بنابر قضیهٔ بنیادی حساب در فصل ۱، نتیجه می‌گیریم $ab \mid n$ (دو شرط $a \mid n$ و $b \mid n$ به تنهایی کافی نیستند تا نتیجه بگیریم $ab \mid n$؛ برای مثال $۳ \mid ۱۲$، $۶ \mid ۱۲$، اما $۱۸ \nmid ۱۲$).

در این حالت، دقیقاً $N = (n/ab) - ۱ = [n/ab] - ۱$ نقطه مشبکه‌ای روی $\overline{AB}$ بجز نقاط انتهایی A و B داریم. در نتیجه، تعداد جواب‌های طبیعی معادلهٔ (۱.۲) روی $\overline{AB}$ برابر است با $[n/ab] - ۱$.

اما اگر اجازه دهیم x و y مقدار صفر هم بگیرند، آنگاه تعداد جواب‌های نامنفی معادلهٔ (۱.۲) روی $\overline{AB}$ برابر خواهد بود با $[n/ab] - ۱ + ۲ = [n/ab] + ۱ = N + ۲$.

حالت ۲. فقط یکی از A و B نقطهٔ مشبکه‌ای است.

در این حالت، n بر یکی از a یا b بخش‌پذیر است، ولی بر هر دو نیست. بنابراین n/ab عددی صحیح نیست. برای مثال، فرض کنید B نقطهٔ مشبکه‌ای باشد (پس $b \mid n$) ولی A نباشد (پس $a \nmid n$). آنگاه A در بازه‌ای به طول δ قرار می‌گیرد که A را در بر می‌گیرد. شکل ۴.۲ را ببینید. بدون شمردن B، تعداد نقاط مشبکه‌ای بین A و B برابر با تعداد بازه‌های کامل به طول δ است. این تعداد برابر با $[n/ab]$ است و تعداد جواب‌های طبیعی (۱.۲) بر روی $\overline{AB}$ را نشان می‌دهد. بنابراین $[n/ab] + ۱ = N + ۱$ جواب نامنفی وجود دارند.

حالت ۳. نه A نقطه‌ای مشبکه‌ای است و نه B.

در اینجا هر دوی نقاط انتهایی A و B درون بازه‌هایی به طول δ هستند که در دو جهت، از A و B می‌گذرند، همان‌طور که در شکل ۴.۲ می‌بینید. در این حالت، تعداد نقطه‌های مشبکه‌ای روی $\overline{AB}$ عددی بزرگ‌تر از تعداد بازه‌های به طول δ روی $\overline{AB}$ است.

می‌توانیم این امر را با جمع‌کردن طول‌های قسمت‌های کسری $\delta_۱$ و $\delta_۲$ بین A و B ببینیم. دو نتیجه محتمل‌اند. اولی این است که اگر $\delta_۱ + \delta_۲ < \delta$ آنگاه تعداد بازه‌های کامل به طول δ برابر است با $[n/ab]$ و تعداد نقطه‌های مشبکه‌ای روی $\overline{AB}$ (یعنی N) یکی بیشتر است: $[n/ab] + ۱$. احتمال دوم این است که $\delta_۱ + \delta_۲ > \delta$، پس تعداد بازه‌های کامل به طول δ برابر است با $N = [n/ab]$ نقطهٔ مشبکه‌ای روی $\overline{AB}$.

پس از بررسی این حالت‌ها، این قضیه را دربارهٔ شمارش نقاط مشبکه‌ای به‌دست می‌آوریم:

قضیهٔ ۱.۲ اگر a، b و n اعداد طبیعی باشند و a و b نسبت به هم اول باشند، آنگاه تعداد نقاط مشبکه‌ای $(x, y) = (p, q)$، $x = p > ۰$ و $y = q > ۰$، روی خط $ax + by = n$ اگر $ab \neq ۰$ برابر است با

$$N = \left[\frac{n}{ab}\right] + \zeta \qquad (۳.۲)$$

که ζ یکی از مقادیر ۱−، ۰ یا ۱ را دارد.

با اینکه دستور (۳.۲) تعداد دقیق را نمی‌دهد، اما سه عدد صحیح متوالی را به‌دست می‌دهد که یکی از آنها برابر تعداد موردنظر است. دیدیم که حالت $\zeta = -۱$ فقط وقتی ممکن است که n/ab عددی صحیح باشد. بنابراین، اگر $n > ab$ معادلهٔ (۱.۲) همیشه دست‌کم یک جواب طبیعی دارد. دیکسون [۱] توضیحات بیشتری دربارهٔ دستور (۳.۲) می‌دهد.

مجموعهٔ مسائل قسمت ۲.۲

۱. استدلالی را که به قضیهٔ ۱.۲ منجر شد، با استفاده از مثال‌های عددی زیر بررسی کنید. در هر حالت شکل بکشید.

الف) $x + y = ۵$ ب) $۲x + y = ۵$

ج) $۳x + ۴y = ۲۴$ د) $۳x + ۲y = ۱۳$

ه) $۴x + ۳y = ۱۱$

۲. ثابت کنید اگر $(p_۰, q_۰)$ جوابی خاص از معادلهٔ (۱.۲) باشد، آنگاه معادلاتی که در (۲.۲) برای (p_k, q_k) داده شد، همهٔ جواب‌های دیگر را به‌دست می‌دهد.

۳. قضیهٔ ۱.۲ را با مثالی عددی نشان دهید.

۴. هاوارد گراسمن مسائل زیاد و جالبی در «تفریح با نقاط مشبکه‌ای» [۲] آورد، ویلیام شاف فهرستی از آنچه در این موضوع منتشر کرده بود، و نیز کتابشناسی‌ای گسترده دربارهٔ کتاب‌های مسئله در هندسه [۳] فراهم کرد. این نمونه از مسائلی است که می‌توان یافت:

تعداد مسیرهای مشبکه‌ای از مبدأ تا نقاط مشبکه‌ای روی خط $x + ۲y = n$ برابر است با جمله nام دنبالهٔ فیبوناچی

$$۱, ۲, ۳, ۵, ۸, ۱۳, ۲۱, \ldots$$

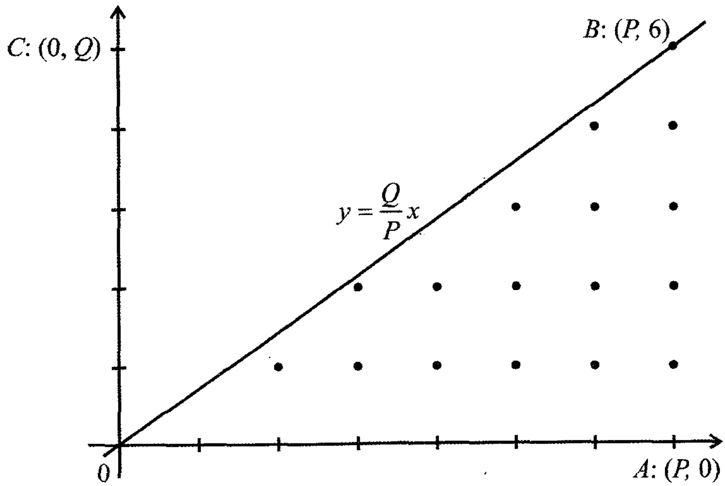
که با $u_۱ = ۱$، $u_۲ = ۲$، $u_۳ = u_۱ + u_۲ = ۳$، ...، $u_n = u_{n-۱} + u_{n-۲}$ تعریف می‌شود. مسیری مشبکه‌ای مانند مسیر تاکسی‌ای است که روی مشبکه، از مبدأ فقط به سمت شمال (بالا) یا شرق (راست) می‌رود. بنابراین، فقط می‌توان به نقاط مشبکه‌ای با مختصات صحیح نامنفی رسید. با شکلی ثابت کنید که اگر $n = ۷$، تعداد مسیرها از O به نقاط مشبکه‌ای $(۷, ۰)$، $(۵, ۱)$، $(۳, ۲)$، $(۱, ۴)$ برابر با $u_۷ = ۲۱ = ۴ + ۱۰ + ۶ + ۱$ است.

۳.۲ نقطه‌های مشبکه‌ای داخل مثلث

چگونه حاصل سری‌ای از اعداد صحیح را می‌یابیم؟ در مورد سری‌های خاص، معمولاً برای حل این مسئله، آن را با دیدی هندسی برحسب تعداد نقطه‌های مشبکه‌ای نگاه می‌کنیم.

قضیهٔ ۲.۲ اگر P و Q دو عدد طبیعی نسبت به هم اول باشند، آنگاه

$$\left[\frac{Q}{P}\right] + \left[\frac{۲Q}{P}\right] + \left[\frac{۳Q}{P}\right] + \cdots + \left[\frac{(P-۱)Q}{P}\right] = \frac{(Q-۱)(P-۱)}{۲}$$



شکل ۵.۲ نقاط مشبکه‌ای درون مثلث.

اثبات. روی مشبکهٔ اصلی Λ، نقاط $O : (\circ, \circ)$، $A : (P, \circ)$، $B : (P, Q)$ و $C : (\circ, Q)$ را مشخص کنید؛ مانند شکل ۵.۲ که به‌ازای $P = ۷$، $Q = ۵$ رسم شده است. بدون از دست رفتن کلیت می‌توانیم فرض کنیم $P > Q$، چون اگر $P < Q$ کافی است نام‌هایشان را عوض کنیم.

چون معادلهٔ قطر OB برابر است با

$$y = \frac{Q}{P}x \quad \text{که} \quad \gcd(Q, P) = ۱ \tag{۴.۲}$$

تنها نقطه‌های مشبکه‌ای روی OB، نقطه‌های O و B هستند. چون اگر نقطهٔ مشبکه‌ای مانند (p, q) روی خط (۴.۲) بین O و B می‌بود، آنگاه $q/p = Q/P$، اما $P > p > \circ$ و $Q > q > \circ$ که با فرض $\gcd(Q, P) = ۱$ (که یعنی کسر Q/P تا حد امکان ساده شده است) در تناقض است.

حالا فرض کنید $x = n$ روی خط (۴.۲) باشد، که در آن $n = ۱, ۲, \ldots, P - ۱$. می‌توانیم بنویسیم

$$[y] = \left[\frac{nQ}{P}\right]$$

این عدد صحیح مختصات عرض نقطهٔ مشبکه‌ای را که روی خط عمودی $x = n$، از همه به نقطهٔ (n, y) نزدیک‌تر است و زیر خط قرار دارد، نشان می‌دهد. از $[y]$ تعداد نقطه‌های مشبکه‌ای روی $x = n$ و زیر OB و بالای محور xها را هم می‌یابیم. بنابراین، می‌توانیم حساب کنیم که چند نقطهٔ مشبکه‌ای درون ΔOAB قرار دارند.

تعداد کل نقطه‌های مشبکه‌ای درون ΔOAB برابر حاصل‌جمع

$$\left[\frac{۱Q}{P}\right]+\left[\frac{۲Q}{P}\right]+\cdots+\left[\frac{(P-۱)Q}{P}\right] \qquad (۵.۲)$$

است. برای مثال در شکل ۵.۲ تعداد کل نقطه‌های مشبکه‌ای درون ΔOAB روی خط‌های $x=۱,۲,۳,۴,۵,۶$ برابر است با

$$\left[\frac{۱\cdot ۵}{۷}\right]+\left[\frac{۲\cdot ۵}{۷}\right]+\left[\frac{۳\cdot ۵}{۷}\right]+\left[\frac{۴\cdot ۵}{۷}\right]+\left[\frac{۵\cdot ۵}{۷}\right]+\left[\frac{۶\cdot ۵}{۷}\right]=۱۲$$

بنابر تقارن، درون مستطیل $OABC$ دقیقاً دو برابر این حاصل‌جمع نقطه‌های مشبکه‌ای وجود دارد، یعنی ۲۴تا.

در حالت کلی، حاصل‌جمع (۵.۲) به‌ازای مثلث دقیقاً نصف تعداد نقطه‌های مشبکه‌ای درون مستطیل $OABC$ است. یعنی این تعداد برابر است با

$$\frac{(P-۱)(Q-۱)}{۲}$$

و بدین صورت، قضیهٔ ۲.۲ ثابت می‌شود.

قضیهٔ ۲.۲ به روش‌های مختلف تعمیم داده شده است. در اینجا دو قضیهٔ دیگر مطرح می‌شود؛ اثبات آنها به‌عنوان تمرین در مجموعهٔ مسائل آمده است.

قضیهٔ ۳.۲ اگر P و Q دو عدد طبیعی باشند و اگر بزرگ‌ترین مقسوم‌علیه مشترک آنها برابر d باشد، آنگاه

$$\left[\frac{۱\cdot Q}{P}\right]+\left[\frac{۲\cdot Q}{P}\right]+\cdots+\left[\frac{(P-۱)Q}{P}\right]=\frac{(P-۱)(Q-۱)}{۲}+\frac{d-۱}{۲}$$

قضیهٔ ۴.۲ اگر $P'=(P-۱)/۲$ و $Q'=(Q-۱)/۲$ که در آن P و Q اعدادی اول و فردند، آنگاه

$$\sum_{j=۱}^{p'}\left[\frac{jQ}{P}\right]+\sum_{j=۱}^{Q'}\left[\frac{jP}{Q}\right]=P'Q'$$

مجموعهٔ مسائل قسمت ۳.۲

۱. توضیح دهید که چرا قسمت سمت راست $\frac{۱}{۲}(P-۱)(Q-۱)+\frac{۱}{۲}(d-۱)$ در دستور قضیهٔ ۳.۲ به‌ازای هر انتخابی برای P و Q عددی صحیح است؟ (d بزرگ‌ترین مقسوم‌علیه مشترک P و Q است.)

۲. مثال‌هایی عددی برای نمایش قضیه‌های ۲.۲، ۳.۲ و ۴.۲ بیاورید.

۳. قضیهٔ ۳.۲ را ثابت کنید.

۴. قضیهٔ ۴.۲ را ثابت کنید.

مراجع

1. L. E. Dickson, "Linear Diophantine Equations and Congruences," Chapter 2 in *History of the Theory of Numbers, Vol II*: Diophantine Analysis (Washington, D.C.: Carnegie Institute, 1920), 64-71.

2. Howard D. Grossman, "Fun with Lattice Points," *Scripta Mathematica* 16 (1950): 207-12.

3. William Schaaf, *Bibliography of Recreational Mathematics*, Vol. 1 (Reston, VA: National Council of Teachers of Mathematics, 1959: reprinted, 1973).

۳ نقاط مشبکه‌ای و مساحت چندضلعی‌ها

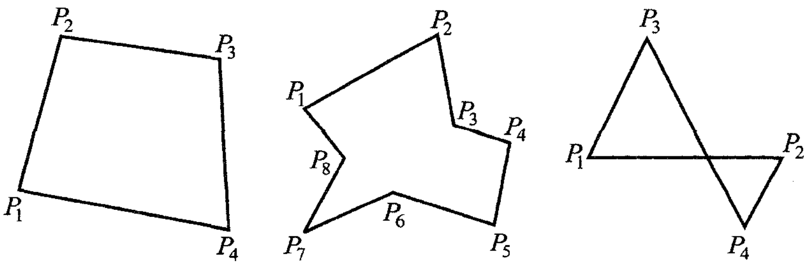
۱.۳ نقطه‌ها و چندضلعی‌ها

ارتباط‌های بسیار و جالبی بین نقطه‌های مشبکه‌ای و مساحت شکل‌های هندسی مانند چندضلعی‌ها و مثلث‌ها وجود دارد. کمی جلوتر در بخش ۲ قضیه‌های زیبای مینکوفسکی دربارهٔ هندسهٔ اعداد را بررسی می‌کنیم. در این فصل مفاهیمی زیبا را دربارهٔ بعضی از این ارتباط‌ها می‌بینیم. با تعریف اصطلاحات اصلی شروع می‌کنیم، و بعد دو قضیهٔ مهم را بررسی می‌کنیم.

منظور از چندضلعی، مجموعه‌ای از نقاط به نام رأس‌ها است که به ترتیبی با پاره‌خط‌هایی که آنها را ضلع‌ها می‌نامیم، به هم وصل شده‌اند. شکل ۱.۳ را ببینید. برای ساختن چندضلعی، نقاط داده شده را به شکل $P_۱, P_۲, \ldots, P_n$ شماره می‌گذاریم و پاره‌خط‌های

$$\overline{P_۱P_۲}, \overline{P_۲P_۳}, \ldots, \overline{P_{n-۱}P_n}, \overline{P_nP_۱}$$

را رسم می‌کنیم. دو ضلع مجاور $P_{k-۱}P_k$ و $P_kP_{k+۱}$ رأس مشترک P_k را دارند. در چندضلعی‌های ساده هیچ دوضلعی نقطهٔ مشترک دیگری ندارند. در شکل ۱.۳، چندضلعی‌های سمت چپ و وسط



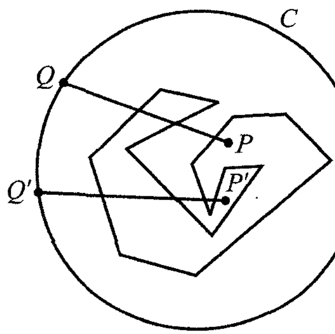
شکل ۱.۳ سمت چپ و وسط: مثال‌هایی از چندضلعی‌های ساده. سمت راست: چندضلعی‌ای غیرساده.

ساده‌اند، و سمت راست نیست. ما فقط با چندضلعی‌های ساده کار داریم.

مرز چندضلعی، مجموعهٔ همهٔ ضلع‌ها و رأس‌هایش است. مرز، صفحه را به دو ناحیه تقسیم می‌کند: درون چندضلعی و بیرون آن. وقتی به دنبال نقطه‌های مشبکه‌ای هستیم، در جاهایی درون، رو یا بیرون این مرزها می‌گردیم.

راحت است که ببینیم نقطه‌هایی مانند P درون چندضلعی است یا نه:

۱. اول تمام چندضلعی را با دایرهٔ بزرگی مانند C که هیچ نقطهٔ مشترکی با چندضلعی ندارد می‌پوشانیم، مانند شکل ۲.۳. چون تعداد متناهی نقطه مانند $P_۱$، $P_۲$، ...، P_n داریم، حتماً دایره‌ای که همهٔ نقطه‌ها را بپوشاند وجود دارد.



شکل ۲.۳ تعیین اینکه نقطه‌ای، درون چندضلعی است یا بیرون آن.

۲. سپس شعاعی دلخواه از P در جهتی رسم می‌کنیم که از هیچ‌یک از n رأس نگذرد، و امتدادش می‌دهیم تا در نقطه‌ای به C برخورد کند، مثلاً در نقطهٔ Q.

۳. اکنون می‌شماریم که این شعاع PQ، چند دفعه از مرز چندضلعی رد شده است. اگر تعداد دفعات فرد باشد، P درون چندضلعی است، و اگر زوج باشد، P بیرون آن است. این حالات ممکن در شکل ۲.۳ با P و P' نمایش داده شده‌اند که در آن شعاع‌های موردنظر، C را به ترتیب، در Q و Q' قطع می‌کنند.

۲.۳ قضیهٔ پیک

فرض کنید $\mathcal{P}$ چندضلعی ساده‌ای باشد و رأس‌هایش روی مشبکهٔ اعداد صحیح باشد که آن را Λ می‌نامیم. ارتباطی جالب بین مساحت $\mathcal{P}$ و تعداد نقطه‌های مشبکه‌ای روی آن و درونش وجود دارد. بنابر نوشتهٔ هوگو اشتاینهاوس، این ارتباط را اولین بار گئورگ پیک در ۱۸۹۹ ثابت کرد، و به همین دلیل، قضیهٔ پیک نامیده شده است.

قضیهٔ ۱.۳ مساحت هر چندضلعی ساده مانند $\mathcal{P}$ که رأس‌هایش، نقطه‌هایی مشبکه‌ای از Λ هستند، با دستور

$$A = I + \frac{۱}{۲}B - ۱ \qquad (۱.۳)$$

به‌دست می‌آید، که در آن I تعداد نقطه‌های مشبکه‌ای درون $\mathcal{P}$، و B تعداد نقطه‌های مشبکه‌ای روی مرز $\mathcal{P}$ از جمله رأس‌هاست.

اثبات معمول قضیهٔ پیک بر این حقیقت بنا شده که مثلثی که رأس‌هایش نقطه‌های مشبکه‌ای‌اند ولی هیچ نقطهٔ مشبکه‌ای دیگری نه روی ضلع‌هایش دارد و نه درونش، مساحتش دقیقاً برابر $\frac{۱}{۲}$ است. دربارهٔ قضیهٔ پیک در جایی دیگر [۱] به کفایت بحث شده است. پس ما اثباتش را نمی‌آوریم.

مجموعهٔ مسائل قسمت ۲.۳

۱. مستطیلی با رأس‌های $(۰,۰), (a,۰), (a,b), (۰,b)$ رسم کنید، که در آن a و b اعدادی صحیح‌اند. برحسب این دو عدد، B (تعداد نقطه‌های مشبکه‌ای روی مرز مستطیل) و I (تعداد نقطه‌های مشبکه‌ای درون مستطیل) را حساب کنید تا قضیهٔ پیک در مورد مستطیل‌ها ثابت شود.

۲. مثلثی با رأس‌های $(۰,۰), (a,۰), (a,b)$ رسم کنید که در آن a و b اعدادی طبیعی‌اند و نسبت به هم اول‌اند. از قضیهٔ پیک استفاده کنید و ثابت کنید تعداد نقطه‌های مشبکه‌ای درون این مثلث برابر است با $I = \frac{۱}{۲}(a-۱)(b-۱)$.

۳. چندضلعی‌ای مانند $P_۱P_۲P_۳P_۴$ رسم کنید که در آن $P_۱ = (۰,۰)$، $P_۳ = (۳,۰)$، $P_۲ = (۶,۳)$ و $P_۴ = (۱,۲)$. ثابت کنید که قضیهٔ پیک در مورد این چندضلعی برقرار نیست. آیا این چندضلعی ساده است؟

۴. چندضلعی $\mathcal{P} : (۰,۰), (۶,۰), (۶,۲), (۴,۵), (۱,۳)$ را رسم کنید. چندضلعی درونی $\mathcal{P}_۱ : (۲,۱), (۴,۲), (۴,۳), (۲,۲)$ را حذف کنید. آیا قضیهٔ پیک در مورد چندضلعی دو همبند $\mathcal{P} - \mathcal{P}_۱$ برقرار است؟

۵. چندضلعی‌ای مانند $\mathcal{P}$ و چندضلعی‌ای دیگر مانند $\mathcal{P}'$ در نظر بگیرید که مرزش کاملاً درون $\mathcal{P}$ قرار می‌گیرد. فرض کنید همهٔ رأس‌های $\mathcal{P}$ و $\mathcal{P}'$ نقطه‌های مشبکه‌ای باشند. ناحیه‌ای را که با مرزهای $\mathcal{P}$ و $\mathcal{P}'$ محدود شده است، $\mathcal{P} - \mathcal{P}'$ بنامید. ثابت کنید که قضیهٔ پیک در مورد چندضلعی دو همبند $\mathcal{P} - \mathcal{P}'$ برقرار نیست و مساحتی که با دستور قضیهٔ پیک به‌دست می‌آید، یک واحد کمتر از مساحت واقعی است.

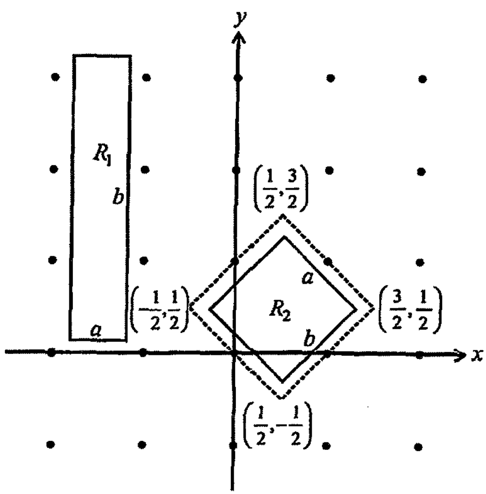
۶. لوزی‌ای را که با معادلهٔ $a|x| + b|y| = ab$ تعریف می‌شود در نظر بگیرید، که در آن a و b اعدادی طبیعی‌اند و بزرگ‌ترین مقسوم‌علیه مشترکشان برابر است با d. دستوری برای یافتن تعداد نقطه‌های مشبکه‌ای درون این لوزی بیابید.

۳.۳ قضیهٔ پوشش نقطه‌های مشبکه‌ای در مورد مستطیل

به یاد بیاورید که Λ مشبکهٔ اصلی نقاط صحیح در صفحهٔ xy است. می‌گوییم مستطیلی دارای ویژگی پوشش نقطه‌های مشبکه‌ای است اگر همیشه، دست‌کم یک نقطهٔ مشبکه‌ای درونش یا روی مرزش باشد، مستقل از اینکه مستطیل کجای صفحه قرار گرفته است؛ ممکن است حدس بزنید اندازهٔ مستطیل مشخص می‌کند که این ویژگی را داشته باشد، و در حقیقت در قضیهٔ بعد، ملاک اندازه به صراحت بیان می‌شود.

قضیهٔ ۲.۳ هر مستطیل با ضلع‌های a و b (که مثلاً $a \leq b$) دارای ویژگی پوشش نقطه‌های مشبکه‌ای است اگر و فقط اگر $a \geq ۱$ و $b \geq \sqrt{۲}$.

اثبات. شرط‌هایی که در قضیه آمده، لازم‌اند. مثلاً فرض کنید $a < ۱$ و b دلخواه باشد. در این‌صورت می‌توانیم مستطیل با ضلع b را موازی محور yها قرار دهیم طوری که هیچ نقطهٔ مشبکه‌ای درون یا روی مرزش نباشد. مستطیل $R_۱$ را در شکل ۳.۳ ببینید. چنین مستطیلی آشکارا ویژگی پوشش نقطه‌های مشبکه‌ای را ندارد. مشابهاً نمی‌توانیم فرض کنیم $b < ۱$ و a دلخواه باشد.



شکل ۳.۳ مستطیل $R_۱$ با $a < ۱$ و مستطیل $R_۲$ با $۱ \leq a \leq b < \sqrt{۲}$.

از طرف دیگر، اگر $۱ \leq a$ اما $b < \sqrt{۲}$ (یعنی اگر $۱ \leq a \leq b < \sqrt{۲}$) آنگاه می‌توانیم مستطیل را با زاویه‌ای ۴۵ درجه نسبت به محور xها دوران دهیم، طوری که کاملاً درون مربع با رأس‌های

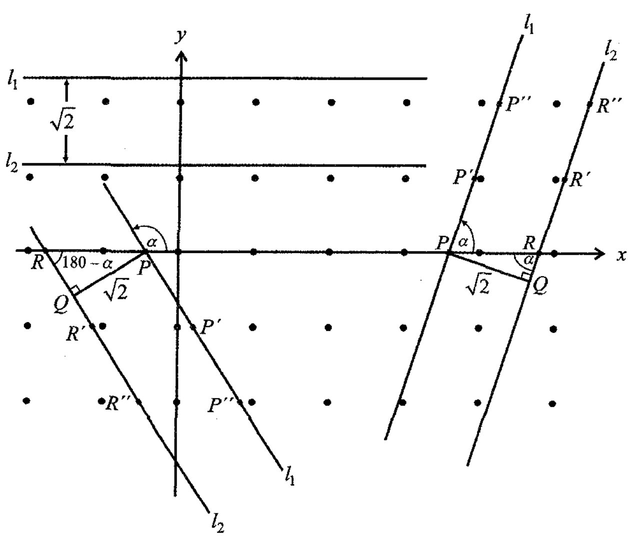
$$\left(\frac{۱}{۲}, -\frac{۱}{۲}\right), \left(\frac{۳}{۲}, \frac{۱}{۲}\right), \left(\frac{۱}{۲}, \frac{۳}{۲}\right), \left(-\frac{۱}{۲}, \frac{۱}{۲}\right)$$

و طول ضلع $\sqrt{۲}$ قرار بگیرد. در شکل ۳.۳، به $R_۲$ توجه کنید. باز هم، مستطیل طوری قرار گرفته است که ویژگی پوشش را ندارد. بنابراین، اگر مستطیلی ویژگی پوشش نقطه‌های مشبکه‌ای را داشته باشد، حتماً $a \geq ۱$ و $b \geq \sqrt{۲}$.

برای اثبات عکس، به این لم نیاز داریم:

لم ۱.۳ فرض کنید $l_۱$ و $l_۲$ دو خط موازی با فاصلهٔ $\sqrt{۲}$ باشند. نواری که از این دو خط و فاصلهٔ بینشان تشکیل می‌شود، در هر جهتی، دارای نامتناهی نقطهٔ مشبکه‌ای است.

اثبات لم ۱.۳. فرض کنید خطوط موازی $l_۱$ و $l_۲$ از هم به فاصلهٔ $\sqrt{۲}$ باشند، و با محور xها یا محور yها موازی باشند؛ شکل ۴.۳، بالا سمت چپ را ببینید. در این‌صورت خطی در مشبکهٔ L یا بین $l_۱$ و $l_۲$ قرار می‌گیرد یا بر یکی از آنها منطبق است، و چنین خطی، نامتناهی نقطهٔ مشبکه‌ای از Λ دارد. بنابراین در این حالات، لم درست است.



شکل ۴.۳ نقطه‌های مشبکه‌ای روی مسیری با عرض $\sqrt{۲}$.

از طرف دیگر، فرض کنید خط‌های $l_۱$ و $l_۲$ محور xها را با زاویهٔ α که $۰ < \alpha < ۹۰^\circ$ یا $۹۰^\circ < \alpha < ۱۸۰^\circ$ قطع کند، همان‌طورکه در شکل‌های پایین و راست در شکل ۴.۳ می‌بینید. پس $۰ < \sin\alpha < ۱$ و از مثلث قائم‌الزاویهٔ PQR می‌بینیم که

$$|\overline{PR}| = \frac{\sqrt{۲}}{\sin\alpha} > \sqrt{۲} > ۱$$

پس با عرض بیشتر از $\sqrt{۲}$، $\overline{PR}$ باید دست‌کم یک نقطهٔ مشبکه‌ای داشته باشد، اما همین حکم در مورد پاره‌خط‌های موازی $\overline{P'R'}$، $\overline{P''R''}$ و ... نیز برقرار است (اینها پاره‌خط‌هایی‌اند که خط‌های موازی $l_۱$ و $l_۲$ از خطوط افقی مشبکهٔ L جدا می‌کنند). پس هر نواری که از $l_۱$ و $l_۲$ تشکیل شود، نامتناهی نقطهٔ مشبکه‌ای دارد. پس لم ۱.۳ ثابت شده است.

اثبات قضیهٔ ۲.۳ (ادامه). کافی است ثابت کنیم که مستطیلی با ضلع‌های ۱ و $\sqrt{۲}$ ویژگی پوشش نقطه‌های مشبکه‌ای را دارد. فرض کنید چنین نباشد. در این صورت می‌توانیم مستطیلی مانند $ABCD$ را روی مشبکهٔ L قرار دهیم، طوری‌که

$$|\overline{AB}| = |\overline{CD}| = \sqrt{۲}$$

و

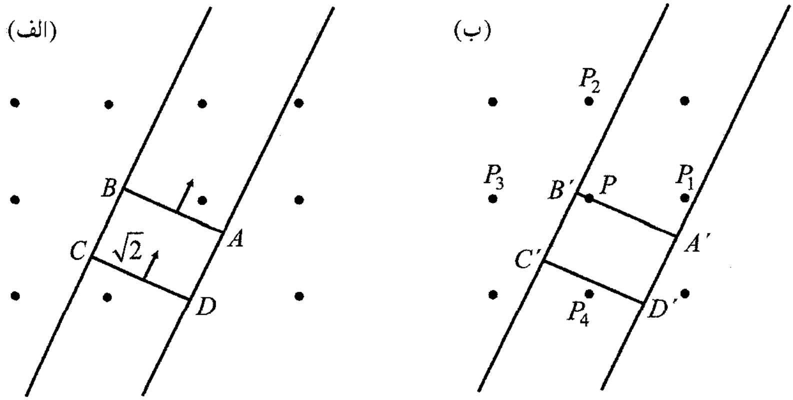
$$|\overline{BC}| = |\overline{AD}| = ۱$$

و طوری که هیچ نقطهٔ مشبکه‌ای Λ را روی مرزش یا درونش نداشته باشد. ضلع‌های این مستطیل آشکار است که نمی‌توانند موازی محور xها یا موازی محور yها باشند، زیرا در غیر این‌صورت دست‌کم یک نقطهٔ مشبکه‌ای درون یا روی $ABCD$ خواهد بود. پس فرض می‌کنیم که ضلع AB موازی هیچ‌یک از محورها نیست. شکل ۵.۳الف را ببینید.

با امتداد AD و BC در دو جهت، می‌توانیم نواری با عرض $\sqrt{۲}$ بسازیم، که بنابر لم ۱.۳، نامتناهی نقطهٔ مشبکه‌ای دارد. اکنون اگر ضلع $ABCD$ را به بالا یا پایین این نوار حرکت دهیم، ضلع AB (یا CD) باید به یکی از این نقطه‌ها برخورد کند یا از نامتناهی نقطهٔ مشبکه‌ای بگذرد.

جای مستطیل را وقتی که به اولین نقطهٔ مشبکه‌ای مانند P روی ضلع AB (یا Q روی CD) می‌رسد در نظر بگیرید. جایی را که مستطیل به آن رسیده است $A'B'C'D'$ بنامید و فرض کنید P روی AB نقطهٔ موردنظر است. به شکل ۵.۳ب نگاه کنید. P را در کجا خواهیم یافت؟ تا جایی که می‌دانیم، می‌تواند A'، B' یا جایی روی پاره‌خط واصلشان باشد.

چون P اولین نقطهٔ مشبکه‌ای است که مستطیل جابه‌جا شده به آن برخورد کرده است، باید تنها نقطهٔ مشبکه‌ای از Λ درون یا روی $A'B'C'D'$ باشد. زیرا فرض کنید نقطهٔ دیگری مانند R



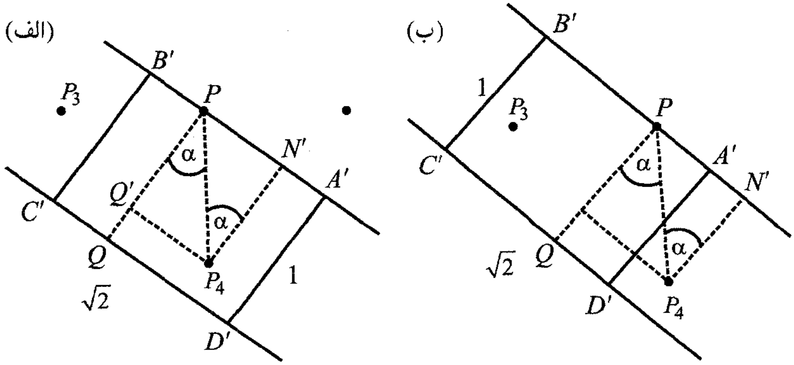
شکل ۵.۳ (الف) مستطیلی روی نواری با عرض $\sqrt{۲}$. (ب) حرکت مستطیل به اولین نقطهٔ مشبکه‌ای (P).

روی‌مرز یا درون مستطیل جابه‌جا شده باشد، همان‌طور که در شکل ۵.۳ب نشان داده شده است. پس یا ضلع AB در حرکت به جای جدید $A'B'C'D'$ قبل از P به R رسیده است (که با فرضمان دربارهٔ P در تناقض است) یا $ABCD$ در جای ابتدایی آن هم شامل R بوده است (که با فرضمان که $ABCD$ هیچ نقطهٔ مشبکه‌ای از Λ نداشته است در تناقض است). بنابراین وضعیت شکل ۵.۳ب، اگر $ABCD$ ویژگی پوشش نقطه‌ها را نداشته باشد، و P با روش ما مشخص شده باشد، رخ نخواهد داد.

اما حالا می‌توانیم ثابت کنیم که اگر همان‌طور که فرض کردیم، ضلع‌های $ABCD$ به طول ۱ و $\sqrt{۲}$ باشند، آنگاه باید موقعیت شکل ۵.۳ب رخ دهد. به بیان دیگر، دست‌کم یکی از نقطه‌های مشبکه‌ای که به P از همه نزدیک‌ترند، در مستطیل جابه‌جا شدهٔ $A'B'C'D'$ قرار می‌گیرد. در شکل ۳-۵الف این نزدیک‌ترین نقطه‌های مشبکه‌ای با $P_۱$، $P_۲$، $P_۳$ و $P_۴$ مشخص شده‌اند.

برای اثبات، دایرهٔ Γ به شعاع ۱ و مرکز P مانند شکل ۶.۳ رسم کنید. قطر گذرا از A' تا B'، قطر گذرا از $P_۱$ و $P_۳$ را قطع می‌کند، چون $A'B'$ افقی نیست. پس دو تا از همسایه‌های مشبکه‌ای P (مثلاً $P_۳$ و $P_۴$) زیر خط گذرا از A' و B' قرار می‌گیرد. این دو نقطهٔ مشبکه‌ای همچنین بالای خط گذرا از C' و D' قرار می‌گیرند، چون $C'D'$ در Q به Γ مماس است. پس وقتی $C'D'$ را از Q نگاه کنیم، زیر هر نقطه‌ای روی محیط قرار می‌گیرد. بنابراین می‌توانیم اثبات کنیم که $P_۳$ و $P_۴$ در بین نواری که با $A'B'$ و $C'D'$ مشخص شده است، قرار می‌گیرد.

حالا می‌خواهیم ثابت کنیم که $P_۳$ یا $P_۴$ باید زیر ضلع‌های $B'C'$ و $A'D'$ یا یکی از آنها قرار بگیرد. برای این کار، زاویهٔ $QPP_۴$ را با α نشان می‌دهیم و از آن برای بررسی $P_۴$ استفاده می‌کنیم، که در ترسیم ما، سمت راست خط گذرا از B' و C' قرار می‌گیرد. فرض کنید یکی از خط‌های عمود



شکل ۶.۳ دایرهٔ Γ با مرکز P.

گذرا از $P_۴$ خط گذرا از $A'B'$ را در نقطهٔ N' قطع کند، و دیگری $\overline{PQ}$ را در Q' قطع کند. اگر $|PA'| \geq \sin\alpha$، آنگاه می‌فهمیم که

$$|\overline{PA'}| \geq \frac{|\overline{PN'}|}{|\overline{PP_۴}|} = |PN'| = \sin\alpha$$

پس

$$|\overline{PA'}| \geq |\overline{Q'P_۴}|$$

و در این حالت، $P_۴$ باید سمت چپ ضلع $A'D'$ یا روی آن باشد.

به بیان دیگر، فرض کنید

$$|\overline{PA'}| < \sin\alpha = |\overline{PN'}|$$

در این حالت، $P_۴$ بیرون $A'B'C'D'$ قرار می‌گیرد، اما در این‌صورت، فاصلهٔ $P_۴$ تا $B'C'$ باید بیش از $\sqrt{۲} = |\overline{A'B'}|$ باشد، در نتیجه، دایره‌ای با مرکز در $P_۴$ و با شعاع $\sqrt{۲}$، $B'C'$ را قطع نمی‌کند، اما از $P_۳$ می‌گذرد. پس اگر $P_۴$ بیرون مستطیل قرار بگیرد، آنگاه $P_۳$ درونش قرار می‌گیرد.

پس این فرض که $ABCD$ می‌تواند روی مشبکهٔ L قرار بگیرد طوری که هیچ نقطهٔ مشبکه‌ای نداشته باشد به تناقضی منجر شد، و قضیهٔ ۲.۳ ثابت شده است.

اثبات قضیهٔ ۲.۳، کار نیون و زوکرمن [۲] است، که علاوه‌بر این، قضیه‌های جالب دیگری هم دربارهٔ پوشش دارند.

مجموعهٔ مسائل قسمت ۳.۳

۱. با آزمایش (مانند ترسیم دقیق) نشان دهید که عدد $\sqrt{۲}$ در لم ۱.۳ را می‌توان با عددی کوچک‌تر عوض کرد. چقدر کوچک‌تر؟ آیا با این عدد کوچک‌تر، قضیهٔ پوششی به‌دست می‌آید؟

۲. به دقت نوار سمت راستی در شکل ۴.۳ را دوباره بسازید و روی پلاستیک شفاف مستطیل دقیقی با اضلاع ۱ و $\sqrt{۲}$ ببرید. خودتان را قانع کنید که اگر نقطهٔ مشبکه‌ای مثل P روی $A'B'$ و نقطهٔ مشبکه‌ای مثل $P_۴$ درون $A'B'C'D'$ باشد، آنگاه نقطهٔ مشبکه‌ای نیز درون $ABCD$ قرار دارد.

۳. نقطه‌ای را که قطرهای مستطیل شفاف مسئلهٔ ۲ به هم می‌رسند، علامت بزنید. آن را روی نقطهٔ مشبکه‌ای قرار دهید.

الف) آیا این مستطیل همیشه نقطهٔ مشبکه‌ای دیگری هم رویش یا درونش دارد؟

ب) چگونه می‌توانید اضلاع را تغییر دهید طوری که این اتفاق رخ دهد؟

ج) این اضلاع چقدر بزرگ‌تر می‌توانند باشند؟

۴. مربع شفاف ۲ × ۲ای درست کنید و نقطه‌ای را که قطرهایش به هم می‌رسند علامت بزنید و از آن استفاده کنید تا سؤال مسئلهٔ ۳ را پاسخ دهید.

مراجع

1. Ross Honsberger, *Ingenuity in Mathematics,* New Mathematical Library Series, Vol. 23 (New York: Random House, 1970), 27-31.

2. Ivan Niven and Herbert Zuckerman, "The Lattice Point Covering Theorem for Rectangles," *Mathematics Magazine* 42 (1969): 85-86.

۴ نقاط مشبکه‌ای در دایره

۱.۴ چند نقطهٔ مشبکه‌ای در دایره یافت می‌شود؟

یکی از اولین کاوش‌ها در این زمینه، توسط ک. ف. گاوس به انجام رسید. او در ۱۸۳۷ در یکی از آثارش [۳] این سؤال را مطرح کرد که چند نقطهٔ مشبکه‌ای درون یا روی دایره‌ای مشخص وجود دارد؟ این سؤال با نمادگذاری ما به‌صورت زیر قابل طرح است:

> $N(n)$، تعداد نقاط مشبکه‌ای درون یا روی مرز دایرهٔ $C(\sqrt{n})$ که دایره‌ای به شعاع $\sqrt{n}$ و به مرکز مبدأ است، چه‌قدر است؟

گاوس مقادیر عددی $N(n)$ را برای nهای از ۱۰ تا ۳۰۰ محاسبه کرد که در جدول ۱.۴ آورده شده‌اند.

جدول ۱.۴ تعداد نقاط مشبکه‌ای درون یا روی دایره به شعاع r

$r=\sqrt{n}$	$N(n)$	$N(n)/n$	$r=\sqrt{n}$	$N(n)$	$N(n)/n$
۱	۵	۵	۹	۲۵۳	⋮
۲	۱۳	۳٫۲۵	۱۰	۳۱۷	۳٫۱۷
۳	۲۹	۳٫$\overline{۲۲}$	۲۰	۱۲۵۷	۳٫۱۴۲۵
۴	۴۹	۳٫۰۶۲۵	۳۰	۲۸۲۱	۳٫۱۳$\overline{۴}$
۵	۸۱	۳٫۲۴	۱۰۰	۳۱۴۱۷	۳٫۱۴۱۷
۶	۱۱۳	⋮	۲۰۰	۱۲۵۶۲۹	۳٫۱۴۰۷۲۵
۷	۱۴۹	⋮	۳۰۰	۲۸۲۶۹۷	۳٫۱۴۱۰$\overline{۷}$
۸	۱۹۷	⋮			

همان‌طور که در جدول مشاهده می‌شود، هرچه n زیادتر می‌شود، نسبت $N(n)$ به n به عدد π نزدیک‌تر و نزدیک‌تر می‌شود. بنابراین می‌توان حدس زد که

$$\lim_{n\to\infty} \frac{N(n)}{n} = \pi = ۳/۱۴۱۵۹\ldots$$

در ۱۹۶۱ میچل [۶]، $N(n)$ را به‌ازای مقادیری بین $\sqrt{n} = ۱$ تا $\sqrt{n} = ۲۰۰,۰۰۰$ محاسبه کرد. البته از آنجا که کامپیوترهایی که با آنها این محاسبات را انجام می‌داد در مقایسه با کامپیوترهای امروزی خیلی کندتر بودند، او همهٔ مقادیر بعد از $\sqrt{n} = ۱۰۰۰$ را محاسبه نکرد بلکه به‌ازای مقادیری با فواصل زیاد آنها را محاسبه کرد. برخی از محاسبات وی در جدول ۲.۴ آمده است.

جدول ۲.۴ تعداد نقاط مشبکه‌ای درون یا روی دایره برای rهای بزرگ

$r = \sqrt{n}$	$N(n)$	$N(n)/n \approx \pi$
۴۰۰	۵۰۲۶۲۵	۳/۱۴۱۴۱...
۵۰۰	۷۸۵۳۴۹	۳/۱۴۱۳۹...
۱۰۰۰	۳۱۴۱۵۴۹	۳/۱۴۱۵۴۹...
۱۰۰۰۰	۳۱۴۱۵۹۲۲۱	۳/۱۴۱۵۹۲...
۱۰۰۰۰۰	۳۱۴۱۵۹۳۹۲۸۱	۳/۱۴۱۵۹۴...
۲۰۰۰۰۰	۱۲۵۶۶۳۷۵۹۰۷۷	۳/۱۴۱۵۹۴...

جدول ۲.۴ نیز این حدس را تقویت می‌کند که وقتی n به ∞ میل می‌کند، نسبت $N(n)/n$ به π میل می‌کند. یعنی مقدار

$$\left|\frac{N(n)}{n} - \pi\right| \qquad (۱.۴)$$

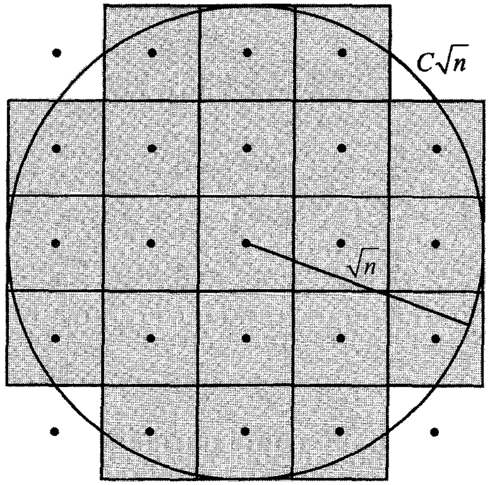
را می‌توان به دلخواه کوچک کرد اگر n به اندازهٔ کافی بزرگ شود.

با دیدگاه هندسی، بهتر می‌توانیم رفتار $N(n)/n$ را درک کنیم. اگر (۱.۴) را در n ضرب کنیم، به کمیت جدید

$$|N(n) - n\pi|,$$

می‌رسیم که از نظر شهودی مفهوم بهتری دارد. $n\pi$ درواقع مساحت دایره به شعاع $r = \sqrt{n}$ است. این سرنخی به دست ما می‌دهد که چگونه با رهیافتی هندسی به سؤال گاوس پاسخ دهیم.

می‌خواهیم $N(n)$، تعداد نقاط مشبکه‌ای درون یا روی دایرهٔ $C(\sqrt{n})$، به شعاع $r = \sqrt{n}$ را برای n دلخواه تقریب بزنیم. ابتدا چنین دایره‌ای را به مرکز $(۰,۰)$، که مبدأ مشبکهٔ نقاط Λ است،



شکل ۱.۴ مربع‌های واحد که مراکزشان درون یا روی $C(\sqrt{n})$ قرار دارد.

رسم می‌کنیم. حال هر نقطهٔ مشبکهٔ Λ را مرکز یک مربع واحد با اضلاع موازی محورهای مختصات فرض می‌کنیم و از میان آنها مربع‌هایی را در نظر می‌گیریم که مرکزشان درون یا روی $C(\sqrt{n})$ است. شکل ۱.۴ را ببینید. مساحت ناحیهٔ سایه خورده، برابر است با $N(n)$.

توجه کنید که بعضی قسمت‌های ناحیهٔ سایه خورده خارج از دیسک $x^۲ + y^۲ \leq n$ قرار دارند و نیز قسمت‌هایی از دیسک سایه نخورده است. بنابراین سعی می‌کنیم $N(n)$ را از بالا و پایین تخمین بزنیم: کوچک‌ترین دیسکی را در نظر می‌گیریم که ناحیهٔ سایه خورده را کاملاً شامل شود و نیز بزرگ‌ترین دیسکی را در نظر می‌گیریم که کاملاً درون ناحیهٔ سایه خورده باشد.

از آنجا که قطر مربع واحد، $\sqrt{۲}$ است، ناحیهٔ سایه خورده، تماماً درون دایرهٔ به شعاع $r = \sqrt{n} + (\sqrt{۲}/۲)$ قرار دارد و مشابهاً دایرهٔ به شعاع $r = \sqrt{n} - (\sqrt{۲}/۲)$، کاملاً درون ناحیهٔ سایه خورده قرار دارد.

نتیجه می‌شود که

$$\pi\left(n - \sqrt{۲n} - \frac{۱}{۲}\right) \leq \pi\left(n - \sqrt{۲n} + \frac{۱}{۲}\right) = \pi\left(\sqrt{n} - \frac{\sqrt{۲}}{۲}\right)^۲$$

$$\leq N(n) \leq \pi\left(\sqrt{n} + \frac{\sqrt{۲}}{۲}\right)^۲ = \pi\left(n + \sqrt{۲n} + \frac{۱}{۲}\right)$$

از این رابطه نتیجه می‌شود

$$\left|\frac{N(n)}{n} - \pi\right| \leq \pi\left(\sqrt{\frac{۲}{n}} + \frac{۱}{۲n}\right) \qquad (۲.۴)$$

وقتی $n \to \infty$، کمیت سمت راست به صفر میل می‌کند. پس ما ثابت کرده‌ایم که $\lim_{n\to\infty} N(n)/n = \pi$، همان‌طور که از جدول‌های ۱.۴ و ۲.۴ به نظر می‌رسید.

جزئیات اثبات فوق، در بخش هشتم مرجع [۵][۱]، به خوبی ارائه شده است.

۲.۴ مجموع دو مربع

گاوس و دیگرانی که کارهای او را دنبال کردند، در جنبه‌های مختلفی از نقاط مشبکه‌ای مربوط به دایره‌ها تحقیق کرده‌اند. همان‌طور که در کتاب *History of the Theory of Numbers* اثر دیکسون [۲] ملاحظه می‌شود، می‌توان شرح مفصل و جذابی دربارهٔ این موضوع نوشت. ولی برای اینکه بحث بیش از حد مفصل نشود، تنها برخی از مسائل کلاسیک نقاط مشبکه‌ای را می‌آوریم و برخی از گزاره‌ها را نیز بدون اثبات ارائه می‌کنیم. بررسی خود را با مطالعهٔ ارتباط بین نقاط مشبکه‌ای و جواب‌های صحیح معادلات و نابرابری‌های مربوط به دایره‌ها و دیسک‌ها ادامه می‌دهیم.

ابتدا تعدادی تعریف ارائه می‌کنیم. فرض کنید ما می‌توانیم عدد صحیح نامنفی n را به‌صورت مجموع مربعات دو عدد صحیح بنویسیم. یعنی فرض کنید که می‌توان n را به‌صورت $n = p^۲ + q^۲$ نوشت که اعداد صحیح p و q می‌توانند مثبت، منفی یا صفر باشند. تعداد نمایش‌های n به‌صورت $p^۲ + q^۲$ را با نمادهای زیر نشان می‌دهیم:

$$R(n) = R(n = p^۲ + q^۲)$$

نمایش‌هایی را که در آنها (p, q) تنها در علامتشان یا ترتیبشان فرق دارند متمایز فرض می‌کنیم و هر کدام را جداگانه به حساب می‌آوریم. اما به‌طور استثناء، $۰^۲ + ۰^۲ = ۰$ را فقط یک‌بار می‌شماریم. در زیر مثال‌هایی از نمایش‌های متمایز و مقادیر $R(n)$ متناظر آنها را آورده‌ایم:

$R(۰) = ۱$، چون $۰^۲ + ۰^۲ = ۰$،

$R(۴) = ۴$، چون $(\pm ۲)^۲ + ۰^۲ = ۰^۲ + (\pm ۲)^۲ = ۴$،

$R(۸) = ۴$، چون $(\pm ۲)^۲ + (\pm ۲)^۲ = ۸$،

$R(۱۰) = ۸$، چون $(\pm ۱)^۲ + (\pm ۳)^۲ = (\pm ۳)^۲ + (\pm ۱)^۲ = ۱۰$.

---

۱. این کتاب با عنوان ابتکارهایی در ریاضیات به فارسی ترجمه شده است با مشخصات زیر:
ابتکارهایی در ریاضیات، راس هانسبرگر، ترجمهٔ سیامک کاظمی، مرکز نشر دانشگاهی، ۱۳۷۱.

دقت کنید که در شمارش تعداد نمایش‌ها، ترتیب و نیز حالت‌های مختلف علامت‌ها را در نظر گرفته‌ایم.

جدول ۳.۴ مقادیر $R(n)$ را به‌ازای $n = ۰$ تا $n = ۲۵$ نشان می‌دهد.

همان‌طور که مشاهده می‌شود، با افزایش n، مقادیر $R(n)$ بسیار نامنظم می‌شوند یعنی هم مقادیر بزرگ را اختیار می‌کند و هم بی‌نهایت بار $R(n) = ۰$ رخ می‌دهد. به عبارت دیگر، خیلی از اعداد، تعداد نمایش‌های زیادی به‌صورت مجموع مربعات دو عدد دارند در حالی که اعداد بی‌شماری

جدول ۳.۴ تعداد نمایش‌های n به‌صورت مجموع دو مربع

n	جواب‌های صحیح $n = p^۲ + q^۲$	$R(n)$	$T(n)$	$T(n)/n$
۰	$(۰,۰)$	۱	۱	
۱	$(۱,۰),(-۱,۰),(۰,۱),(۰,-۱)$	۴	۵	۵٫۰۰
۲	$(۱,۱),(۱,-۱),(-۱,۱),(-۱,-۱)$	۴	۹	۴٫۵۰
$۳ = ۴ \cdot ۰ + ۳$		۰	۹	۳٫۰۰
$۴ = ۲^۲$	$(۲,۰),(-۲,۰),(۰,۲),(۰,-۲)$	۴	۱۳	۳٫۲۵
$۵ = ۴ \cdot ۱ + ۱$	$(۲,۱),(-۲,۱),(۲,-۱),(-۲,-۱)$			
	$(۱,۲),(-۱,۲),(۱,-۲),(-۱,-۲)$	۸	۲۱	۴٫۲۰
$۶ = ۲ \cdot (۴ \cdot ۰ + ۳)$		۰	۲۱	۳٫۵۰
$۷ = ۴ \cdot ۱ + ۳$		۰	۲۱	۳٫۰۰
$۸ = ۲^۳$	$(۲,۲),(-۲,۲),(۲,-۲),(-۲,-۲)$	۴	۲۵	۳٫۱۳
$۹ = ۳^۲ = (۴ \cdot ۰ + ۳)^۲$	$(۳,۰),(-۳,۰),(۰,۳),(۰,-۳)$	۴	۲۹	۳٫۲۲
$۱۰ = ۲ \cdot (۴ \cdot ۱ + ۱)$	$(\pm ۳,\pm ۱),(\pm ۱,\pm ۳)$	۸	۳۷	۳٫۷۰
$۱۱ = ۴ \cdot ۲ + ۳$		۰	۳۷	۳٫۳۶
$۱۲ = ۲^۲ \cdot (۴ \cdot ۰ + ۳)$		۰	۳۷	۳٫۰۸
$۱۳ = ۴ \cdot ۳ + ۱$	$(\pm ۲,\pm ۳),(\pm ۳,\pm ۲)$	۸	۴۵	۳٫۴۶
$۱۴ = ۲ \cdot (۴ \cdot ۱ + ۳)$		۰	۴۵	۳٫۲۱
$۱۵ = ۵ \cdot (۴ \cdot ۰ + ۳)$		۰	۴۵	۳٫۰۰
$۱۶ = ۲^۴$	$(\pm ۴,۰),(۰,\pm ۴)$	۴	۴۹	۳٫۰۶
$۱۷ = ۴ \cdot ۴ + ۱$	$(\pm ۴,\pm ۱),(\pm ۱,\pm ۴)$	۸	۵۷	۳٫۳۵
$۱۸ = ۲ \cdot (۴ \cdot ۰ + ۳)^۲$	$(\pm ۳,\pm ۳)$	۴	۶۱	۳٫۳۹
$۱۹ = ۴ \cdot ۴ + ۳$		۰	۶۱	۳٫۲۱
$۲۰ = ۲^۲ \cdot (۴ \cdot ۱ + ۱)$	$(\pm ۴,\pm ۲),(\pm ۲,\pm ۴)$	۸	۶۹	۳٫۴۵
$۲۱ = (۴ \cdot ۰ + ۳) \cdot (۴ \cdot ۱ + ۳)$		۰	۶۹	۳٫۲۰
$۲۲ = ۲ \cdot (۲ \cdot ۴ + ۳)$		۰	۶۹	۳٫۱۳
$۲۳ = ۴ \cdot ۵ + ۳$		۰	۶۹	۳٫۰۰
$۲۴ = ۲^۳ \cdot (۴ \cdot ۰ + ۳)$		۰	۶۹	۲٫۸۸
$۲۵ = (۴ \cdot ۱ + ۱)^۲$	$(\pm ۵,۰),(۰,\pm ۵),(\pm ۳,\pm ۴),(\pm ۴,\pm ۳)$	۱۲	۸۱	۳٫۲۴

هم هستند که هیچ چنین نمایشی ندارند. گزارهٔ اخیر را در بخش بعد اثبات خواهیم کرد. وقتی یک دنبالهٔ عددی چنین رفتار نامنظمی به‌ازای $n \to \infty$ دارد، نظریه اعداددان‌ها معمولاً به بررسی مقادیر میانگین چنین دنباله‌ای می‌پردازند.

ساده‌ترین مقدار میانگینی که می‌توان در نظر گرفت، میانگین عادی است. یعنی جمع n عدد اول دنباله تقسیم بر n. درواقع، قرار می‌دهیم

$$T(n) = R(۰) + R(۱) + R(۲) + \cdots + R(n)$$

و میانگین زیر را در نظر می‌گیریم:

$$\frac{T(n)}{n} = \frac{R(۰) + R(۱) + R(۲) + \cdots + R(n)}{n}$$

پیش از آنکه این میانگین را بررسی کنیم، به دیدگاه هندسی باز می‌گردیم.

دقت کنید که دایرهٔ $C(\sqrt{n})$، مرز دیسک $D(\sqrt{n})$ است که به‌صورت زیر تعریف می‌شود:

$$D(\sqrt{n}) : p^۲ + q^۲ \leq n$$

هر نقطهٔ مشبکه‌ای (p,q) در $D(\sqrt{n})$، یک جواب صحیح (یعنی جوابی که p و q اعداد صحیح باشند) از نابرابری بالا است. بنابراین تعداد جواب‌های صحیح این نابرابری، دقیقاً همان $N(n)$ است.

چگونه تعداد جواب‌های صحیح این نابرابری را بشماریم؟ ایدهٔ اصلی این است که می‌توانیم تعداد جواب‌های صحیح هر یک از معادلات زیر را بشماریم و بعد آنها را جمع بزنیم:

$$p^۲ + q^۲ = ۰ \quad و \quad p^۲ + q^۲ = ۱ \quad و \quad p^۲ + q^۲ = ۲ \quad و \quad \ldots \quad و \quad p^۲ + q^۲ = n$$

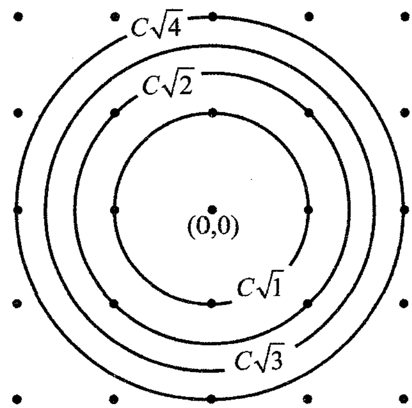
که به ترتیب عبارتند از:

$$R(۰) = ۱ \quad و \quad R(۱) = ۴ \quad و \quad R(۲) = ۴ \quad و \quad \ldots \quad و \quad R(n)$$

بنابراین مجموع $T(n) = R(۰) + R(۱) + \cdots + R(n)$ دقیقاً برابر است با $N(n)$، یعنی تعداد نقاط مشبکه‌ای (p,q) درون یا روی دایرهٔ $C(\sqrt{n})$. به‌عنوان مثال، جدول ۳.۴ نشان می‌دهد که

$$T(۴) = R(۰) + R(۱) + \cdots + R(۴) = ۱ + ۴ + ۴ + ۰ + ۴ = ۱۳$$

همان‌طورکه شکل ۲.۴ نشان می‌دهد، این تعداد دقیقاً برابر است با تعداد نقاط مشبکه‌ای روی دایره‌های $C(۰)$، $C(\sqrt{۱})$، $C(\sqrt{۲})$، $C(\sqrt{۳})$ و $C(\sqrt{۴})$.



شکل ۲.۴ نقاط مشبکه‌ای روی دایره‌های به شعاع $\sqrt{n}$ به‌ازای $n = ۱, ۲, ۳, ۴$.

همچنین می‌توان در جدول‌های ۳.۴ و ۱.۴ مشاهده کرد که مقدار

$$T(n) = R(\circ) + R(۱) + \cdots + R(n)$$

به‌ازای $n = ۱, ۴, ۹, ۱۶, ۲۵$ دقیقاً برابر با مقدار $N(n)$ برای شعاع‌های $\sqrt{n} = ۱, ۲, ۳, ۴, ۵$ است.

نهایتاً چون $R(n) = N(n)$، از آنچه در بخش قبل گفته شد، نتیجه می‌شود وقتی $n \to \infty$،

$$\frac{R(n)}{n} = \frac{N(n)}{n} \to \pi$$

البته در جدول ۳.۴، این رفتار حدی به روشنی قابل مشاهده نیست چون مقدار n به اندازهٔ کافی بزرگ نیست.

۳.۴ چه اعدادی را می‌توان به‌صورت جمع دو مربع نمایش داد؟

همان‌طور که از جدول ۳.۴ مشاهده می‌شود، همهٔ اعداد صحیح نامنفی n را نمی‌توان به شکل $n = p^۲ + q^۲$ نمایش داد: مثلاً $R(۳) = \circ$، دقت کنید همان‌طور که در شکل ۲.۴ می‌توان دید، دایرهٔ $C(\sqrt{۳})$ از هیچ نقطهٔ مشبکه‌ای نمی‌گذرد، در اینجا دو سؤال مطرح می‌شود:

۱. آیا راهی برای تشخیص اینکه چه اعداد صحیح نامنفی را می‌توان به‌صورت مجموع مربع دو عدد صحیح نمایش داد وجود دارد؟

۲. اگر n به‌صورت جمع دو مربع قابل نمایش باشد، آیا فرمولی برای تعداد چنین نمایش‌هایی وجود دارد؟

هر دوی این سؤال‌ها بسیار قدیمی هستند. در کتاب $Arithmetic$ اثر دیوفانتوس، که در حدود سال ۲۵۰ بعد از میلاد، نوشته شده است، این دو مسئله مطرح شده‌اند، اگرچه معنای گزاره‌ها در آنجا تا حدودی مبهم است. جواب سؤال (۱)، اولین بار در سال ۱۶۲۵ میلادی توسط ریاضی‌دان هلندی، آلبرت گیرارد (۱۶۳۲-۱۵۹۵) بیان شد. اندکی بعد پیر دو فرما (۱۶۶۵-۱۶۰۱) نیز پاسخی بدون اثبات ارائه کرد. اولین اثبات‌های شناخته شده توسط لئونارد اویلر (۱۷۸۳-۱۷۰۷) در سال ۱۷۴۹ ارائه شد.

نشان دادن اینکه اعدادی به فرم‌های خاص قابل نمایش به‌صورت مجموع دو مربع نیستند دشوار نیست. بجز مثال $R(۳) = ۰$ که قبلاً گفته شد، جدول ۳.۴ نشان می‌دهد که برای $n = ۷, ۱۱, ۱۵, ۱۹, ۲۳$ نیز $R(n) = ۰$. ویژگی مشترک این اعداد این است که همگی قابل نمایش به‌صورت $۴k + ۳$ هستند. این ویژگی همان‌طور که قضیهٔ زیر نشان می‌دهد واقعاً مهم است.

قضیهٔ ۱.۴ هیچ عدد صحیح به فرم $۴k + ۳$، که $k = ۰, ۱, ۲, \ldots$، را نمی‌توان به‌صورت $p^۲ + q^۲$ به‌ازای p و q صحیح نمایش داد.

اثبات. اگر p زوج باشد، (یعنی $p = ۲h$)، آنگاه $p^۲ = ۴h^۲$ بر ۴ بخش‌پذیر است. اما اگر p فرد باشد، (مثلاً $p = ۲h + ۱$)، آنگاه باقیماندهٔ $p^۲$ در تقسیم بر ۴ برابر ۱ است، چون

$$p^۲ = (۲h + ۱)^۲ = ۴h^۲ + ۴h + ۱ = ۴(h^۲ + h) + ۱$$

بنابراین در تقسیم $p^۲ + q^۲$ بر ۴، سه حالت پیش می‌آید:

۱. اگر p و q هر دو زوج باشند، باقیمانده صفر می‌شود.

۲. اگر یکی از آنها زوج و دیگری فرد باشد، باقیمانده ۱ می‌شود.

۳. اگر هر دو فرد باشند، باقیمانده ۲ می‌شود.

پس در هیچ حالتی باقیماندهٔ $p^۲ + q^۲$ بر ۴ برابر ۳ نیست، بنابراین اعداد صحیح به شکل $۴k + ۳$ را نمی‌توان به‌صورت جمع دو مربع نوشت.

قضیهٔ ۱.۴ نشان می‌دهد که چرا $R(n)$ به‌ازای $n = ۳, ۷, ۱۱, ۱۵, \ldots$، صفر می‌شود. اما چرا در جدول ۳.۴، صفرهای دیگر بسیاری هم هست؟ جواب این سؤال را با بررسی دقیق‌تر قضایایی دربارهٔ اینکه چه اعدادی به‌صورت جمع دو مربع قابل نمایش‌اند می‌یابیم.

از قضیهٔ یکتایی تجزیه آغاز می‌کنیم؛ برای اثباتی از این قضیه، به مرجع [۷][۱] اثر نیون مراجعه کنید. این قضیه بیان می‌دارد که هر عدد صحیح مثبت $n > ۱$ را می‌توان به یک و فقط یک طریق به شکل حاصل‌ضرب زیر نوشت:

$$n = ۲^{\beta} p_۱^{\alpha_۱} p_۲^{\alpha_۲} \dots p_s^{\alpha_s}$$

که $p_۱$، $p_۲$، ...، p_s اعداد اول فرد متمایزی هستند که توان‌های آنها، $\alpha_۱$، $\alpha_۲$، ...، α_s، صفر نیستند. اگر n فرد باشد، $\beta = ۰$؛ در غیر این صورت β بزرگ‌ترین توان ۲ است که n را می‌شمارد. با در نظر گرفتن چنین تجزیه‌ای برای n، می‌توانیم قضیهٔ مهم زیر را بیان کنیم.

قضیهٔ ۲.۴ عدد صحیح مثبت n، مجموع دو مربع کامل است اگر و تنها اگر در تجزیهٔ n، عوامل اولی که به شکل $۴k + ۳$ هستند، توانشان زوج باشد.

مثلاً، اعداد صحیح مثبت ۳، ۶، ۷، ۱۱، ۱۲، ۱۴، ۱۵، ۱۹، ۲۱، ۲۲، ۲۳ و ۲۴ را نمی‌توان به‌صورت مجموع دو مربع نمایش داد ولی ۹ و ۱۸ را می‌توان.

ما قضیهٔ ۲.۴ را در اینجا ثابت نمی‌کنیم چراکه اثبات آن ساده نیست؛ خوانندهٔ علاقه‌مند می‌تواند به مرجع [۴] مراجعه کند. با این حال، یکی از گام‌های مهم اثبات قضیهٔ ۲.۴ را در ادامه توضیح می‌دهیم: این گام مهم، اتحاد

$$(a^۲ + b^۲)(c^۲ + d^۲) = (ac + bd)^۲ + (ad - bc)^۲ \qquad (۳.۴)$$

است که منتسب به لئوناردو فیبوناچی (حدود ۱۲۵۰-۱۱۷۰) است و وی آن را در کتاب *Liber Abaci* در سال ۱۲۰۲ آورده است. این اتحاد نشان می‌دهد که دو عدد که هرکدام به‌صورت مجموع دو مربع قابل نمایش باشند، حاصل‌ضربشان نیز مجموع دو مربع است.

مثال زیر نشان می‌دهد که این قضیه چگونه در اثبات قضیهٔ ۲.۴ به کار می‌رود. با توجه به جدول ۳.۴، می‌بینیم که

$$۴ = ۲^۲ = (\pm ۲)^۲ + ۰^۲ = ۰^۲ + (\pm ۲)^۲$$

و

$$۹ = ۳^۲ = (\pm ۳)^۲ + ۰^۲ = ۰^۲ + (\pm ۳)^۲$$

۱. این کتاب با عنوان اعداد: گویا و گنگ به فارسی ترجمه شده است با مشخصات زیر:
اعداد: گویا و گنگ، ایوان نیون، ترجمهٔ غلامحسین اخلاقی‌نیا، مرکز نشر دانشگاهی، ۱۳۶۷.

با قرار دادن $a = ۲$، $b = ۰$، $c = ۳$ و $d = ۰$ در اتحاد فوق، نتیجه می‌شود

$$۴ \cdot ۹ = ۳۶ = (۲ \cdot ۳ + ۰ \cdot ۰)^۲ + (۲ \cdot ۰ - ۰ \cdot ۳)^۲ = ۶^۲ + ۰^۲$$

بنابراین، نمایشی از ۳۶ به‌صورت مجموع دو مربع ساخته‌ایم. همهٔ نمایش‌های دیگر ۳۶ نیز از همین راه به‌دست می‌آیند، تنها کافی است ترتیب‌ها و علامت‌های دیگری در نمایش‌های ۴ و ۹ به کار ببریم.
مشابهاً

$$۱۸ = ۲ \cdot ۳^۲ = (۱^۲ + ۱^۲)(۳^۲ + ۰^۲) = ۳^۱ + ۳^۲$$

یک نمایش از ۱۸ به‌صورت مجموع دو مربع می‌دهد.

درواقع، اگر بتوانیم نشان دهیم که هر عدد اول به شکل $۴k + ۱$ را می‌توان به‌صورت مجموع دو مربع نمایش داد، آنگاه (۳.۴) نتیجه می‌دهد که حاصل‌ضربی از چنین اعدادی نیز مجموع دو مربع است. از طرفی مجموع دو مربع اگر در یک مربع کامل ضرب شود، باز هم مجموع دو مربع است، و از آنجا که حاصل‌ضرب عوامل اول با توان زوج، یک مربع کامل است، این نشان می‌دهد که شرایط موجود در قضیهٔ ۲.۴ کافی است.

مجموعهٔ مسائل قسمت ۳.۴

۱. نشان دهید قضیهٔ ۲.۴، قضیهٔ ۱.۴ را نتیجه می‌دهد.

۲. قدرمطلق حاصل‌ضرب دو عدد مختلط، برابر است با حاصل‌ضرب قدرمطلقشان. با استفاده از این حقیقت، اتحاد (۳.۴) را نتیجه بگیرید.

۴.۴ نمایش اعداد اول به‌صورت مجموع دو مربع

همچنان‌که در قضیهٔ ۲.۴ دیدیم بعضی از اعداد اول را می‌توان به شکل مجموع دو مربع نوشت. قضیهٔ ژرف و معروفی برای تعداد راه‌های چنین نمایشی وجود دارد.

قضیهٔ ۳.۴ هر عدد اول به فرم $l = ۴k + ۱$ را می‌توان به‌صورت $l = p^۲ + q^۲$ نوشت و تنها یک زوج از اعداد صحیح p و q (که $۰ < p < q$) با این خاصیت وجود دارد.

شرط $۰ < p < q$ برای این است که حالت‌هایی را که از جابه‌جا کردن p و q یا منفی کردن آنها به‌دست می‌آید کنار بگذاریم. بنابراین با احتساب آنها، ۸ حالت به‌دست می‌آید که عبارتند از

$$(p, q)(-p, q)(p, -q)(-p, -q)(q, p)(-q, p)(q, -p)(-q, -p)$$

بنابراین وقتی $۱ + ۴k$ عددی اول باشد، $R(۴k + ۱) = ۸$، که این را در جدول ۳.۴ نیز می‌توان مشاهده کرد.

قضیهٔ ۳.۴ تاریخچهٔ طولانی‌ای دارد [۱، ۲، ۸]. فرما آن را در حاشیهٔ نسخه‌ای که از کتاب دیوفانتوس داشت نوشت، و همچنین آن را در نامه‌ای به تاریخ ۲۵ دسامبر ۱۶۴۰، به مناسبت تبریک کریسمس به ف. م. مرسن (۱۶۴۸-۱۵۸۸)، پژوهشگر بزرگی در زمینهٔ اعداد اول، مطرح کرد.

همان‌طور که قبلاً گفته شد، اولین اثبات منتشر شده، متعلق به اویلر است. آلکس تو (۱۹۲۲-۱۸۶۳)، که نتایج مهمی در نظریهٔ جدید معادلات دیوفانتی از آن وی است، اثبات دیگری با استفاده از قضایای سادهٔ همنهشتی ارائه کرده است.

قضیهٔ ۳.۴ ادعا می‌کند که عدد مورد نظر را تنها به یک صورت می‌توان به شکل مجموع دو مربع نوشت. چگونه می‌توان این یکتایی را ثابت کرد؟ اویلر مشاهده کرد که اگر یک عدد صحیح فرد را بتوان به دو صورت مختلف به شکل مجموع دو مربع نوشت، آنگاه می‌توان آن را تجزیه کرد، و بنابراین نمی‌تواند عددی اول باشد. اکنون اثبات اویلر را می‌آوریم.

اثبات اویلر. فرض کنید عدد اول $l = ۴k + ۱$ را به دو صورت مختلف نمایش داده‌ایم: به شکل $l = a^۲ + b^۲$ و نیز به شکل $l = c^۲ + d^۲$، که a و c فرد و b و d زوج هستند و $a, b, c, d > ۰$. اکنون نشان می‌دهیم که در این صورت l تجزیه می‌شود و این با اول بودن l در تناقض است.

از آنجا که $l = a^۲ + b^۲ = c^۲ + d^۲$، داریم

$$(a - c)(a + c) = (d + b)(d - b) \qquad (۴.۴)$$

چون $a \neq c$ و $b \neq d$، هیچ کدام از عوامل فرمول (۴.۴) صفر نیست. با قرار دادن $k = \gcd(a - c, b - d)$، می‌نویسیم

$$b - d = kt \quad \text{و} \quad a - c = ks$$

که در آن $\gcd(s, t) = ۱$. چون هر دوی $a - c$ و $b - d$ زوج هستند، ۲ هر دو را می‌شمارد. بنابراین ۲ باید k را نیز بشمارد؛ پس k زوج است.

با جایگذاری در (۴.۴)، به‌دست می‌آوریم $ks(a + c) = kt(b + d)$، معادلاً

$$s(a + c) = t(b + d) \qquad (۵.۴)$$

از آنجاکه $\gcd(s, t) = ۱$، باید داشته باشیم $t \mid (a+c)$ و $s \mid (b+d)$. آنگاه از (۵.۴)، نتیجه می‌شود

$$\frac{a + c}{t} = \frac{b + d}{s} = n$$

بنابراین

$$\begin{aligned} a+c &= nt \\ b+d &= ns \end{aligned} \tag{۶.۴}$$

بنابراین، n یک مقسوم‌علیه مشترک $(a+c)$ و $(b+d)$ است. پس $n \mid (a+c, b+d)$.

ادعا می‌کنیم $n=(a+c,b+d)$. زیرا فرض کنید

$$nr = (a+c, b+d)$$

آنگاه اعداد صحیح $j_۱$ و $j_۲$ وجود دارند که

$$nrj_۲ = b+d \quad \text{و} \quad nrj_۱ = a+c$$

با جایگذاری این روابط در (۶.۴)، به‌دست می‌آوریم

$$nrj_۲ = ns \quad \text{و} \quad nrj_۱ = nt$$

و در نتیجه

$$rj_۲ = s \quad \text{و} \quad rj_۱ = t$$

اما این نتیجه می‌دهد که $r \mid \gcd(s,t) = ۱$، و در نتیجه $r = ۱$. بنابراین $n = \gcd(a+c, b+d)$؛ و چون $a+c$ و $b+d$ هر دو زوج هستند، n نیز زوج است.

اکنون با توجه به اینکه k و n زوج هستند، می‌توانیم l را به حاصل‌ضرب دو عدد صحیح تجزیه کنیم:

$$l = \left[\left(\frac{k}{۲}\right)^۲ + \left(\frac{n}{۲}\right)^۲\right](s^۲ + t^۲)$$

که هیچ کدام از عوامل، ۱ نیست، چون k, n, s, t همگی ناصفراند.

درستی تجزیهٔ فوق را با محاسبهٔ حاصل‌ضرب سمت راست می‌توان دید:

$$\begin{aligned} \frac{۱}{۴}[(kt)^۲ + (ks)^۲ + (tn)^۲ + (ts)^۲] \\ &= \frac{۱}{۴}[(d-b)^۲ + (a-c)^۲ + (a+c)^۲ + (d+b)^۲] \\ &= \frac{۱}{۴}[۲(a^۲+b^۲) + ۲(c^۲+d^۲)] = \frac{۱}{۴}(۲l + ۲l) \\ &= l \end{aligned}$$

این با فرض اول بودن l در تناقض است، بنابراین قضیهٔ ۳.۴ اثبات شد.

۵.۴ فرمولی برای $R(n)$

در آغاز بخش ۳.۴ سؤال زیر را مطرح کردیم:

اگرعدد n به‌صورت مجموع دو مربع قابل نمایش باشد، تعداد کل چنین نمایش‌هایی چه‌قدر است؟

به عبارت دیگر، آیا فرمولی برای $R(n) = R(n = p^۲ + q^۲)$ وجود دارد؟

این سؤال توسط آ. م. لژاندر (۱۷۵۲-۱۸۳۳) در قضیهٔ زیر جواب داده شده است. در بیان صورت قضیه از نماد همنهشتی استفاده کرده‌ایم: منظور از $u \equiv v \pmod{m}$ این است که $u - v$ بر m بخش‌پذیر است.

قضیهٔ ۴.۴ فرض کنید $n \geq ۱$ دارای A مقسوم‌علیه $\alpha_۱, \ldots, \alpha_A$ باشد که $\alpha_i \equiv ۱ \pmod{۴}$ و دارای B مقسوم‌علیه $\beta_۱, \ldots, \beta_B$ باشد که $\beta_j \equiv -۱ \pmod{۴}$. آنگاه $R(n) = ۴(A - B)$.

دقت کنید که در این قضیه، همه‌ی مقسوم‌علیه‌ها مورد نظر است نه فقط مقسوم‌علیه‌های اول. به عنوان مثال، جدول ۴.۴ را ببینید.

جدول ۴.۴ مثال‌هایی از قضیهٔ ۴.۴

n	$R(n)$	مقسوم‌علیه‌های n	A^a	B^b	$۴(A-B)$
۲	۴	۱, ۲	۱	۰	$۴(۱) = ۴$
۵	۸	۱, ۵	۲	۰	$۴(۲) = ۸$
۷	۰	۱, ۷	۱	۱	$۴(۰) = ۰$
۶۵	۱۶	۱, ۵, ۱۳, ۶۵	۴	۰	$۴(۴) = ۱۶$
۲۰۰	۱۲	۱, ۲, ۴, ۵, ۸, ۱۰, ۲۰, ۲۵, ۴۰, ۵۰, ۱۰۰, ۲۰۰	۳	۰	$۴(۳) = ۱۲$

a تعداد مقسوم‌علیه‌هایی که $\equiv ۱ \pmod{۴}$

b تعداد مقسوم‌علیه‌هایی که $\equiv -۱ \pmod{۴}$

برای دیدن کلیتی از اثبات قضیهٔ ۴.۴، خواننده می‌تواند به تمرین‌های پایان همین بخش مراجعه کند که در آنها اثباتی که ژاکوبی در سال ۱۸۳۴ برای این قضیه ارائه کرده، آورده شده است.

اکنون سؤال دیگری مطرح می‌کنیم:

آیا فرمولی برای محاسبه مجموع $T(n) = R(۰) + R(۱) + \cdots + R(n)$ وجود دارد؟

جواب این سؤال در یکی از دست‌نوشته‌های گاوس [۳] که پس از مرگش منتشر شد، آمده است. او ثابت کرد که مقدار دقیق این مجموع با فرمول زیر داده می‌شود:

$$T(n) = ۱ + ۴\left\{\left[\frac{n}{۱}\right] - \left[\frac{n}{۳}\right] + \left[\frac{n}{۵}\right] - \left[\frac{n}{۷}\right] + \cdots\right\} \qquad (۷.۴)$$

که $[t]$، مانند فصل ۲، نشان دهندهٔ بزرگ‌ترین عدد صحیح کوچک‌تر یا مساوی t است. به‌طور خاص، دقت کنید که اگر $۲k + ۱ > n$ آنگاه $[n/(۲k+۱)] = ۰$.

البته برای مقادیر بزرگ n، فرمول (۷.۴) خیلی کارآمد نیست. فرمول کارآمدتری به‌صورت زیر وجود دارد:

$$T(n) = ۱ + ۴\sum_{k=۰}^{[\sqrt{n}]}\left[\sqrt{n-k^۲}\right] \qquad (۸.۴)$$

به‌عنوان مثال، با استفاده از فرمول (۸.۴)، به‌دست می‌آید:

$$\begin{aligned} T(۱۰۰) &= ۱ + ۴\{\left[\sqrt{۱۰۰}\right] + \left[\sqrt{۹۹}\right] + \left[\sqrt{۹۶}\right] + \left[\sqrt{۹۱}\right] + \left[\sqrt{۸۴}\right] \\ &+ \left[\sqrt{۷۵}\right] + \left[\sqrt{۶۴}\right] + \left[\sqrt{۵۱}\right] + \left[\sqrt{۳۶}\right] + \left[\sqrt{۱۹}\right]\} \\ &= ۱ + ۴(۱۰ + ۹ + ۹ + ۹ + ۹ + ۸ + ۸ + ۷ + ۶ + ۴) = ۳۱۷ \end{aligned}$$

سرپینسکی در مرجع [۴] اثباتی از فرمول (۸.۴) ارائه می‌دهد و ارتباط آن را با فرمول گاوس (۷.۴)، نشان می‌دهد. هم‌ارز بودن این دو فرمول، به افتخار جوزف لیوویل (۱۸۸۲-۱۸۰۹)، به اتحاد لیوویل معروف است.

مجموعهٔ مسائل قسمت ۵.۴

۱. آیا درست است که اگر $n = ۴k + ۶$، آنگاه $R(n) = ۰$؟ اگر خیر، یک مثال نقض ارائه کنید.

۲. ثابت کنید اگر $n = ۱۲k + ۹$، و k بر ۳ بخش‌پذیر نباشد، آنگاه $R(n) = ۰$.

۳. $R(۱۲۲۵) = R(۵^۲ \cdot ۷^۲)$ را محاسبه کنید.

۴. $T(۱۲۲۵)$ را محاسبه کنید.

۵. برای به‌دست آوردن p و qای که $n = p^۲ + q^۲$ (یا معادلاً $n - p^۲ = q^۲$)، کافی است مقادیر $p = ۰, ۱, ۲, ۳, \ldots$ را که قدرمطلق آنها کوچک‌تر یا مساوی $\sqrt{n}$ است در $n - p^۲$ قرار دهیم

و ببینیم که آیا مربع کامل هست یا نه. نشان دهید برای n ثابت، تفاضل جملات متوالی دنبالهٔ $n - ۰^۲$، $n - ۱^۲$، $n - ۲^۲$، ...، همان دنبالهٔ اعداد فرد ۱، ۳، ۵، ... است.

۶. با استفاده از ایدهٔ سؤال ۵، مقادیر $R(۵)$، $R(۱۰)$ و $R(۲۵)$ را محاسبه کنید.

۷. (اختیاری) در ۱۸۳۴، گ. ژ. ژاکوبی (۱۸۵۱-۱۸۰۴) فرمول $R(n) = ۴(A - B)$ در قضیهٔ ۴.۴ را ثابت کرد. اثبات وی مقدماتی نبود و در آن از اتحادی استفاده می‌کرد که خود در مطالعات عمیقش در توابع بیضوی آن را به‌دست آورده بود. اثبات را مختصراً در زیر می‌آوریم.

اثبات ژاکوبی. ژاکوبی اتحاد زیر را اثبات کرد:

$$(۱ + ۲x + ۲x^۴ + ۲x^۹ + ۲x^{۱۶} + \cdots)^۲ = ۱ + ۴\left(\frac{x}{۱ - x} - \frac{x^۳}{۱ - x^۳} + \frac{x^۵}{۱ - x^۵} - \cdots\right)$$

اگر عبارت سمت چپ را بسط دهیم و جملات حاصل را برحسب توان‌های x مرتب کنیم،

$$۱ + a_۱x + a_۲x^۲ + a_۳x^۳ + \cdots + a_nx^n + \cdots ;$$

در این صورت $a_n = R(n)$. مشابهاً، اگر عبارت سمت راست را بسط دهیم و به شکل

$$۱ + b_۱x + b_۲x^۲ + b_۳x^۳ + \cdots$$

بنویسیم، آنگاه $b_n = ۴(A - B)$. نهایتاً، با برابر قرار دادن ضرایب توان‌های یکسان در دو طرف، به‌دست می‌آید $R(n) = ۴(A - B)$.

سعی کنید اثبات ژاکوبی از $R(n) = ۴(A - B)$ را برای $a_۱$، $a_۲$، ...، $a_۵$ و $b_۱$، $b_۲$، ...، $b_۵$ انجام دهید. توجه کنید که

$$\frac{x}{۱ - x} = x + x^۲ + x^۳ + \cdots$$

$$\frac{x^۲}{۱ - x^۲} = x^۲ + x^۴ + x^۶ + \cdots$$

مراجع

1. L. E. Dickson, "Methods of Factoring," Chapter 14 in *History of the Theory of Numbers*, Vol. 1: Divisibility and Primality (Washington, D. C.: Carnegie Institute, 1919), 360.

2. ________, "Sum of Two Squares" Chapter 6 in *History of the Theory of Numbers, Vol. II: Diophantine Analysis* (Washington, D. C.: Carnegie Institute, 1920), 225.

3. C. F. Gauss, *Werke* (Göttingen: Gesellschaft der Wissenschaften, 1863-1933).

4. G. H. Hardy and E. M. Wright, Chapter 10. Theorem 366, in *An Introduction to the Theory of Numbers,* 5th ed. (Oxford: Oxford University Press, 1983).

5. Ross Honsberger, "Writing a Number as a Sum of Two Squares," Essay 8 in *Ingenuity in Mathematics,* New Mathematical Library Series, Vol. 23 (New York: Random House, 1970), 61-66.

6. H. L. Mitchell III, *Numerical Experiments on the Number of Lattice Points in the Circle* (Stanford, CA: Stanford University, Applied Mathematics and Statistics Labs, 1961).

7. Ivan Niven, Appendix B in *Numbers: Rational and Irrational,* New Mathematical Library Series, Vol 1 (New York and Toronto: Random House, 1961).

8. Oystein Ore, *Number Theory and Its History* (New York: McGraw-Hill, 1948: reprinted with supplement, New York: Dover, 1988).

9. W. Sierpinski, *Elementary Theory of Numbers*, 2nd ed., Andrzej Schinzel, ed., North-Holland Mathematical Library, Vol. 31 (Amsterdam and New York: North-Holland: Warsaw: Polish Scientific Publishers, 1988).

۵ قضیهٔ بنیادی مینکوفسکی

۱.۵ روش هندسی مینکوفسکی

همچنان که در بخش ۱.۱ به آن اشاره شد، هندسهٔ اعداد با کارهای هرمان مینکوفسکی شروع شد و هم‌اکنون یکی از شاخه‌های مهم از نظریهٔ اعداد است. پیوست ج، شما را با زندگی این ریاضیدان بزرگ آشنا می‌کند.

هندسهٔ اعداد با مسئلهٔ حل‌پذیری نامعادله‌ها در اعداد صحیح در ارتباط است. چنین نامعادله‌هایی را که ما در جستجوی جواب‌های صحیح آنها هستیم، نامعادله‌های دیوفانتی می‌نامند. سال‌ها قبل از مینکوفسکی، چارلز ارمیت (۱۹۰۱-۱۸۲۲)، با استفاده از روش‌های جبری، چندین قضیه کلی را در مورد جواب‌های این نامعادله‌ها اثبات کرد. مهم‌ترین قضیه به‌جا مانده از او را می‌توان در نامه‌ای یافت که او در حدود سال ۱۸۴۵ به کارل ژاکوبی نوشت. همچون ارمیت، مینکوفسکی به این مسایل علاقه‌مند بود، اما روش او با همهٔ پیشینیان متفاوت بود.

روش مینکوفسکی از یک دیدگاه هندسی نشأت می‌گرفت. او شرط‌های ساده‌ای را یافت که تحت آنها نواحی صفحه شامل نقاط مشبکه هستند. او همچنین نتایج خود را به فضای nـبعدی تعمیم داد و توانست به این وسیله اثبات‌های جدید و ساده‌تری برای نتایج جبری ارمیت ارائه کند. وقتی در حدود سال ۱۸۹۰، مینکوفسکی، ارمیت را از دست‌آوردهای خود مطلع کرد، ارمیت با شوق و هیجان علاقه‌مندی خود را به کشف‌های او ابراز داشت.

این خود مینکوفسکی بود که این حوزهٔ مطالعه را هندسهٔ اعداد نامگذاری کرد. نتیجهٔ بررسی‌های او در این موضوع در دو کتاب به زبان آلمانی، Geometrie der Zahlen (۱۸۹۶) [۶] و Diophantische Approximationen (۱۹۰۷) [۷] منتشر شد؛ کتاب دوم کمی ساده‌تر است. برای دیدن یک توضیح مدرن، عمیق و با قدرت به کَسِلز [۱] نگاه کنید.

مثال صفحهٔ بعد یک نمونه از مسائل مورد توجه این ریاضیدان بزرگ است:

آیا برای هر عدد حقیقی α، اعداد صحیح m و n، $m \neq ۰$، چنان وجود دارند که $\left|\alpha - \left(\frac{n}{m}\right)\right| \leq \frac{۱}{۲m}$؟

یک راه پاسخگویی به این سؤال این است که عدد صحیح دلخواه $m > ۱$ را در نظر بگیریم، و سپس عدد صحیح n را چنان بیابیم که فاصلهٔ آن از αm کمترین مقدار ممکن باشد. می‌دانیم که

$$|\alpha m - n| \leq \frac{۱}{۲}$$

بنابراین

$$\left|\alpha - \frac{n}{m}\right| \leq \frac{۱}{۲m}$$

این نشان می‌دهد که در واقع بینهایت زوج از اعداد صحیح m و n می‌توانند جواب این نامعادله باشند. هر چه m را بزرگ‌تر در نظر بگیریم، تقریب ما بهتر خواهد بود. علاوه‌براین، اگر α عدد گنگ باشد، نامساوی اکید خواهند بود، چرا؟ چون در این‌صورت، αm نیز گنگ است و بنابراین نمی‌تواند دقیقاً در فاصلهٔ یک‌دوم واحد از یک عدد صحیح قرار بگیرد.

با دیدگاه مینکوفسکی می‌توان این واقعیت را به‌طور هندسی بیان کرد:

نوار محدود به خطوط مستقیم $\alpha x - y = \frac{۱}{۲}$ و $ax - y = -\frac{۱}{۲}$ شامل بینهایت نقطهٔ مشبکه است.

این نوار می‌تواند بسیار باریک باشد، ولی به هر حال، این نتیجه همچنان برقرار است. این نتیجه نباید ما را متعجب کند چرا که همچنان که در بخش ۶.۱ یاد گرفتیم هر مستطیلی که نسبت به مبدأ متقارن باشد، علاوه‌بر نقطهٔ $(۰, ۰)$ شامل نقاط مشبکهٔ دیگری نیز خواهد بود به شرطی که مساحت آن از ۴ بیشتر باشد.

فرض کنید که ما به دنبال تقریب گویای بهتری برای یک عدد حقیقی داده شده هستیم. به‌ازای کدام (در صورت وجود) مقادیر صحیح m، αm به‌طور خوبی به عدد صحیح n نزدیک است؟ ما در فصل ۶ نشان خواهیم داد که در واقع برای تعداد نامتناهی از اعداد صحیح m و n، $m \neq ۰$، تفاضل $\alpha - \left(\frac{n}{m}\right)$ در نامساوی زیر صدق می‌کند:

$$\left|\alpha - \frac{n}{m}\right| < \frac{۱}{۲m^۲} \tag{۱.۵}$$

برای دیدن یک تعبیر هندسی به مسئلهٔ ۲ نگاه کنید.

مجموعهٔ مسائل قسمت ۱.۵

۱. نوار محدود به خطوط $y - \alpha x = \frac{۱}{۲}$ و $y - \alpha x = -\frac{۱}{۲}$ را در نظر بگیرید:

الف) نشان دهید که این نوار نسبت به مبدأ متقارن است.

ب) عرض نوار را برحسب α بیان کنید.

ج) عدد ثابت k را برحسب α چنان بیابید که مستطیلی که با استفاده از خطوط $x+\alpha y = k$ و $x + \alpha y = -k$ از نوار جدا می‌شود، کوچک‌ترین مستطیلی باشد که در درون یا روی مرز آن نقطه‌ای مشبکه علاوه‌بر $(۰,۰)$ وجود دارد.

د) به قسمت‌های (ب) و (ج) برای حالتی که $\alpha = \sqrt{۳}$ است پاسخ دهید.

۲. با ضرب کردن نامعادلهٔ (۱.۵) در $۲m^۲$، نامعادلهٔ هم‌ارز زیر به‌دست می‌آید.

$$-۱ \le ۲\alpha m^۲ - ۲mn \le ۱. \qquad (۱'.۵)$$

برای یک α داده شده، تعدادی نامتناهی از اعداد صحیح m و n در نامساوی (۱.۵) صدق می‌کنند. این ادعا معادل این است که ناحیه S، مشخص شده با شرط $(۱'.۵)$ شامل تعدادی نامتناهی از نقاط مشبکه است.

الف) نشان دهید که S نسبت به مبدأ متقارن است.

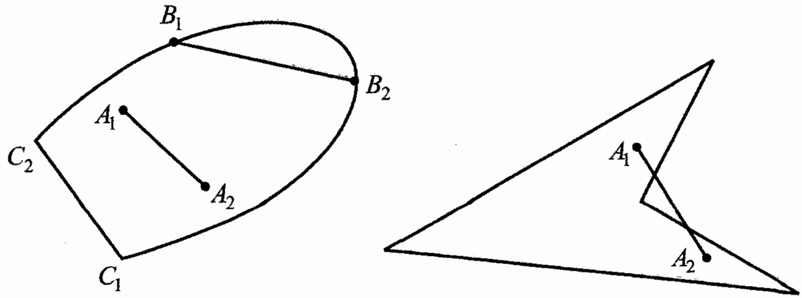
ب) ثابت کنید که S ناحیه‌ای است که بین دو هذلولی مزدوج با مجانب‌های $x = ۰$ و $y - \alpha x = ۰$ قرار دارد.

۲.۵ Mـ مجموعه‌های مینکوفسکی

مینکوفسکی شکلی کلیدی را در صفحه معرفی کرد که ما آن را Mـ مجموعه می‌نامیم. شکل دقیق یک Mـ مجموعه از مسئله‌ای به مسئلهٔ دیگر فرق می‌کند، اما هر Mـ مجموعه‌ای باید از هر دو خاصیت زیر برخوردار باشد.

خاصیت ۱. یک Mـ مجموعه محدب است.

یک مجموعه از نقاط را محدب می‌نامیم درصورتی که شامل همهٔ نقاط روی هر پاره‌خطی باشد که دو نقطه دلخواه از مجموعه را به هم وصل می‌کند؛ به شکل ۱.۵ نگاه کنید.



شکل ۱.۵ چپ: مجموعهٔ محدب. راست: مجموعهٔ غیرمحدب.

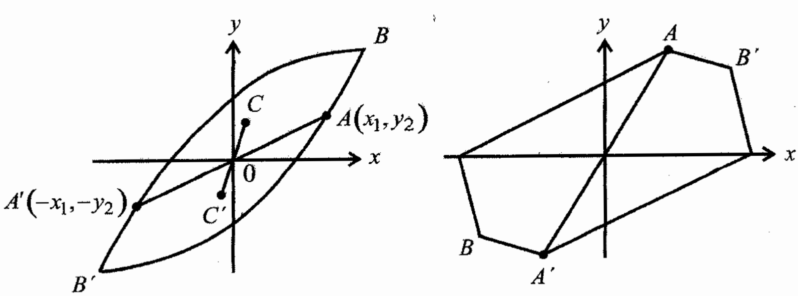
گاهی مینکوفسکی از تعریف دیگری برای تحدب استفاده می‌کرد. بنابر تعریف او، یک Mـ مجموعه محدب است درصورتی که بتوان از هر نقطهٔ P روی مرز M خط l را چنان رسم کرد که همهٔ شکل M در یک طرف l قرار گیرد.

خاصیت ۲. یک Mـ مجموعه نسبت به نقطه‌ای مانند O متقارن است.

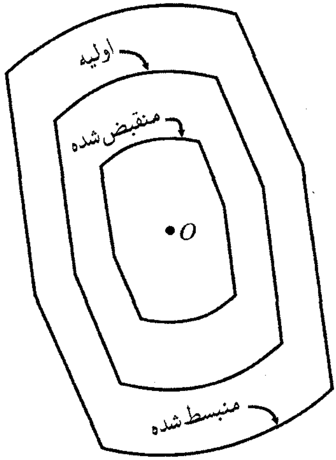
این یعنی، برای هر نقطهٔ P از مجموعهٔ M، نقطهٔ P' نیز که روی خط گذرنده از P و O چنان قرار دارد که $|\overline{P'O}| = |\overline{OP}|$، در مجموعه است.

نقطهٔ O مرکز تقارن مجموعه نامیده می‌شود. برای راحتی، ما معمولاً Mـ مجموعه‌ها را، به گونه‌ای قرار می‌دهیم که مبدأ مختصات، یعنی نقطهٔ $(\circ, \circ)$، مرکز آنها باشد؛ به شکل ۲.۵ نگاه کنید.

از خاصیت (۲) نتیجه می‌شود که در صورتی‌که چنان مجموعه‌ای شامل نقطه‌ای به مختصات (a, b) باشد، همچنین شامل نقطه‌ای به مختصات $(-a, -b)$ است. واضح است که مبدأ مختصات پاره‌خطی را که بین یک نقطه و تصویر متقارن آن قرار دارد نصف می‌کند؛ برای مثال، به پاره‌خط $\overline{AA'}$ در شکل ۲.۵ نگاه کنید.



شکل ۲.۵ دو Mـ مجموعه با مرکز $(\circ, \circ)$.



شکل ۳.۵ تغییر سایز، تقارن را حفظ می‌کند.

به راحتی می‌توان یک Mـ مجموعهٔ به مرکز $(\circ, \circ)$ را منبسط یا منقبض کرد. برای این کار کافی است که نقطهٔ (x, y) از مجموعه را به نقطهٔ (tx, ty) بنگاریم؛ در اینجا، t عددی حقیقی است. این تغییر سایز، Mـ مجموعهٔ مشابهی را به‌وجود می‌آورد که همچون Mـ مجموعهٔ اولیه نسبت به مبدأ متقارن است؛ به شکل ۳.۵ نگاه کنید.

اگرچه ما تاکنون مدل‌هایی را در نظر گرفته‌ایم که در صفحه قرار دارند، بدیهی است که تعریف ما از Mـ مجموعه‌ها به راحتی قابل تعمیم به مجموعه‌هایی با ابعاد بالاتر است. برای مثال، در فضای ۳ بعدی، مکعب‌ها، کره‌ها، و بیضی‌وارهای متقارن نسبت به مبدأ، Mـ مجموعه هستند. ما فقط بر مفاهیم مینکوفسکی در صفحه تمرکز خواهیم کرد و از بررسی ابعاد بالاتر و مشکل‌تر پرهیز خواهیم کرد. لیوسترنیک [۵]، منبعی عالی برای شکل‌های محدب و چندوجهی‌ها است.

مجموعهٔ مسائل قسمت ۲.۵

۱. مجموعهٔ محدب Q شامل سه نقطهٔ غیرهمخط A، B و C است. ثابت کنید که Q شامل همهٔ مثلث ABC است.

۲. مینکوفسکی ثابت کرد که اگر بتوان چندضلعی محدب Q را به تعدادی متناهی چندضلعی با تقارن مرکزی تجزیه کرد، آنگاه Q نیز دارای تقارن مرکزی است.

الف) با کشیدن چند شکل درستی این قضیه را بررسی کنید.

ب) درصورتی که کلمهٔ «محدب» را از صورت قضیه حذف کنیم چه اتفاقی خواهد افتاد؟ توضیح دهید. کشیدن شکل فراموش نشود!

۳. ثابت کنید که اشتراک دو مجموعهٔ در صفحه محدب است.

۳.۵ قضیهٔ بنیادی مینکوفسکی

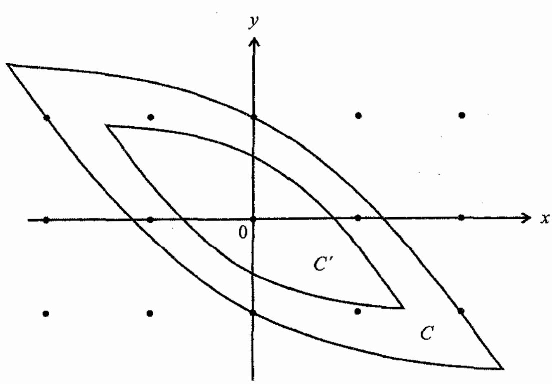
ما هم‌اکنون قضیهٔ بنیادی هندسهٔ اعداد را بیان و اثبات خواهیم کرد.

قضیهٔ ۱.۵ (قضیهٔ بنیادی مینکوفسکی) فرض کنید که مرکز Mـ مجموعهٔ دوبعدی C در مبدأ قرار دارد و مساحت C بزرگ‌تر یا مساوی ۴ است. در این‌صورت، C علاوه‌بر O شامل نقاط مشبکهٔ Λ است؛ Λ می‌تواند روی مرز یا درون C باشد.

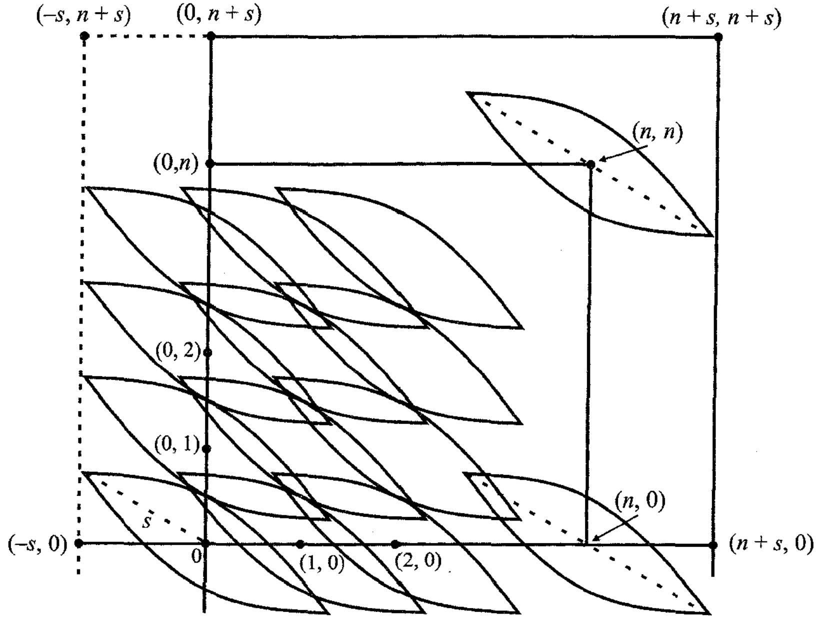
اثبات. Mـ مجموعهٔ C با مرکز $(\circ,\circ)$ و مساحت $A > ۴$ را در نظر بگیرید. با نگاشتن هر نقطهٔ (x,y) از C به نقطهٔ $(\frac{x}{۲},\frac{y}{۲})$، C را منقبض می‌کنیم؛ به شکل ۴.۵ نگاه کنید. این انقباض، منجر به Mـ مجموعهٔ C' خواهد شد که متشابه Mـ مجموعهٔ C است و طول هر پاره‌خط در آن درست نصف طول پاره‌خط متناظر در مجموعهٔ C است. با این حساب، در مورد مساحت C'، که آن را با A' نمایش می‌دهیم، داریم:

$$A' = \left(\frac{۱}{۲}\right)^۲ A = \frac{۱}{۴}A$$

چون $A > ۴$، پس $A' > ۱$.



شکل ۴.۵ Mـ مجموعهٔ C به C' انقباض یافته است.



شکل ۵.۵ انتقال‌های C' همپوشی دارند.

اکنون یک نسخه از C' را روی هر یک از نقاط مشبکه قرار می‌دهیم. به بیان دیگر، Mـ مجموعهٔ C' را از مبدأ به نقطهٔ (p, q) با مختصات صحیح انتقال می‌دهیم. بنابراین، اگر نقطهٔ (x', y') نقطه‌ای از C' باشد، نقطهٔ $(x' + p, y' + q)$ متناظر با آن و در انتقال یافتهٔ C' به مرکز (p, q) است.

نگاهی به این انتقال‌ها در شکل ۵.۵ بیاندازید.

آیا آنها همپوشی دارند؟ آیا نقطه‌ای در صفحه هست که به بیشتر از یک انتقال تعلق داشته باشد؟

ما نشان خواهیم داد که این انتقال‌ها واقعاً همپوشی دارند، و در نتیجه، Mـ مجموعهٔ اولیه، مجموعهٔ C، باید علاوه‌بر مبدأ شامل نقطهٔ مشبکه دیگری نیز باشد.

در ابتدا به مربعی توجه می‌کنیم که رئوس آن در نقاط $(۰, ۰)$، $(n, ۰)$، (n, n) و $(۰, n)$ قرار دارد؛ در اینجا، n عددی صحیح است. به شکل ۵.۵ نگاه کنید. روی مرز و درون این مربع، $(n + ۱)^۲$ نقطهٔ مشبکه قرار دارد. هر یک از این $(n + ۱)^۲$ نقطهٔ مشبکه مرکز یکی از انتقال‌های C' است. مجموع مساحت‌های این $(n + ۱)^۲$ انتقال برابر است با $(n + ۱)^۲ A'$.

فرض کنید بیشترین فاصلهٔ نقاط C' از مبدأ s است. در این‌صورت، همهٔ این $(n + ۱)^۲$ تا Mـ مجموعه در مربعی به ضلع $n + ۲s$ و مساحت $(n + ۲s)^۲$ قرار دارند. دوباره به شکل ۵.۵ نگاه کنید. نشان خواهیم داد که مجموع مساحت‌های $(n + ۱)^۲$ انتقالِ C' بیشتر از مساحت مربعی

است که شامل آنها است؛ یعنی، نشان خواهیم داد که

$$(n+۱)^۲A' > (n+۲s)^۲ \tag{۲.۵}$$

از اینجا نتیجه خواهیم گرفت که انتقال‌ها باید همپوشی داشته باشند.

برای اثبات نامساوی (۲.۵)، $(n+۲s)^۲$ را از دو طرف کم می‌کنیم و سپس نامساوی هم‌ارزی را که به‌دست می‌آید اثبات می‌کنیم.

$$(n+۱)^۲A' - (n+۲s)^۲ = (A'-۱)n^۲ + ۲n(A'-۲s) + A' - ۴s^۲ > ۰ \tag{۳.۵}$$

چون $A' > ۱$، ضریب $n^۲$ در عبارت درجهٔ دوم (۳.۵) مثبت است و در نتیجه عبارت مذکور برای مقادیر به اندازهٔ کافی بزرگ از n مثبت است. ما n را به‌قدری بزرگ انتخاب می‌کنیم که عبارت (۳.۵) مثبت باشد. در این‌صورت، $(n+۱)^۲A' > (n+۲s)^۲$ و انتقال‌های C' در مربع مربوط همپوشی خواهند داشت.

اکنون می‌توان دید که هر انتقالِ C' با انتقال دیگری همپوشی دارد. دو مجموعهٔ متداخل به مرکز $(p_۱, q_۱)$ و $(p_۲, q_۲)$ را در نظر بگیرید؛ به شکل ۶.۵ نگاه کنید. در این‌صورت، هر انتقال سومی به مرکز نقطهٔ مشبکه دلخواه $(p_۰, q_۰)$ باید دارای نقاط مشترکی با انتقال چهارمی به مرکز نقطهٔ مشبکه $(p_۰ + p_۲ - p_۱, q_۰ + q_۲ - q_۱)$ باشد. به‌ویژه، مجموعه C'، به مرکز $(۰, ۰)$، دارای نقاط مشترکی با انتقالِ C'' به مرکز (p, q) است که در آن $p = p_۲ - p_۱$ و $q = q_۲ - q_۱$؛ به شکل ۷.۵ نگاه کنید. بنابراین، هر نقطهٔ (x'', y'') از C'' را می‌توان به صورت

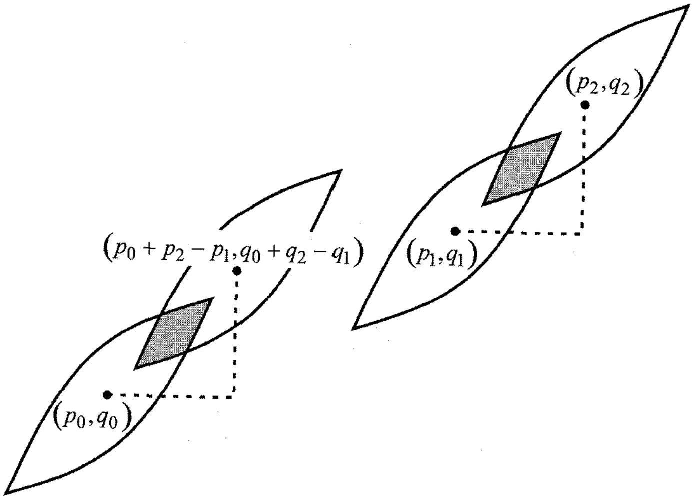
$$x'' = x' + p, \qquad y'' = y' + q$$

نوشت که در آن (x', y') نقطهٔ متناظر در C' است. بنابراین، اگر دو انتقال همپوشی داشته باشند، هر انتقال دیگری هم حداقل با یک انتقال همپوشی دارد.

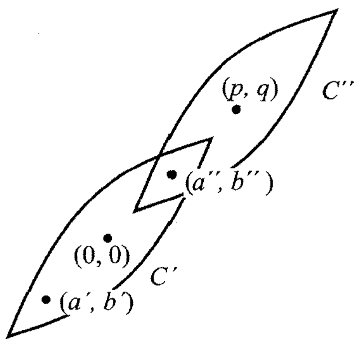
اکنون فرض کنید که نقطهٔ (a'', b'') در C' و همچنین در C'' است. باید نقطه‌ای مانند (a', b') در C' چنان وجود داشته باشد که

$$a'' = a' + p, \qquad b'' = b' + q \tag{۴.۵}$$

چون C' متقارن است، شامل نقطهٔ $(-a', -b')$ نیز هست. چون C' محدب است، شامل نقطهٔ میانی هر پاره‌خطی است که دو نقطهٔ دلخواه از آن را به‌هم وصل می‌کند. مختصات نقطه‌ای که در وسط



شکل ۶.۵ انتقالِ مجموعه‌های متداخل.



شکل ۷.۵ نقاط مشترک بین C' و انتقالش C''.

نقاط (a'', b'') و $(-a', b')$ قرار دارد

$$\left(\frac{a''-a'}{۲}, \frac{b''-b'}{۲}\right)$$

است که بنابر (۴.۵)، همان $\left(\frac{p}{۲}, \frac{q}{۲}\right)$ است. بنابراین C' شامل نقطهٔ $\left(\frac{p}{۲}, \frac{q}{۲}\right)$ است، و این در حالی است که نقطهٔ (p, q) نقطه‌ای با مختصات صحیح و مرکز C'' است. از اینجا نتیجه می‌شود که Mـ مجموعهٔ اولیهٔ ما، یعنی C، شامل نقطهٔ مشبکهٔ (p, q) است.

آیا اثبات ما کامل است؟ نه کاملاً، چون ما فرض کردیم که مساحت C بزرگ‌تر از ۴ است درحالی که قضیه ۱.۵ ادعا می‌کندکه حتی در حالت $A = ۴$، C شامل یک نقطهٔ مشبکه روی مرزیا در درون آن است.

اکنون، فرض کنید $A = ۴$، همچنین فرض کنید که C بجز $(۰,۰)$ شامل هیچ نقطهٔ مشبکهٔ دیگری در دورن و یا روی مرز آن نیست. بنابراین فاصلهٔ نقاط مشبکه و نقاط C از مقدار مثبتی مانند δ بزرگ‌تر است. اکنون C را به آرامی منبسط می‌کنیم تا جایی که فاصلهٔ همهٔ نقاط Mـ مجموعهٔ حاصل، C^*، از نزدیک‌ترینِ نقطهٔ مشبکه کمتر از $\frac{\delta}{۲}$ نباشد. اکنون، مساحت C^* بزرگ‌تر از ۴ است ولی هنوز بجز $(۰,۰)$ شامل هیچ نقطهٔ مشبکهٔ دیگری نیست. ولی این با نتیجهٔ قبلی ما در تناقض است. بنابراین، C باید علاوه‌بر مبدأ شامل نقطهٔ مشبکهٔ دیگری نیز، در درون یا روی مرز باشد. این اثبات قضیهٔ بنیادی مینکوفسکی را کامل می‌کند.

اثباتی که ما ارائه کردیم اساساً همان اثباتی است که خود مینکوفسکی ارائه کرده است. برای دیدن اثبات‌های دیگر این قضیه به فهرست تهیه شده توسط کاکسما [۴] نگاه کنید. برای دیدن اثبات هاجز [۲] که یکی از جالب‌ترین اثبات‌های قضیهٔ بنیادی است، به هاردی و رایت [۳] نگاه کنید. همچنین توصیه می‌کنیم به اثبات موردل [۸] هم نگاهی بیاندازید.

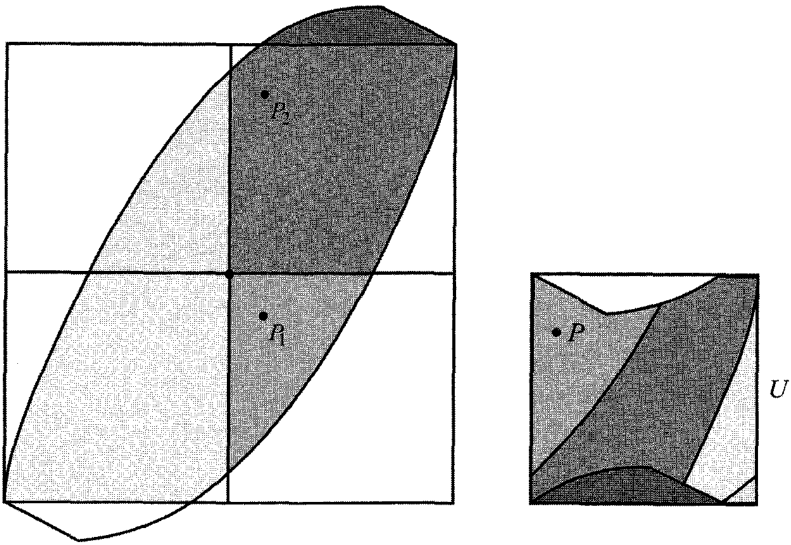
مجموعهٔ مسائل قسمت ۳.۵

۱. مساحت Mـ مجموعهٔ C، برابر با ۶ و ماکزیمم فاصلهٔ نقاط C از $(۰,۰)$ برابر با ۵ است. کوچک‌ترین عدد صحیح مثبت n را چنان پیدا کنید که $(n+۱)^۲A' > (n+۲s)^۲$؛ در اینجا، A' و s، کمیت‌های تعریف شده در متن هستند.

۲. با استفاده از خطوط راست، شکلی غیرمحدب رسم کنید که نسبت به مبدأ متقارن و مساحت آن بزرگ‌تر از ۴ باشد. اما بجز نقطهٔ $(۰,۰)$ شامل هیچ نقطهٔ مشبکهٔ دیگری در درون یا روی مرزش نباشد.

۳. آنچه در ادامه می‌آید طرح اثبات بلیکفلت برای قضیهٔ بنیادی مینکوفسکی است. اثبات او شبیه اثبات ما است. بجز در قسمتی که ما نشان دادیم تفاضل مختصات دو نقطه از C' صحیح است؛ به روابط (۴.۵) نگاه کنید. در اینجا، Mـ مجموعهٔ C' با مساحت $A' > ۱$ را در نظر بگیرید. همچنین فرض کنید C' به‌وسیلهٔ مشبکه L به چند قطعه تقسیم شده است؛ به شکل ۸.۵ نگاه کنید.

ما هر قطعه را در درون مربع واحد U قرار می‌دهیم به‌طوری که قطعه موردنظر همان مکانی را اشغال کند که در مشبکهٔ اولیه اشغال می‌کرده است. چون $A' > ۱$ درحالی که مساحت $U = ۱$ بعضی از قطعات C' در U همپوشی دارند. فرض کنید $D_۱$ و $D_۲$ قطعاتی از C' هستند که در U همپوشی دارند و همچنین فرض کنید $P_۱$ و $P_۲$ نقاطی از $D_۱$ و $D_۲$ هستند که وقتی $D_۱$ و $D_۲$ را در U قرار می‌دهیم بر هم منطبق می‌شوند.



شکل ۸.۵ مربع مشبکه و مربع واحد.

الف) این اثبات را با نشان دادن اینکه تفاضل مختصات $P_۱$ و $P_۲$ صحیح است کامل کنید.

ب) همچون اثبات ارائه شده در متن، با استفاده از تقارن و تحدب C' نشان دهید که C علاوه‌بر $(۰,۰)$ شامل نقطهٔ مشبکهٔ دیگری نیز هست.

۴. مطالعه کنید: اثبات موردل برای قضیهٔ بنیادی مینکوفسکی را مطالعه کنید.

۴.۵ (اختیاری) قضیهٔ مینکوفسکی در nبعد

مینکوفسکی قضایای خود را به صفحه محدود نکرد و آنها را به بسیاری از فضاهای nـ بعدی تعمیم داد. در اینجا، ما یکی از این قضیه‌ها را بدون اثبات بیان می‌کنیم.

قضیهٔ ۲.۵ (قضیهٔ عام مینکوفسکی) هر مجموعهٔ محدب (یا جسم) در فضای nـ بعدی که نسبت به مبدأ متقارن و حجم آن بزرگ‌تر از ۲^n است، علاوه‌بر $(۰,۰,\dots,۰)$ شامل نقطهٔ $(x_۱,x_۲,\dots,x_n)$ با مختصات صحیح است.

در این صورت عام، که برای هر مجموعهٔ محدب متقارنی کار می‌کند، نمی‌توان عدد ۲^n را با عدد کوچک‌تری جایگزین کرد. برای اثبات این ادعا، فقط کافی است که مکعب زیر را در فضای nـ بعدی در نظر بگیریم:

$$|x_۱|<۱, |x_۲|<۱, \dots, |x_n|<۱$$

واضح است که این مکعب مجموعه‌ای محدب و متقارن است، و حجم آن دقیقاً ۲^n است، اما بجز مبدأ شامل هیچ نقطهٔ مشبکهٔ دیگری نیست.

ما می‌توانیم تعبیر هندسی کلی‌تر دیگری را هم بیان کنیم.

تبدیل خطی زیر را درنظر بگیرید:

$$y_۱ = \alpha_{۱۱}x_۱ + \alpha_{۱۲}x_۲ + \cdots + a_{۱n}x_n$$
$$y_۲ = \alpha_{۲۱}x_۱ + \alpha_{۲۲}x_۲ + \cdots + \alpha_{۲n}x_n$$
$$\vdots$$
$$y_n = \alpha_{n۱}x_۱ + \alpha_{n۲}x_۲ + \cdots + \alpha_{nn}x_n$$

در اینجا، ضرایب α_{ij} حقیقی هستند و Δ، دترمینان ماتریس ضرایب، صفر نیست. به عبارتی، این یک تبدیل آفین عام است که xـ فضا را به توی yـ فضا می‌نگارد. این تبدیل، دستگاه نقاط با مختصات صحیح از xـ فضا را به توی یک دستگاه از نقاط از yـ فضا می‌نگارد. مختصات این نقاط لزوماً صحیح نیست ولی ما همچنان این دستگاه جدید را مشبکه می‌نامیم.

اجازه دهید این مشبکه در yـ فضا را دقیق‌تر بررسی کنیم. فرض کنید $A_۱ = (\alpha_{۱۱}, \alpha_{۲۱}, \alpha_{۳۱}, \ldots, \alpha_{n۱})$ نقطه‌ای در yـ فضا باشد که متناظر است به نقطهٔ $(۱, ۰, ۰, \ldots, ۰)$ در xـ فضا؛ فرض کنید $A_۲ = (\alpha_{۱۲}, \alpha_{۲۲}, \ldots, \alpha_{n۲})$ نقطه‌ای در yـ فضا باشد که متناظر است به نقطهٔ $(۰, ۱, ۰, \ldots, ۰)$ در xـ فضا؛ نقاط $A_۳$، ...، A_n نیز به همین ترتیب تعریف می‌شوند. نقطهٔ دلخواه P از مشبکه را می‌توان با استفاده از نمایش برداری به‌صورت زیر نوشت:

$$\overrightarrow{OP} = m_۱\overrightarrow{OA_۱} + m_۲\overrightarrow{OA_۲} + \cdots + m_n\overrightarrow{OA_n}$$

در اینجا، $m_۱$، $m_۲$، ...، m_n، همهٔ مقادیر صحیح را اتخاذ می‌کنند. بردارهای $\overrightarrow{OA_۱}$ ، $\overrightarrow{OA_۲}$، ...، $\overrightarrow{OA_n}$ ساختاری را تشکیل می‌دهند که به آن متوازی‌السطوح اساسی مشبکه می‌گویند.

تبدیل آفین ما یک مجموعه (یا جسم) با حجم V در xـ فضا را به یک مجموعه با حجم $V' = V \cdot |\Delta|$ در yـ فضا می‌نگارد. $|\Delta|$ حجم متوازی‌السطوح است که آن را دترمینان مشبکه می‌نامیم. اکنون می‌توانیم قضیهٔ بنیادی مینکوفسکی را برای yـ فضاها بیان کنیم.

قضیهٔ ۳.۵ (قضیهٔ بنیادی مینکوفسکی در yـ فضا) فرض کنید L مشبکه‌ای با دترمینان Δ در فضای nـ بعدی باشد. در این‌صورت، هر حجم محدب متقارن نسبت به مبدأ که حجم آن از $۲^n\Delta$ بیشتر باشد، علاوه‌بر مبدأ شامل نقطهٔ دیگری از L است.

مراجع

1. J. W. S. Cassels, *Introduction to the Geometry of Numbers,* in Classics of Mathematics Series (1971: corrected reprint, Berlin: Springer-Verlag, 1997).

2. G. Hajós, "Ein neuer Beweis eines Satzes von Minkowski," *Acta Litt. Sci.* (Szeged) 6 (1934):224-5.

3. G. H. Hardy and E. M. Wright, notes for Chapter 3 in *An Introduction to the Theory of Numbers,* 5th ed. (Oxford: Oxford University Press, 1983), 37.

4. J. F. Koksma, *Diophantische Approximationen* (New York: Chelsea, 1936), 13.

5. L. A. Lyusternik, *Convex Figures and Polyhedra*: 1st ed. (1956) traslated from Russian and adapted by Donald L. Barrett (Boston: D. C. Heath, 1966).

6. Hermann Minkowski, *Geometrie der Zahlen,* Bibliotheca Mathematic Teubneriana, Vol. 40 (Leipzig: Teubner, 1910; New York and London: Johnson Reprint Corp., 1988). First section of 240 pages appeared in 1896.

7. ———, *Diophantische Approximationen: Eine Einfuhrung in die Zahlentheorie* (reprinted, New York: Chelsea, 1957).

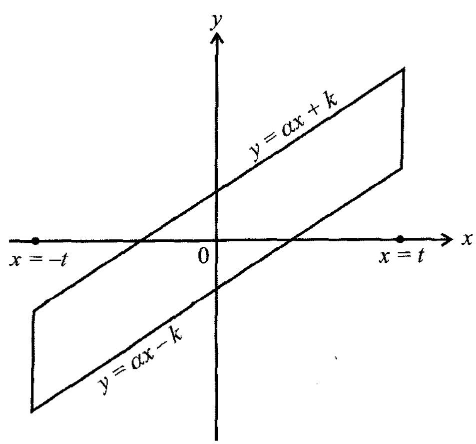
8. L. J. Mordell, "On Some Arithmetical Results in the Geometry of Numbers," *Compositio Math.* 1 (1934): 248-53.

۶ کاربردهایی از قضیه‌های مینکوفسکی

۱.۶ تقریب‌زدن اعداد حقیقی

خواننده‌های علاقه‌مند می‌توانند برای به‌دست آوردن اطلاعات بیشتر در مورد کشف‌های هرمان مینکوفسکی در هندسهٔ اعداد به منتخب آثار او [۴] به زبان آلمانی نگاه کنند. در آنجا می‌توان مشاهده کرد که چگونه مینکوفسکی عمیقاً وارد موضوع شده، مسئله‌های آن را مورد بررسی قرار داده و قضایای آن را در سه‌بعد و ابعاد بالاتر اثبات کرده است. در این فصل ما بررسی خواهیم کرد که چگونه بعضی از نتایج حاصل از کار او به ما کمک خواهد کرد تا با دقت ممکن اعداد حقیقی را با استفاده از اعداد گویا تقریب بزنیم.

به عنوان اولین کاربرد قضیهٔ بنیادی مینکوفسکی، تقریب زیر را اثبات خواهیم کرد. متوازی‌الاضلاع شکل ۱.۶ در درک این تقریب به ما کمک خواهد کرد.



شکل ۱.۶ متوازی‌الاضلاع برای اثبات قضیهٔ ۱.۶.

قضیهٔ ۱.۶ برای عدد حقیقی α و عدد صحیح $t > ۰$، که می‌تواند هر چقدر که می‌خواهیم بزرگ باشد، اعداد صحیح q و p، که هر دو صفر نیستند، چنان وجود دارند که $|q - \alpha p| \leq \frac{۱}{t}$.

اثبات. Mـ مجموعهٔ مورد استفاده در این اثبات، متوازی‌الاضلاعی است که با چهار خط زیر محدود شده است؛ به شکل ۱.۶ نگاه کنید.

$$y - \alpha x = k, \qquad y - \alpha x = -k, \qquad x = t, \qquad x = -t.$$

طول قاعدهٔ این متوازی‌الاضلاع $۲t$ و ارتفاع آن $۲k$ است، بنابراین مساحت آن برابر با $A = ۲t \cdot ۲k = ۴tk$ است. بنابراین اگر برای عدد صحیح و مثبت t، قرار دهیم $k = \frac{۱}{t}$، خواهیم داشت $A = ۴$. بنابر قضیهٔ بنیادی مینکوفسکی، روی مرز متوازی‌الاضلاع یا درون آن علاوه‌بر نقطهٔ $(۰, ۰)$ نقطهٔ مشبکهٔ دیگری مانند (p, q) نیز وجود دارد. این گزاره دو نتیجه را برای مقادیر p و q به همراه دارد. اول اینکه:

$$-t \leq p \leq t, \qquad \text{یا} \qquad |p| \leq t$$

دوم اینکه:

$$\alpha p - k \leq q \leq \alpha p + k.$$

چون $k = \frac{۱}{t}$، می‌توان این عبارت را به شکل زیر بازنویسی کرد:

$$\alpha p - \frac{۱}{t} \leq q \leq \alpha p + \frac{۱}{t}, \quad t > ۰ \quad \text{برای}$$

با کم کردن αp خواهیم داشت: $\frac{-۱}{t} \leq q - \alpha p \leq \frac{۱}{t}$؛ بنابراین، $|q - \alpha p| \leq \frac{۱}{t}$. این قضیهٔ ۱.۶ را اثبات می‌کند.

یادداشت. بنابر قضیهٔ مذکور، p و q، هر دو صفر نیستند. اگر $p \neq ۰$، آنگاه

$$\left|\frac{q}{p} - \alpha\right| \leq \frac{۱}{|p|t}$$

در اینجا، وقتی t خیلی بزرگ باشد، $\frac{۱}{|p|t}$ خیلی کوچک خواهد بود. بنابراین، $\frac{q}{p}$ در این نامساوی یک تقریب گویای عالی برای عدد حقیقی α است.

۲.۶ قضیهٔ اول مینکوفسکی

هم اکنون، با به کارگیری قضیهٔ بنیادی مینکوفسکی برای یک Mـ مجموعه دیگر، نقاط مشبکه‌ای را به‌دست می‌آوریم که به‌ازای آنها دو فرم خطی به‌طور همزمان کراندار هستند. به این قضیه، قضیهٔ اول مینکوفسکی می‌گویند؛ مواظب باشید که آن را با قضیهٔ بنیادی، قضیهٔ ۱.۶، اشتباه نگیرید.

قضیهٔ ۲.۶ (قضیهٔ اول مینکوفسکی) دو فرم خطی زیر را در نظر بگیرید:

$$\xi = \alpha x + \beta y,$$

$$\Delta = \alpha\delta - \beta\gamma \neq ۰ \quad (\text{دترمینان})$$

$$\eta = \gamma x + \delta y$$

در اینجا، α، β، γ و δ اعداد حقیقی دلخواه هستند. در این‌صورت، اعداد صحیح p و q، که هر دو صفر نیستند، چنان وجود دارند که نامساوی‌های زیر به‌طور همزمان برقرار است:

$$|\xi| = |\alpha p + \beta q| \leq \sqrt{|\Delta|}, \qquad |\eta| = |\gamma p + \delta q| \leq \sqrt{|\Delta|}$$

اثبات. Mـ مجموعهٔ مورد استفاده در این اثبات، متوازی‌الاضلاعی است که با چهار خط زیر محدود شده است؛ به شکل ۲.۶ نگاه کنید.

$$\text{به‌ازای } k > ۰ ،\quad \alpha x + \beta y = \pm k, \qquad \gamma x + \delta y = \pm l$$

در اینجا، دترمینان مخالف صفر است: $\Delta = \alpha\delta - \beta\gamma \neq ۰$. مساحت این متوازی‌الاضلاع دو برابر مساحت مثلث $A : (x_۱, y_۱)$، $B : (x_۲, y_۲)$ و $C : (x_۳, y_۳)$ است. چون متوازی‌الاضلاع متقارن است، داریم: $(x_۳, y_۳) = (-x_۱, -y_۱)$.

از هندسهٔ تحلیلی به یاد داریم که چگونه مساحت مثلث ABC را به شکل یک دترمینان بنویسیم:

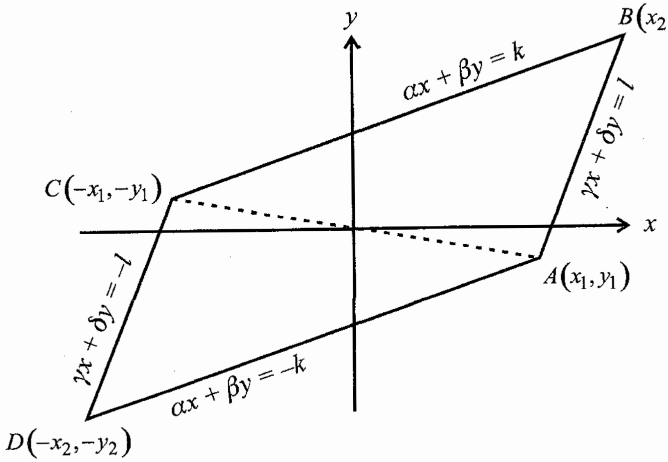
$$\text{مساحت } ABC = \frac{۱}{۲}\begin{vmatrix} x_۱ & y_۱ & ۱ \\ x_۲ & y_۲ & ۱ \\ x_۳ & y_۳ & ۱ \end{vmatrix} = \frac{۱}{۲}\begin{vmatrix} x_۱ & y_۱ & ۱ \\ x_۲ & y_۲ & ۱ \\ -x_۱ & -y_۱ & ۱ \end{vmatrix}$$

آخرین دترمینان را برحسب ستون آخر بسط می‌دهیم، داریم:

$$\text{مساحت } ABC = |x_۱ y_۲ - x_۲ y_۱| \tag{۱.۶}$$

مختصات A و B چه هستند؟ ما آنها را با حل دو دستگاه معادلات خطی زیر می‌یابیم:

$$\begin{aligned} \alpha x + \beta y &= k \\ \gamma x + \delta y &= l, \end{aligned} \quad \text{و} \quad \begin{aligned} \alpha x + \beta y &= -k \\ \gamma x + \delta y &= l \end{aligned}$$



شکل ۲.۶ متوازی‌الاضلاع برای اثبات قضیهٔ ۲.۶.

جواب‌های این دو دستگاه به ترتیب برابرند با:

$$x_1 = \frac{-1}{\Delta}(\delta k + \beta l) \qquad x_2 = \frac{1}{\Delta}(\delta k - \beta l)$$
و
$$y_1 = \frac{1}{\Delta}(\alpha l + \gamma k) \qquad y_2 = \frac{1}{\Delta}(\alpha l - \gamma k)$$

با جایگذاری این مقادیر در (۱.۶) مساحت مثلث را به‌دست می‌آوریم:

$$ABC \text{ مساحت } = \frac{2k|l||\alpha\delta - \beta\gamma|}{\Delta^2} = \frac{2k|l|}{|\Delta|} = 2k\left|\frac{l}{\Delta}\right|$$

اگر این نتیجه را دو برابر کنیم، مساحت متوازی‌الاضلاع شکل ۲.۶ را به‌دست می‌آوریم:

$$A = 4k\left|\frac{l}{\Delta}\right|$$

اکنون با انتخاب $l = \frac{\Delta}{k}$، که در آن k می‌تواند هر عدد مثبت دلخواهی باشد، داریم $A = 4$. بنابر قضیهٔ مینکوفسکی، اعداد صحیح p' و q'، که هر دو صفر نیستند، چنان وجود دارند که:

$$|\alpha p' + \beta q'| \le k, \qquad |\gamma p' + \delta q'| \le \frac{|\Delta|}{k}$$

به‌ویژه، اگر $k = \sqrt{|\Delta|}$، آنگاه اعداد صحیح p و q، که هر دو صفر نیستند، چنان وجود دارند که دو نامساوی زیر به‌طور همزمان برقرار است:

$$|\alpha p + \beta q| \le \sqrt{|\Delta|}, \qquad |\gamma p + \delta q| \le \sqrt{|\Delta|}$$

این دقیقاً همان چیزی است که می‌خواستیم اثبات کنیم.

به شرطی که برای دترمینان در نظر گرفتیم توجه کنید. اگر $\Delta = \circ$، آنگاه $\frac{\alpha}{\beta} = \frac{\gamma}{\delta}$ و $\eta = \left(\frac{\beta}{\delta}\right)\eta = \xi$؛ که چندان جالب توجه نیست.

مجموعهٔ مسائل قسمت ۲.۶

۱. قضیهٔ اول مینکوفسکی را برای فرم‌های خطی $\xi = ۲۳\circ x + ۲\circ۱y$ و $\eta = ۴۵۹x - ۴\circ\circ y$ به‌کار برید. مقادیر واقعی $x = p$ و $y = q$ را که در این قضیه صدق می‌کنند، پیدا کنید.

۲. مسئله را برای فرم‌های $\xi = ۲۳\circ x + ۲\circ۱y$ و $\eta = ۴۵۹x + ۴\circ\circ y$ تکرار کنید.

۳.۶ قضیهٔ دوم مینکوفسکی

در این بخش یکی از کاربردهای قضیهٔ اول مینکوفسکی مطرح می‌شود. دوباره نیاز داریم که دترمینان صفر نباشد.

قضیهٔ ۳.۶ (**قضیهٔ دوم مینکوفسکی**) دو فرم خطی زیر را در نظر بگیرید.

$$\xi = \alpha x + \beta y$$

$$\Delta = \alpha\delta - \beta\gamma \neq \circ \quad (\text{دترمینان})$$

$$\eta = \gamma x + \delta y$$

α، β، γ و δ اعداد حقیقی هستند. در این‌صورت، اعداد صحیح p و q، که حداقل یکی از آنها صفر نیست، چنان وجود دارند که

$$|\xi\eta| = |\alpha p + \beta q| \cdot |\gamma p + \delta q| \leq \frac{۱}{۲}|\Delta|$$

اثبات. دو فرم داده شده در صورت قضیه را با هم جمع و از هم کم می‌کنیم:

$$\xi + \eta = (\alpha + \gamma)x + (\beta + \delta)y,$$
$$\xi - \eta = (\alpha - \gamma)x + (\beta - \delta)y$$

سپس، D، دترمینان این تبدیل جدید را به روش معمول پیدا می‌کنیم:

$$D = (\alpha + \gamma)(\beta - \delta) - (\alpha - \gamma)(\beta + \delta)$$
$$= -۲(\alpha\delta - \beta\gamma) = -۲\Delta \neq \circ$$

بنابراین، $|D| = ۲|\Delta|$.

بنابر قضیهٔ ۲.۶ می‌توان دو عدد صحیح p و q را که حداقل یکی از آنها صفر نیست، چنان پیدا کرد که به‌طور همزمان:

$$|\xi+\eta| \leq \sqrt{|D|} = \sqrt{۲|\Delta|},$$
$$|\xi-\eta| \leq \sqrt{|D|} = \sqrt{۲|\Delta|}$$

از دو عدد $|\xi|+|\eta|$ و $|\xi-\eta|$، آنکه بزرگ‌تر است برابر است با $|\xi+\eta|$؛ این یعنی،

$$|\xi|+|\eta| = \max\{|\xi+\eta|, |\xi-\eta|\}$$

با توجه به اینکه هر دو عدد $|\xi+\eta|$ و $|\xi-\eta|$ کوچک‌تر از یا مساوی با $\sqrt{۲|\Delta|}$ است، داریم:

$$|\xi|+|\eta| \leq \sqrt{۲|\Delta|} \qquad (۲.۶)$$

برای برداشتن آخرین قدم، به نابرابری میانگین حسابی ـ هندسی نیاز داریم. این نابرابری بیان می‌کند که اگر a و b دو عدد حقیقی مثبت باشند، آنگاه

$$\sqrt{ab} \leq \frac{a+b}{۲} \quad \text{یا} \quad ab \leq \left(\frac{a+b}{۲}\right)^{۲}$$

این نامساوی درست است، چون $a+b-۲\sqrt{ab} = (\sqrt{a}-\sqrt{b})^{۲} \geq ۰$، بنابراین $۲\sqrt{ab} \leq a+b$؛ یا به‌عبارتی، $\sqrt{ab} \leq \frac{(a+b)}{۲}$. با استفاده از این نابرابری‌ها داریم

$$|\xi\eta| = |\xi|\cdot|\eta| \leq \left(\frac{|\xi|+|\eta|}{۲}\right)^{۲} \leq \left(\frac{\sqrt{۲|\Delta|}}{۲}\right)^{۲} = \frac{۱}{۲}|\Delta|$$

در اینجا، اثبات قضیهٔ ۳.۶ به پایان می‌رسد.

یادداشت. در واقع، عدد $\frac{۱}{۲}$ در قضیهٔ ۳.۶ «بهترین ثابت ممکن» نیست. می‌توان ثابت کرد که اعداد صحیح p و q، که حداقل یکی از آنها صفر نیست، چنان وجود دارند که

$$|\xi\eta| \leq \frac{|\Delta|}{\sqrt{۵}}$$

عدد $\sqrt{۵}$، به این تعبیر بهترین ثابت ممکن است که اگر آنرا با هر عدد بزرگ‌تری جایگزین کنیم قضیهٔ ما برقرار نخواهد بود. برای دیدن اثبات نسبتاً مشکل این بهبود به هاردی و رایت [۱، فصل ۴، قضیهٔ ۴۵۴] نگاه کنید.

مسئلهٔ قسمت ۳.۶

۱. قضیهٔ دوم مینکوفسکی را برای دستگاه خطی $\xi = x - \pi y$ و $\eta = x - ey$ به‌کار برید؛ در اینجا $\pi = ۳/۱۴۱۵۹\ldots$ و $e = ۲/۷۱۸۲۸\ldots$.

۴.۶ تقریب‌زدن اعداد گنگ

به‌عنوان کاربردی از قضیهٔ دوم مینکوفسکی، قضیه دیگری را بیان و اثبات می‌کنیم. این قضیه در رابطه با تقریب اعداد گنگ به وسیلهٔ اعداد گویا است و ما به آن در فصل ۵ اشاره کردیم.

قضیهٔ ۴.۶ عدد گنگ α را در نظر بگیرید. اعداد گویایی $\frac{p}{q}$، با مخرج به دلخواه بزرگ، چنان وجود دارند که $\left|\left(\frac{p}{q}\right) - \alpha\right| \le \frac{۱}{۲q^۲}$.

اثبات. دو فرم خطی زیر را در نظر بگیرید:

$$\xi = t(x - \alpha y), \qquad \eta = \frac{y}{t}, \quad t \neq ۰$$

در اینجا، α عدد گنگ داده شده و t عددی غیرصفر است که می‌تواند به دلخواه ما بزرگ باشد. دترمینان این فرم‌ها برابر است با

$$\Delta = \begin{vmatrix} -t\alpha & t \\ \frac{۱}{t} & ۰ \end{vmatrix} = -۱ \neq ۰$$

پس، $|\Delta| = ۱$. بنابر قضیهٔ ۳.۶، اعداد صحیح p و q، که حداقل یکی از آنها صفر نیست، چنان وجود دارند که:

$$|\xi\eta| = |t(p - \alpha q)| \cdot \left|\frac{q}{t}\right| \le \frac{|-۱|}{۲} = \frac{۱}{۲} \tag{۳.۶}$$

با ساده کردن این نابرابری داریم:

$$|p - \alpha q| \cdot |q| \le \frac{۱}{۲} \tag{۴.۶}$$

به کمک نامساوی (۲.۶) که در قضیهٔ ۳.۶ استفاده شد، همچنین داریم:

$$|\xi| + |\eta| = |t(p - \alpha q)| + \left|\frac{q}{t}\right| \le \sqrt{۲|\Delta|} = \sqrt{۲} \tag{۵.۶}$$

از (۵.۶) نتیجه می‌شود که

$$|p-\alpha q| \leq \frac{\sqrt{۲}}{t} \qquad (۶.۶)$$

ادعا می‌کنیم که با بزرگ کردن t به اندازهٔ کافی، می‌توانیم q را از هر عدد صحیح داده شده N بزرگ‌تر کنیم. برای عدد صحیح $q \neq ۰$، تعریف زیر را در نظر بگیرید:

$$\min_{\text{صحیح } p} |p-\alpha q| = m(q)$$

چون α گنگ است، برای هر عدد صحیح q داریم: $m(q) > ۰$. برای $q = ۰$ داریم:

$$m(۰) = \min_{\text{صحیح } p \neq ۰} |p| = ۱$$

اکنون، تعریف می‌کنیم:

$$m = \min\left(m(۰), m(۱), \ldots, m(N)\right)$$

t را چنان انتخاب کنید که $\frac{\sqrt{۲}}{t} < m$. با این حساب و بنابر (۶.۶)، $|p-\alpha q| < m$. اما این نابرابری برای $q \leq N$ برقرار نیست، چون برای این qها، $m \leq m(q)$. بنابراین، q از عدد صحیح داده شدهٔ N بزرگ‌تر است. با تقسیم (۴.۶) بر $q^{۲}$، نابرابری مطلوب به‌دست می‌آید،

$$\left|\frac{p}{q}-\alpha\right| \leq \frac{۱}{۲q^{۲}}$$

یادداشت. قضیهٔ ۴.۶ نشان می‌دهد که ما می‌توانیم هر عدد صحیح α را، با دقت مطلوب، با عدد گویای $\frac{p}{q}(q \neq ۰)$ تقریب بزنیم. دوباره این نتیجه، «بهترین ممکن» نیست. قضیهٔ معروفی از هورویتس [۳] بیان می‌کند که هر عدد حقیقی α دارای تعداد نامتناهی تقریب گویای $\frac{p}{q}$ است به‌طوری که

$$\left|\frac{p}{q}-\alpha\right| \leq \frac{۱}{\sqrt{۵}q^{۲}}$$

در اینجا، عدد $\sqrt{۵}$، «بهترین ممکن» است چون هر عدد بزرگ‌تری را که جایگزین آن کنیم، قضیه برقرار نخواهد بود [۱، فصل ۱۱، قضیهٔ ۱۹۴].

۵.۶ قضیهٔ سوم مینکوفسکی

بالاخره، برای کامل کردن بحث، قضیهٔ سوم مینکوفسکی را بیان می‌کنیم. اثبات آن بسیار مشکل‌تر از قضایای دیگر است، به همین دلیل ما آن را در اینجا اثبات نمی‌کنیم.

قضیهٔ ۵.۶ (قضیهٔ سوم مینکوفسکی) اگر ξ، η و Δ همچون قضیهٔ ۳.۶باشند. آنگاه به هر زوج از اعداد حقیقی ζ و σ می‌توان زوجی از اعداد صحیح p و q را چنان متناظر کرد که $|(\xi-\zeta)(\eta-\sigma)| \le \frac{1}{4}|\Delta$.

یادداشت. فرض کنید که در قضیهٔ ۵.۶ قرار دهیم $\xi = p - \alpha q$ ، $\eta = q$، $\zeta = c$ و $\sigma = 0$؛ در اینجا، α عددی گنگ است. با جایگزینی داریم:

$$|(p-\alpha q-c)q| \le \frac{1}{4}$$

یا

$$|p-\alpha q-c| \le \frac{1}{4|q|}$$

به شرطی که $q \neq 0$. برای دیدن اثباتی از قضیهٔ ۵.۶ و همچنین سؤال‌های جالب نشأت گرفته از این نابرابری‌ها، به هاردی و رایت [۱، فصل ۲۴، قسمت ۸.۶] نگاه کنید.

۶.۶ دستگاه تقریب‌های دیوفانتی

اکنون، در انتهای این فصل، نشان می‌دهیم که چگونه می‌توان از قضیهٔ مینکوفسکی برای بررسی دستگاه تقریب‌های دیوفانتی استفاده کرد. منظور از این دستگاه، تقریب همزمان n عدد گنگ α_1، α_2، ...، α_n، با n عدد گویا با مخرج‌های برابر است.

قضیهٔ ۶.۶ n عدد حقیقی α_1، α_2، ...، α_n را در نظر بگیرید. تعداد نامتناهی مجموعه در اعداد صحیح p_1، p_2، ...، p_n و $p \ge 1$ چنان وجود دارند که به‌طور همزمان،

$$\left|\alpha_1 - \frac{p_1}{p}\right| < \frac{1}{p^{(n+1)/n}}$$
$$\left|\alpha_2 - \frac{p_2}{p}\right| < \frac{1}{p^{(n+1)/n}}$$
$$\vdots$$
$$\left|\alpha_n - \frac{p_n}{p}\right| < \frac{1}{p^{(n+1)/n}}$$

اثبات. فرض کنید s عددی کوچک‌تر از ۱ است. ناحیهٔ K از $\mathbb{R}^{n+1}$، همهٔ نقاط $(x_1, x_2, \dots, x_n, y)$ است که در نابرابری‌های زیر صدق می‌کنند:

$$|x_i - \alpha_i y| \leq s, \quad i = ۱, ۲, \ldots, n, \quad |y| \leq s^{-n}$$

ناحیهٔ K، متوازی‌السطوحی به مرکز مبدأ است؛ بسته، محدب و نسبت به مبدأ متقارن است.

ادعا می‌کنیم که حجم آن $۲^{n+۱}$ است. برای اثبات این ادعا، از نگاشت خطی زیر، از $x_۱$، $x_۲$، ...، x_n، yـ فضا به $u_۱$، $u_۲$، ...، u_n، vـ فضا استفاده می‌کنیم:

$$u_i = \frac{۱}{s}(x_i - \alpha_i y), \quad v = s^n y$$

این نگاشت ناحیهٔ K از $x_۱$ ، $x_۲$، ...، x_n، yـ فضا را به توی ناحیهٔ H از $u_۱$، $u_۲$، ...، u_n، vـ فضا که با نابرابری‌های زیر تعریف می‌شود می‌نگارد:

$$|u_i| \leq ۱, \quad |v| \leq ۱$$

آشکارا، H مکعبی با طول یال ۲ در $\mathbb{R}^{n+۱}$ است. بنابراین $\mathrm{vol}(H) = ۲^{n+۱}$. با توجه به اینکه دترمینان ژاکوبی این نگاشت برابر با ۱ است، نگاشت‌ها اندازهٔ حجم را تغییر نمی‌دهد. در نتیجه، $\mathrm{vol}(K) = ۲^{n+۱}$.

بنابراین، بنابر قضیهٔ بنیادی مینکوفسکی، ناحیه K، علاوه‌بر مبدأ $O : (۰, ۰, \ldots, ۰)$، شامل نقطهٔ مشبکهٔ دیگری نیز هست: $(p_۱, p_۲, \ldots, p_n, p)$. پس

$$|p_i - \alpha_i p| \leq s, \quad i = ۱, ۲, \ldots, n, \quad |p| \leq s^{-n}. \tag{۷.۶}$$

می‌توانیم فرض کنیم $p \geq ۰$؛ اگر چنین نبود می‌توان علامت همهٔ p_iها و p را عوض کرد. ادعا می‌کنیم که p مثبت است. اگر $p = ۰$، بنابر نابرابری (۷.۶) داریم: $|p_i| \leq s$. اما از اول s را کوچک‌تر از ۱ انتخاب کرده بودیم و p_iها اعداد صحیح هستند، پس همهٔ آنها باید صفر باشند؛ این یعنی، $(p_۱, p_۲, \ldots, p_n, p) = (۰, ۰, \cdots, ۰)$. ولی این با انتخاب ما در تناقض است.

با تقسیم اولین n نابرابری در (۷.۶) بر p، داریم:

$$\left|\frac{p_i}{p} - \alpha_i\right| \leq \frac{s}{p}$$

از آخرین نابرابری در (۷.۶) نتیجه می‌گیریم که $s \leq p^{\frac{-۱}{n}}$. با قرار دادن این در نابرابری قبلی، داریم:

$$\left|\frac{p_i}{p} - \alpha_i\right| \leq \frac{۱}{p^{۱+\frac{۱}{n}}}, \quad i = ۱, ۲, \ldots, n \tag{۸.۶}$$

و این همان چیزی است که مایل به اثبات آن بودیم.

برای نشان دادن اینکه این نابرابری‌ها دارای تعداد نامتناهی جواب است، می‌توان هر مجموعهٔ متناهی از جواب‌ها (۸.۶) را در نظر گرفت و s را چنان کوچک انتخاب کرد که برای همهٔ جوابها در این مجموعهٔ متناهی $|p_i - \alpha_i p| > s$. با این حساب، هر جوابی برای (۷.۶)، آشکارا با همهٔ این جواب‌های (۸.۶) متفاوت است.

تکلیف خواندنی برای فصل ۶

قضیهٔ بنیادی مینکوفسکی به‌طور ضمنی بیان می‌کند که اگر مربعی به ضلع ۲ را چنان روی مشبکه Λ قرار دهیم که مرکز مربع روی یکی از نقاط مشبکه قرار گیرد، به‌طور حتم، نقطهٔ مشبکهٔ دیگری هم درون مربع یا روی آن وجود دارد. اثبات ارائه شده توسط هیلبرت و کوهن ـ وسن [۲] را مطالعه کنید و به تأثیر ایده‌های شهودی مینکوفسکی بر آن توجه کنید.

مراجع

1. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed. (Oxford: Oxford University Press, 1983).

2. David Hilbert and S. Cohn-Vossen, *Geometry and the Imagination*, translated by P. Nemenyi (New York: Chelsea, 1952), 41.

3. A. Hurwitz, "Über die angenä herte Darstellung der Irrationalzahlen durch rationale Brüche," *Mathematische Annalen* 39 (1891): 279-84.

4. Hermann Minkowski, *Ausgewahlte Arbeiten zur Zahlentheorie und zur Geometrie. Mit D. Hilbert's Gedachtnisre auf H. Minkowski (Göttingen, 1909)* [*Selected Papers on Number Theory and Geometry, With D. Hilbert's Commemorative Address in Honor of H. Minkowski*], Teubner-Archiv zur Mathematik. Vol. 12. E. Kratzel and B. Weissbaeh, eds. (Leipzig: Teubner, 1989).

۷ تبدیل‌های خطی و مشبکه‌های صحیح

۱.۷ تبدیل‌های خطی

کسانی که بخش اختیاری ۴.۵ را مطالعه کرده‌اند احتمالاً هم‌اکنون با بیشتر موضوعاتی که در این فصل بحث خواهیم کرد آشنا هستند. از طرفی، ما امیدواریم که این کتاب همهٔ خوانندههایش را به درک قضیه‌های دشوارتر هندسهٔ اعداد و حتی مطالعه بیشتر و مستقل در این حوزه ترغیب کرده باشد. یکی از پیش‌نیازهای چنین مطالعه‌ای، آگاهی داشتن از تبدیلات خطی است. در این فصل، ما کمی با چگونگی استفاده از تبدیلات خطی در مطالعهٔ مشبکه‌های صحیح آشنا خواهیم شد. اجازه دهید که با تعریف تبدیل‌های خطی شروع کنیم.

درصورتی که نقطهٔ (x, y) از صفحه توسط تبدیل خطی T به نقطهٔ (x', y') نگاشته شود، می‌توان (x', y') را با استفاده از یک زوج از معادلات خطی برحسب x, y نوشت. با استفاده از نمادها می‌توان نوشت:

$$T: \quad \begin{aligned} x' &= ax + by \\ y' &= cx + dy \end{aligned} \qquad \Delta = ad - bc \neq \circ$$

در اینجا، ضرایب d, c, b, a اعداد حقیقی ثابت هستند. ما فرض می‌کنیم که دترمینان تبدیل، $\Delta = ad - bc$ صفر نیست. به‌طور نمادین، نگاشته شدن نقطه (x, y) به نقطهٔ (x', y') را تحت تبدیل T به‌صورت زیر نمایش می‌دهیم:

$$T: (x, y) \longrightarrow (x', y')$$

علاوه بر غیرصفر بودن دترمینان، فرض اساسی دیگر ما این است که هر دو نقطهٔ (x, y) و (x', y') در یک دستگاه مختصات رسم می‌شوند. چرا این فرض مهم است؟ زیرا در غیر این صورت

به راحتی سردرگم خواهیم شد. برای مثال، تبدیل زیر را در نظر بگیرید:

$$T_1: \quad \begin{aligned} x' &= x + y \\ y' &= x - y \end{aligned} \qquad \Delta = -1 - 1 = -2$$

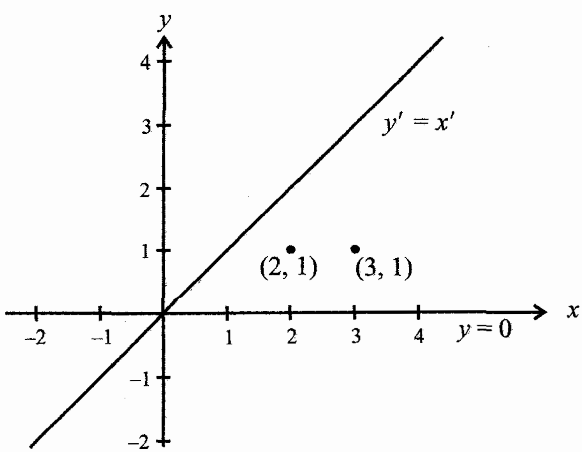
ابتدا با جمع کردن، $x' + y'$، پس با کم کردن، $x' - y'$، می‌توان x و y را برحسب x' و y' نوشت:

$$x = \frac{1}{2}(x' + y'), \qquad y = \frac{1}{2}(x' - y')$$

تحت T_1، محور xها، $y = 0$، به توی خط $x' - y' = 0$ نگاشته می‌شود که دیگر محور xها نیست. فکر نکنید که T_1 محور xها را به خط $y' = x'$ تبدیل می‌کند. در عوض، فکر کنید که خط $y = 0$ در ابتدا منطبق بر محور xها بود ولی اکنون منطبق بر خط $y' = x'$ است. شما می‌توانید هر دوی این خطوط را در شکل ۱.۷ با هم مشاهده کنید. در همین شکل، می‌توان نقطهٔ $(x, y) = (2, 1)$ را مشاهده کرد که تحت T_1 به نقطهٔ $(3, 1)$ نگاشته شده است. دوباره توجه کنید که این دو نقطه نیز با توجه به محورهای اولیه رسم شده‌اند.

تبدیل معکوس T را با T^{-1} نمایش می‌دهیم؛ T^{-1} تابعی است که تبدیل T را خنثی می‌کند. برای مثال، معادلات تبدیل قبلی را در نظر بگیرید:

$$T: \quad \begin{aligned} x' &= ax + by \\ y' &= cx + dy \end{aligned} \qquad \Delta = ad - bc \neq 0$$



شکل ۱.۷ تبدیل خطی T_1: $y' = x - y$، $x' = x + y$.

اگر x و y را برحسب x' و y' محاسبه کنیم، تبدیل معکوس به‌دست می‌آید:

$$T^{-1}: \quad \begin{aligned} x &= a_1x' + b_1y' \\ y &= c_1x' + d_1y' \end{aligned} \qquad \Delta_1 = a_1d_1 - b_1c_1 \neq 0$$

در اینجا، $a_1 = \frac{d}{\Delta}$، $b_1 = \frac{-b}{\Delta}$، $c_1 = \frac{-c}{\Delta}$ و $d_1 = \frac{a}{\Delta}$. دترمینان تبدیل معکوس برابر است با

$$\Delta_1 = a_1d_1 - b_1c_1 = \frac{ad - bc}{\Delta^2} = \frac{1}{\Delta} \neq 0$$

این یعنی، دترمینان تبدیل معکوس، معکوس ضربی Δ، دترمینان تبدیل T است.

این گزاره، دو نتیجه به همراه دارد. اول اینکه، تبدیلاتی که دترمینان آنها صفر است دارای معکوس نیستند، به همین دلیل ما فقط با تبدیلاتی کار می‌کنیم که دترمینان آنها صفر نیست. دوم اینکه، در آینده ما با تبدیلات ویژه‌ای با دترمینان $\Delta = \pm 1$ کار خواهیم کرد، برای این تبدیلات، همچنین داریم $\Delta_1 = \pm 1$.

تبدیلات خطی دارای خواص مفید بسیاری هستند. در اینجا ما پنج خاصیت بسیار مفید را فهرست می‌کنیم. تحت تبدیل خطی T:

۱. نقطه به نقطه و خط به خط نگاشته می‌شود.

۲. مقاطع مخروطی (دایره، بیضی و غیره) به مقاطع مخروطی نگاشته می‌شوند.

۳. اگر نقطه‌ای یک پاره‌خط را به یک نسبت مشخص تقسیم کند، تبدیل یافتهٔ آن نیز تبدیل یافتهٔ پاره‌خط را به همان نسبت تقسیم می‌کند. (یک نتیجه این گزاره برای ما این است که Mـ مجموعه‌ها به Mـ مجموعه‌ها نگاشته می‌شوند.)

۴. وقتی a، b، c و d اعداد تعریف کنندهٔ تبدیل خطی T، اعداد صحیح هستند و دترمینان تبدیل برابر با $\Delta = ad - bc = \pm 1$ است، آنگاه چنانچه x و y اعداد صحیح باشند، x' و y' نیز اعداد صحیح هستند و برعکس. به عبارت دیگر، یک تبدیل خطی با ضرایب صحیح و دترمینان ± 1، نقاط مشبکه را به نقاط مشبکه می‌نگارد؛ همین گزاره برای T^{-1}، تبدیل معکوس T برقرار است.

۵. تحت تبدیل‌های خطی با دترمینان $\Delta = \pm 1$، مساحت ناوردا است.

خودتان در مسئله ۱، خاصیت‌های (۱) تا (۳) را اثبات خواهید کرد. خاصیت (۴) در مسئله ۴ به کار برده می‌شود. اثبات خاصیت (۵) سخت‌تر و نیازمند حساب دیفرانسیل و انتگرال است؛ بنابراین

درستی آن را بدون اثبات می‌پذیریم. اگرچه به راحتی می‌توان بررسی کرد که تحت یک تبدیل خطی با دترمینان $\Delta = \pm ۱$، مساحت مثلث‌ها و مستطیل‌ها ناوردا است. از طرفی، در حساب دیفرانسیل و انتگرال مقدماتی، مفهوم مساحت براساس حد مجموع مستطیل‌های تقریب زننده است.

مجموعهٔ مسائل قسمت ۱.۷

۱. برای تبدیل خطی T:

الف) خاصیت (۱) را اثبات کنید.

ب) خاصیت (۲) را اثبات کنید.

ج) خاصیت (۳) را اثبات کنید.

۲. نقاط $(۰, ۰)$، $(۱, ۰)$، $(۱, ۲)$ و$(۰, ۲)$ چهار رأس یک مستطیل هستند.

الف) با استفاده از تبدیلT: $x' = x$ و $y' = x + y$، این مستطیل را تبدیل کنید و تصویر آن را رسم کنید.

ب) مساحت مستطیل اولیه و مساحت تصویر آن تحت T را محاسبه کنید.

۳. نقاط $(۰, ۰)$، $(۱۰, ۰)$ و $(۱۰, ۱۰)$ سه رأس یک مثلث هستند. این مثلث تحت تبدیل T: $x = x' + y'$ و $y = x' + ۲y'$، به یک مثلث جدید تبدیل می‌شود.

الف) دترمینان T را محاسبه کنید.

ب) مساحت مثلث اولیه و مثلث تبدیل یافته را با هم مقایسه کنید.

۴. تحت تبدیل T: $x' = ۲x + ۳y$ و $y' = ۴x + ۶y$، رئوس $(۰, ۰)$، $(۱, ۰)$، $(۱, ۱)$ و $(۰, ۱)$ از یک مربع به نقاط $(۰, ۰)$، $(۲, ۴)$، $(۵, ۱۰)$ و $(۳, ۶)$ تبدیل می‌شوند. بنابراین، تحت T،

$$(x, y) = (۰, ۱) \to (x', y') = (۳, ۶)$$

الف) تصویر مربع داده شده را تحت T رسم کنید.

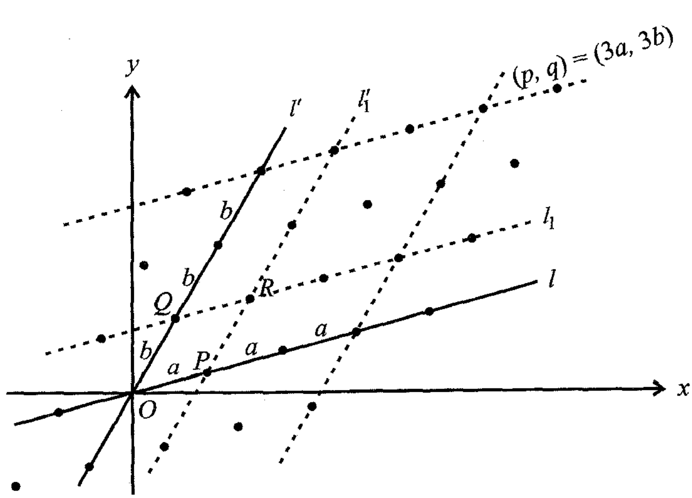
ب) آیا تبدیل معکوس $T^{-۱}$ وجود دارد که $(x', y') = (۳, ۶) \to (x, y) = (۰, ۱)$؟ توضیح دهید.

۲.۷ مشبکه‌های عام

در فصل ۱، ما مشبکه اصلی خطوط L و مشبکه‌ـنقطه‌ای اصلی Λ، حاصل از تلاقی خطوط L را معرفی کردیم. چون بحث اصلی ما درمورد نقاط مشبکه است، از این به بعد به‌طور خلاصه از «مشبکه» به جای «مشبکه‌های نقطه‌ای» استفاده خواهیم کرد. اما قبل از هر چیز، اجازه دهید کمی تأمل کنیم و مفهوم عام یک مشبکه را مورد توجه قرار دهیم.

در صفحهٔ xy، نقطهٔ O را به‌عنوان مبدأ و دو نقطهٔ P و Q را چنان انتخاب کنید که O، P و Q هم‌خط نباشند؛ به شکل ۲.۷ نگاه کنید. خط l، گذرنده از O و P، و همچنین خط l'، گذرنده از O و Q را رسم کنید. روی l، بازه‌های به طول $a = |\overline{OP}|$، و به همین ترتیب، روی l'، بازه‌های به طول $b = |\overline{OQ}|$ را جدا کنید. اکنون دو دستگاه از خطوط را رسم کنید: اول، از نقاطی که روی l مشخص کرده‌اید و با فاصلهٔ یکسان از یکدیگر قرار دارند، خطوطی موازی l' رسم کنید؛ دوم، از نقاطی که روی l' مشخص کرده‌اید و با فاصلهٔ یکسان از یکدیگر قرار دارند، خطوطی موازی l را رسم کنید. این دو دستگاه از خطوط یک مشبکه را شکل می‌دهند. نقاط حاصل از تلاقی این خطوط، نقاط مشبکه نامیده می‌شوند و همهٔ چنین نقاطی با هم یک مشبکهٔ نقطه‌ای است.

ما چه ساخته‌ایم؟ همچنان که شکل ۲.۷ نشان می‌دهد، ما صفحه را به تعداد نامتناهی متوازی‌الاضلاع تقسیم کرده‌ایم، همهٔ آنها همنهشت با متوازی‌الاضلاع $OPRQ$ و در وضعیتی شبیه آن هستند. گفته می‌شود که چنین مشبکه‌ای بر پایهٔ سه نقطهٔ O، P و Q بنا نهاده شده است. درواقع، دقیق‌تر این

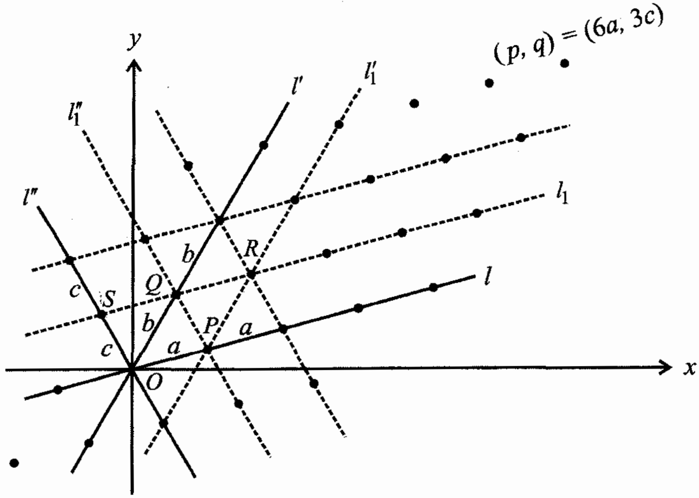


شکل ۲.۷ ساختن یک مشبکهٔ نقطه‌ای.

است که این مشبکه بر پایهٔ دو پاره‌خط جهت‌دار (یا بردار) $\overrightarrow{OP}$ و $\overrightarrow{OQ}$ بنا نهاده شده است، چرا که فقط با داشتن این دو پاره‌خط جهت‌دار هم می‌توان مشبکه را ساخت.

وقتی مشبکه‌ای بر پایهٔ سه نقطهٔ O، P و Q باشد، $OPRQ$ را متوازی‌الاضلاع اصلی مشبکه می‌گوییم. متوازی‌الاضلاعی که رئوس آن نقاط مشبکه هستند ولی هیچ نقطهٔ مشبکه دیگری روی مرز یا درون آن نیست، متوازی‌الاضلاع اولیه می‌نامیم. برای مثال، در شکل ۲.۷، $OPRQ$ اولیه است.

توجه به این واقعیت مهم است که دو مشبکهٔ کاملاً متفاوت می‌توانند مشبکهٔ نقطه‌ای یکسانی تولید کنند. برای مثال، در شکل ۳.۷، مشبکه‌ای که بر پایهٔ $\overrightarrow{OP}$ و $\overrightarrow{OS}$ قرار دارد، همان دستگاه از نقاط مشبکه را تولید می‌کند که مشبکه‌ای که بر پایهٔ $\overrightarrow{OP}$ و $\overrightarrow{OQ}$ قرار دارد. دو مشبکه‌ای که نقاط مشبکه‌ای یکسانی تولید می‌کنند، هم‌ارز می‌گوییم.



شکل ۳.۷ مشبکه‌های نقطه‌ای هم‌ارز.

۳.۷ خواص مشبکهٔ اصلی Λ

اکنون وقت بیان چند اصطلاح کلیدی است. مشبکهٔ نقطه‌ای اصلی Λ بر پایهٔ سه نقطهٔ $O : (0, 0)$، $P : (1, 0)$ و $Q : (0, 1)$ قرار دارد. متوازی‌الاضلاع اصلی آن، مربع واحد $OPRQ$، اولیه است. نقاط مشبکهٔ Λ، (p, q)، دارای مختصات صحیح هستند.

اکنون، فرض کنید (p, q)، نقطهٔ مشبکهٔ دلخواهی از Λ باشد. می‌توانیم روی (p, q)، تبدیل T را اعمال کنیم:

$$T: \quad \begin{aligned} p' &= ap + bq \\ q' &= cp + dq \end{aligned} \qquad \Delta = ad - bc \neq \circ \tag{۱.۷}$$

a، b، c و d اعداد صحیح داده شده هستند. هر نقطه مشبکه از Λ به (p', q')، نقطه‌ای مشبکه از Λ' تبدیل می‌شود، چون p' و q'، هر دو آشکارا صحیح هستند. به عبارت دیگر، نقاط مشبکهٔ Λ' نقاط Λ هستند.

این تبدیل خطی، سؤال جالب زیر را به همراه دارد:

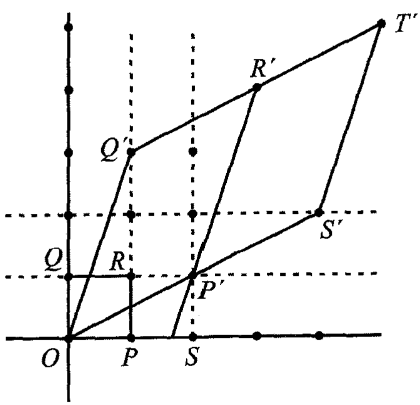
> آیا نقاط مشبکهٔ Λ'، به ترتیبی، همان نقاط مشبکهٔ Λ هستند، یا Λ' زیرمجموعه‌ای از نقاط Λ است؟

برای مثال، فرض کنید که نقاط مشبکهٔ Λ تحت تبدیل زیر قرار بگیرند:

$$T_۲: \quad \begin{aligned} p' &= ۲p + q \\ q' &= p + ۳q \end{aligned} \qquad \Delta = (۲ \cdot ۳) - (۱ \cdot ۱) = ۶ - ۱ = ۵$$

با نگاه به شکل ۴.۷، متوجهٔ ظهور یک مشبکهٔ جدید می‌شویم:

$$\begin{aligned} O &:(\circ, \circ) \to O' : (\circ, \circ) = \circ : (\circ, \circ) \\ P &:(۱, \circ) \to P' : (۲, ۱) \\ R &:(۱, ۱) \to R' : (۳, ۴) \\ Q &:(\circ, ۱) \to Q' : (۱, ۳) \end{aligned}$$

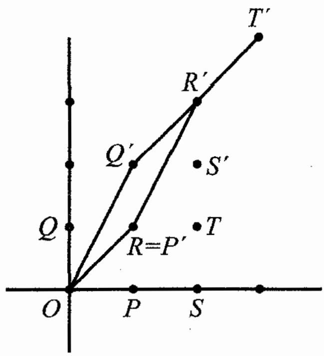


شکل ۴.۷ تبدیل Λ به زیرمجموعهٔ Λ'.

بنابراین، مشبکهٔ Λ که بر پایهٔ $\overrightarrow{OP}$ و $\overrightarrow{OQ}$ بود تبدیل به مشبکه جدید Λ' می‌شود که بر پایهٔ $\overrightarrow{OP'}$ و $\overrightarrow{OQ'}$ است و همهٔ نقاط آن همچنان نقاط Λ هستند. برای مثال، متوازی‌الاضلاع اولیهٔ $OPRQ$ تبدیل می‌شود به متوازی‌الاضلاع غیر اولیهٔ $OP'R'Q'$ از Λ'. مربع مجاور، $PSP'R$ از Λ، تبدیل می‌شود به متوازی‌الاضلاع مجاور، $P'S'T'R'$ از Λ'، و به همین ترتیب. اگرچه همهٔ نقاط مشبکهٔ Λ' نقاطی از Λ هستند، بعضی از نقاط Λ، نقاط Λ' نیستند. بنابراین Λ' یک زیرمجموعهٔ Λ است.

اکنون مثال دیگری از یک تبدیل با نتیجه‌ای متفاوت با قبل داریم. با ارجاع به شکل ۵.۷، تبدیل زیر را در نظر بگیرید:

$$T_۳: \quad \begin{aligned} p' &= p + q \\ q' &= p + ۲q \end{aligned} \qquad \Delta = (۱ \cdot ۲) - (۱ \cdot ۱) = ۲ - ۱ = ۱$$



شکل ۵.۷ Λ' و Λ هم‌ارز هستند.

مشاهده کنید که

$$\begin{aligned} O &:(۰, ۰ \to O' : (۰, ۰) = O : (۰, ۰) \\ P &:(۱, ۰) \to P' : (۱, ۱) = R : (۱, ۱) \\ R &:(۱, ۱) \to R' : (۲, ۳) \\ Q &:(۰, ۱) \to Q' : (۱, ۲) \end{aligned}$$

در اینجا چه اتفاقی می‌افتد؟ این بار، متوازی‌الاضلاع اولیهٔ $OPRQ$ به متوازی‌الاضلاع اولیهٔ $ORR'Q'$، و مربع‌های مجاور به متوازی‌الاضلاع‌های مجاور تبدیل می‌شوند. نقاط مشبکهٔ Λ'، نقاط مشبکهٔ Λ

را دوباره تولید می‌کنند، بنابراین همهٔ نقاط Λ هم‌زمان نقاط Λ' نیز هستند. می‌توان گفت، تحت $T_۳$، مشبکه Λ «به توی خودش» تبدیل یافته است. به عبارت دیگر، Λ' با Λ هم‌ارز است.

این دو نتیجهٔ متفاوت، سؤال جدیدی را ایجاد می‌کنند:

چرا یک تبدیل خطی، Λ را به توی خودش تبدیل می‌کند در حالی که تبدیل خطی دیگر چنین نمی‌کند؟

احتمالاً شما تاکنون حدس زده‌اید که جواب به نوعی به دترمینان مربوط است، به‌ویژه به اینکه آیا $|\Delta|$ برابر است با ۱ یا نه.

برای بررسی نقش دترمینان، دوباره نگاهی به تبدیل (۱.۷) می‌کنیم:

$$T: \quad \begin{aligned} p' &= ap + bq \\ q' &= cp + dq \end{aligned} \qquad \Delta \neq ۰$$

a، b، c و d صحیح هستند. می‌دانیم که هر نقطهٔ (p, q) از Λ تبدیل به نقطه (p', q') از Λ می‌شود. با محاسبهٔ p و q برحسب p' و q'، تبدیل معکوس را به‌دست می‌آوریم:

$$T^{-۱}: \quad \begin{aligned} p &= \frac{dp' - bq'}{\Delta} \\ q &= \frac{aq' - cp'}{\Delta} \end{aligned} \tag{۲.۷}$$

با قرار دادن $\Delta = ad - bc = \pm ۱$ در (۲.۷)، داریم:

$$T^{-۱}: \quad \begin{aligned} p &= \pm(dp' - bq') \\ q &= \pm(aq' - cp') \end{aligned}$$

این تضمین می‌کند که همهٔ مقادیر صحیح p' و q' منجر به مقادیر صحیح برای p و q خواهند شد. بنابراین هر نقطهٔ مشبکه: (p', q')، متناظر است با یک نقطهٔ مشبکه از Λ: (p, q)؛ بنابراین، Λ به‌توی خودش تبدیل می‌گردد.

اجازه دهید کمی دقیق‌تر به شرایط مطلوب برای تبدیل Λ به توی خودش نگاه کنیم. به‌ویژه، درمورد دترمینان داریم:

برای اینکه تبدیل T، Λ را به یک مشبکهٔ هم‌ارز تبدیل کند، مطلقاً لازم است که $\Delta = ab - bc = \pm ۱$.

فرض کنید که ما فقط می‌دانیم که $\Delta \neq ۰$ و تبدیل T در (۱.۷)، Λ را به توی خودش تبدیل می‌کند. این یعنی، نه‌تنها نگاشت T همهٔ نقاط مشبکه را به نقاط مشبکه می‌نگارد، بلکه هر نقطهٔ مشبکه از Λ' تصویر نقطهٔ مشبکه‌ای از Λ تحت T است. به عبارت دیگر، $T^{-۱}$، تبدیل معکوس داده شده در (۲.۷)، هر نقطهٔ مشبکهٔ (p', q') از Λ' را به نقطهٔ مشبکه‌ای از Λ می‌نگارد. برای مثال، $T^{-۱}$ نقطهٔ $(p', q') = (۱, ۰)$ از Λ' را به نقطهٔ مشبکه‌ای (p, q) از Λ می‌نگارد.

از این هم‌ارزی نتیجه می‌شود که مقادیر حاصل از (۲.۷) به‌ازای $q' = ۰$ و $p' = ۱$ باید صحیح باشد. این یعنی، هر دو مقدار زیر صحیح هستند:

$$p = \frac{dp' - bq'}{\Delta} = \frac{(d \cdot ۱) - (b \cdot ۰)}{\Delta} = \frac{d}{\Delta}$$

و

$$q = \frac{aq' - cp'}{\Delta} = \frac{(a \cdot ۰) - (c \cdot ۱)}{\Delta} = -\frac{c}{\Delta}$$

می‌توان این حکم را با استفاده از نماد مربوط به بخش‌پذیری به این صورت نوشت: $\Delta \mid d$ و $\Delta \mid c$. علاوه بر این، $T^{-۱}$ باید نقطهٔ $(p', q') = (۰, ۱)$ از Λ' را به نقطهٔ مشبکه‌ای (p, q) از Λ تبدیل کند. پس به‌طور مشابه داریم: $\Delta \mid b$ و $\Delta \mid a$.

به این ترتیب، Δ هر یک از اعداد صحیح a، b، c و d را می‌شمارد. پس، $\Delta^۲ \mid ad$ و $\Delta^۲ \mid bc$، بنابراین

$$\Delta^۲ \mid ad - bc = \Delta$$

یا $\Delta^۲ \mid \Delta$. با این حساب، $\frac{۱}{\Delta} = \frac{\Delta}{\Delta^۲}$ عددی صحیح است. پس لزوماً داریم: $\Delta = \pm ۱$.

ما هم‌اکنون قضیهٔ زیر را اثبات کردیم.

قضیهٔ ۱.۷ اعداد صحیح a، b، c و d را در نظر بگیرید. شرط لازم و کافی برای اینکه تبدیل T: $p' = ap + bq$ و $q' = cp + dq$، Λ را به توی خودش تبدیل کند این است که $\Delta = ad - bc = \pm ۱$.

با توجه به مساحت‌ها تحت تبدیل، می‌توان قضیهٔ ۱.۷ را از زاویهٔ دیگری نگاه کرد. مشبکهٔ نقطه‌ای Λ' را در نظر بگیرید که بر پایهٔ سه نقطهٔ غیر هم‌خط $O : (۰, ۰)$ و $P' : (a, c)$ و $Q' : (b, d)$ از Λ قرار دارد؛ به شکل‌های ۴.۷ و ۵.۷ نگاه کنید. همهٔ نقاط مشبکه (p', q') از Λ' توسط معادلات زیر به‌دست می‌آیند:

$$p' = pa + qb$$
$$q' = pc + qd \qquad (۳.۷)$$

p و q می‌توانند هر عدد صحیح دلخواهی باشند. ضمناً، خواننده‌های آشنا با بردارها مشاهده خواهند کرد که معادله‌های (۳.۷) را می‌توان تنها با یک معادلهٔ برداری نمایش داد:

$$(p', q') = p(a, c) + q(b, d)$$

این معادله، همهٔ ترکیب‌های خطی با ضرایب صحیح را برای دو بردار مستقل خطی (a, c) و (b, d) به‌دست می‌دهد.

اکنون به کمک شکل ۴.۷ نشان می‌دهیم که مساحت چگونه تحت تبدیل خطی تغییر می‌کند. برای باز تولید همهٔ نقاط مشبکهٔ Λ'، نقاط $(۰, ۰)$: O، $(۲, ۱)$: P' و $(۱, ۳)$: Q' را به‌عنوان پایه در نظر می‌گیریم و معادله‌های زیر را اعمال می‌کنیم:

$$\begin{aligned} p' &= ۲p + q \\ q' &= p + ۳q \end{aligned} \qquad \Delta = (۲ \cdot ۳) - (۱ \cdot ۱) = ۵$$

به ترتیب فرض کنید:

$$(p, q) = (۱, ۱), (۲, ۰), (۲, ۱)$$

فوراً داریم:

$$(p', q') = (۳, ۴), (۴, ۲), (۵, ۵)$$

ـــ اینها، نقاط R'، S' و T' هستند.

مساحت متوازی‌الاضلاع $OP'R'Q'$ دو برابر مساحت مثلث $OP'Q'$ است:

$$OP'R'O' \text{ مساحت } = ۲ . \frac{۱}{۲} \begin{vmatrix} ۰ & ۰ & ۱ \\ a & b & ۱ \\ c & d & ۱ \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc = \Delta$$

از نقاط O، P' و Q' به همین ترتیب استفاده کردیم. اگر این فرمول را برای نقاط O، Q' و P' که در جهت عکس جهت‌دهی شده‌اند استفاده می‌کردیم، حاصل برابر بود با $(ad - bc)$. در هر صورت، مساحت برابر است با $|ad - bc|$.

با استفاده از این تفسیر می‌توان قضیهٔ ۱.۷ را به‌گونه‌ای دیگر دید:

قضیهٔ ۲.۷ شرط لازم و کافی برای اینکه مشبکهٔ Λ' بر پایهٔ $\overrightarrow{OP'}$ و $\overrightarrow{OQ'}$ با Λ هم‌ارز باشد این است که متوازی‌الاضلاع تعریف شده با $\overrightarrow{OP'}$ و $\overrightarrow{OQ'}$ دارای مساحت واحد باشد.

مجموعهٔ مسائل قسمت ۳.۷

۱. ثابت کنید که تبدیل T در (۱.۷) نمی‌تواند دو نقطهٔ متفاوت (p_1, q_1) و (p_2, q_2) از Λ را به تنها یک نقطهٔ (p', q') از Λ' تبدیل کند.

۲. دو تبدیل مثال بزنید که هر یک Λ را به توی خودش تبدیل می‌کند. برای هر یک طرحی همچون شکل ۴.۷ رسم کنید.

۳. آیا می‌توان متوازی‌الاضلاع $OPRQ$ را چنان ساخت که O، P، R و Q نقاط مشبکهٔ Λ باشند و در عین حال مساحت متوازی‌الاضلاع کمتر از ۱ باشد؟ توضیح دهید.

۴. مطالعه کنید: دربارهٔ «سری فیری» مطالعه کنید؛ فصل ۵، ابتکارهایی در ریاضیات، مؤلف: راس هانسبرگر، مترجم: سیامک کاظمی، ناشر: مرکز نشر دانشگاهی، ۱۳۷۱.

۴.۷ نقاط مشاهده شدنی

با نگاه از مبدأ $O : (\circ, \circ)$، نقطهٔ P از Λ را مشاهده شدنی گوییم در صورتی که هیچ نقطهٔ مشبکه‌ای از Λ مسیر دید ما را مسدود نکرده باشد؛ یعنی، هیچ نقطهٔ مشبکه‌ای از Λ روی پاره $\overline{OP}$، پاره‌خطی که O را به P وصل می‌کند، نباشد. در فصل ۱، شرط لازم و کافی را برای اینکه یک نقطه مشاهده شدنی باشد اثبات کردیم: نقطه $P : (p, q)$ از مبدأ $O : (\circ, \circ)$ مشاهده شدنی است اگر و تنها اگر p و q نسبت به هم اول باشند. همچنان که قضیهٔ زیر نشان می‌دهد، مفهوم نقاط مشاهده شدنی ایده‌های جدیدی را برای تعیین موقعیت نقاط مشبکه به همراه دارد:

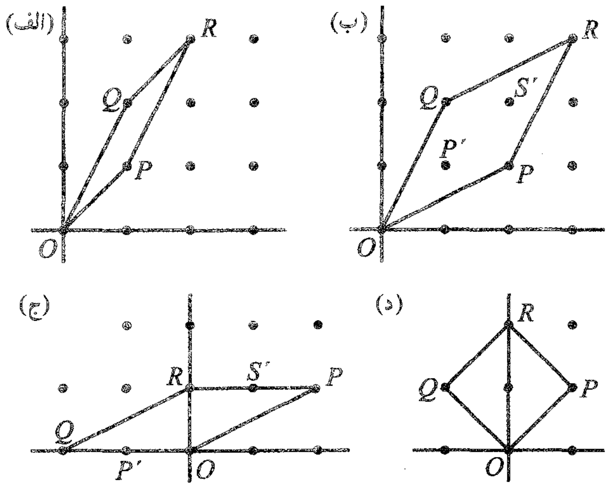
قضیهٔ ۳.۷ اگر P و Q دو نقطهٔ مشاهده شدنی Λ باشند، و اگر مساحت متوازی‌الاضلاع K بر پایهٔ $\overrightarrow{OP}$ و $\overrightarrow{OQ}$ برابر با δ باشد، آنگاه:

۱. اگر $\delta = ۱$، هیچ‌کدام از نقاط Λ درون K نیست؛

۲. اگر $\delta > ۱$، حداقل یک نقطه از Λ درون K است.

اثبات. (۱) فوراً از قضیهٔ ۲.۷ نتیجه می‌شود. فرض کنید، $\delta = ۱$ و یک نقطهٔ مشبکه از Λ درون K است. در این صورت، مشبکه Λ' بر پایهٔ $\overrightarrow{OP}$ و $\overrightarrow{OQ}$ هم‌ارز Λ نخواهد بود و این تناقض است با حکم قضیهٔ ۲.۷؛ شکل ۶.۷ الف، حالتی را نمایش می‌دهد که $\delta = ۱$.

برای اثبات (۲)، فرض می‌کنیم $\delta > ۱$، بنابراین Λ و Λ' هم‌ارز نیستند. در این صورت، متوازی‌الاضلاع اصلی K باید علاوه بر رئوسش شامل حداقل یک نقطهٔ مشبکه دیگر S' در درون



شکل ۶.۷ متوازی‌الاضلاع بر پایهٔ نقاط مشاهده شدنی P و Q. در (الف)، $\delta = 1$؛ در (ب)، (ج) و (د)، $\delta > 1$.

یا روی مرزش باشد. همچنان که شکل‌های ۶.۷ ب و ۶.۷ ج نشان می‌دهد تقارن Λ به این معنی است که عموماً K، علاوه بر S'، شامل P'، نقطهٔ مشبکهٔ دومی نیز هست، چون هر نقطهٔ S' در مثلث PQR دارای یک نقطهٔ متناظر P'، در مثلث همنهشت OPQ است. دو نقطهٔ S' و P' حتی می‌توانند در محل تلاقی OR و PQ، قطرهای K، منطبق باشند؛ به شکل ۶.۷ د نگاه کنید.

۸ تعبیرهای هندسی فرم‌های درجهٔ دوم

۱.۸ نمایش درجهٔ دوم

مطالعهٔ فرم‌های درجهٔ دوم با دو یا چند متغیر ما را با پیشرفته‌ترین قسمت‌های نظریهٔ اعداد درگیر خواهد کرد. تمام جلد سوم تاریخ نظریهٔ اعداد دیکسون [۶] به این موضوع اختصاص دارد ـــ و دیکسون این تاریخ را تا ۱۹۲۰ بیشتر دنبال نکرد! ژوزف لویی لاگرانژ (۱۸۱۳-۱۷۳۶)، برجسته‌ترین ریاضیدان قرن هیجدهم (او را تنها می‌توان با اویلر مقایسه کرد)، اولین کسی بود که ثابت کرد هر عدد صحیح مثبت را می‌توان به شکل مجموع حداکثر چهار مربع کامل نوشت (به بخش ۶.۸ نگاه کنید.) نظریهٔ لاگرانژ دربارهٔ فرم‌های درجهٔ دوم از سال ۱۷۷۳ شروع به توسعه کرد و بعداً توسط هم‌عصران جوان‌تر لاگرانژ، لژاندر و گاوس ساده‌تر شد و تعمیم یافت.

یک فرم درجهٔ دوم دوتایی چیست؟ آن عبارتی است به شکل

$$f(x,y) = ax^۲ + ۲bxy + cy^۲ \tag{۱.۸}$$

که در آن a، $۲b$ و c اعداد صحیح، x و y دو متغیر حقیقی هستند (به همین دلیل از صفت «دوتایی» استفاده شد). ما به رفتار فرم‌های درجه دومی علاقه‌مندیم که در آنها x و y اعداد صحیح هستند. مسئلهٔ کلاسیکی که به چنین فرم‌های درجه دومی مربوط می‌شود، مسئلهٔ نمایش است:

> برای یک فرم درجهٔ دوم مفروض، کدام اعداد صحیح n را می‌توان با $f(x,y)$ نمایش داد به شرطی که x و y نیز تنها مقادیر صحیح را بپذیرند؟

به‌عبارت دیگر:

> کدام اعداد صحیح n را می‌توان به فرم $n = ax^۲ + ۲bxy + cy^۲$ بیان کرد؟

هم‌اکنون جواب این سؤال برای تعداد زیادی از فرم‌های درجهٔ دوم خاص از قبیل $n = x^۲ + y^۲$، $n = x^۲ + ۲y^۲$ $n = x^۲ + ۳y^۲$ و ... معلوم است. اما هیچ نظریهٔ کلی وجود ندارد که به ما بگوید کدام اعداد صحیح را می‌توان به شکل یک فرم درجهٔ دوم دلخواه نمایش داد.

با وجود این، پاسخ بسیاری از سؤال‌ها مربوط به فرم‌های درجهٔ دوم دست‌یافتنی است. یکی از این سؤال‌ها را می‌توان به هندسهٔ اعداد ربط داد و برای حل آن قضیهٔ بنیادی مینکوفسکی را به بازی گرفت. سؤال این است:

> کوچک‌ترین عدد M که نامساوی $|f(x,y)| \geq M$ برای همهٔ مقادیر صحیح x، y برقرار است چیست؟

اگر ما واقعاً بتوانیم M را پیدا کنیم می‌توانیم بگوییم که کران پایین یا مینیمم $|f(x,y)|$ را پیدا کرده‌ایم. معمولاً پیدا کردن دقیق M پروژه‌ای بلندپروازانه محسوب می‌شود. در چنین حالت‌هایی سعی خواهیم کرد که یک کران بالای غیربدیهی برای M پیدا کنیم.

در این فصل ما فقط به یک نوع از فرم‌های درجهٔ دوم توجه می‌کنیم، فرم‌هایی که برای آنها $f(x,y) \geq ۰$. (توجه کنید که $f(۰,۰) = ۰$.) چنین فرمی، یک فرم درجهٔ دوم معین مثبت نامیده می‌شود. برای اطمینان از مثبت بودن همهٔ مقادیر غیرصفر باید روی (۱.۸) شرط بگذاریم. به‌ویژه، باید مبیّن عبارت زیر مثبت باشد؛ یعنی $d = ac - b^۲ > ۰$.

$$f(x,y) = ax^۲ + ۲bxy + cy^۲ \tag{۲.۸}$$

در اینجا، $a > ۰$، b و c، اعداد صحیح هستند. مثبت بودن مبیّن، مجموعه مقادیری را که فرم اتخاذ خواهد کرد محدود می‌کند. توجه کنید که ما از ابتدا فرض کردیم که $a > ۰$، بنابراین باید همچنین داشته باشیم که $c > ۰$. اکنون $f(x,y)$ را در a ضرب و سپس مربع را کامل می‌کنیم:

$$af(x,y) = (ax + by)^۲ + (ac - b^۲)y^۲$$

چون $d = ac - b^۲ > ۰$، عبارت سمت راست برای همهٔ مقادیر صحیح x و y، بجز $(۰,۰)$، مثبت است. بنابراین، مشاهده می‌کنیم که چنین فرمی تنها می‌تواند ۰ یا اعداد مثبت را نمایش دهد.

۲.۸ یک کران بالا برای مینیمم مقدار مثبت

چگونه مینیمم یا کران پایین یک فرم درجهٔ دوم معین مثبت را پیدا کنیم؟ اجازه دهید مروری مختصر بر تکنیک‌هایی داشته باشیم که به ما امکان استفاده از ایده‌های هندسی مینکوفسکی را خواهند داد.

دوباره به فرم درجهٔ دوم (۲.۸) نگاه کنید. آیا می‌بینید که ما می‌توانیم (۲.۸) را به‌صورت یک ترکیب خطی از مربع‌های دو فرم خطی بنویسیم؟ با اضافه و کم کردن جملهٔ $\left(\frac{b^2}{a}\right) y^2$ و سپس با جایگزین کردن مبیّن d، داریم:

$$\begin{aligned} f(x,y) &= ax^2 + 2bxy + \frac{b^2}{a}y^2 + cy^2 - \frac{b^2}{a}y^2 \\ &= a\left(x^2 + \frac{2b}{a}xy + \frac{b^2}{a^2}y^2\right) + \left(\frac{ac-b^2}{a}\right)y^2 \qquad (۳.۸) \\ &= a\left(x + \frac{b}{a}y\right)^2 + \frac{d}{a}y^2 \end{aligned}$$

درواقع، می‌توان به تعداد نامتناهی روش، $f(x,y)$ را به شکل ترکیبی خطی از مربعات دو فرم خطی نوشت. برای این کار، ابتدا یک تبدیل خطی دلخواه را روی $f(x,y)$ اعمال می‌کنیم:

$$\begin{aligned} x &= \alpha x_1 + \beta y_1 \\ y &= \gamma x_1 + \delta y_1 \qquad (۴.۸) \end{aligned}$$

α، β، γ و δ صحیح هستند و $\Delta = \alpha\delta - \beta\gamma = \pm 1$. این تبدیل خطی $f(x,y)$ را به فرم زیر تبدیل می‌کند:

$$g(x_1,y_1) = a_1x_1^2 + 2b_1x_1y_1 + c_1y_1^2$$

در اینجا،

$$\begin{aligned} a_1 &= a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \\ b_1 &= (a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta) \\ c_1 &= a\beta^2 + 2b\beta\delta + c\delta^2 \end{aligned}$$

دوباره، می‌توانیم مربع‌ها را کامل کنیم و $g(x_1,y_1)$ را به فرم (۳.۸) بنویسیم.

اکنون ادعا می‌کنیم که $f(x,y)$ و $g(x_1,y_1)$ اساساً یکی هستند، به این معنی که هر دوی آنها دقیقاً مجموعهٔ یکسانی از اعداد صحیح را نمایش می‌دهند. درواقع، فرض کنید برای زوجی از اعداد صحیح (p,q)، داریم $f(p,q) = n$؛ این یعنی:

$$n = f(p,q) = ap^2 + 2bpq + cq^2$$

سپس، با حل دستگاه معادلات (۴.۸) برای x_1 و y_1، می‌بینیم که

$$\begin{aligned} x_1 &= \frac{1}{\Delta}(\delta x - \beta y) = (\pm 1)(\delta p - \beta q) = p_1 \\ y_1 &= \frac{1}{\Delta}(-\gamma x + \alpha y) = (\pm 1)(-\gamma p + \alpha q) = q_1 \end{aligned}$$

صحیح هستند، و مهم‌تر اینکه، $g(p_1, q_1) = n$.

به یاد آورید که می‌توانیم قضیهٔ بنیادی مینکوفسکی را برای یک Mـ مجموعه به مرکز مبدأ و با مساحت بزرگ‌تر از یا مساوی با ۴ به‌کار ببریم و علاوه‌بر مبدأ وجود نقاط مشبکهٔ دیگری را روی مرز یا درون مجموعه تضمین کنیم. بنابراین، مایلیم مسئلهٔ جبری خود را که همان پیدا کردن مینیمم مقدار مثبت حاصل از یک فرم درجهٔ دوم با مبیّن مثبت است را به‌طور هندسی تعبیر کنیم. این یعنی، مایلیم، Mـ مجموعهٔ مربوطی را پیدا کنیم که در شرایط قضیهٔ بنیادی مینکوفسکی صدق می‌کند.

برای شروع، با در دست داشتن شرط لازم و کافی $d > 0$، می‌دانیم که همهٔ مقادیر غیرصفر $f(x,y) = n$ اعداد صحیح مثبت هستند، بنابراین می‌توان آنها را به شکل مربع اعداد حقیقی نوشت. پس،

$$f(x,y) = a\left(x + \frac{b}{a}y\right)^2 + \frac{d}{a}y^2 = s^2 \tag{۵.۸}$$

چون $f(-x,-y) = f(x,y) = s^2$، بیضی معرفی شده در (۵.۸) نسبت به مبدأ متقارن است؛ بنابراین، یک Mـ مجموعه است. اکنون می‌خواهیم مساحت آن را محاسبه کنیم. با استفاده از تبدیل

$$\begin{aligned} X &= x + \frac{b}{a}y \\ Y &= y \end{aligned} \tag{۶.۸}$$

(۵.۸) به شکل زیر درمی‌آید:

$$aX^2 + \left(\frac{d}{a}\right)Y^2 = s^2,$$

یا

$$\frac{X^2}{\frac{s^2}{a}} + \frac{Y^2}{\frac{s^2 a}{d}} = 1$$

این معادلهٔ یک بیضی به مرکز مبدأ مختصات در صفحه XY است که قطرهای آن منطبق بر محور Xها و محور Yها است. درواقع، این بیضی نیز یک Mـ مجموعه است و چون دترمینان تبدیل (۶.۸) برابر است با ۱، مساحت آن با مساحت بیضی دوران‌یافتهٔ (۵.۸) در صفحهٔ xy برابر است.

اکنون لم زیر را برای مساحت بیضی اثبات می‌کنیم.

لم ۱.۸ فرض کنید که معادلهٔ بیضی داده‌شدهٔ E، $\left(\frac{X^2}{M^2}\right) + \left(\frac{Y^2}{N^2}\right) = 1$ باشد. در این‌صورت، مساحت E از فرمول $A_E = \pi MN$ به‌دست می‌آید.

اثبات. تبدیل خطی داده‌شده با $X_۱ = \left(\frac{t}{M}\right) X$ و $Y_۱ = \left(\frac{t}{N}\right) Y$ را در نظر بگیرید. تحت این تغییر متغیر، معادلهٔ بیضی به معادلهٔ دایره تبدیل می‌شود:

$$C : X_۱^۲ + Y_۱^۲ = t^۲$$

مساحت این دایره برابر است با $A_C = \pi t^۲$. از طرف دیگر، دترمینان تبدیل برابر است با $\frac{t^۲}{MN}$، بنابراین اگر از اول t را چنان انتخاب کنیم که $t^۲ = MN$، دترمینان تبدیل برابر با ۱ و مساحت بیضی و دایره با هم برابر خواهد بود. این ادعای لم را اثبات می‌کند.

اکنون می‌بینیم که تحت تبدیل خطی (۶.۸)، فرم درجهٔ دوم $f(x, y) = s^۲$ به یک بیضی با مساحت

$$A = \pi \left(\frac{s}{\sqrt{a}}\right) \left(\frac{s\sqrt{a}}{\sqrt{d}}\right) = \frac{\pi s^۲}{\sqrt{d}}$$

تبدیل می‌شود و به این ترتیب، Mـ مجموعه‌ای با همان مساحت مشخص می‌شود.

اکنون، می‌توانیم قضیهٔ بنیادی مینکوفسکی را به‌کار بگیریم. فرض کنید که مساحت بیضی (۵.۸) را برابر با ۴ قرار دهیم؛ این یعنی،

$$s^۲ = \frac{۴}{\pi}\sqrt{d} \qquad \text{یا} \qquad \frac{\pi s^۲}{\sqrt{d}} = ۴$$

بنابراین، حداقل یک نقطهٔ مشبکهٔ $(x, y) = (p, q) \neq (۰, ۰)$ در درون یا روی $f(x, y) = s^۲$ چنان وجود دارد که

$$ap^۲ + ۲bpq + cq^۲ \leq s^۲ = \frac{۴}{\pi}\sqrt{d}$$

قضیهٔ زیر این نتیجه را جمع‌بندی می‌کند.

قضیهٔ ۱.۸ اگر $a > ۰$ و $d = ac - b^۲ > ۰$، آنگاه حداقل یک زوج از اعداد صحیح p و q، که هر دو صفر نیستند، چنان وجود دارد که:

$$f(p, q) = ap^۲ + ۲bpq + cq^۲ \leq \frac{۴}{\pi}\sqrt{d}$$

۳.۸ یک کران بالای بهتر

ثابت $M_۱ = \left(\frac{۴}{\pi}\right)\sqrt{d}$ در قضیهٔ ۱.۸ بهترین کران بالای ممکن برای مقدار مینیمم مطلوب M، نیست. اگرچه روش هندسی مینکوفسکی بسیار مؤثر است، از آن نمی‌توان برای پیدا کردن کوچک‌ترین

مقدار مجاز $M_{۱}$ استفاده کرد. برای بهبود $M_{۱}$، ما از روش جبری کورکین و زولوتارف [۱۵]، دو ریاضیدان برجستهٔ روس در قرن نوزدهم، استفاده می‌کنیم. برای بررسی عمیق‌تر کار آنها نگاه کنید به [۱۳، فصل ۲].

فرض کنید $(\mathbb{X}, \mathbb{Y}) = (p, q)$ نقطهٔ مشبکه‌ای باشد که کمترین مقدار عددی فرم درجه دوم معین مثبت زیر را به‌دست می‌دهد:

$$f(\mathbb{X}, \mathbb{Y}) = A\mathbb{X}^{۲} + ۲B\mathbb{X}\mathbb{Y} + C\mathbb{Y}^{۲} \qquad (۷.۸)$$

در اینجا، $A > ۰$ و $d_{۱} = AC - B^{۲} > ۰$. آشکارا، p و q باید نسبت به هم اول باشند، چرا که اگر $\gcd(p, q) = s > ۱$، آنگاه $p = sp_{۱}$ و $q = sq_{۱}$، که در این‌صورت

$$f(p, q) = s^{۲} f(p_{۱}, q_{۱})$$

این یعنی، مقدار عددی $f(p_{۱}, q_{۱})$ کمتر از $f(p, q)$ است.

اگر $\gcd(p, q) = ۱$، دو عدد صحیح m و n چنان وجود دارند که $pm + qn = ۱$. بنابراین تبدیل خطی

$$\mathbb{X} = px - ny$$

$$\mathbb{Y} = qx + my$$

دارای دترمینان $\Delta = pm + qn = ۱$ است و نقطهٔ مشبکهٔ $(\mathbb{X}, \mathbb{Y}) = (p, q)$ را به نقطهٔ مشبکه $(x, y) = (۱, ۰)$ تبدیل می‌کند. فرم درجهٔ دوم (۷.۸) تبدیل می‌شود به فرم درجهٔ دوم

$$g(x, y) = ax^{۲} + ۲bxy + cy^{۲} \qquad (۸.۸)$$

که چون $\Delta = ۱$، همان مقادیری را به‌دست می‌دهد که $f(\mathbb{X}, \mathbb{Y})$.

اکنون (۸.۸) را به‌صورت زیر می‌نویسیم:

$$\begin{aligned} g(x, y) &= a\left(x^{۲} + ۲\frac{b}{a}xy + \frac{c}{a}y^{۲}\right) \\ &= a\left[(x + b'y)^{۲} + (c' - b'^{۲})y^{۲}\right], \qquad b' = \frac{b}{a}, c' = \frac{c}{a} \end{aligned}$$

چون $f(p, q)$ مینیمال است، $g(۱, ۰) = a$ دقیقاً همان مینیمال است. بنابراین، بجز در $(۰, ۰)$ برای همه نقاط مشبکه مقدار عددی $g(x, y)$ بزرگ‌تر از یا مساوی با $a > ۰$ است.

فرض کنید $|b'| \geq \frac{۱}{۲}$ و K نزدیک‌ترین عدد صحیح به b' باشد. قرار می‌دهیم $\epsilon = k - b'$؛ بنابراین $\frac{۱}{۲} \leq |\epsilon| = |k - b'|$. اکنون تبدیل خطی دیگری را اعمال می‌کنیم:

$$x = x' - ky'$$

$$y = y'$$

دترمینان این تبدیل خطی نیز برابر با ۱ است. این $g(x, y)$ را، برای همهٔ نقاط مشبکهٔ (x', y')، به فرم $Q(x', y')$ تبدیل می‌کند:

$$\begin{aligned} Q(x', y') &= a\left[(x' - ky' + b'y')^۲ + (c' - b'^۲)y'^۲\right] \\ &= a\left[(x' - \epsilon y')^۲ + (c' - b'^۲)y'^۲\right] \geq a \end{aligned}$$

اجازه دهید نقطهٔ مشبکهٔ $(x', y') = (۰, ۱)$ را امتحان کنیم. فوری می‌بینیم که:

$$Q(۰, ۱) = a\left[\epsilon^۲ + (c' - b'^۲)\right] = a\epsilon^۲ + a(c' - b'^۲) \geq a$$

که در آن

$$a(c' - b'^۲) \geq a - a\epsilon^۲ = a(۱ - \epsilon^۲)$$

یا

$$a\left(\frac{c}{a} - \frac{b^۲}{a^۲}\right) = \frac{ac - b^۲}{a} = \frac{d}{a} \geq a(۱ - \epsilon^۲)$$

مقدار مبیّن d چیست؟ داریم

$$\epsilon = k - b' = k - \frac{b}{a} \quad \text{و} \quad \epsilon^۲ = \left(k - \frac{b}{a}\right)^۲ \leq \frac{۱}{۴}$$

این نتیجه می‌دهد که

$$a(۱ - \epsilon^۲) = a\left[۱ - \left(k - \frac{b}{a}\right)^۲\right] \geq \frac{۳}{۴}a$$

در نتیجه، برای مقدار مبیّن داریم:

$$d \geq \frac{۳}{۴}a^۲ \quad \text{یا} \quad a \leq \frac{۲}{\sqrt{۳}}\sqrt{d}$$

از آنجایی که مینیمم مطلق $g(x, y)$ برابر با a است، داریم

$$M_۲ = \frac{a}{\sqrt{d}} \leq \frac{۲}{\sqrt{۳}} \quad \text{یا} \quad a = M_۲\sqrt{d}$$

اما به‌یاد آورید که مینیمم فرم خاص $x^۲+xy+y^۲$ برابر با ۱ است؛ در اینجا، $b=\frac{۱}{۲}$ و $d=\frac{۳}{۴}$. از طرفی $M_۲\sqrt{\frac{۳}{۴}}\leq ۱ = a$ نمی‌تواند برقرار باشد مگر اینکه $M_۲\geq\sqrt{\frac{۴}{۳}}$. بنابراین، باید داشته باشیم $M_۲=\frac{۲}{\sqrt{۳}}$.

حتی در حالتی که $|b'|<\frac{۱}{۲}$ و $k=۰$ باشد نیز به همین نتیجه می‌رسیم. به این ترتیب، قضیهٔ بعدی را اثبات کرده‌ایم و قضیهٔ ۱.۸ را بهبود بخشیده‌ایم.

قضیهٔ ۲.۸ فرض کنید $f(x,y)=ax^۲+۲bxy+cy^۲$ یک فرم درجهٔ دوم معین مثبت است که در آن، $a>۰$ و $d=ac-b^۲>۰$. در این‌صورت، اعداد صحیح p و q، که حداقل یکی از آنها صفر نیست، چنان وجود دارند که

$$|f(p,q)|=f(p,q)\leq\frac{۲}{\sqrt{۳}}\sqrt{d}$$

مثال. فرم درجهٔ دوم

$$f(x,y)=۲۵x^۲+۱۲۶xy+۱۶۲y^۲$$

باید دارای مقدار مینیممی باشد

$$\leq\frac{۲}{\sqrt{۳}}\sqrt{(۲۵)(۱۶۲)-(۶۳)^۲}=۱۰{,}۳۹\ldots$$

چون ضرایب در $f(x,y)$ صحیح هستند، مینیمم کمتر از یا برابر با ۱۰ است.

۴.۸ (اختیاری) کران برای مینیمم‌های فرم‌های درجهٔ دوم با بیش از دو متغیر

مطالب این بخش برای خوانندگانی است که آشنایی بیشتری با فرم‌های درجهٔ دوم دارند. همهٔ مطالب بدون اثبات بیان می‌شوند ولی به منابع لازم برای پیگیری بیشتر ارجاع داده شده است. به هر حال نخواندن این بخش خللی در روند مطالعهٔ این کتاب وارد نخواهد کرد.

قسمت ۳.۸ روش‌های توسعه یافته توسط کورکین و زولوتارف برای پیدا کردن کران مینیمال غیرصفر یک فرم درجهٔ دوم معین مثبت با دو متغیر، یا فرم درجهٔ دوم معین مثبت دوتایی، را معرفی کرد. این دو ریاضیدان همچنین روش هوشمندانه‌ای را برای فرم‌هایی با بیش از دو متغیر خلق کردند؛ توصیف آنها از این روش، «توسعهٔ فرم درجهٔ دوم براساس مینیمم‌هایش» است.

فرض کنید X یک nـتایی است: $X = (x_۱, x_۲, \ldots, x_n)$. فرض کنید $Q(X) = Q(x_۱, x_۲, \ldots, x_n)$ یک فرم درجهٔ دوم معین مثبت با مبیّن $d > ۰$ است. ما مایل به پاسخ‌گویی به سؤال زیر هستیم که به تعبیری تعمیم کارهای قسمت‌های ۲.۸ و ۳.۸ است.

> برای $\epsilon > ۰$ دلخواه، کوچک‌ترین عدد حقیقی مثبت M_n که برای آن nـتایی غیرصفر $X \in \mathbb{Z}^n$ چنان وجود دارد که $Q(X) \leq M_n + \epsilon$ چیست؟

اگر فرم $Q(X)$ با مبیّن d، این کران پایین را اتخاذ کند، از مینیمم $Q(X)$ برای $X \neq (۰)$ صحبت خواهیم کرد. چون این عدد به شکل حاصل‌ضرب مقداری ثابت در توانی کسری از d است، عدد ثابت مذکور را با m_n نمایش می‌دهیم.

مینکوفسکی [۱۸] با استفاده از روش‌های هندسی ثابت کرد که اگر $Q(x)$ یک فرم درجهٔ دوم معین مثبت با n متغیر باشد، آنگاه nـتایی‌هایی از اعداد صحیح X چنان وجود دارد که

$$۰ < Q(X) \leq \frac{۴}{\pi}\left[\Gamma\left(۱+\frac{n}{۲}\right)\right]^{\frac{۲}{n}} d^{\frac{۱}{n}} = m_n d^{\frac{۱}{n}} = M_n$$

در اینجا $\Gamma(x)$، همان تابع گامای معروف است.

در ۱۹۱۴، بلیکفلت [۱] (از او در فصل ۹ بیشتر خواهیم شنید) با استفاده از روشی که به تازگی توسط خود او در هندسهٔ اعداد توسعه یافته بود، توانست نتیجهٔ زیر را جایگزین نتیجهٔ مینکوفسکی کند:

$$۰ < Q(X) \leq \frac{۲}{\pi}\left[\Gamma\left(۱+\frac{n+۲}{۲}\right)\right]^{\frac{۲}{n}} d^{\frac{۱}{n}} = M'_n d^{\frac{۱}{n}}$$

بزرگی این بهبود چقدر است؟ با نتیجهٔ مینکوفسکی، مقدار مجانبی m_n برابر است با $\frac{(۲n)}{(\pi e)}$؛ این یعنی، $m_n \to \frac{(۲n)}{(\pi e)}$ وقتی $n \to \infty$. به‌طور صوری، می‌نویسیم $m_n \sim \frac{(۲n)}{(\pi e)}$. اما با نتیجهٔ بلیکفلت، $m'_n \sim \frac{n}{(\pi e)}$ که نصف حد به‌دست آمده توسط مینکوفسکی است. مینکوفسکی همچنین ثابت کرد که مقدار مجانبی m_n نمی‌تواند کمتر از $\frac{n}{(۲\pi e)}$ باشد.

$m_۲$، کمترین مقدار برای $n = ۲$، اولین بار توسط ارمیت [۹] به‌دست آمد؛ گاوس [۷] نیز این مقدار را می‌دانست. برای $n = ۳, ۴, ۵$، مینیمم‌ها توسط کورکین و زولوتارف پیدا شد [۱۵, ۱۶, ۱۷]، و بالاخره، بلیکفلت [۲] مقادیر مینیمم را برای $n = ۶, ۷, ۸$ به‌دست آورد. این مینیمم‌ها عبارتند از:

$$m_۲ = \frac{۲}{\sqrt{۳}}, \quad m_۳ = \sqrt[۳]{۲}, \quad m_۴ = \sqrt{۲}, \quad m_۵ = \sqrt[۵]{۸}$$
$$m_۶ = \sqrt[۶]{\frac{۶۴}{۳}}, \quad m_۷ = \sqrt[۷]{۶۴}, \quad m_۸ = ۲$$

۵.۸ تقریب زدن با اعداد گویا

قضیه ۲.۸ را می‌توان برای مسألهٔ تقریب زدن اعداد گنگ به‌وسیلهٔ اعداد گویا استفاده کرد. درواقع، به آسانی می‌توان ثابت کرد که تعداد نامتناهی عدد گویای $\frac{m}{n}$، برای $n \neq ۰$، چنان وجود دارند که

$$\left|\alpha - \frac{m}{n}\right| \leq \frac{۲}{\sqrt{۳}n^۲}$$

در اینجا α می‌تواند هر عدد حقیقی دلخواهی باشد. درجهٔ تقریب متناسب است با $\frac{۱}{n^۲}$، پس نسبتاً تقریب خوبی محسوب می‌شود. برای جزییات بیشتر نگاه کنید به [۱۳، ص ۴۰].

اکنون عبارت (۵.۸) برای فرم درجهٔ دوم $f(x, y)$ را کمی تغییر می‌دهیم:

$$f(x,y) = \left(\sqrt{a}x + \frac{b}{\sqrt{a}}y\right)^۲ + \left(\sqrt{\frac{d}{a}}y\right)^۲$$

توجه کنید که در این عبارت جدید، ضرایب چندجمله‌ای‌های داخل پرانتزها گویا نیستند. اگرچه به محض اینکه چنین اجازه‌ای را به خود بدهیم خواهیم دید که هر فرم درجهٔ دومی را می‌توان به شکل مجموع مربعات دو عبارت خطی نوشت. با استفاده از این، برای عدد حقیقی α فرم درجهٔ دوم زیر را در نظر می‌گیریم:

$$\begin{aligned} Q(m,n) &= \left(\frac{\alpha n - m}{\epsilon}\right)^۲ + \epsilon^۲ n^۲ \\ &= \frac{۱}{\epsilon^۲}m^۲ - ۲\frac{\alpha}{\epsilon^۲}mn + \left(\frac{\alpha}{\epsilon^۲} + \epsilon^۲\right)n^۲ \end{aligned}$$

m و n اعداد صحیح، و مبیّن برابر است با

$$d = \frac{۱}{\epsilon^۲}\left(\frac{\alpha}{\epsilon^۲} + \epsilon^۲\right) - \frac{\alpha^۲}{\epsilon^۴} = ۱$$

ϵ عدد مثبت دلخواه است.

بنابر قضیهٔ ۲.۸، همواره می‌توان دو عدد صحیح m و n را که هر دو صفر نیستند، چنان پیدا کنیم که

$$\left(\frac{an - m}{\epsilon}\right)^۲ + \epsilon^۲ n^۲ \leq \frac{۲}{\sqrt{۳}}$$

دو نامساوی زیر نتیجه می‌شود:

$$\left|\alpha - \frac{m}{n}\right| \leq \frac{\epsilon}{|n|}\sqrt{\frac{۲}{\sqrt{۳}}} \qquad n > ۰ \qquad (۹.۸)$$

$$|n| \leq \frac{۱}{\epsilon}\sqrt{\frac{۲}{\sqrt{۳}}}$$

چون α گنگ است، $\circ = \left|\alpha - \left(\frac{m}{n}\right)\right|$ نمی‌تواند صفر باشد. بنابراین، باید تعداد نامتناهی اعداد گویای $\frac{m}{n}$، با $n > \circ$، در اولین نابرابری (۹.۸) صدق کنند. برای دیدن این، به سادگی می‌توان مقادیر کوچک‌تر و کوچک‌تری را به ϵ نسبت داد؛ برای هر مقدار ϵ، عدد گویایی وجود خواهد داشت. این کسرها نمی‌توانند همه با هم برابر باشند، چون وقتی $\epsilon \to \circ$، داریم $\left|\alpha - \left(\frac{m}{n}\right)\right| \to \circ$.

اگر با استفاده از نامساوی دوم (۹.۸)، ϵ را در نامساوی اول حذف کنیم، خواهیم داشت

$$\left|\alpha - \frac{m}{n}\right| \leq \frac{۲}{\sqrt{۳}n^۲} \quad n > \circ \tag{۱۰.۸}$$

بنابراین ثابت کردیم که تعداد نامتناهی کسر گویای $\frac{m}{n}$ وجود دارد که α را تقریب می‌زنند. دقت تقریب با مربع مخرج کسر نسبت معکوس دارد.

البته، این از نتیجه‌ای که «بهترین ممکن» باشد بسیار دور است. هرویتز [۱۴] ثابت کرد که برای هر عدد گنگ α، تعداد نامتناهی عدد گویای $\frac{m}{n}$ با $n > \circ$، چنان وجود دارند که

$$\left|\alpha - \frac{m}{n}\right| < \frac{۱}{\sqrt{۵}n^۲}$$

عدد $\sqrt{۵}$ بهترین ثابت ممکن است، به این معنی که اگر $\sqrt{۵}$ را با هر عدد بزرگ‌تری جایگزین کنیم قضیهٔ دیگر درست نخواهد بود. با مقایسهٔ ثابت‌ها، مشاهده می‌کنیم که $\frac{۱}{\sqrt{۵}} = ۰/۴۴۷۲\ldots$ از ثابت قبلی ما $\frac{۲}{\sqrt{۳}} = ۱/۱۴۱۵۵\ldots$ کوچک‌تر است. اگرچه با استفاده از (۱۰.۸) هم می‌توان تقریب‌های نسبتاً خوبی به‌دست آورد.

۶.۸ مجموع چهار مربع

در ۱۶۲۱، کلود باشه دو مزیریاک (۱۶۳۸-۱۵۸۱)، یکی از علاقه‌مندان پرشور کارهای دیوفانتوس، بدون اثبات بیان کرد که هر عدد صحیح مثبت n را می‌توان به شکل مجموع چهار مربع صحیح نوشت. یعنی، هر عدد صحیح مثبت n را می‌توان به‌صورت

$$n = x^۲ + y^۲ + z^۲ + w^۲$$

نوشت که در آن x، y، z و w صحیح هستند.

اثبات ادعای باشه چندان ساده نیست. فرما در یکی از حاشیه‌نویسی‌های معروفش بیان می‌کند که قضیه را اثبات کرده است؛ ادعای او می‌تواند حقیقت داشته باشد ولی ما هیچگاه نخواهیم فهمید. اویلر بزرگ و مبتکر در خلال سال‌های ۱۷۳۰ و ۱۷۵۰ چندین بار تلاش کرد قضیه را اثبات کند ولی

هر بار شکست خورد. وقتی بالاخره لاگرانژ در ۱۷۷۰ اولین اثبات قضیه را منتشر کرد، خود را مدیون کارهای پیشگامانهٔ اویلر می‌دانست. درواقع او وارث کرسی اویلر در آکادمی پروسی فردریک بزرگ در برلین هم بود [۵].

ما قضیهٔ لاگرانژ را بیان و اثبات می‌کنیم.

قضیهٔ ۳.۸ (قضیهٔ لاگرانژ) هر عدد صحیح مثبت را می‌توان به‌صورت مجموع مربعات چهار عدد صحیح نوشت.

ریاضیدانان بسیاری تلاش کردند که اثباتی از قضیهٔ لاگرانژ ارائه دهند. اثبات زیر متعلق است به داونپورت [۳]، اثبات او به نوعی شبیه اثبات گریس [۸] و اصلاح‌شدهٔ یکی از اثبات‌های ارمیت در ۱۸۵۳ [۱۰، ۱۱] است. همچنین نگاه کنید به [۱۲]. برخلاف داونپورت، ارمیت از قضیهٔ بنیادی مینکوفسکی استفاده نکرد (این قضیه در زمان او وجود نداشت)؛ ارمیت از نتایج خودش در مورد مینیمم فرم‌های درجهٔ دوم معین مثبت استفاده کرد.

داونپورت ادعا نکرد که اثبات او اثبات ایده‌آلی برای قضیه لاگرانژ است، اما به هر حال این اثبات کاملاً در راستای اهداف ما قرار دارد. این اثبات، نه‌تنها ساده و کم جزییات است، بلکه مثالی عالی برای نشان دادن این است که چگونه می‌توان از هندسهٔ اعداد برای اثبات نتیجه‌ای کاملاً حسابی استفاده کرد.

همهٔ اثبات‌های مستقیمی که از قضیه لاگرانژ ارائه می‌شوند نیازمند لم زیر هستند.

لم ۲.۸ برای هر عدد صحیح مثبت و فرد m، اعداد صحیح a و b چنان وجود دارند که $a^۲ + b^۲ + ۱ = mk$، که در آن k عددی صحیح است.

به‌طور خلاصه، $a^۲ + b^۲ + ۱$ بر m بخش‌پذیر است. آنهایی که با مفهوم و نماد همنهشتی آشنا هستند، می‌نویسند: $a^۲ + b^۲ + ۱ \equiv ۰ \pmod{m}$.

این لم را مفروض می‌گیریم چرا که اثبات آن ما را حسابی به دردسر می‌اندازد. اثبات آن نیازمند استفاده از «ماندهٔ درجهٔ دوم» در حالتی است که $m = p$، استفاده از استقراء روی ν برای حالتی که $m = p^\nu$ و ترکیبی از این نتایج برای m دلخواه است [۴].

اثبات قضیهٔ لاگرانژ. با تعریف چهار فرم خطی $\mathbb{X}$، $\mathbb{Y}$، $\mathbb{Z}$، $\mathbb{W}$ برحسب چهار متغیر x، y، z و w، شروع می‌کنیم:

$$\begin{aligned}
\mathbb{X} &= mx \qquad + az + bw \\
\mathbb{Y} &= \qquad my + bz - aw \\
\mathbb{Z} &= \qquad\qquad z \\
\mathbb{W} &= \qquad\qquad\quad w
\end{aligned}$$

دترمینان این فرم‌های خطی برابر است با

$$\Delta = \begin{vmatrix} m & 0 & a & b \\ 0 & m & b & -a \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} = m^2 \qquad (11.8)$$

محاسبهٔ این دترمینان بسیار ساده است زیرا «مثلثی» است و اعداد زیر قطر اصلی همگی صفر هستند. بنابراین حاصل آن برابر است با حاصل‌ضرب اعداد روی قطر: m، m، ۱ و ۱.

اکنون فرض کنید که x، y، z و w همهٔ مقادیر ۰، ۱$\pm$، ۲$\pm$، ... را اتخاذ کنند. نقاط متناظر، $(\mathbb{X}, \mathbb{Y}, \mathbb{Z}, \mathbb{W})$ها، یک مشبکه خواهند بود در فضای ۴ بعدی با دترمینان $\Delta = m^2$.

می‌خواهیم مجموع مربعات، $\mathbb{X}^2 + \mathbb{Y}^2 + \mathbb{Z}^2 + \mathbb{W}^2$ را محاسبه کنیم. اگر از برابری‌های (۱۱.۸) استفاده کنیم، یک محاسبهٔ ساده (اما کسالت‌آور) نشان می‌دهد که این مجموع برابر است با

$$m(mx^2 + my^2 - 2axy - 2ayw + 2bxy + 2byz) + \\ (a^2 + b^2 + 1)w^2 + (a^2 + b^2 + 1)y^2$$

اولین جملهٔ این عبارت بر m بخش‌پذیر است و با توجه به لم ۲.۸، دو جملهٔ بعدی نیز بر m بخش‌پذیرند. بنابراین برای همهٔ x، y، z و wها داریم

$$\mathbb{X}^2 + \mathbb{Y}^2 + \mathbb{Z}^2 + \mathbb{W}^2 = km \qquad (12.8)$$

k عدد صحیح مثبتی است.

فرض کنید که ثابت کرده‌ایم که علاوه‌بر ۰ نقطهٔ مشبکهٔ دیگری نیز وجود دارد که برای آن

$$\mathbb{X}^2 + \mathbb{Y}^2 + \mathbb{Z}^2 + \mathbb{W}^2 < 2m \qquad (13.8)$$

در این‌صورت، از (۱۲.۸) نتیجه می‌شد که اعداد صحیحی، که همگی صفر نیستند، چنان وجود دارند که

$$\mathbb{X}^2 + \mathbb{Y}^2 + \mathbb{Z}^2 + \mathbb{W}^2 = m$$

این قضیهٔ لاگرانژ را برای mهای فرد اثبات می‌کند؛ این همان کاری است که می‌خواهیم با سود جستن از نگاه هندسی مینکوفسکی انجام دهیم.

نامعادلهٔ (۱۳.۸) نمایش‌دهندهٔ یک کره با شعاع $\sqrt{۲m}$، در فضای ۴ـبعدی است. با استفاده از انتگرال‌گیری می‌توان نشان داد که حجم یک کرهٔ چهاربعدی با شعاع r، برابر است با

$$\frac{۱}{۲}\pi^{۲}r^{۴} = \frac{۱}{۲}\pi^{۲}(۲m)^{۲}$$

برای استفاده از صورت عام قضیهٔ بنیادی مینکوفسکی در فضای nـبعدی (قضیهٔ ۳.۵)، کافی است نشان دهیم که حجم این کره بزرگ‌تر است از $۲^{۴}\Delta = ۲^{۴}m^{۲}$. باید نشان دهیم:

$$\frac{۱}{۲}\pi^{۲}(۲m)^{۲} > ۲^{۴}m^{۲}$$

بعد از ساده کردن، داریم: $۸ < \pi^{۲}$؛ که یک نابرابری درست است.

این قضیهٔ لاگرانژ را برای هر عدد صحیح مثبت و فرد m اثبات می‌کند. این نتیجه به‌راحتی قابل تعمیم به اعداد زوج است، چرا که اگر

$$m = \mathbb{X}^{۲} + \mathbb{Y}^{۲} + \mathbb{Z}^{۲} + \mathbb{W}^{۲}$$

آنگاه

$$۲m = (\mathbb{X}+\mathbb{Y})^{۲} + (\mathbb{X}-\mathbb{Y})^{۲} + (\mathbb{Z}+\mathbb{W})^{۲} + (\mathbb{Z}-\mathbb{W})^{۲}$$

این بحث را با بیان بدون اثبات یک قضیهٔ دیگر به پایان می‌رسانیم.

قضیهٔ ۴.۸ تعداد نمایش‌های عدد صحیح مثبت n به‌صورت مجموع چهار مربع، در صورتی‌که نمایش‌هایی که فقط در ترتیب اعداد یا علامت آنها با هم متفاوتند را واقعاً مجزا در نظر بگیریم، برابر با هشت برابر مجموع مقسوم علیه‌هایی از n است که مضرب ۴ نیستند.

با تقلید از نمادگذاری بخش ۳.۴، برای تعداد نمایش‌های مجزای n به‌صورت مجموع چهار مربع می‌نویسیم:

$$R_{۴}(n) = R(n = p^{۲} + q^{۲} + r^{۲} + s^{۲})$$

پس، قضیهٔ ۴.۸ تعمیمی است از قضیهٔ ۴.۴؛ با کمی نمادگذاری بیشتر، داریم:

$$R_{۴}(n) = ۸\sum_{\substack{d \mid n \\ ۴ \nmid d}} d$$

به‌عنوان مثال:

$$۶ = (\pm ۲)^۲ + (\pm ۱)^۲ + (\pm ۱)^۲ + ۰^۲$$

برای این ترتیب از اعداد، $۸ = ۲^۳$ انتخاب علامت داریم. علاوه بر این می‌توان زوج یک‌ها را در $\binom{۴}{۲} = ۶$ مکان ممکن قرار داد و این، دو مکان برای صفر باقی می‌گذارد. بنابراین ۶ را می‌توان به $۲ \times ۶ \times ۸$ راه به‌صورت مجموع چهار مربع نوشت. به طریق دیگر، مقسوم علیه‌های d از ۶ به صورت $d = ۱, ۲, ۳, ۶$ است، پس

$$R_۴(۶) = ۸ \sum_{\substack{d \mid ۶ \\ ۴ \nmid d}} d = ۸(۱ + ۲ + ۳ + ۶) = ۹۶$$

مراجع

1. H. F. Blichfeldt, "A New Principle in the Geometry of Numbers with Some Applications," *Transactions of the AMS* 15:3 (July 1914): 227-35.

2. ________, "The Minimum Values of Positive Quadratic Forms in Six, Seven, and Eight Variables," *Mathematisehe Zeitschrift* 39 (1934): 1-15.

3. Harold Davenport,"The Geometry of Numbers," *Math Gazette* 31 (1947): 206-10.

4. ________, *The Higher Arithmetic* (New York: Dover, 1983), 124.

5. L. E. Diekson, Preface to *History of the Theory of Numbers, Vol. II: Diophantine Analysis* (Washington, D. C,: Carnegie Institute, 1920). x.

6. ________, *History of the Theory of Numbers, Vol. III: Quadratic and Higher Forms* (Washington, D. C.: Carnegie Institute, 1923).

7. C. F. Gauss, *Werke* (G ottingen: Gesellschaft der Wissennschaften, 1863-1933).

8. J. H. Grace, "The Four Square Theorem," *Journal of the London Mathematical Society* 2 (1927): 3-8.

9. Charles Hermite, "Letters de Hermite á M. Jacobi," *J. reine angew: Math.* 40 (1850): 261-315.

10. ———, *Comptes Rendus Paris 37 (1835).*

11. ———, *J. reine angew: Math.* 47 (1854): 343-5, 364-8.

12. ———, *Oeuvres,* Vol. I (Paris: E. Picard, 1905), 288.

13. David Hilbert and S. Cohn-Vossen, *Geometry and the Imagination,* translated by P. Nemenyi (New York: Chelsea, 1952).

14. A. Hurwitz, "Über die angennäherte Darstellung der Irrationalzahlen durch rationale Brüche," *Mathematische Annalen* 39 (1891): 279-84.

15. A. Korkine and E. I. Zolotareff, "Sur les formes quadratiques positives quaternaires," *Mathematische Annalen* 5 (1827): 581-3.

16. ———, "Sur les formes quadratiques," *Mathematische Annalen* 6 (1873): 366-89.

17. ———, "Sur les forms quadratiques positives," *Mathematische Annalen* 11 (1877): 242-92.

18. Hermann Minkowski, "Über die positiven quadratischen Formen un über kettenbruchähmliche Algorithm," *J. reine agnew: Math* 107 (1891): 209-12.

۹ اصلی جدید در هندسهٔ اعداد

۱.۹ قضیهٔ بلیکفلت

حدود ۱۸۹۱، هرمان مینکوفسکی با کشف قضیهٔ بنیادی خود حوزهٔ جدیدی از مطالعه را گشود که او آن را هندسهٔ اعداد نام نهاد. با استفاده از این قضیه و تعمیم‌های آن، مینکوفسکی توانست بسیاری از مسائل سخت نظریهٔ اعداد را حل کند. در فصل ۶، ما چند تا از کاربردهای ساده‌تر قضیه‌های مینکوفسکی را بررسی کردیم.

با وجود هیجانی که کارهای مرزشکن مینکوفسکی ایجاد کرده بود، ۱۵ سال طول کشید تا اصلی جدید در هندسهٔ اعداد کشف شود. افتخار این موفقیت نصیب هانس فردریک بلیکفلت[1] شد. او در سال ۱۹۱۴ قضیه‌ای را منتشر کرد که از آن پس سهم مهم و بزرگی در هندسهٔ اعداد داشته است. بعد از بیان، این قضیه تقریباً به‌طور شهودی واضح به نظر می‌رسد، اما چنان مؤثر و قوی است که خود بلیکفلت و افراد دیگر پس از او، با استفاده از آن موفق به اثبات نتایجی شده‌اند که با قضیه‌های مینکوفسکی قابل دسترسی نبوده است. یک زندگی‌نامهٔ کوتاه از بلیکفلت در پیوست ج، بعد از زندگی‌نامهٔ مینکوفسکی، ارائه شده است.

در این فصل قضیهٔ بلیکفلت معرفی می‌شود. برای سادگی، ما آن را برحسب فضای دوبعدی، $\mathbb{R}^2$، و نه فضای تعمیم‌یافتهٔ nبعدی بلیکفلت، $\mathbb{R}$، صورت‌بندی خواهیم کرد. بعد از اثبات قضیهٔ بلیکفلت به چند تا از کارهایی که می‌توان با استفاده از آن روی Mـ مجموعه‌های مینکوفسکی انجام داد نظری خواهیم انداخت.

در ابتدا باید چند مفهوم را تعریف کنیم. فرایند انتقال دادن یعنی انتقال دادن یک شکل مسطح به یک دستگاه مختصات جدید با یک مبدأ متفاوت چنان که نقاط مشبکهٔ آن دارای مختصات جدیدند. ساختار انتقال‌یافته، در ابتدا شکل و اندازهٔ اولیه را حفظ می‌کند، اما در ادامه و در صورت تمایل می‌تواند

1. Hans Frederik Blichfeldt

منبسط یا منقبض گردد. دوران محورهای مختصات آنها را در یک موقعیت جدید قرار می‌دهد و زاویهٔ بین آنها را حفظ می‌کند. تغییر مکان موازی، به‌طور ساده، همان انتقال است بدون دوران دادن محورهای مختصات؛ این یعنی جهت اولیه حفظ می‌شود. بالاخره، همچون بخش ۳.۳، یک مجموعه نقاط یک نقطهٔ مشبکه را می‌پوشاند درصورتی که نقطهٔ مشبکه درون آن مجموعه و یا روی مرز آن باشد.

قضیهٔ ۱.۹ (قضیهٔ بلیکفلت) اگر A، مساحت مجموعهٔ دوبعدی C، بزرگ‌تر از عدد صحیح n باشد، آنگاه می‌توان با یک تغییر مکان موازی، C را به گونه‌ای قرار داد که حداقل $n+1$ نقطهٔ مشبکهٔ Λ را بپوشاند.

از این قضیه، فوراً نتیجه می‌شود که اگر مساحت C برابر با n باشد، آنگاه می‌توان با یک انتقال، C را به‌گونه‌ای قرار داد که n نقطهٔ مشبکه را بپوشاند.

۲.۹ اثبات قضیهٔ بلیکفلت

ما قضیهٔ بلیکفلت را با تحلیلی هندسی و با بریدن، کپه‌کردن و سوراخ‌کردن یک ناحیهٔ سطح ــ البته، مجازاً ــ اثبات می‌کنیم.

فرض کنید که C ناحیه‌ای مسطح یا مجموعه‌ای از نقاط است که جایی روی مشبکهٔ نقطه‌ای Λ قرار دارد. فرض نکرده‌ایم که C محدب یا دارای تقارن مرکزی است. مربع‌های مشبکهٔ Λ، C را به قسمت‌های C_1، C_2،... و C_k تقسیم می‌کنند؛ این قسمت‌ها روی مربع‌های متناظرشان R_1، R_2،... و R_k قرار دارند. شکل ۱.۹ الف، ناحیهٔ بسیار سادهٔ C را نمایش می‌دهد؛ اعداد ۱ تا ۵ به مجموعه‌های C_1 تا C_5 اشاره می‌کنند.

اکنون مربع دیگر R از Λ را به دور از C در نظر می‌گیریم و با تغییر مکان‌های موازی، هر یک از مربع‌های R_i را به روی آن انتقال می‌دهیم. با انتقال این مربع‌ها، C_1، C_2،... و C_k جایی شبیه این‌بار روی R قرار می‌گیرند؛ به شکل ۱.۹ ب نگاه کنید. می‌توانیم فکر کنیم که این مربع‌ها روی مربع R، لایه‌لایه روی هم انباشته می‌شوند.

قبل از ادامه به لم زیر نیاز داریم.

لم ۱.۹ مربع R دست‌کم شامل یک نقطهٔ X است که حداقل $n+1$ بار با قسمت‌های C_1، C_2،... و C_k پوشیده می‌شود.

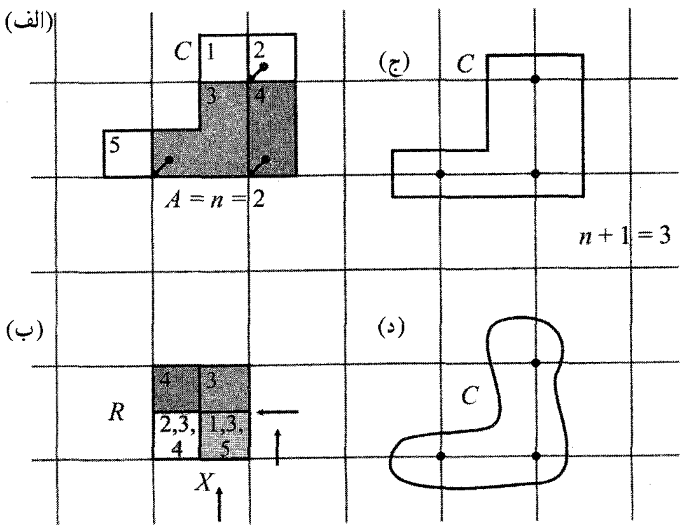
اثبات لم ۱.۹. فرض کنید که هر یک از نقاط R بیشتر از n بار با قسمت‌های C_1، C_2،... و C_k پوشیده نمی‌شود. در این‌صورت، مساحت این قسمت‌ها روی هم نمی‌تواند بیشتر از n باشد. در نتیجه،

مجموعه مساحت این قسمت‌ها وقتی سر جای اصلی خود در C هم برمی‌گردند نمی‌تواند بیشتر از n باشد. اما این با فرض ما که C دارای مساحتی بیشتر از n است، در تناقض است. بنابراین، R باید دست‌کم شامل یک نقطهٔ X باشد که حداقل $n + ۱$ بار با مجموعه‌های C_i پوشیده می‌شود.

برای برداشتن قدم بعدی برای اثبات قضیهٔ بلیکفلت، تصور کنید که یک سوزن را به‌طور مستقیم در این $n + ۱$ مجموعهٔ (یا لایهٔ) روی R فرو می‌کنیم. اکنون هر یک از مجموعه‌ها یک سوراخ کوچک دارند و مکان نسبی همهٔ این سوراخ‌ها نسبت به مربع R یکسان است. وقتی همهٔ مربع‌ها در R را به مکان اولیهٔ آنها در C برگردانیم چه می‌شود؟ آشکارا، موقعیت همهٔ سوراخ‌های کوچک نسبت به مربع خودشان همان است که نسبت به R بود. بنابراین هر انتقالی که یکی از سوراخ‌های کوچک را به یک نقطهٔ مشبکه انتقال دهد، همهٔ سوراخ‌های دیگر را هم به نقاط مشبکه انتقال می‌دهد.

«سوراخ‌های کوچکی» را که از شکل ۱.۹ ب به شکل ۱.۹ الف انتقال داده شده‌اند بررسی کنید. اگر C را کمی به سمت پایین و چپ سُر بدهیم، شکل ۱.۹ ج به‌دست می‌آید که در آن سوراخ‌های کوچک نقاط مشبکه را پوشانده‌اند. چون C حداقل $n + ۱$ سوراخ دارد، وقتی آن را انتقال می‌دهیم حداقل $n + ۱$ نقطهٔ مشبکه را می‌پوشاند. این قضیهٔ ۱.۹ را اثبات می‌کند.

ما برای راحت دیدن اثبات از مستطیل‌ها استفاده کردیم. اما همین اثبات برای هر مجموعهٔ دیگری هم کار می‌کند؛ به شکل ۱.۹ د نگاه کنید.



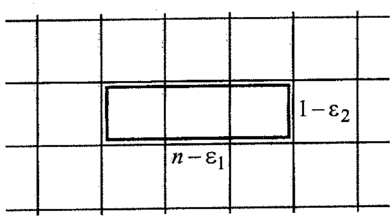
شکل ۱.۹ اثبات قضیهٔ بلیکفلت

۳.۹ تعمیمی از قضیهٔ بلیکفلت

قضیهٔ کلی‌تر بعدی را بدون اثبات بیان می‌کنیم.

قضیهٔ ۲.۹ می‌توان مجموعهٔ کراندار C با مساحت A را روی Λ چنان انتقال داد که تعداد نقاط مشبکه‌ای را که می‌پوشاند بزرگ‌تر از A باشد.

بجز Cـ مجموعه‌های خاص، قضیهٔ ۲.۹ بهترین ممکن است. چرا؟ مستطیل شکل ۲.۹ را در نظر بگیرید. اضلاع این مستطیل موازی محور xها و محور yها، و طول اضلاع آن، $n-\epsilon_1$ و $1-\epsilon_2$ است. در اینجا، n عددی صحیح و مثبت، و ϵ_1 و ϵ_2 اعداد مثبتی هستند که می‌توانند به دلخواه کوچک باشند. مساحت C برابر است با $n-\epsilon = (n-\epsilon_1)(1-\epsilon_2)$ که در آن $\epsilon \to 0$ وقتی $\epsilon_1 \to 0$ و $\epsilon_2 \to 0$. بنابراین $n-1 < A < n$. بنابر قضیهٔ ۱.۹، ما می‌توانیم C را چنان انتقال دهیم که n یا تعداد بیشتری نقطهٔ مشبکه را شامل شود. هر چند، همچنان که شکل ۲.۹ نشان می‌دهد، آن نمی‌تواند بیشتر از n نقطهٔ مشبکه را شامل شود. این نشان می‌دهد که قضیهٔ ۲.۹ بهترین ممکن است چرا که ما مجموعهٔ C را چنان ساختیم که بیشتر از $[A]+1$ نقطهٔ مشبکه را نمی‌پوشاند. بنابراین، کران پایین نمی‌تواند افزایش یابد.

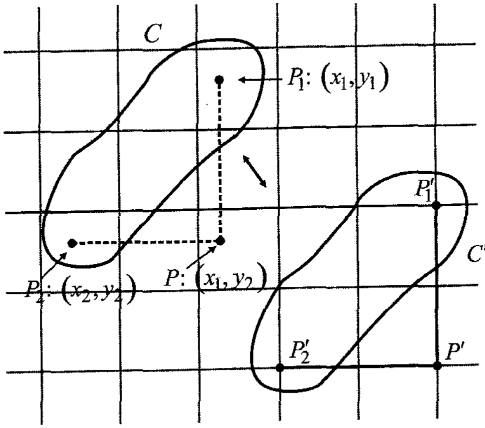


شکل ۲.۹ مجموعهٔ C با مساحتی کمتر از n ولی به اندازهٔ دلخواه نزدیک به n.

هر دوی قضایای ۱.۹ و ۲.۹ به عنوان حالت‌های خاص از قضیهٔ عامتری که بلیکفلت در ۱۹۱۴ ثابت کرد نتیجه می‌شود. بلیکفلت، نه‌تنها با فضای nـ بعدی $\mathbb{R}^n$ کار کرد، بلکه از تعریف عامتری هم برای نقاط مشبکهٔ $\mathbb{R}^n$ استفاده کرد. امروزه، قضیهٔ بلیکفلت معمولاً به شکل زیر و با استفاده از مفهوم نقاط تفاضلی بیان می‌گردد.

قضیهٔ ۳.۹ فرض کنید که C مجموعه‌ای کراندار از نقاط $\mathbb{R}^2$ و با مساحتی بیشتر از ۱ باشد. در این صورت C حداقل شامل دو نقطهٔ $P_1 : (x_1, y_1)$ و $P_2 : (x_2, y_2)$ است که مختصات «نقطهٔ تفاضلی» آنها $P : (x_1 - x_2, y_1 - y_2)$ صحیح است؟

اثبات. C را هر کجای Λ که می‌خواهید، قرار دهید. بنابر قضیهٔ بلیکفلت، می‌توان C را به موقعیت جدید C' چنان انتقال داد که حداقل دو نقطهٔ مشبکهٔ P'_1 و P'_2 را بپوشاند. به شکل ۳.۹ نگاه کنید.



شکل ۳.۹ انتقال C به C' و برعکس

مشاهده کنید که طول‌های $|\overline{P'_{۲}P'}|$ و $|\overline{P'P'_{۱}}|$ صحیح و برابر با طول‌های $|\overline{P_{۲}P}|$ و $|\overline{PP_{۱}}|$ هستند. بنابراین، وقتی C' را به C برمی‌گردانیم، $x_{۲} - x_{۱}$ و $y_{۲} - y_{۱}$ نیز صحیح هستند.

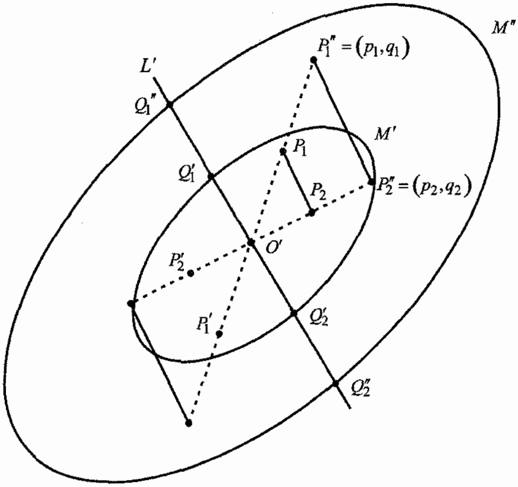
۴.۹ برگشت به قضیهٔ مینکوفسکی

فرض کنید که مجموعهٔ C در قضیه ۱.۹، یک Mـ مجموعه مینکوفسکی باشد، یعنی، یک مجموعهٔ محدب که نسبت به نقطهٔ O، مرکز تقارنش، متقارن است. در این‌صورت، قضیهٔ بنیادی مینکوفسکی از قضیه بلیکفلت به‌دست می‌آید. برای اینکه ببینیم چرا، اجازه دهید که قضیهٔ مینکوفسکی را دوباره بیان و آن را با استفاده از قضیهٔ بلیکفلت اثبات کنیم.

قضیهٔ ۴.۹ (مینکوفسکی) اگر M مجموعه‌ای کراندار، متقارن و با مساحتی بزرگ‌تر از ۴ باشد، آنگاه علاوه‌بر مبدأ، شامل نقطهٔ مشبکهٔ دیگری نیز هست.

اثبات. با یک Mـ مجموعهٔ مینکوفسکی به مرکز O شروع می‌کنیم، آن را با حفظ شکل کوچک می‌کنیم تا مساحت آن برابر شود با $۱ + \epsilon$؛ ϵ عدد مثبتی است که بعداً آن را مشخص خواهیم کرد. بنابر قضیهٔ ۱.۹، این شکل را می‌توان به موقعیت جدید M' انتقال داد تا دو (یا بیشتر) نقطهٔ مشبکه $P_{۱}$ و $P_{۲}$ را بپوشاند. به شکل ۴.۹ نگاه کنید.

فرض کنید O' مرکز تقارن M' است و $P'_{۱}$ و $P'_{۲}$ نقاط مشبکه و قرینهٔ قطری $P_{۱}$ و $P_{۲}$ هستند. چون M' محدب است، متوازی‌الاضلاع $P_{۱}P_{۲}P'_{۱}P'_{۲}$ به‌طور کامل درون مجموعهٔ نقاط تعریف شده توسط M' و مرز آن قرار می‌گیرد.



شکل ۴.۹ انقباض و انتقال M به M'، انبساط به M''.

اکنون خط L' را چنان رسم کنید که از O' بگذرد، موازی $P_۱P_۲$ باشد و مرز M' را در نقاط $Q_۱$ و $Q_۲$ قطع کند. چون $P_۱$ و $P_۲$ نقاط مشبکه هستند، مختصات آنها، $(p_۱, q_۱)$ و $(p_۲, q_۲)$، صحیح است. بنابراین شیب L'، $\frac{(q_۲-q_۱)}{(p_۲-p_۱)}$، گویاست. آشکارا، به دلیل تحدب M'، چهارضلعی $Q_۱Q_۲P_۲P_۱$ در M است، و همچنین طول پاره‌خط $\overline{Q_۱Q_۲}$ بزرگ‌تر است از یا مساوی است با طول پاره‌خط $\overline{P_۱P_۲}$:

$$|\overline{Q_۱Q_۲}| \geq |\overline{P_۱P_۲}| = \sqrt{(p_۲ - p_۱)^۲ + (q_۲ - q_۱)^۲}$$

بعد، ابعاد M' را دوباره با حفظ شکل بزرگ می‌کنیم تا ابعاد خطی آن دو برابر شود. به این ترتیب، مجموعهٔ M'' با مساحت $۴(۱+\epsilon) = ۴ + ۴\epsilon$ به‌دست می‌آید: طول پاره‌خط‌های $\overline{Q_۱Q_۲}$ و $\overline{P_۱P_۲}$ نیز دو برابر می‌شود تا پاره‌خط‌های انبساط یافتهٔ $\overline{Q_۱''Q_۲''}$ و $\overline{P_۱''P_۲''}$ شکل بگیرند؛ $Q_۱''$ و $Q_۲''$ روی مرز M'' قرار دارند، درحالی که، نقاط $P_۱''$ و $P_۲''$ روی مرز یا درون M'' قرار دارند. علاوه‌بر این، چون مساحت M بزرگ‌تر از ۴ است و چون متشابه با M'' است، ما می‌توانیم ϵ را چنان انتخاب کنیم که انتقال M به مرکز O' شامل M'' باشد.

اکنون M'' را به موقعیت اولیهٔ خود برمی‌گردانیم تا مرکز تقارنش O' به مبدأ O برگردد و خط L' تبدیل شود به خط L که از مبدأ می‌گذرد:

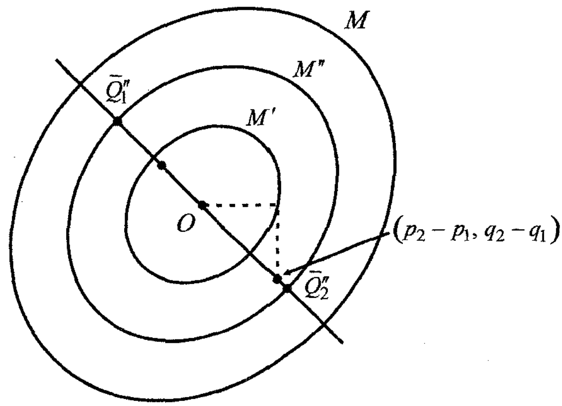
$$L : y = \frac{q_۲ - q_۱}{p_۲ - p_۱}x$$

ادعا می‌کنیم که حداقل دو نقطهٔ مشبکه روی پاره‌خط انتقال‌یافتهٔ $\overline{Q''_۱Q''_۲}$ وجود دارد. درواقع، می‌بینیم که روی خط L، نزدیک‌ترین نقاط مشبکه به مبدأ، نقاط $\pm(p_۲ - p_۱, q_۲ - q_۱)$ هستند. اما برای فاصلهٔ هر یک از این نقاط از مبدأ داریم:

$$\sqrt{(p_۲ - p_۱)^۲ + (q_۲ - q_۱)^۲} \leq |\overline{Q_۱Q_۲}| = |\overline{QQ_۱}| = |\overline{QQ_۲}|$$

بنابراین هر دوی این نقاط مشبکه در M'' قرار می‌گیرند.

اکنون می‌توانیم ϵ را مشخص کنیم. مجموعهٔ اولیهٔ ما M، دارای مساحتی بزرگ‌تر از ۴ است: $A_M = ۴ + \delta$. اگر قرار دهیم $\epsilon < \frac{\delta}{۴}$، آنگاه $A_{M''} < A_M$؛ بنابراین $M'' \subset M$ و این قضیه را تمام می‌کند. به شکل ۵.۹ نگاه کنید.



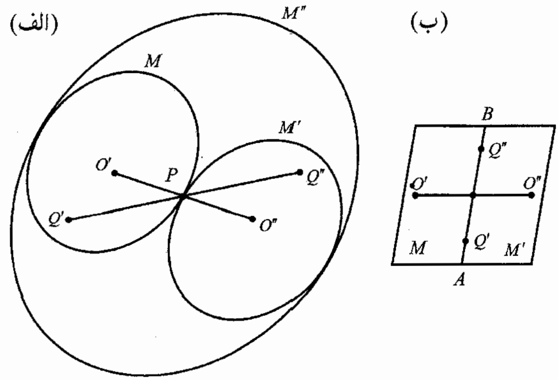
شکل ۵.۹ Mـ مجموعه‌های دوباره انتقال‌یافته.

۵.۹ کاربردهایی از قضیهٔ بلیکفلت

همچنان که مثال زیر نشان می‌دهد، استفاده بلیکفلت از انتقال‌ها بسیاری از زوایای قضایای مینکوفسکی را روشن می‌کند.

قضیهٔ ۵.۹ فرض کنید مساحت یک Mـ مجموعهٔ مینکوفسکی به مرکز مبدأ O برابر است با $۴A$ دراین صورت، علاوه‌بر مبدأ، Mـ مجموعهٔ مذکور دارای بیشتر از $[A] - ۱$ زوج از نقاط مشبکه است.

اثبات. فرض کنید یک Mـ مجموعهٔ مینکوفسکی با مساحت A داریم. همچنین، فرض کنید $n - ۱ < A \leq n$. دراین‌صورت، می‌توان با یک انتقال، Mـ مجموعه را جایی قرار داد که $n > A$



شکل ۶.۹ نقاط مشبکهٔ متناظر در انتقال‌ها.

نقطهٔ مشبکه را بپوشاند. یک بار دیگر آن را انتقال می‌دهیم تا یکی از این نقاط مشبکه مثلاً P روی مرز M قرار بگیرد. فرض کنید مرکز این مجموعهٔ انتقال یافته، O' باشد. خط $O'P$ را به O'' به گونه‌ای امتداد می‌دهیم که $O'P = PO''$. اکنون، Mـ مجموعهٔ M' را به‌گونه‌ای می‌سازیم که با M برابر و نحوهٔ قرارگرفتنش مانند آن است، اما مرکز تقارنش O'' است. به شکل ۶.۹ الف نگاه کنید.

به‌وضوح، P روی مرز M' است. علاوه‌بر این، به هر نقطهٔ مشبکهٔ Q' از M، نقطهٔ مشبکهٔ Q'' از M'' چنان متناظر می‌شود که $Q'P = PQ''$. ممکن است Q'' در M نباشد. مگر اینکه خط $Q'PQ''$ قسمتی از یک مرز مشترک بین M و M' باشد.

اگر فعلاً این حالت را کنار بگذاریم، تعداد نقاط مشبکه‌ای که با M و M' پوشش داده می‌شوند برابر خواهد بود با $۲(n-۱)+۱ = ۲n-۱$. اکنون M را چنان انتقال می‌دهیم که O' با P منطبق شود، سپس آن را چنان بزرگ می‌کنیم که ابعادش دو برابر M شود. این مجموعهٔ جدید، M''، دارای مساحت $۴A$ است و $۲n-۱$ نقطهٔ مشبکه‌ای را که در بالا ذکر شد و P را می‌پوشاند. بنابراین، اگر $n > A$، آنگاه، علاوه‌بر P، $n-۱$ زوج از نقاط مشبکه با M'' پوشانده می‌شوند. با برگرداندن M'' به نقطهٔ O قضیه تمام است.

اما در حالتی که M' و M دارای مرز مشترک AB هستند چه اتفاقی می‌افتد؟ به شکل ۶.۹ ب نگاه کنید. روی این خط مشترک، فرض کنید Q' نزدیک‌ترین نقطهٔ مشبکه به یک از دو سر AB باشد، مثلاً A. در این‌صورت، می‌توانیم در استدلال بالا به جای P از Q' استفاده کنیم و همان نتیجهٔ قبلی را به‌دست آوریم.

تأکید می‌کنیم که قضیهٔ ۱۹۱۴ بلیکفلت بسیار غنی‌تر از این است که تنها گامی باشد برای به‌دست آوردن نتایج مینکوفسکی. در واقع، بلیکفلت از قضیهٔ خودش بسیار استفاده کرد که بسیاری از آنها

برای خواندن بسیار سخت هستند. در قسمت ۴.۸ به یکی از کاربردهای مهم قضیهٔ بلیکفلت اشاره شد؛ اکنون دوباره آن را به شکل زیر بیان می‌کنیم.

قضیهٔ ۶.۹ فرض کنید f فرم درجهٔ دوم معین مثبتی با مبیّن $d > ۰$ باشد. در این‌صورت، اعداد صحیح $l_۱$، $l_۲$، ...، l_n، که همگی صفر نیستند، چنان وجود دارند که $f(l_۱, l_۲, \ldots, l_n)$ کمتر است از یا مساوی است با

$$\frac{۲}{\pi}\left[\Gamma\left(۱ + \frac{n+۲}{۲}\right)\right]^{\frac{۲}{n}} d^{\frac{۱}{n}}.$$

در اینجا Γ، همان تابع گامای معروف است.

بلیکفلت، دنباله‌ای طولانی از تحقیقات را در مورد مینیمم‌های فرم‌های درجهٔ دوم انجام داد که در نهایت منجر به اثر معروف او «مقادیر مینیمم فرم‌های درجهٔ دوم مثبت با شش، هفت و هشت متغیر» (*Math. Zeit.*, Vol. 39, 1934, pp. 1-15) شد. کار او به خودی خود یک دستاورد عظیم است ــ جایگاه بلندی که نه تنها قضایای مینکوفسکی بلکه بسیاری از مسیرهای جدید از آن آغاز می‌گردند.

۱۰ قضیهٔ مینکوفسکی (اختیاری)

۱.۱۰ تاریخچهٔ کوتاهی از مسئله

در سال ۱۸۶۶، بلیکفلت (۱۸۹۴-۱۸۲۱)، یکی از بزرگ‌ترین ریاضیدانان روسیه، قضیهٔ زیر را اثبات کرد.

قضیهٔ ۱.۱۰ فرض کنید θ عددی گنگ و α عددی حقیقی است چنانچه معادلهٔ $x-\theta y-\alpha=0$ دارای هیچ جواب صحیحی نیست. در این‌صورت، به‌ازای هر ϵ مثبت داده‌شده، تعداد نامتناهی زوج از اعداد صحیح p و q چنان وجود دارد که

$$|q(p-\theta q-\alpha)|<2 \tag{1.10}$$

و به‌طور همزمان، $|p-\theta q-\alpha|<\epsilon$.

اثبات بلیکفلت طولانی و درواقع حدود ۴۰ صفحه بود [۷]. او فقط از حساب و به‌طور خاص از کسرهای مسلسل استفادهٔ فراوان کرد. ارمیت [۳]، در سال ۱۸۷۹ ثابت کرد که می‌توان ثابت ۲ در (۱.۱۰) را با $\frac{1}{2}$ و درواقع با $\sqrt{\frac{2}{27}}$ جایگزین کرد. او نیز فقط از روش‌های حسابی استفاده کرد. اوضاع تا سال ۱۹۰۱ چندان تغییری نکرد تا اینکه مینکوفسکی با استفاده از روش‌های هندسی خود قضیهٔ زیر را اثبات کرد.

قضیهٔ ۲.۱۰ اگر θ عددی گنگ، و اگر α عدد حقیقی و غیرصحیح باشد که معادلهٔ $x-\theta y-\alpha=0$ دارای هیچ جواب صحیحی نیست، آنگاه، به‌ازای هر ϵ مثبت داده‌شده، تعداد نامتناهی زوج از اعداد صحیح p و q چنان وجود دارد که

$$|q(p-\theta q-\alpha)|<\frac{1}{4}$$

و به‌طور همزمان، $|p-\theta q-\alpha|<\epsilon$.

۲.۱۰ اثباتی برای قضیهٔ مینکوفسکی

اثبات زیر توسط بلیکفلت در یک مجموعه از درس‌نامه‌ها و در سال ۱۹۳۶ ارائه شده است. ابزار اصلی او برای اثبات قضیهٔ ۲.۱۰، جایگزین کردن فرم خطی ناهمگن $x - \theta y - \alpha$ با فرم همگن $x - \theta y - \alpha z$ است، او ابتدا متغیر جدید z را وارد کرد و سپس z را برابر با ۱ گرفت. ابزار دوم، وارد کردن پارامتر مثبت t است.

در دستگاه مختصات معمولی xyz، منشور κ_t را چنان در نظر می‌گیریم که با شش صفحهٔ زیر محدود شده باشد.

$$\kappa_t : \quad \begin{array}{l} |x - \theta y - \alpha z| + t|y| = \sqrt{t} \\ |z| = ۲ \end{array} \qquad (۲.۱۰)$$

t یک پارامتر مثبت و در اختیار ما است. در ابتدا، t را چنان انتخاب می‌کنیم که:

$$\sqrt{t} < \min\{\epsilon, \alpha - [\alpha], ۱ - \alpha + [\alpha]\}$$

طبق معمول، $[\alpha]$ بزرگ‌ترین عدد صحیح است که از α کوچک‌تر یا با آن مساوی است، بنابراین، $\sqrt{t} < \frac{۱}{۲}$. واضح است که منشور κ_t یک Mـمجموعهٔ مینکوفسکی در فضای ۳ـبعدی است.

می‌توان شش صفحهٔ (۲.۱۰) را به‌صورت سه جفت صفحهٔ موازی دید:

$$\begin{cases} x + (t - \theta)y - \alpha z + \sqrt{t} = ۰ \\ x + (t - \theta)y - \alpha z - \sqrt{t} = ۰ \end{cases}$$
$$\begin{cases} x + (-t - \theta)y - \alpha z + \sqrt{t} = ۰ \\ x + (-t - \theta)y - \alpha z - \sqrt{t} = ۰ \end{cases} \qquad (۳.۱۰)$$
$$\begin{cases} z + ۲ = ۰ \\ z - ۲ = ۰ \end{cases}$$

در هندسهٔ تحلیلی فضایی فرمولی برای محاسبهٔ حجم منشوری که با شش صفحهٔ دوبه‌دو موازی محدود شده باشد وجود دارد. فرض کنید معادلهٔ این صفحات به‌صورت زیر باشد:

$$\begin{cases} a_۱ x + b_۱ y + c_۱ z + d_۱ = ۰ \\ a_۱ x + b_۱ y + c_۱ z + d_۲ = ۰ \end{cases}$$
$$\begin{cases} a_۲ x + b_۲ y + c_۲ z + e_۱ = ۰ \\ a_۲ x + b_۲ y + c_۲ z + e_۲ = ۰ \end{cases}$$

$$\begin{cases} a_3x + b_3y + c_3z + f_1 = 0 \\ a_3x + b_3y + c_3z + f_2 = 0 \end{cases}$$

در این‌صورت $|\nabla|$، حجم این منشور با استفاده از فرمول زیر محاسبه می‌گردد:

$$\nabla = -\frac{(d_1 - d_2)(e_1 - e_2)(f_1 - f_2)}{\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}} \qquad (4.10)$$

(بهترین راه به‌دست آوردن این فرمول استفاده از آنالیز برداری است.) با به‌کار بردن فرمول (۴.۱۰) برای شش صفحهٔ (۳.۱۰)، داریم:

$$\nabla_t = -\frac{(2\sqrt{t})(2\sqrt{t})(4)}{\begin{vmatrix} 1 & t-\theta & -\alpha \\ 1 & -t-\theta & -\alpha \\ 0 & 0 & 1 \end{vmatrix}} = \frac{-16t}{\begin{vmatrix} 1 & t-\theta \\ 1 & -t-\theta \end{vmatrix}} = \frac{-16t}{-2t} = 8 \qquad (5.10)$$

توجه کنید که دترمینان ۳ × ۳ بالا با استفاده از عناصر سطر سوم آن بسط داده شد.

چون $\nabla_t = 2^3$، بنابر قضیهٔ بنیادی مینکوفسکی حداقل یک زوج غیرصفر از نقاط مشبکهٔ $P_1 : (p_1, q_1, r_1)$ و $P_{-1} : (-p_1, -q_1 - r_1)$ درون یا روی κ_t وجود دارد. به‌وضوح، چون κ_t از بالا و پایین محدود به صفحات $z = 2$ و $z = -2$ است، تنها مقادیر صحیحی که r_1 می‌تواند اتخاذ کند ۲±، ۱± و ۰ است: $r_1 = \pm 2, \pm 1, 0$.

در این مرحله، مهم است که نشان دهیم می‌توان به گونه‌ای کار کرد که: $|r_1| = 0$ یا ۱. برای این کار، ابعاد κ را کمی در امتداد محور zـها به‌طور یکنواخت کم می‌کنیم و به‌طور همزمان ابعاد دیگر آن را چنان افزایش می‌دهیم که حجم ∇_t همچنان برابر ۸ باقی بماند.

اکنون منشور κ_h را که با شش صفحهٔ زیر محدود شده است، در نظر می‌گیریم:

$$\begin{cases} x + (t-\theta)y - \alpha z + \sqrt{t}(1+h) = 0 \\ x + (t-\theta)y - \alpha z - \sqrt{t}(1+h) = 0 \end{cases}$$

$$\begin{cases} x + (-t-\theta)y - \alpha z + \sqrt{t}(1+h) = 0 \\ x + (-t-\theta)y - \alpha z - \sqrt{t}(1+h) = 0 \end{cases}$$

$$\begin{cases} z+\dfrac{۲}{(۱+h)^{۲}}=۰ \\ z-\dfrac{۲}{(۱+h)^{۲}}=۰ \end{cases}$$

دوباره، با استفاده از فرمول (۴.۱۰)، ∇_h، حجم κ_h را پیدا می‌کنیم:

$$\nabla_h=\frac{(۱+h)^{۲}(۲\sqrt{t})(۲\sqrt{t})\dfrac{۴}{(۱+h)^{۲}}}{\begin{vmatrix} ۱ & t-\theta & -\alpha \\ ۱ & -t-\theta & -\alpha \\ ۰ & ۰ & ۱ \end{vmatrix}}=۸$$

بنابراین، حداقل یک زوج از نقاط مشبکهٔ $P_{۲}:(p_{۲},q_{۲},r_{۲})$ و $P_{-۲}:(-p_{۲},-q_{۲},-r_{۲})$ داخل و یا روی سطح κ_h چنان وجود دارد که ۱ یا $۰=|r_{۲}|$.

برای هر مقداری از h که $۱>h>۰$، تعداد نقاط مشبکهٔ درون یا روی مرز κ_h متناهی است. اکنون اگر $h\to ۰$، $\kappa_h\to\kappa_t$. در حد، دو امکان متفاوت داریم:

۱. حداقل یک زوج از نقاط مشبکه درون یا روی κ_t چنان وجود دارد که ۱ یا $۰=|r_{۲}|$.

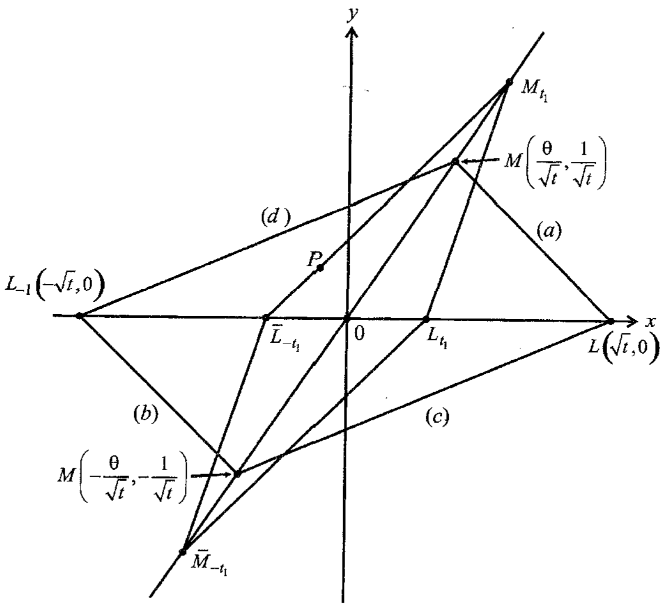
۲. به مقداری برای h می‌رسیم، مثلاً $h=g>۰$، که κ_g شامل یک زوج از نقاط مشبکه است که ۱ یا $۰=|r_{۲}|$. اما برای مقادیر کوچک‌تر h (که $g>h>۰$)، هیچ نقطهٔ مشبکه‌ای داخل κ_h وجود ندارد که ۱ یا $۰=|r_{۲}|$.

به‌وضوح، حالت دوم اتفاق نمی‌افتد، چون حجم هر یک از منشورها برابر است با ۸ و هر یک از منشورها باید شامل نقاط مشبکهٔ غیرصفر باشد؛ برای این نقاط مشبکه، تنها مقادیری که $|r_{۲}|$ می‌تواند داشته باشد ۰ یا ۱ است.

دوباره منشور κ_t را در نظر می‌گیریم. می‌توانیم فرض کنیم که برای یک مقدار دلخواه t، زوجی از نقاط مشبکهٔ $P_{۱}$ و $P_{-۱}$ داریم که: ۱ یا $۰=r_{۱}$.

ابتدا فرض کنید که برای t مذکور، یک زوج از نقاط مشبکهٔ $P_{۱}:(p_{۱},q_{۱},۰)$ و $P_{-۱}:(-p_{۱},-q_{۱},۰)$ داریم که $۰=r_{۱}$. نقطهٔ $P_{۱}$، درون یا روی متوازی‌الاضلاع Q_t قرار خواهد گرفت. با توجه به (۳.۱۰)، اضلاع این متوازی‌الاضلاع دو زوج خطوط موازی (a)، (b) و (c)، (d) هستند:

$$(a): x+(t-\theta)y-\sqrt{t}=۰$$



شکل ۱.۱۰ صفحهٔ $z = ۰$

$$
\begin{aligned}
(b) &: x + (t-\theta)y + \sqrt{t} = ۰ \\
(c) &: x + (-t-\theta)y - \sqrt{t} = ۰ \qquad (۶.۱۰) \\
(d) &: x + (-t-\theta)y + \sqrt{t} = ۰
\end{aligned}
$$

به شکل ۱.۱۰ نگاه کنید.

خطوط (a) و (c) یکدیگر را در $L : (\sqrt{t}, ۰)$، و خطوط (a) و (d) یکدیگر را در $M : \left(\frac{\theta}{\sqrt{t}}, \frac{۱}{\sqrt{t}}\right)$ قطع می‌کنند. قطرهای متوازی‌الاضلاع Q_t ثابت‌اند و روی خطوط $y = ۰$ و $x - \theta y = ۰$ قرار دارند. مساحت این متوازی‌الاضلاع، A، دو برابر مساحت مثلث $LMM_{-۱}$ است:

$$
\begin{aligned}
A &= ۲ \cdot \frac{۱}{۲} \begin{vmatrix} \sqrt{t} & ۰ & ۱ \\ \frac{\theta}{\sqrt{t}} & \frac{۱}{\sqrt{t}} & ۱ \\ -\frac{\theta}{\sqrt{t}} & -\frac{۱}{\sqrt{t}} & ۱ \end{vmatrix} = \sqrt{t} \begin{vmatrix} \frac{۱}{\sqrt{t}} & ۱ \\ -\frac{۱}{\sqrt{t}} & ۱ \end{vmatrix} + \begin{vmatrix} \frac{\theta}{\sqrt{t}} & \frac{۱}{\sqrt{t}} \\ -\frac{\theta}{\sqrt{t}} & -\frac{۱}{\sqrt{t}} \end{vmatrix} \\
&= (\sqrt{t}) \left(\frac{۲}{\sqrt{t}}\right) + ۰ \\
&= ۲
\end{aligned}
$$

نقطهٔ $P_۱$ نمی‌تواند روی قطر $x - \theta y = ۰$ باشد. چرا که اگر آنجا باشد، آنگاه $p_۱ - \theta q_۱ = ۰$، یا $\theta = \frac{p_۱}{q_۱}$، که غیرممکن است چون θ گنگ است. علاوه بر این، چون $\sqrt{t} < \frac{۱}{۲}$، مبدأ تنها نقطهٔ مشبکه‌ای است که روی قطر $y = ۰$ قرار دارد.

حالا، به‌تدریج مقدار t را افزایش می‌دهیم. نقاط M و $M_{-۱}$ روی قطر $x - \theta y = ۰$ از هم دور می‌شوند، در حالی‌که L و $L_{-۱}$ به‌سمت مبدأ حرکت می‌کنند. بالاخره، به مقداری از t می‌رسیم، $t = t_۱$، که برای آن، نقطهٔ $P_۱$ روی یکی از ضلع‌های $Q_{t_۱} = L_{t_۱}M_{t_۱}L_{-t_۱}M_{-t_۱}$ قرار می‌گیرد. افزایش بیشتر t، باعث خواهد شد که $P_۱$ خارج Q_t بیافتد.

نمی‌توان دو زوج مجزا از نقاط مشبکه درون یا روی $Q_{t_۱}$ داشت. چرا که در این‌صورت مساحت بزرگ‌تر از ۲ خواهد بود؛ البته حالتی که رأس‌های $Q_{t_۱}$ نقاط مشبکه هستند استثنا است، اما چند لحظه قبل نشان دادیم که روی $x - \theta y = ۰$ یا روی $y = ۰$ نقطهٔ مشبکهٔ ناصفری وجود ندارد.

اکنون به قسمت اصلی این اثبات هندسی رسیده‌ایم. برای $t = t_۱$، فرض کنید که نقطهٔ مشبکهٔ $P_۱$ روی یکی از اضلاع $Q_{t_۱}$ باشد. با کمی کاهش در t، مثلاً از $t = t_۱$ به $t = t_۱ - \beta$، به‌ازای $\beta > ۰$، هیچ نقطهٔ مشبکه‌ای بجز $(۰, ۰)$ در $Q_{t_۱ - \beta}$ وجود نخواهد داشت. بنابراین، در طول این کاهش در t، باید نقطهٔ مشبکه‌ای در منشور $\kappa_{t_۱ - \beta}$ باشد که برای آن $|r_۱| = ۱$. چون تعداد این نقاط مشبکه متناهی است، وقتی که t، از $t_۱ - \beta$ به $t_۱ - \gamma$، برای $\gamma > \beta > ۰$، کاهش پیدا می‌کند، حداقل یکی از این نقاط در درون و یا روی $\kappa_{t_۱ - \gamma}$ قرار می‌گیرد.

پس، برای مقداری از t بین $t_۱ - \gamma$ و $t_۱ - \beta$، حداقل یک نقطهٔ مشبکهٔ $P : (p, q, ۱)$ چنان وجود دارد که:

$$|p - \theta q - \alpha| + t|q| < \sqrt{t}. \qquad (۷.۱۰)$$

اما،

$$\sqrt{|a| \cdot |b|} \leq \frac{۱}{۲}\{|a| + |b|\}$$

بنابراین،

$$\sqrt{t|p - \theta q - \alpha| \cdot |q|} \leq \frac{|p - \theta q - \alpha| + t|q|}{۲} < \frac{\sqrt{t}}{۲}$$

با به توان رساندن هر دو طرف، داریم

$$|p - \theta q - \alpha| \cdot |q| < \frac{۱}{۴} \qquad (۸.۱۰)$$

از طرفی، با توجه به (۷.۱۰) و کران مذکور روی $\sqrt{t}$، داریم

$$\circ < |p - \theta q - \alpha| < \sqrt{t} < \epsilon \qquad (۹.۱۰)$$

چون ϵ می‌توان به اندازهٔ دلخواه کوچک باشد و چون ما فرض کردیم که به‌ازای همهٔ اعداد صحیح p و q داریم $p - \theta q - \alpha \neq \circ$، پس (۹.۱۰) و در نتیجه (۸.۱۰) برای تعداد نامتناهی از زوج‌های صحیح (p_ϵ, q_ϵ) صادق خواهند بود.

علاوه بر این، اگر در (۷.۱۰) داشته باشیم، $q = \circ$ آنگاه $|p - \alpha| < \sqrt{t}$. چون α صحیح نیست، p نمی‌تواند از یکی از دو عدد صحیح $[\alpha]$ و $[\alpha] + ۱$ به α نزدیک‌تر باشد. بنابراین

$$|p - \alpha| \geq \alpha - [\alpha]$$

یا

$$|p - \alpha| \geq [\alpha] + ۱ - \alpha$$

اما فرض کرده بودیم که $\sqrt{t} < \min\{\epsilon, \alpha - [\alpha], [\alpha] + ۱ - \alpha\}$. این تناقض ثابت می‌کند که $q \neq \circ$.

بالاخره، این امکان را در نظر بگیرید که بجز نقطهٔ $(\circ , \circ)$ هیچ نقطهٔ مشبکهٔ دیگری در چهارضلعی Q_t که با (۶.۱۰) تعریف شده است نباشد. در این‌صورت، وقتی که t در بازه‌ای شبیه آنچه که در بالا دیدیم قرار می‌گیرد، κ_t باید شامل یک نقطهٔ مشبکه باشد که $z_۱ = ۱$:$P_۱(x_۱, y_۱, ۱)$. دوباره، (۷.۱۰) نتیجه می‌شود. این اثبات قضیهٔ ۲.۱۰ را تمام می‌کند.

یادداشت. برای دیدن سؤال‌های سخت‌تری حول و حوش این قضیه به هاردی و رایت [۲] نگاه کنید.

۳.۱۰ کاربردی از قضیهٔ مینکوفسکی

همچنان‌که در فصل‌های قبل از قضایای مینکوفسکی برای تقریب زدن اعداد گنگ با اعداد گویا استفاده کردیم، اکنون نیز می‌توانیم از قضیهٔ چبیشف و مینکوفسکی نیز به همین منظور استفاده کنیم، اما این بار با قوت بیشتر. فرض کنید m، عدد صحیح مثبت دلخواه است. اعداد صحیح a و b را چنان انتخاب می‌کنیم که $\gcd(m, a, b) = ۱$. فرض کنید عدد گویای θ داده شده است. مایلیم ثابت مثبت c را چنان تعیین کنیم که برای آن تعداد نامتناهی عدد گویای $\frac{p}{q}$ با خاصیت زیر وجود داشته باشد:

$$\left|\theta - \frac{p}{q}\right| < cq^{-۲}, \qquad p \equiv a(\bmod m), q \equiv b(\bmod m) \qquad (۱۰.۱۰)$$

بزرگ‌ترین کران پایین چنین cهایی را با $c(\theta, m, a, b)$ نمایش می‌دهیم.

این مسئله اولین بار توسط اسکات [۶] و برای $m = 2$ حل شد. او نشان داد که برای θ، a و b دلخواه، $c(\theta, 2, a, b) \leq 1$. بعداً، کاکسما [۵] مسئله را برای m دلخواه حل کرد و نشان داد که $c(\theta, m, a, b) \leq \frac{1}{4}m^2$. اثبات مستقیماً از قضیهٔ ۲.۱۰ به‌دست می‌آید.

قضیهٔ ۳.۱۰ فرض کنید $m \geq 2$ عدد صحیح دلخواه باشد و اعداد صحیح a و b چنان باشند که $\gcd(m, a, b) = 1$. به‌ازای هر عدد گنگ θ، تعداد نامتناهی عدد گویای $\frac{p}{q}$ چنان وجود دارند که

$$\left|\theta - \frac{p}{q}\right| < cq^{-2}, \qquad p \equiv a(\mod m), q \equiv b(\mod m)$$

در اینجا، $c > \frac{1}{4}m^2$.

اثبات. بنویسید $p = p'm + a$ و $q = q'm + b$. هر دو طرف نابرابری (۱۰.۱۰) را در q^2 ضرب می‌کنیم، داریم:

$$|\theta q^2 - pq| < c$$

با جایگزین کردن p و q، داریم

$$\begin{aligned}&|\theta(q'm + b)^2 - (p'm + a)(q'm + b)|\\&\qquad = |(q'm + b)(q'm\theta + b\theta - p'm - a)| < c\end{aligned}$$

با تقسیم این عبارت بر m^2 و ساده کردن آن، داریم:

$$\begin{aligned}\left|\left(q' + \frac{b}{m}\right)\left[q'\theta + \left(\frac{b}{m}\right)\theta - p' - \frac{a}{m}\right]\right| &< cm^{-2}\\ |(q' + t)(q'\theta - p' + t\theta - s)| &< cm^{-2}\\ |(q' + t)(q'\theta - p' - \alpha)| &< cm^{-2} \qquad (11.10)\end{aligned}$$

در اینجا، $\alpha = s - t\theta$.

اکنون با جایگزین کردن p' و q' برحسب p و q، می‌بینیم که $q'\theta - p' - \alpha = \frac{(q\theta - p)}{m}$. چون θ گنگ است، این عبارت آخری هیچ‌گاه صفر نخواهد بود، پس می‌توانیم قضیهٔ ۲.۱۰ را در مورد نابرابری بالا به‌کار بریم. بخصوص،

$$|(q' + t)(q'\theta - p' - \alpha)| = |q'(q'\theta - p' - \alpha) + t(q'\theta - p' - \alpha)|$$

$$\leq |q'(q'\theta - p' - \alpha)| + |t(q'\theta - p' - \alpha)|$$

بنابر قضیه:

$$|q'(q'\theta - p' - \alpha)| + |t(q'\theta - p' - \alpha)| < \frac{۱}{۴} + t\epsilon = \frac{۱}{۴} + \epsilon'$$

برای $\epsilon' > ۰$ داده شده و تعداد نامتناهی اعداد گویای $\frac{p'}{q'}$. بنابراین، (۱۱.۱۰)برای $cm^{-۲} > \frac{۱}{۴}$ صادق است. این قضیهٔ ۳.۱۰ را اثبات می‌کند و نشان می‌دهد که $c(\theta, m, a, b) \leq \frac{۱}{۴}m^۲$.

یادداشت. برای این اثبات و بسیاری از نتایج مربوط نگاه کنید به [۱].

۴.۱۰ اثبات قضیهٔ عام

بلیکفلت از روش بالا برای اثبات قضیهٔ کلی‌تر زیر که اولین بار در ۱۹۰۱ توسط مینکوفسکی اثبات شده بود استفاده کرد:

قضیهٔ ۵.۱۰ فرض کنید α، β، γ، δ، $\xi_۰$ و $\eta_۰$ اعداد حقیقی هستند و $\alpha\delta - \beta\gamma = ۱$. در این‌صورت، اعداد صحیح p و q چنان وجود دارند که

$$|(\alpha p + \beta q - \xi_۰)(\gamma p + \delta q - \eta_۰)| \leq \frac{۱}{۴}$$

رماک (۱۹۱۳)، موردل (۱۹۲۸)، لاندائو (۱۹۳۱)، بلیکفلت (۱۹۳۲)، سیال (۱۹۳۵) و نیون (۱۹۶۱)، این قضیه را اثبات کرده‌اند. برای دیدن فهرست کامل‌تری از اشخاصی که این قضیه را اثبات کرده‌اند به کاکسما [۴] نگاه کنید.

مراجع

1. P. M. Gruber and C. G. Lekkerkerker, Sections 47.3-47.6 in *Geometry of Numbers,* 2nd ed (Amsterdam and New York: North-Holland, 1987), 556-66.

2. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* 5th ed. (Oxford: Oxford University Press, 1983).

3. Hermite, Charles, "Sur une extension donnée á la théorie des fractions continues par M. Tchebychev," *J. reine angew: Math.* 88 (1879): 10-15.

4. J. F. Koksma, *Diophantische Approximationen* (New York: Chelsea. 1936).

5. ———, "Sur l'approximation des nombres irrationals sous une condition supplementaire," *Simon Steven* 28 (1951): 199-202.

6. W. T. Scott, "Approximation to Real Irrationals by Certain Classes of Rational Fractions," *Bulletin of the AMS* 46 (1940): 124-9.

7. P. L. Tchebychef, *Oeuvres de Tchebychef,* translated into French by A. Markoff and N. Sonin (reprinted, New York: Chelsea).

الف

اعداد صحیح گاوسی
پیتر د. لکس

الف.۱ اعداد مختلط

ما در بخش قبل از ویژگی‌هایی برای نقاط مشبکه استفاده کردیم، که مربوط به ساختار جمعی صفحه بود، مثل انتقال یک مجموعه در صفحه. اما اگر صفحه را به عنوان صفحهٔ مختلط در نظر بگیریم، نقاط مشبکه‌ای، دارای ساختار ضربی هم می‌شوند. در این پیوست به بررسی این ساختار ضربی می‌پردازیم.

می‌دانیم هر نقطهٔ (x,y) در صفحه به شکل $z=x+iy$ در صفحهٔ مختلط است، که x را قسمت حقیقی و y را قسمت موهومی این عدد مختلط می‌نامیم. عمل جمع در اعداد مختلط، همانند انتقال در صفحه است. ضرب این اعداد به شکل

$$(x+iy)(u+iv)=xu-yv+i(xv+yu)$$

تعریف می‌شود که همان‌طور که در ضابطهٔ بالا مشاهده می‌شود، عمل ضرب، همانند دوران و تجانس در صفحه است.

اندازهٔ هر عدد مختلط $z=x+iy$، به شکل

$$|z|=\sqrt{x^۲+y^۲}$$

تعریف می‌شود. به کمک قضیهٔ فیثاغورس، مشاهده می‌شود این مقدار دقیقاً برابر فاصلهٔ نقطهٔ z از مبدأ است.

$\overline{z}=x-iy$ را مزدوج $z=x+iy$ می‌نامیم که تصویر نقطهٔ z نسبت به محور حقیقی است. رابطهٔ $z\overline{z}=|z|^۲$ به راحتی از تعاریف بالا به‌دست می‌آید. و همچنین، اندازهٔ حاصل‌ضرب دو عدد مختلط برابر حاصل‌ضرب اندازه‌های آن دو عدد مختلط است.

اعداد مختلط همانند نقاط مشبکه‌ای هستند. اعدادی مثل $g = a + ib$، که a و b اعداد صحیح باشند را اعداد صحیح گاوسی می‌نامند و به راحتی دیده می‌شود جمع و ضرب اعداد صحیح گاوسی، عدد صحیح گاوسی است و اعداد صحیح گاوسی تشکیل یک حلقه می‌دهند. همان‌طورکه در حلقهٔ اعداد صحیح حقیقی مفاهیمی چون بخش‌پذیری، اعداد اول و تجزیهٔ یکتا به عوامل اول بررسی شد، علاقمندیم در این حلقه هم، چنین مفاهیمی را بررسی کنیم.

چهار عدد

$$۱, -۱, i, -i$$

را یکه‌های حلقهٔ اعداد صحیح گاوسی می‌نامیم و با u نمایش می‌دهیم. تنها این چهار عدد دارای وارون ضربی هستند و اندازهٔ همهٔ آنها برابر ۱ است.

مجموعهٔ مسائل قسمت الف.۱

۱. نشان دهید هیچ عدد صحیح گاوسی غیریکه‌ای وجود ندارد که دارای وارون ضربی در حلقهٔ اعداد صحیح گاوسی باشد.

۲. نشان دهید اگر $a + bi \neq \pm ۱, \pm i$ آنگاه $|a + bi| > ۱$.

۳. نشان دهید $(a + bi)(a - bi)$ عددی صحیح گاوسی است.

الف.۲ تجزیهٔ اعداد صحیح گاوسی

هر گاه عدد صحیح گاوسی g را بتوان به شکل حاصل‌ضرب دو عدد صحیح گاوسی f و h نوشت خواهیم داشت:

$$g = fh \qquad (۱)$$

و گوییم g بر f و h بخش‌پذیر است و معادلهٔ (۱)، تجزیه‌ای از g است که f و h عوامل g هستند. ما می‌توانیم تمام عوامل عدد صحیح گاوسی g را به کمک معادلهٔ (۱) به‌دست آوریم، از معادلهٔ (۱) داریم:

$$|g| = |f|\,|h|$$

اگر $g = fh$ باشد. طوری‌که f و h یکه نباشند این تجزیه را، تجزیهٔ نابدیهی‌ای از g می‌نامیم. چون اندازهٔ هر عدد صحیح گاوسی که صفر و یکه نباشد، از یک بزرگ‌تر است. هر عامل نابدیهی از g، اندازه‌ای کمتر از $|g|$ دارد. متناهی عدد صحیح گاوسی f وجود دارد که چنین‌اند. برای نشان دادن

اینکه g بر همهٔ آنها بخش‌پذیر است، می‌توانیم از خارج‌قسمت

$$\frac{g}{f} = \frac{g\overline{f}}{|f|^۲}$$

استفاده کنیم و مشاهده کنیم آیا این خارج‌قسمت عدد صحیح گاوسی است یا خیر.

عدد صحیح گاوسی q را اول می‌نامیم، اگر تنها تجزیه‌اش بدیهی باشد؛ یعنی $q = ur$ که عامل u یکه است. دو عدد اول گاوسی را معادل گوییم، اگر تنها تفاوت آنها، در عامل یکه‌شان باشد.

مثال ۱. $(۲ + i)(۲ - i) = ۵$ بنابراین ۵ در اعداد صحیح گاوسی، اول نیست.

مثال ۲. ادعا می‌کنیم $۱ + i$ اول است. می‌دانیم

$$|۱ + i| = \sqrt{۱^۲ + ۱^۲} = \sqrt{۲}$$

کمترین مقدار برای اندازهٔ یک عدد صحیح گاوسی غیرصفر، یک است. طبق مسئلهٔ ۳ در قسمت الف.۱، بعد از آن، $\sqrt{۲}$، کمترین مقدار برای اندازهٔ یک عدد صحیح گاوسی است. بنابراین در تجزیهٔ $۱ + i = vw$، یکی از عامل‌ها باید دارای اندازهٔ یک باشد. در نتیجه این عامل یکه است.

مجموعهٔ مسائل قسمت الف.۲

۱. نشان دهید اگر q اول باشد، $\overline{q}$ نیز چنین است.

۲. نشان دهید اعداد اول q و $\overline{q}$ که $q \neq \overline{q}$، جز در حالتی که $q = (۱ + i)u$، معادل نیستند.

الف.۳ قضیهٔ اساسی حساب

دو عدد صحیح گاوسی g و h را نسبت به هم اول گوییم، هرگاه تنها عامل مشترکشان یکه باشد.

از فصل ۱، قضیهٔ اساسی حساب برای اعداد صحیح حقیقی را به یاد دارید. اگر a و b نسبت به هم اول باشند، ۱ را می‌توان به شکل ترکیب خطی از a و b نوشت.

$$na + mb = ۱, \qquad m \text{ و } n \text{ صحیح هستند}$$

نشان می‌دهیم چنین نتیجه‌ای در اعداد صحیح گاوسی نیز برقرار است.

قضیهٔ الف.۱ (قضیهٔ اساسی حساب مختلط) اگر g و h اعداد صحیح گاوسی غیرصفری باشند که نسبت به هم اول هستند، آنگاه ۱ را می‌توان به شکل ترکیب خطی از g و h نوشت.

$$rg + th = ۱ \qquad r \text{ و } t \text{ اعداد صحیح گاوسی هستند} \tag{۲}$$

در اثبات این قضیه از الگوریتم اقلیدسی استفاده شده است، مثل اثبات قضیهٔ مشابه در مورد اعداد صحیح حقیقی. ما این مطلب را در لم زیر خواهیم دید.

لم الف.۱ دو عدد صحیح گاوسی g و h مفروض‌اند، بدون اینکه از کلیت مسئله کم شود، فرض می‌کنیم

$$|g| \leq |h|$$

آنگاه عدد صحیح گاوسی‌ای مانند f موجود است که

$$|h - fg| < |g| \tag{۳}$$

اثبات لم الف.۱. برای یکی از یکه‌های u، ثابت می‌کنیم

$$|h - ug| < |h| \tag{۴}$$

این حکم به راحتی به کمک هندسه دیده می‌شود. شکل الف. ۱ را ببینید، نقطهٔ h روی دایرهٔ به مرکز مبدأ و شعاع $|h|$ قرار دارد و چهار نقطهٔ $h+ig, h-ig, h+g, h-g$ روی دایره به مرکز h و به شعاع $|g|$ قرار دارند. یکی از این نقاط، درون زاویه‌ای به اندازهٔ $\frac{\pi}{۲}$ و به رأس h قرار دارد و خط گذرنده از h و مبدأ نیمساز این زاویه است. این نقطه را $h_۱$ می‌نامیم و

$$h_۱ = h - u_۱ g$$

چون $|g| \leq |h|$، از شکل الف. ۱ نتیجه می‌شود، $|h_۱| < |h|$. و این نتیجه نامساوی (۴) را اثبات می‌کند. فرض کنید P، پای عمود از مبدأ، O، به ضلعی از زاویه باشد و Q نقطهٔ تقاطع دایره به مرکز h و شعاع $|g|$، با ضلع زاویه باشد. به روشنی خواهیم داشت $|h_۱| \leq |Q|$. مثلث قائم‌الزاویهٔ QPh متساوی‌الساقین است، پس $|h - P| = |P| = |h|/\sqrt{۲}$ و

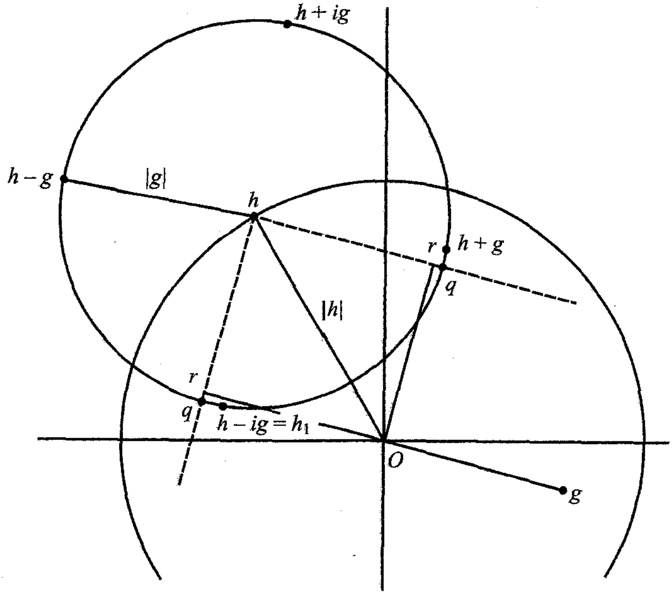
$$|h - Q| = |g|,$$
$$|P - Q| = \pm\left(|g| - \frac{|h|}{\sqrt{۲}}\right)$$

و به کمک قضیهٔ فیثاغورس،

$$|Q|^۲ = \left(|g| - \frac{|h|}{\sqrt{۲}}\right)^۲ + \left(\frac{|h|}{\sqrt{۲}}\right)^۲ = |g|^۲ - \sqrt{۲}|g|\,|h| + |h|^۲$$

چون $|g| \leq |h|$،

$$|Q|^۲ \leq |h|^۲ + |g|^۲ - \sqrt{۲}|g|^۲ = |h|^۲ - \left(\sqrt{۲} - ۱\right)|g|^۲$$



شکل الف.۱

پس

$$|h_{۱}|^{۲} \leq |h|^{۲} - \left(\sqrt{۲} - ۱\right) |g|^{۲}$$

اگر $|g| > |h_{۱}|$، نامساوی (۳) به‌ازای $f = u_{۱}$ اثبات می‌شود، در غیر این‌صورت همین فرایند را برای $h_{۱}$، به جای h، انجام می‌دهیم و در گام دوم عدد صحیح گاوسی

$$h_{۲} = h_{۱} - u_{۲}g = (h - u_{۱}g) - u_{۲}g = h - (u_{۱} + u_{۲})g = h - f_{۲}g$$

را به‌دست می‌آوریم. همچنین اگر $|g| > |h_{۲}|$، حکم برقرار است. و اگر چنین نباشد، روند قبلی را ادامه می‌دهیم و دنباله‌ای از اعداد صحیح گاوسی مانند h_j به شکل $h - fg$ به‌دست می‌آوریم که اندازه‌شان بعد از هر مرحلهٔ این روند با مقداری مشخص کاهش می‌یابد بنابراین بعد از متناهی مرحله خواهیم داشت $|g| > |h_k|$، و این امر اثبات لم را کامل می‌کند.

اثبات قضیهٔ الف.۱. حال برای اثبات قضیهٔ اساسی حساب به کمک این لم تمام اعداد صحیح گاوسی به شکل (۲) را بررسی می‌کنیم؛ این اعداد را می‌توان به شکل $rg + th$ نمایش داد که در آن t و r اعداد صحیح گاوسی هستند. در بین این اعداد، عدد صحیح گاوسی غیرصفری را در نظر

می‌گیریم که کوچک‌ترین اندازه را دارد و آن را با

$$s = rg + gh$$

نمایش می‌دهیم. از طرفی g و h غیرصفر و به شکل اعداد معرفی‌شده در (۲) هستند و چون s کوچک‌ترین اندازهٔ مثبت را در بین این اعداد داراست، پس

$$|s| \leq |g|, \qquad |s| \leq |h|$$

h و s در فرضیات لم صدق می‌کنند، بنابراین طبق لم نتیجه می‌گیریم عدد صحیح گاوسی‌ای مانند f موجود است که

$$|h - fs| < |s|$$

از طرفی $h - fs$ به شکل اعداد معرفی‌شده در (۲) است و چون s کوچک‌ترین اندازهٔ مثبت را در بین این اعداد دارد خواهیم داشت:

$$h - fs = \circ$$

و بنابراین h بر s بخش‌پذیر است. مشابهاً می‌توان نتیجه گرفت، g بر s بخش‌پذیر است و چون g و h نسبت به هم اول هستند، پس تنها عامل مشترکشان یکه‌ها هستند، بنابراین s یکه است. این امر اثبات می‌کند که یکی از یکه‌ها دارای نمایش به شکل معرفی‌شده در (۲) است و در این‌صورت، این یکه می‌تواند خود h باشد

$$rh + tg = \text{۱} \tag{۵}$$

و این مطلب اثبات قضیه را به اتمام می‌رساند.

توجه کنید که اثبات اینکه (۵) دارای جواب است، غیرساختنی است.

مسئلهٔ قسمت الف.۳

۱. به کمک لم الف. ۱ الگوریتمی اقلیدسی برای به‌دست آوردن جواب معادلهٔ (۵) بنویسید.

الف.۴ تجزیهٔ یکتای اعداد صحیح گاوسی

قضیهٔ اساسی حساب در اعداد مختلط، نتایجی دربارهٔ بخش‌پذیری و تجزیهٔ اعداد صحیح گاوسی دارد که مشابه آنها برای اعداد صحیح حقیقی نیز برقرار است.

قضیهٔ الف.۲ اگر g و h اعداد صحیح گاوسی نسبت به هم اول باشند و hk بر g بخش‌پذیر باشد آنگاه k بر g بخش‌پذیر است.

اثبات. چون g و h نسبت به هم اول هستند، طبق قضیهٔ اساسی، اعداد صحیح گاوسی r و t موجودند که

$$rg + th = ۱$$

طرفین تساوی بالا را در k ضرب می‌کنیم. بنابراین خواهیم داشت:

$$rgk + thk = k$$

طبق فرض قضیه، می‌دانیم hk بر g بخش‌پذیر است پس هر دوی جملات سمت چپ معادلهٔ بالا بر g بخش‌پذیر است، بنابراین سمت راست معادله نیز بر g بخش‌پذیر است و اثبات کامل است.

قضیهٔ زیر به سرعت از قضیهٔ الف.۲ نتیجه می‌شود.

قضیهٔ الف.۳ فرض کنید q عدد اول گاوسی باشد که fg بر q بخش‌پذیر است. آنگاه f یا g بر q بخش‌پذیر است.

اثبات. فرض کنید f بر q بخش‌پذیر نباشد بنابراین q و f نسبت به هم اول هستند. پس طبق قضیهٔ الف.۲، g بر q بخش‌پذیر است.

مسئلهٔ قسمت الف.۴

۱. نشان دهید هر عدد صحیح گاوسی را می‌توان به شکل یکتایی به صورت حاصل‌ضرب اعداد اول نوشت با صرف‌نظر از عوامل یکه.

الف.۵ اعداد اول گاوسی

این قسمت مسئلهٔ توصیف تمام اعداد اول گاوسی را حل می‌کند. پاسخ چهار قسمت دارد:

قضیهٔ الف.۴ الف) هر عدد اول p، در حلقهٔ اعداد صحیح حقیقی به شکل $۴n + ۳$، عدد اول گاوسی است.

ب) هر عدد اول صحیح حقیقی p، به شکل $۴n + ۱$ را می‌توان به شکل یکتایی به‌صورت $p = q\bar{q}$ تجزیه کرد که q عدد اول گاوسی است.

ج) عدد ۲، عدد اول گاوسی نیست و قابل تجزیه به شکل $۲ = i(۱ - i)^۲$ است.

د) همهٔ اعداد اول گاوسی، توسط یکی از قسمت‌های الف، ب، ج قابل بیان است.

اثبات. ابتدا با اثبات الف شروع می‌کنیم.

اگر p عدد اول صحیحی به شکل $۴n + ۳$ باشد و عدد اول گاوسی نباشد، باید دارای تجزیهٔ نابدیهی $p = st$ باشد که در آن s و t اعداد صحیح گاوسی غیر یکه‌ای هستند و داریم:

$$p^۲ = |s|^۲|t|^۲$$

چون p عدد اول صحیح است تنها تجزیهٔ نابدیهی برای $p^۲$، به شکل $p \cdot p$ است. بنابراین

$$|s|^۲ = |t|^۲ = p$$

حال می‌توانیم s را به شکل $a + ib$ بیان کنیم که a و b اعداد صحیحی باشند و بنابراین

$$a^۲ + b^۲ = p$$

مربع هر عدد صحیح به پیمانه ۴، یک یا صفر است بنابراین حاصل‌جمع فوق، هیچگاه به شکل $۴n + ۳$ نمی‌شود این تناقض اثبات قسمت الف قضیهٔ الف.۴ را کامل می‌کند.

برای اثبات قسمت ب قضیهٔ الف.۴ نیاز به بررسی قضیهٔ ویلسن داریم.

قضیهٔ الف.۵ (**ویلسن**) فرض کنید p عدد اول صحیحی باشد، آنگاه

$$(p - ۱)! \equiv -۱ \qquad (\text{به پیمانهٔ } p)$$

اثبات قضیهٔ ویلسن. مجموعهٔ همهٔ دسته‌های همنهشتی به پیمانهٔ p را با $R(p)$ نمایش می‌دهیم. $R(p)$ شامل p عضو است که هر عضو، را می‌توان با باقی‌مانده‌های تقسیم به p مشخص کرد: $۰, ۱, ۲, \ldots, p - ۱$. چون $R(p)$ نسبت به عمل جمع و عمل ضرب بسته است، عمل ضرب و جمع را در $R(p)$ تعریف می‌کنیم و بنابراین $R(p)$ یک حلقهٔ جابه‌جایی تشکیل می‌دهد. ادعا می‌کنیم $R(p)$ میدان است، یعنی هر عضو ناصفر از $R(p)$، دارای وارون ضربی است.

عدد a که بر p بخش‌پذیر نباشد را در نظر بگیرید. ادعا می‌کنیم هیچ دوتایی از اعداد a، $۲a$، $\ldots$، $(p - ۱)a$ به پیمانهٔ p همنهشت نیستند. برای اثبات ادعایمان فرض کنید $r \not\equiv s$ ادعا می‌کنیم $ar \not\equiv as$، زیرا $ar - as = a(r - s)$ و هیچ‌یک از a و $r - s$ بر p بخش‌پذیر نیست. بنابراین حاصل‌ضربشان نیز بر p بخش‌پذیر نیست. چون $p - ۱$ عدد a، $۲a$، $\ldots$، $(p - ۱)a$ بر p بخش‌پذیر نیستند، متناظرند با $p - ۱$ عدد ۱، ۲، $\ldots$، $p - ۱$، که این $p - ۱$ عدد، همان باقی‌مانده‌های تقسیم هر عدد بر p است و این اعداد به پیمانهٔ p، نظیر به نظیر همنهشت هستند. به‌خصوص وجود دارد rای که $ar \overset{p}{\equiv} ۱$ در نتیجه r وارون ضربی a است.

بعضی از دسته‌های همنهشتی، خودشان وارون ضربی خودشان، هستند. مثل ۱ و $(p-۱)$ که به پیمانهٔ p همنهشت ۱ هستند و هیچ دستهٔ همنهشتی دیگری نیست که چنین خاصیتی داشته باشد یعنی $r^۲ \stackrel{p}{\not\equiv} ۱$، مگر اینکه $r^۲ \stackrel{p}{\equiv} ۱$ یا $r^۲ \stackrel{p}{\equiv} -۱$. این مطلب به راحتی اثبات می‌شود. $(r+۱)(r-۱) = r^۲ - ۱$ که بر p بخش‌پذیر نیست مگر اینکه p برابر با $r-۱$ یا $r+۱$ باشد.

حال آماده هستیم که قضیهٔ ویلسن را اثبات کنیم. می‌دانیم

$$(p-۱)! = ۱ \cdot ۲ \cdot \cdots \cdot (p-۱)$$

در این حاصل‌ضرب هر عامل به‌جز اولین عامل و آخرین عامل دارای وارون ضربی است که حاصل‌ضربشان به پیمانهٔ p، با ۱ همنهشت است. این مطلب اثبات می‌کند $(p-۲)! \stackrel{p}{\equiv} ۱$ و با ضرب عامل $p-۱$ به دو طرف این تساوی داریم:

$$(p-۱)! \stackrel{p}{\equiv} p-۱ \stackrel{p}{\equiv} -۱$$

در ادامهٔ اثبات قسمت ب از قضیهٔ الف.۴، می‌توانیم $(p-۱)!$ را به شکل زیر فاکتور بگیریم:

$$(p-۱)! = \left[۱ \cdot ۲ \cdot \cdots \cdot \frac{p-۱}{۲}\right]\left[(p-۱)\cdot(p-۲)\cdot \cdots \cdot \frac{p+۱}{۲}\right] = fg$$

هر کدام از عامل‌های f و g حاصل‌ضرب $\frac{p-۱}{۲}$ عامل هستند و jامین عامل از g با قرینهٔ jامین عامل f همنهشت است، بنابراین خواهیم داشت:

$$g \stackrel{p}{\equiv} (-۱)^{\frac{p-۱}{۲}} \cdot f$$

حال وقتی p به شکل $۴n+۱$ باشد آنگاه $\frac{p-۱}{۲}$ عدد زوج است. بنابراین در این حالت $g \stackrel{p}{\equiv} f$. طبق قضیهٔ ویلسن داریم، $f^۲ \stackrel{p}{\equiv} -۱$ که در واقع یعنی $f^۲ + ۱$ بر p بخش‌پذیر است. قسمت بعدی از نوشته‌های هندسه‌دان بزرگ، یانوش بویوئی به‌دست می‌آید [نگاه کنید به

Elemér Kiss, “Fermats’ Theorem in János Bólyai’s Manuscripts,” *Mat Pannonica* 6(1995): 344-8].

بویوئی، $f^۲+۱$ را در حلقهٔ اعداد گاوسی چنین تجزیه کرد:

$$f^۲ + ۱ = (f+i)(f-i)$$

همان‌طور که نشان دادیم، این حاصل‌ضرب در p بخش‌پذیر است. اگر p عدد اول گاوسی باشد، یکی از عامل‌های $f+i$ و $f-i$ را می‌شمارد که این امر ممکن نیست؛ زیرا اگر

$$f \pm i = p(a+ib)$$

داریم $pb = \pm ۱$، که غیرقابل قبول است. در نتیجه p عدد اول گاوسی نیست.

فرض کنید q عدد اول گاوسی باشد که p بر q بخش‌پذیر باشد، یعنی $p = qw$. بنابراین داریم $p = \overline{q}\,\overline{w}$ و در نتیجه p بر $\overline{q}$ نیز بخش‌پذیر است. حال چون q و $\overline{q}$ هر دو اول هستند و متمایزند، طبق قضیهٔ الف.۳، p بر حاصل‌ضربشان، $q\overline{q} = |q|^۲$ بخش‌پذیر است و چون p عدد اول صحیحی است، $p = |q|^۲$ و این مطلب اثبات قسمت ب را کامل می‌کند.

اکنون اثبات قسمت د از قضیهٔ الف.۴. برای اثبات این امر که همه اعداد اول گاوسی غیرصحیح q توسط قسمت ب و ج قابل بیان هستند، نشان می‌دهیم $|q|^۲$ یک عدد اول صحیح است. قرار می‌دهیم $c = |q|^۲$، پس $c = q\overline{q}$. حال اگر c اول نباشد، قابل تجزیه است و اعداد صحیح a و b وجود دارد که $c = ab$ به طوری‌که هر دو از ۱ بزرگ‌ترند. بنابراین $q\overline{q} = ab$ و این نشان می‌دهد ab بر q بخش‌پذیر است. طبق قضیهٔ الف.۳، a یا b بر q بخش‌پذیر است. فرض کنید $a = qf$. چون q عدد صحیحی نیست در نتیجه f یکه نیست. با قرار دادن تجزیه a در تساوی $q\overline{q} = ab$ داریم:

$$qfb = q\overline{q}$$

هر دو طرف تساوی بر q بخش‌پذیر است، بنابراین $fb = \overline{q}$ و این تساوی نشان می‌دهد $\overline{q}$ دارای تجزیهٔ نابدیهی است، که امکان‌پذیر نیست. زیرا $\overline{q}$ عدد اول گاوسی است. می‌دانیم $q\overline{q}$ عدد اول صحیحی است پس به قسمت ب و ج برمی‌گردیم و این مطلب اثبات قضیهٔ الف.۴ را کامل می‌کند.

الف.۶ مطالبی بیشتر دربارهٔ اعداد اول گاوسی

قضیهٔ الف.۴، نتیجهٔ جالبی را در بردارد که خواهیم دید:

نتیجهٔ ۱. هر عدد اول صحیحی مانند p که به شکل $۴n + ۱$ باشد را می‌توان به‌صورت یکتا، به شکل حاصل‌جمع مربع‌های دو عدد صحیح a و b نوشت.

$$p = a^۲ + b^۲$$

یعنی اگر $p = a^۲ + b^۲ = a_۱^۲ + b_۱^۲$، آنگاه دو عدد $a + bi$ و $a_۱ + b_۱ i$ فقط در عامل یکه‌ای متفاوت هستند.

اثبات نتیجهٔ ۱ را به عنوان تمرین به خواننده محول می‌کنیم.

نتیجهٔ ۲. عدد مثبت m را می‌توان به شکل حاصل‌جمع مربع‌های دو عدد صحیح به شکل

$$m = a^۲ + b^۲ \qquad (۶)$$

نوشت اگر و تنها اگر هر مقسوم‌علیه اول صحیح‌اش که به شکل $۴n + ۳$ است به تعداد زوج بار تکرار شود.

اثبات. تجزیه m به شکل $m = st$ را در نظر می‌گیریم، که در آن s حاصل‌ضرب تمام مقسوم‌علیه‌های اول صحیح m است که به شکل $۴n + ۳$ هستند، و t حاصل‌ضرب آنچه که باقی می‌ماند است. اگر هر عامل اول s، به تعداد زوج بار تکرار شود؛ s مربع کامل است و بنابراین برای r که عدد صحیحی باشد داریم $m = r^۲t$.

هر عامل اول صحیح عدد t مانند p_j، برابر ۲ یا به شکل $۴n + ۱$ است. بنابراین طبق نتیجهٔ ۱ خواهیم داشت $p_j^۲ = a_j^۲ + b_j^۲$ که در آن a_j و b_j اعداد صحیح هستند. حاصل‌ضرب مجموع مربعات، خود مجموع مربعات است:

$$(a^۲ + b^۲)(c^۲ + d^۲) = (ac - bd)^۲ + (ad + bc)^۲$$

بنابراین با تکرار این روند، می‌توان نتیجه گرفت که حاصل‌ضرب $t = \Pi p_j$، مجموع مربعات دو عدد صحیح است و در این‌صورت داریم:

$$r^۲t = st = m$$

برعکس، برای نشان دادن اینکه شرایط اعمال شده روی s لازم است، فرض می‌کنیم m را می‌توان به شکل بیان شده در (۶) نوشت. در حلقهٔ اعداد گاوسی، m را می‌توان به این شکل تجزیه کرد:

$$m = (a + ib)(a - ib)$$

فرض کنید m، بر عدد اول صحیح p که به شکل $۴n + ۳$ است، بخش‌پذیر است. حال طبق قضیهٔ الف.۴، p عدد اول گاوسی است و طبق قضیهٔ الف.۳، $a + ib$ یا $a - ib$ بر p بخش‌پذیر است، اکنون قرار می‌دهیم

$$a + ib = pw \qquad (۷)$$

و با مزدوج‌گیری از دو طرف داریم:

$$a - ib = p\overline{w} \qquad (۷')$$

این مطلب نشان می‌دهد، $a + ib$ و $a - ib$، هر دو بر p بخش‌پذیر هستند در نتیجه m بر $p^۲$ بخش‌پذیر خواهد بود. با ادامهٔ این کار، عامل‌های اول به شکل $۴n + ۳$ را جفت‌جفت حذف می‌کنیم و در متناهی مرحله، همه را حذف کرده‌ایم. بنابراین هر عامل اول از m که به شکل $۴n + ۳$ است به تعداد زوج بار تکرار می‌شود؛ این همان ادعای نتیجهٔ ۲ است.

به‌علاوه مشاهده می‌کنیم، اگر a و b در نمایش (۶) نسبت به هم اول باشند، آنگاه m بر هیچ عدد اولی به شکل $۴n + ۳$ بخش‌پذیر نیست. زیرا با اضافه کردن و کم کردن معادلات (۷) و ('۷) خواهیم داشت که a و b هر دو بر p بخش‌پذیرند که با فرض در تناقض است.

۳، ۷، ۱۱، ۱۹، ۲۳، ... اول و به شکل $۴n + ۳$ هستند. از طرف دیگر ۵، ۱۳، ۱۷، ۲۹، ... اول و به شکل $۴n + ۱$ هستند. این بخش را با نشان دادن اینکه نامتناهی عدد اول از هر یک از این دو نوع وجود دارد تمام می‌کنیم. با کمی دستکاری در استدلال کلاسیک اقلیدس، می‌توان نامتناهی بودن اعداد اول به شکل $۴n + ۳$ را نشان داد. با فرض خلف مسئله را حل می‌کنیم. فرض کنیم تعداد چنین اعداد اولی متناهی باشد: $p_۱, p_۲, \dots, p_k$، قرار می‌دهیم، $s = ۴\Pi p_j$ پس $s - ۱ \overset{۴}{\equiv} ۳$. عامل $s - ۱$ را به عامل‌های اول صحیح حقیقی تجزیه می‌کنیم. حداقل یکی از این عامل‌های اول به شکل $۴n + ۳$ است زیرا در غیر این‌صورت حاصل‌ضرب آنها به پیمانهٔ ۴ همنهشت ۱ می‌شود از طرفی این عامل اول $s - ۱$ نسبت به s اول است. بنابراین این عامل اول با هیچ‌یک از p_jها برابر نیست.

حال فرض کنید تعداد اعداد اول به شکل $۴n + ۱$ متناهی باشد: $p_۱, p_۲, \dots, p_k$. قرار می‌دهیم:

$$a = \Pi p_j$$

تعریف می‌کنیم:

$$m = a^۲ + ۱$$

حال چون a و ۱ نسبت به‌هم اول‌اند، می‌توانیم به کمک مشاهدات بالا، نتیجه بگیریم تمام عوامل اول حقیقی m به شکل $۴n + ۱$ هستند. $a^۲$ بر هیچ‌یک از این عوامل بخش‌پذیر نیست. بنابراین آنها با p_jها متفاوت هستند.

ب فشرده‌ترین بسته‌بندی برای جسم‌های محدب

همچنان که در مقدمه ذکر شد، مسائل نقاط مشبکه نه‌تنها محور هندسهٔ اعداد، بلکه در ارتباطی گسترده با ریاضیات مدرن و کاربردهایش هستند. آنها در نظریه‌های گروه‌های متناهی، فرم‌های درجهٔ دوم، ترکیبیات و روش‌های عددی برای محاسبهٔ انتگرال‌های nـ بعدی ظاهر می‌شوند. آنها در شیمی و فیزیک، به‌ویژه در بلورشناسی، و در طراحی کدها برای انتقال، ذخیره و دریافت داده‌ها کاربرد دارند. در این پیوست، نگاهی مختصر به بسته‌بندی کروی خواهیم داشت که خود در توسعهٔ کدهای تشخیص و تصحیح خطا نقشی اساسی دارد. در واقع، مسئلهٔ پیدا کردن راهی برای بسته‌بندی متراکم کره‌ها توی یک فضای داده شده با مسئلهٔ پیدا کردن کدهای کارآمد تصحیح خطا معادل است. اگرچه بحث ما بسیار مختصر خواهد بود، معرفی ما از هندسهٔ اعداد بدون این بحث کامل نبود.

ب.۱ بسته‌بندی در نقاط مشبکه

فرض کنید K یک مجموعهٔ محدب، یا جسم، و نسبت به مبدأ، نقطهٔ O، متقارن است. فرض کنید که ما یک مشبکهٔ پذیرفتنی برای K داریم؛ یعنی مشبکه‌ای که بجز مبدأ، هیچ نقطه‌ای درون K ندارد. اگر ابعاد خطی K نصف شوند تا K به $\frac{1}{2}K$ منقبض شود و اگر نسخه‌های این جسم را چنان روی مشبکه قرار دهیم که مرکزشان روی نقاط مشبکه قرار گیرد، نسخه‌های حاصل هیچ همپوشی نخواهند داشت. برعکس، اگر مشبکهٔ ما، علاوه بر O، نقطهٔ دیگری هم درون K داشت، جسم‌های حاصل همپوشی می‌داشتند. بنابراین، یک مشبکهٔ پذیرفتنی برای K دقیقاً به معنی مشبکه‌ای است که امکان یک بسته‌بندی بدون همپوشی را برای جسم محدب $\frac{1}{2}K$ فراهم می‌کند.

اکنون اجازه دهید چگالی این بسته‌بندی را در یک مشبکهٔ پذیرفتنی مورد توجه قرار دهیم؛ منظور از چگالی در اینجا، نسبتی از فضا است که توسط انتقال‌های جسم $\frac{1}{2}K$ اشغال شده است. حجم هر یک از انتقال‌ها را با $V\left(\frac{1}{2}K\right)$ نمایش می‌دهیم. تعداد نقاط مشبکه در مکعبی به حجم V با بزرگ شدن به V/Δ نزدیک خواهد شد که در اینجا، Δ نشان دهندهٔ حجم ناحیهٔ اصلی مشبکهٔ

پذیرفتنی مورد نظر است. (به یاد آورید که وقتی مشبکه با بردارهای (a,c) و (b,d) تولید می‌شود، $|ad-bc| = |\Delta|$.) بنابراین، حجم کل انتقال‌هایی که توسط V احاطه می‌شوند، با توجه به اینکه مرکز این انتقال‌ها روی نقاط مشبکه است، برابر است با $V\left(\frac{1}{2}K\right)V/\Delta$. با این حساب، برای چگالی بسته‌بندی داریم:

$$\frac{V\left(\frac{1}{2}K\right)}{\Delta} = \frac{V(K)}{2^n\Delta}$$

وقتی Δ کوچک‌ترین مقدار ممکن باشد، چگالی بزرگ‌ترین مقدار ممکن خواهد بود. اگر K مجموعه‌ای با حداقل یک مشبکهٔ پذیرفتنی باشد، تعریف می‌کنیم

$$\Delta(K) = \inf \Delta(L)$$

که در اینجا، اینفیمم (یا بزرگ‌ترین کران پایین) روی همهٔ مشبکه‌های پذیرفتنی برای K گرفته می‌شود. عدد $\Delta(K)$ را دترمینان بحرانی K و مشبکه‌ای که برای آن $\Delta(L) = \Delta(K)$ باشد را مشبکهٔ بحرانی K می‌نامند. بنابراین اگر چگالی فشرده‌ترین بسته‌بندی K را با $\delta(K)$ نمایش دهیم، داریم

$$\delta(K) = \frac{V(K)}{2^n\Delta(K)} \le 1$$

عدد $\delta(K)$ تحت هیچ تبدیل خطی‌ای تغییر نخواهد کرد چرا که تحت چنین تبدیلی هر دوی $V(K)$ و $\Delta(K)$ در مقدار یکسانی ضرب خواهند شد.

اجسامی وجود دارد که برای آنها $\delta(K) = 1$؛ مکعب واحد در $\mathbb{R}^n$ و شش‌ضلعی منتظم در $\mathbb{R}^2$، مثالی از این اجسام هستند. نسخه‌های این جسم‌ها می‌توانند به گونه‌ای قرار داده شود که درون آنها هیچ همپوشی نداشته باشد، و به این ترتیب، آنها می‌توانند همهٔ فضا را پر کنند. مراکز این انتقال‌ها یک مشبکه خواهند بود؛ به این معنی که اگر u و v مرکز باشند، $u+v$ و $u-v$ هم‌مرکز هستند.

ب.۲ فشرده‌ترین بسته‌بندی دایره‌ها در $\mathbb{R}^2$

برخلاف مربع‌ها و شش‌ضلعی‌ها، نمی‌توان با چیدن دایره‌ها یک ناحیهٔ دلخواه در صفحه را پر کرد مگر اینکه اجازهٔ همپوشی را به آنها بدهیم. اما فرض کنید که ما اجازهٔ چنین همپوشی‌ای را ندهیم و در عوض اصرار کنیم که دایره‌ها حداکثر در یک نقطه با هم تماس داشته باشند. اکنون، تا چه اندازه می‌توان آنها را به‌طور کارآمدی بسته‌بندی کرد؟

دایرهٔ واحد به مرکز مبدأ مختصات را در نظر بگیرید. محیط این دایره از نقطه $(1,0)$ می‌گذرد. ما مشبکهٔ پذیرفتنی‌ای را برای این قرص واحد بسته، D، در نظر می‌گیریم که شامل نقطهٔ $(1,0)$ باشد.

به این ترتیب، محور xها شامل نقاط مشبکه به شکل $(n, ۰)$ است که در آن n عدد صحیح است؛ همهٔ نقاط مشبکهٔ دیگر، روی خطوط موازی محور xها و بالا یا پایین آن قرار دارند. فاصلهٔ عمودی نزدیک‌ترین خط از این خطوط مشبکه به محور xها حداقل $\sqrt{۳/۲}$ واحد است. در واقع، فرض کنید نقطهٔ مشبکهٔ (p, q) چنان است که $p > ۰$ و $q < \sqrt{۳/۲}$. نقطهٔ مشبکهٔ زیر را در نظر بگیرید:

$$(p, q) - ([p], ۰) = (p - [p], q)$$

این نقطهٔ مشبکه یا نقطهٔ $(۰, q)$ است یا نقطه‌ای است داخل نوار افقی محدود به خطوط $x = ۰$ و $x = ۱$. اگر $\frac{۱}{۲} \le p - [p] \le ۰$، قرار می‌دهیم $p_۱ = p - [p]$؛ اگر $\frac{۱}{۲} < p - [p] < ۱$، قرار می‌دهیم $p_۱ = p - [p] - ۱$. در هر حالت، $|p_۱| \le \frac{۱}{۲}$ خواهد بود. اما در این حالت، داریم:

$$p_۱^۲ + q^۲ < \left(\frac{۱}{۲}\right)^۲ + \left(\frac{\sqrt{۳}}{۲}\right)^۲ = ۱$$

این نامساوی نشان می‌دهد که نقطهٔ $(p_۱, q)$، نقطهٔ مشبکه‌ای در درون قرص واحد است. اما این، با تعریف یک مشبکهٔ پذیرفتنی برای D در تناقض است.

مشبکه‌ای را که با دو بردار $(۱, ۰)$ و $\left(\frac{۱}{۲}, \frac{\sqrt{۳}}{۲}\right)$ تولید می‌شود را در نظر بگیرید. به‌وضوح، این مشبکه برای D پذیرفتنی است چون امکان بسته‌بندی $\frac{۱}{۲}K$ را فراهم می‌کند. علاوه بر این، ل. فِجِز توث [۶] در سال ۱۹۴۰ ثابت کرد که این مشبکه بحرانی نیز هست و بنابراین، $\Delta(D) = \sqrt{۳}/۲$. توجه کنید این مشبکهٔ بحرانی یک شش‌ضلعی است که رأس‌های آن در $(\pm ۱, ۰)$ و $\left(\pm\frac{۱}{۲}, \pm\frac{\sqrt{۳}}{۲}\right)$ قرار دارند. بنابراین، چگالی فشرده‌ترین بسته‌بندی مشبکه برای D برابر است با

$$\delta(D) = \frac{v(D)}{۴\Delta(D)} = \frac{\pi}{۴\left(\frac{\sqrt{۳}}{۲}\right)} = \frac{\pi}{۲\sqrt{۳}} = ۰/۹۰۶۶۸۹۹۶\cdots$$

دلیل علاقه‌مندی به چگالی بهینه در دو بعد کاملاً موجه است. جواب این مسئله برای بسیاری از موضوع‌های عملی از قبیل بهترین روش قرار دادن رشته سیم‌ها در یک مقطع از کابل دارای اهمیت است. در مورد دایره‌ها در $\mathbb{R}^۲$ می‌توان چیزهای بسیار بیشتری را اثبات کرد. خوانندهٔ علاقه‌مند می‌تواند مقالهٔ ب. سگر و ک. ماهلر را با عنوان «On the Densest Packing of Circles» [۱۴] مطالعه کند.

ب.۳ بسته‌بندی کره‌ها در $\mathbb{R}^n$

در $\mathbb{R}^n$، یک دستگاه از کره‌ها با حجم V را یک بسته‌بندی گوییم در صورتی‌که هیچ دو کرهٔ دستگاه دارای یک نقطهٔ درونی مشترک نباشند. در بخش قبل، برای $n = ۲$، یک مشبکهٔ بحرانی برای دایره‌های

واحد ساختیم و چگالی آن را محاسبه کردیم. برای $n = ۳$، تاریخ مسئله جالب است. این تاریخ به‌طور مفصل توسط فیلیپ گریفیتس در *American Mathematical Monthly* [۸] و توماس هیلز در Notices of the AMS [۱۱] شرح داده شده است. ما در اینجا فقط مرورکوتاهی خواهیم داشت.

در اواخر ۱۵۰۰، سر والتر رالی در نامه‌ای به یک ریاضی‌دان انگلیسی به نام توماس هریوت، این سؤال را مطرح کرد که کارآمدترین راه برای تلنبار کردن گلوله‌های توپ در عرشهٔ یک کشتی چیست. هریوت، سؤال را برای ستاره‌شناسی به نام یوهان کپلر فرستاد. کپلر حدس زد که چگال‌ترین بسته‌بندی همان روشی است که دریانوردان به‌طور معمول گلوله‌های توپ را تلنبار می‌کنند یا کمی لطیف‌تر، همان روشی است که امروز میوه‌فروشان پرتقال‌ها را روی هم می‌چینند. این به حدس کپلر معروف شد و به خاطر تحقیقات ریاضی زیادی که حول و حوش آن شکل گرفت برای سال‌ها به‌عنوان یک مسئلهٔ مهم مطرح بود.

در هر میوه‌فروشی، می‌توان میوه‌هایی را مشاهده کرد که لایه‌لایه روی هم چیده شده‌اند. پایین‌ترین لایه، مستطیل شکل است و هر یک از لایه‌های بعدی روی «سوراخ‌های گود» و طبیعی لایهٔ قبلی چیده شده‌اند و شکل کلی ساختاری هرمی شکل دارد. مراکز این میوه‌ها (یا گلوله‌های توپ) مشبکه‌ای را شکل می‌دهند که به مشبکهٔ مکعبی با وجوه مرکزی[1] (به اختصار مشبکهٔ fcc) معروف است. آنها را می‌توان به‌طور ساده با مجموعهٔ نقاط مشبکهٔ (x, y, z) در $\mathbb{Z}^۳$ توصیف کرد که $x + y + z$ زوج است. چگالی این بسته‌بندی برابر است با

$$\delta(K) = \frac{\pi}{\sqrt{۱۸}} = ۰/۷۴۰۵ \cdots$$

بنابراین، تعبیر سؤال متداول ما در مورد این بسته‌بندی کروی این است که آیا این بسته‌بندی در میان همهٔ بسته‌بندی‌ها ماکسیمال است. گاوس در ۱۸۳۱ [۷] اثبات کرد که مشبکهٔ fcc بحرانی است؛ این یعنی، مشبکهٔ fcc در میان همهٔ بسته‌بندی‌های مشبکه، چگال‌ترین است.

ولی مسئله هنوز خیلی پیچیده است چرا که همهٔ بسته‌بندی‌ها مشبکه نیستند، حل مسئله کلی‌تر بسیار سخت بود. ل. فِجِز توث در ۱۹۵۳، با تحویل مسئله به یک مسئله محاسباتی سخت ولی قابل انجام با کامپیوتر قدمی بزرگ برداشت. برای سال‌ها، بهترین کران شناخته شده، کرانی بود که توسط سی.اِ. راجرز [۱۳] در ۱۹۵۸ داده شد. او نشان داد که چگالی هیچ بسته‌بندی کروی نمی‌تواند از ۰/۷۷۹۶۰۰۰ بیشتر باشد. در زمانی نه‌چندان دور، بالاخره حدس کپلر توسط هیلز اثبات شد؛ او از پیشرفت‌های متأخر در ریاضیات و توان محاسباتی وسیع کامپیوترها [۹, ۱۰] برای اثبات نتیجهٔ مورد نظرش استفاده کرد. مقاله‌ای که در بالا ذکر شد [۱۱]، مروری خوب بر تاریخ مسئله و شرحی قابل فهم از کار او ارائه می‌دهد.

1. face-centered cubic lattice

اکنون، برای $n = ۴$، مشبکهٔ معروف به مشبکهٔ صفحهٔ شطرنج را در نظر می‌گیریم. همانند مشبکهٔ fcc، مشبکهٔ صفحهٔ شطرنج با مجموعهٔ نقاط (x, y, z, w) در $\mathbb{Z}^۴$ تعریف می‌شود که برای آنها $x + y + z + w$ زوج است. مجموعهٔ بردارهای $(۲, ۰, ۰, ۰)$، $(۱, ۱, ۰, ۰)$، $(۱, ۰, ۱, ۰)$ و $(۱, ۰, ۰, ۱)$ یک مجموعه از بردارهای مولد است. بنابراین $\Delta = ۲$ و کره دارای شعاعی به طول $\frac{\sqrt{۲}}{۲}$ است. بنابراین، چگالی این مشبکه برابر خواهد بود با

$$\delta(K) = \frac{\pi^۲}{۱۶} = ۰/۶۱۶۹\ldots$$

کورکین و زولوتارف [۱۲] در ۱۸۷۲ ثابت کردند که مشبکهٔ صفحهٔ شطرنج بحرانی و بنابراین، $\frac{\pi^۲}{۱۶}$ چگالی ماکسیمال در بین بسته‌بندی‌های مشبکه است. برای دیدن این نتیجه و بسیاری از نتایج دیگر در ابعاد بالاتر، به کتابی که در ۱۹۸۸ توسط کانوی و اسلوان تحت عنوان *Sphere Packings, Lattices and Groups* [۵] منتشر شد نگاه کنید. این کتاب، مقدمه‌ای ساده، بسیار عالی و جمع‌بندی‌ای کامل از آنچه تا آن زمان درمورد بسته‌بندی کروی شناخته شده بود ارائه می‌دهد. علاوه بر این، ما مایلیم خوانندهٔ علاقه‌مند را به کتاب تامپسون، *Error-Correcting codes through Sphere Packings to Simple Groups* [۱۵] ارجاع دهیم. این کتاب، جمع‌بندی‌ای خوب از نتایج شناخته شده، تصویری شفاف از ارتباط میان سه حوزهٔ مذکور در عنوان کتاب و تاریخی بسیار جالب از آنها را ارائه می‌دهد.

درواقع، بلیکفلت اولین فردی بود که برای چگالی فشرده‌ترین بسته‌بندی کروی در ابعاد دلخواه، کرانی کوچک‌تر از ۱ به‌دست آورد. این در مقالهٔ معروف او در ۱۹۱۴ [۱] منتشر شد، اما اثبات او فقط مربوط به بسته‌بندی‌های مشبکه‌ای بود. او قضیهٔ زیر را اثبات کرد:

قضیهٔ ۴.۱۰ (بلیکفلت) $\delta(k)$، چگالی فشرده‌ترین بسته‌بندی از کره‌های معادل در $\mathbb{R}^n$، بیشتر از $\frac{n+۲}{(\sqrt{۲})^{n+۲}}$ نیست:

$$\delta(K) \leq \frac{n+۲}{(\sqrt{۲})^{n+۲}}$$

بلیکفلت، بعداً بعضی از مشبکه‌های بحرانی را در شش، هفت و هشت بعد پیدا کرد [۲-۴]. او [۳]، همچنین نتیجهٔ قضیهٔ ۴.۱۰ را چنان تعمیم داد که برای بسته‌بندی‌های دلخواه نیز کار کند.

مراجع

1. H. F. Blichfeldt, “A New Principle in the Geometry of Numbers with Some Applications,” *Transactions of the AMS* 15:3 (July 1914): 227-35.

2. ________, "On the Minimum Value of Positive Real Quadratic Forms in 6 Variables," *Bulletin of the AMS* 31 (1925): 386.

3. ________, "The Minimum Value of Quadratic Forms, and the Closest Packing of Spheres." *Mathematische Annalen* 101 (1929): 605-8.

4. ________, "The Minimum Values of Positive Quadratic Forms in Six, Seven, and Eight Variables," *Mathematische Zeitschrift* 39 (1934): 1-15.

5. J. G. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups* (New York and Berlin: Springer-Verlag, 1988), Preface and Chapter 1, 1-30.

6. L. Fejes Toth, "Über Einen geometrischen Satz," *Mathematische Zeitschrift* 46 (1940): 79-83.

7. C. F. Gauss, "Besprechung des Buchs von L. A. Seeber: Untersuchungen über die Eigeschaften der positiven ternaren quadratischen Formen usw.," *Göttingsche Gelehrte Anzeigen* (July 9, 1831); reprinted in *Werke*, Vol. 2 (Göttingen: Gesell-schaft der Wissenschaften, 1876), 188-96.

8. Phillip A. Griffiths, "Mathematics at the Turn of the Millennium," *American Mathematical Monthly* 107 (2000): 1-14.

9. Thomas Hales, "Sphere Packings. I," *Discrete Comp. Geom.* 17 (1997): 1-15.

10. ________, "Sphere Packings. II," *Discrete Comp. Geom.* 18 (1997): 135-49.

11. ________, " Cannonballs and Honeycombs," *Notices of the AMS* 47 (2000): 440-9.

12. A. Korkine and E. I. Zolotareff, "Sur les formes quadratiques positives quaternaires," *Mathematische Annalen* 5 (1872): 581-3.

13. C. A. Rogers, "The Packing of Equal Spheres," *Proceedings of the London Mathematical Society* 8 (1958): 609-20.

14. B. Segre and K. Mahler, "On the Densert Packing of Circles," *American Mathematical Monthly* 51 (1944): 261-70.

15. Thomas M. Thompson, *From Error-Correcting Codes through Sphere Packings to Simple Groups*, Carus Monograph Series, No. 21 (Washington, DC: MAA, 1983).

ج زندگی‌نامه‌های مختصر

هرمان مینکوفسکی (۱۸۶۴-۱۹۰۹)

هیچ‌چیز زیباتر از حقیقت نیست، و حقیقت از همه‌چیز دوست داشتنی‌تر است.
ـــ شعار مینکوفسکی

هرمان مینکوفسکی در ۱۸۶۴ در آلکسوتن روسیه متولد شد و در کونشیزبرگ آلمان رشد کرد و بیشتر عمر دانشگاهیش را هم همان‌جا گذراند. او به سرعت مدارج دانشگاهی را طی کرد و در ۱۸۸۵ به درجهٔ دکتری رسید، در ۱۸۸۷ مدرس دانشگاه بن شد و در ۱۸۹۲ به درجهٔ استادی رسید. مینکوفسکی در تعطیلات معمولاً به کونشیزبرگ برمی‌گشت تا با داوید هیلبرت (۱۸۶۲-۱۹۴۳) و آدولف هورویتس (۱۸۵۸-۱۹۱۹) همکاری کند. او مدتی هم در کونشیزبرگ مستقر شد و در ۱۸۹۴ در دانشگاه آنجا به مقام استادی رسید و در ۱۸۹۵ استادِ تمام شد. با این حال او شیفتهٔ زوریخ سوئیس بود و در ۱۸۹۶ در آنجا استادِ تمام شد و سال بعد ازدواج کرد. بالاخره، مینکوفسکی برای اینکه باز با هیلبرت باشد در ۱۹۰۲ به گوتینگن رفت و در ۱۹۰۹ در همان‌جا به‌طور غیرمنتظره‌ای بر اثر آپاندیس حاد درگذشت ـــ در حالی‌که فقط چهل‌وپنج سال داشت و در اوج کار علمی بود.

مینکوفسکی نابغه‌ای پیش‌رس بود. او در ۱۸۸۰، درحالی که هنوز شانزده سالش تمام نشده بود، تحصیلات دبیرستانی را در کونشیزبرگ تمام کرد و به دانشگاه رفت. او در پنج نیمسال تحصیلی زیر نظر هاینریش [مارتین] وبر و والدمار فوگت تحصیل کرد. سپس به مدت سه نیمسال به برلین رفت و دوره‌هایی را با ادوارد کومر، لئوپولد کرونکر، کارل وایرشتراس، هرمان [لودویک فردیناند] فون هلمهولتس و گوستاف [روبرت] کیرشهوف گذراند. بعضی از این نام‌ها نشان می‌دهند که مینکوفسکی به‌طور جدی فیزیک هم می‌خوانده و این هم به نوبهٔ خود علت علاقهٔ بعدیش ـــ نظریهٔ نسبیت ـــ را معلوم می‌کند.

در ۱۸۸۱ فرهنگستان فرانسه برای جایزهٔ بزرگش مسئلهٔ سختی دربارهٔ فرم‌های درجهٔ دوم مطرح

کرد و شرکت‌کنندگان می‌بایست راه‌حلشان را بدون نام خودشان و با نام مستعار ارائه می‌کردند. راه‌حل شامل اثبات و تکمیل قضیه‌هایی از فردیناند آیزنشتاین (۱۸۵۲-۱۸۲۳) بود که خودش شاگرد گاوس و عدهٔ قابل توجهی از گروه داوران بود. آیزنشتاین در بیست‌ونه سالگی درگذشته بود، و شگفت آنکه خود مینکوفسکی هم وقتی راه‌حل مسئلهٔ فرهنگستان را کامل می‌کرد هنوز هجده‌ساله هم نشده بود و جایزه را یک سال بعد، در ۱۸۸۳ دریافت کرد.

جایزهٔ بزرگ آن سال به‌طور مشترک به مینکوفسکی و هنری [جان استفن] اسمیت (۱۸۸۳-۱۸۲۶)، ریاضیدان انگلیسی [ایرلندی‌تبار] اعطا شد. اسمیت، که جایزه یک ماه پس از مرگش به او اعطا شد، به خاطر ده سالی که به بررسی تقریباً هر چیز شایان توجه در نظریهٔ اعداد پرداخته بود مشهور بود و گزارش این بررسی‌ها را از ۱۸۵۹ تا ۱۸۶۵ در مجلدهای انجمن بریتانیایی منتشر می‌کرد. این گزارش‌ها هنوز هم نمونهٔ کار اصیل تمیز و دقیق هستند. اسمیت دو مقاله هم در مجموعه مقالات انجمن سلطنتی در ۱۸۶۴ (سال تولد مینکوفسکی!) و ۱۸۶۸ داشت که در آنها مسئلهٔ سال ۱۸۸۱ فرهنگستان فرانسه را حل کرده بود. اسمیت کارش را در ۱۸۸۲ به فرهنگستان فرستاد و تصمیم گرفته شد که جایزه به‌طور مشترک اعطا شود.

متأسفانه، تصمیم فرهنگستان عواقب ناخوشایندی برای مینکوفسکی داشت. هم اعتبار جایزهٔ بزرگ بسیار زیاد بود و هم نگاه ضدآلمانی پس از جنگ‌های فرانسه و اتریش، و در نتیجه بعضی از دانشمندان به جایزهٔ مشترک معترض شدند و در مطبوعات به مینکوفسکی حمله می‌کردند و او را متهم به سرقت علمی می‌کردند. در مقابل، بزرگان فرهنگستان فرانسه مانند کامی ژردان، ژاک برتران و شارل ارمیت به دفاع از مینکوفسکی برخاستند. ژردان در آن ایام ناخوشایند به خود او نامه‌ای نوشت و او را به گرمی تشویق کرد: «سخت بکوش، مرد جوان؛ قول می‌دهم که هندسه‌دان مشهوری خواهی شد!»

چنان‌که گفتیم، مینکوفسکی در فیزیک هم مانند ریاضیات مستعد بود. وقتی آلبرت اینشتین ــ که هنوز چندان شناخته شده نبود ــ در ۱۹۰۵ مقالهٔ سی‌صفحه‌ایش را در جلد هفدهم آنالن دِر فیزیک منتشر کرد، مینکوفسکی آن را به‌دقت مطالعه کرد و بالاخره، با شروع از اصولی که اینشتین مطرح کرده بود، کارهای مهمش را در زمینهٔ نظریهٔ نسبیت خاص انجام داد. او در ۱۹۰۸ سخنرانی‌هایی با عنوان فضا و زمان ایراد کرد و در آنها نگاه جدیدی به فضا و زمان مطرح کرد. یکی از دستاوردهای اساسی مینکوفسکی این بود که جرم و انرژی متناسب‌اند. بعدها، مینکوفسکی این نظریه را تعمیم داد و به این نتیجه رسید که ماده، شعاع نور را جذب می‌کند.

اندکی بعد، او درگذشت ــ ذهنی درخشان و فعال آرام گرفت. چه کسی می‌داند که استعدادهای شگرف او چه تأثیری می‌توانست بر حوزه‌هایی که فیزیک به آنها می‌پرداخت بگذارد؟ دست‌کم در ریاضیات یادگار او پیش روی ماست: «هندسهٔ اعداد»ش که به آن عشق می‌ورزید، همچنان یاد او را زنده نگاه می‌دارد.

هانس فردریک بلیکفلت (۱۹۴۵-۱۸۷۳)

هانس فردریک بلیکفلت در ۱۸۷۳ در دهی در ناحیهٔ گرونبک دانمارک متولد شد. در خانوادهٔ پدری او کشاورز، وزیر و اسقف یافت می‌شد و در خانوادهٔ مادریش هم عالمان و معلمان بسیاری وجود داشتند. بلیکفلت، پیش از اینکه در ۱۸۸۸ با پدر و برادرخواندهٔ بزرگ‌ترش به آمریکا مهاجرت کند، در امتحان‌های دولتی که زیر نظر دانشگاه کپنهاگ برگزار می‌شد با درجهٔ ممتاز موفق شده بود. در همان دوران، خودش روش حل صورت کلی معادله‌های چندجمله‌ای درجهٔ سه و چهار را کشف کرد ــ کاری قابل اعتنا، از کسی که هنوز به پانزده‌سال هم نرسیده است.

بلیکفلت جوان، جثه‌ای تنومند داشت و همین امر در چهار سال اول ورودش به آمریکا که «هر کار یدی‌ای می‌کرد» ــ عمدتاً در صنایع چوب‌بری شمال‌غربی اقیانوس آرام ــ به‌خوبی به او کمک کرد. او از ۱۸۹۲ تا ۱۸۹۴ به‌عنوان نقشه‌کش در شهر و ناحیهٔ واتکم، واشینگتن کار کرد، و در آنجا بود که مهندسان کارفرمایش متوجه استعداد غیرعادی او در ریاضیات شدند و او را تشویق کردند که درخواستی برای پذیرش در دانشگاه تازه‌تأسیس استنفورد در کالیفرنیا بفرستد.

بلیکفلت در سپتامبر ۱۸۹۴ در استنفورد پذیرفته شد و تا ژوئن ۱۸۹۶ دورهٔ کارشناسی و در ۱۸۹۷ دورهٔ کارشناسی ارشدش را گذراند. او با روش «انتخاب آزاد» که در آن زمان در استنفورد رایج بود توانست به‌طور متمرکز به ریاضیات بپردازد و به‌سرعت به اهدافش برسد.

در اواخر قرن نوزدهم میلادی، معمول بود که ریاضیدانان جوان مشتاق برای درس‌های پیشرفته به آلمان بروند. مقرر شد که بلیکفلت به دانشگاه لایپزیگ برود و زیر نظر سوفوس لی (۱۸۹۹-۱۸۴۲) تحصیل کند.

بلیکفلت در سال تحصیلی ۱۸۹۸-۱۸۹۷ زیر نظر لی کار کرد و بر «نظریهٔ لی» گروه‌های پیوسته مسلط شد، و در ۱۸۹۸ عنوان دکتری را با درجهٔ بسیار ممتاز دریافت کرد. پایان‌نامهٔ دکتریش، «دربارهٔ ردهٔ خاصی از تبدیل‌ها در فضای سه‌بعدی»، در ۱۹۰۰ در امریکن جورنال آو متمتیکس (جلد ۲۲، صص، ۱۱۳-۱۲۰) منتشر شد. بلیکفلت به استنفورد برگشت و چهل سال در آنجا تدریس کرد. او در ۱۹۱۳ به درجهٔ استادی رسید و از ۱۹۲۷ تا ۱۹۳۸ رئیس بخش ریاضی بود. بلیکفلت تعداد نسبتاً کمی مقاله منتشر کرده است ــ چیزی حدود بیست و پنج مقالهٔ پژوهشی. او دو کتاب هم تألیف کرده است: گروه‌های متناهی تبدیل‌های همگن خطی و گروه‌های متناهی هم‌خطی‌سازی.

آنچه گفتیم همهٔ قابلیت‌های بلیکفلت را به‌نحو مناسب نشان نمی‌دهد. او به بسیاری از مسئله‌های دشوار زمان خودش پرداخت و بعضی را حل کرد، اما بسیاری از کارهایی را که انجام داده بود ناتمام رها کرد. تقریباً همیشه، وقتی مسئله را به‌جایی می‌رساند که برای خودش قانع‌کننده بود، زحمت تنظیم یادداشت‌هایش برای انتشار آنقدر برایش زیاد بود که به‌کلی از خیر آن می‌گذشت. خبره‌ای گفته است

که بلیکفلت «بشکه‌ای از چیزهای خوب» به‌جا گذاشته است. در بسیاری از مواقع، او فقط چکیدهٔ دستاوردهایش را در بولتن انجمن ریاضی آمریکا منتشر می‌کرد و کار را رها می‌کرد. دو کار او که به‌کار خوانندگان این کتاب می‌آیند عبارت‌اند از مقالهٔ ۱۹۱۴ او («اصلی جدید در هندسهٔ اعداد و برخی از کاربردهای آن») و کار ۱۹۳۴ او («مقدارهای کمینهٔ فرم‌های درجهٔ دوم مثبت با شش، هفت و هشت متغیر») که به‌ترتیب در فصل‌های ۸ و ۹ به آنها اشاره کردیم.

او عنوان‌ها و نشان‌های فراوانی دریافت کرد؛ از جمله معاونت انجمن ریاضی آمریکا (۱۹۱۲)، انتخاب در فرهنگستان ملی علوم در ۱۹۲۰، عضویت در شورای ملی پژوهش از ۱۹۲۴ تا ۱۹۲۷، و شوالیهٔ محفل دنه‌بروگ (دانمارک).

مراجع

1. Harold M. Bacon, *Dictionary of American Biography, Third Supplement, 1941-45* (New York: Scribner, 1973): see Blichfeldt.

2. E. T. Bell, "Jams Frederik Blichfeldt," *National Academy Biographical Memoirs,* Vol. 26, 181-7.

3. ________, *Development of Mathematics,* reprint of 2nd ed. (New York: Dover, 1992): re: Minkowski.

4. Florian Cajori, *A History of Mathematics* (New York: Macmillan, 1931).

5. J. Fang, *Hilbert* (New York: Paideia Press, 1970): re: Minkowski.

6. David Hilbert, "Hermann Minkowski," *Math. Annalen* 68(1910): 455-71.

جواب‌ها و راهنمایی

فصل ۱

۱. الف) $y = \frac{۲}{۳}x + \frac{۱}{۵}$ (چون ۳ بر ۵ بخش‌پذیر نیست). مثال‌های دیگر، مشابه همین مثال هستند.

ب) $y = \frac{۲}{۱۵}x + \frac{۱}{۳}$ (زیرا ۱۵ | ۳). $(p_۰, q_۰) = (۵, ۱)$؛

$$\left\{(p_k, q_k) = (۵ + ۱۵k, ۱ + ۲k), \mid \text{ عددی صحیح است. } k\right\}$$

۲. راهنمایی: با استفاده از فرمول فاصله، d_k، طول پاره‌خطی را که بین دو نقطهٔ $(p_{k-۱}, q_{k-۱})$ و (p_k, q_k) قرار دارد، پیدا کنید. اگر d_k تابعی از k نباشد، آنگاه از هر نقطه به هر نقطهٔ مشبکهٔ مجاور مقداری ثابت است.

۳. راهنمایی: فرض کنید $x = p_۱ + k(p_۲ - p_۱)$ و $y = q_۱ + k(q_۲ - q_۱)$. از این واقعیت استفاده کنید که $q_۱ = mp_۱ + b$ و $q_۲ = mp_۲ + b$.

۴. به وضوح، $(p, q) = (n, m)$ روی خط راست و n و m نسبت به هم اولند.

$$\left|(n, m)\right| = \sqrt{n^۲ + m^۲}$$

اگر $(p_۱, q_۱)$ روی خط باشد، آنگاه $mp_۱ = nq_۱$. چون $n \mid p_۱$. $\gcd(n, m) = ۱$. مثلاً $nr_۱ = p_۱$. پس $q_۱ = mr_۱$. بنابراین

$$\left|(p_۱, q_۱)\right| = \sqrt{n^۲r_۱^۲ + m^۲r_۱^۲} = r_۱\sqrt{n^۲ + m^۲} \geq \left|(n, m)\right|$$

۵. خیر. اگر (p, q) روی خط باشد، آنگاه $\sqrt{۲} = q/p$.

۶. الف) فرض کنید $p = q = ۱$.

$$\left|\sqrt{۲}p - q\right| < \left|۱/۴۱۴۲۱۳۶(۱) - ۱\right| = ۰/۴۱۴۲۱۳۶ < \epsilon = \frac{۱}{۲} = ۰/۵$$

ب) فرض کنید $p = ۱۰$، $q = ۱۴$.

$$\left|\sqrt{۲}(۱۰) - ۱۴\right| < |۱۴/۱۴۲۱۳۶ - ۱۴| = ۰/۱۴۲۱۳۶ < \epsilon = \frac{۱}{۵} = ۰/۲$$

ج) فرض کنید $p = ۵$، $q = ۷$.

$$\left|\sqrt{۲}(۵) - ۷\right| = \frac{۱}{۲}\left|\sqrt{۲}(۱۰) - ۱۴\right| < \left(\frac{۱}{۲}\right)\frac{۱}{۵} = \frac{۱}{۱۰} = ۰/۱$$

بخش ۱.۲

۱. الف) $۴ = [۴/۱] = [۱/۳ + ۲/۸]$، درحالی که $۳ = ۱ + ۲ = [۱/۳] + [۲/۸]$.

ب) $۲ = [۲] = \left[\frac{۵/۴}{۲/۷}\right]$، درحالی که $۲/۵ = \frac{۵}{۲} = \frac{[۵/۴]}{[۲/۷]}$.

ج) $۹ = [۹/۶۲] = \left[(۳/۷)(۲/۶)\right]$، درحالی که $۶ = (۳)(۲) = [۳/۷][۲/۶]$.

۲. فرض کنید $x = [x] + \zeta$، که در آن $۰ \leq \zeta < ۱$.

$$[x+n] = \left[[x] + \zeta + n\right] = \left[\left([x]+n\right) + \zeta\right] = [x] + n$$

۳. راهنمایی: $[n] = n$ و $[-n] = -n$ اگر n صحیح باشد، $x = [x] + \zeta$ و $-x = -[x] - \zeta$

اگر x صحیح نباشد، بنابراین $[-x] = -[x] - ۱$.

۴. $[x/n] = \left[\left([x]+\zeta\right)/n\right] = \left[\left([x]/n\right) + (\zeta/n)\right]$، که در آن $\zeta/n < ۱/n$.

$$[x]/n = q + (r/n)$$

که در آن $۰ \leq r \leq n - ۱$. بنابراین

$$q < \left(\frac{[x]}{n}\right) + \left(\frac{\zeta}{n}\right) < q + \frac{n-۱}{n} + \frac{۱}{n} = q + ۱$$

و

$$\left[\frac{x}{n}\right] = \left[\frac{[x]}{n} + \frac{\zeta}{n}\right] = q$$

۵. $[۲x] + [۲y] = \left[۲\left([x] + \zeta_۱\right)\right] = \left[۲\left([y] + \zeta_۲\right)\right] = ۲[x] + [۲\zeta_۱] + ۲[y] + [۲\zeta_۲]$.

$[x] + [y] + [x+y] = [x] + [y] + \left[[x] + \zeta_۱ + [y] + \zeta_۲\right] = ۲[x] + ۲[y] + [\zeta_۱ + \zeta_۲]$.

اگر $۰ \leq \zeta_۱$، $\zeta_۲ < \frac{۱}{۲}$، آنگاه $۰ \leq ۲\zeta_۱$، $۲\zeta_۲ < ۱$، یا $[\zeta_۱ + \zeta_۲] = ۰ = [۲\zeta_۱]$. اگر $۰ \leq \zeta_۱ < \frac{۱}{۲}$، $\frac{۱}{۲} \leq \zeta_۲ < ۱$، آنگاه $[۲\zeta_۱] = ۰$، $[۲\zeta_۲] = ۱$، $[\zeta_۱ + \zeta_۲] = ۰$ یا ۱. اگر $\frac{۱}{۲} \leq \zeta_۱$، $\zeta_۲ < ۱$، آنگاه $[\zeta_۱ + \zeta_۲] = ۱ = [۲\zeta_۲] = [۲\zeta_۱]$.

۶. اگر $a < b$، آنگاه $\circ \times b < a < \text{۱} \times b$، درحالی‌که $[a/b] = \circ$. اگر $a = b$، آنگاه $a = \text{۱} \times b$، درحالی‌که $[a/b] = \text{۱}$. اگر $a > b$، قسمت مثبت خط اعداد حقیقی را به بازه‌های به هم متصل به طول b تقسیم کنید. چون a باید در بازه‌ای مانند $kb < a < (k+\text{۱})b$، برای عدد صحیحی مانند k، قرار گیرد، می‌توانیم بنویسیم $a = kb + r$. بنابراین $\left[\frac{a}{b}\right] = \left[k + \left(\frac{r}{b}\right)\right] = k$.

۷. راهنمایی: نمودارهای x، $[x]$، $-[x]$ و $[-x]$ را رسم کنید. سپس توجه کنید که

$$-[-x] = -\left[-[x] - \zeta\right] = -\left(-[x]\right) - [-\zeta] = [x] - (-\text{۱}) = [x] + \text{۱}$$

۸. اگر $x = n$، صحیح باشد، آنگاه $\left[x + \frac{\text{۱}}{\text{۲}}\right] = \left[n + \frac{\text{۱}}{\text{۲}}\right] = n = x$. اگر $n < x < n + \frac{\text{۱}}{\text{۲}}$، آنگاه $n + \frac{\text{۱}}{\text{۲}} < x + \frac{\text{۱}}{\text{۲}} < n + \text{۱}$ و $\left[x + \frac{\text{۱}}{\text{۲}}\right] = n$. اگر $n < x < n + \frac{\text{۱}}{\text{۲}}$، آنگاه $n + \text{۱} < x + \frac{\text{۱}}{\text{۲}} < n + \frac{\text{۳}}{\text{۲}}$، بنابراین $\left[x + \frac{\text{۱}}{\text{۲}}\right] = n + \text{۱}$. اگر $x = n + \frac{\text{۱}}{\text{۲}}$ ، آنگاه $\left[x + \frac{\text{۱}}{\text{۲}}\right] = [n + \text{۱}] = n + \text{۱}$.

۹. با یک دستکاری کوچک در مسألهٔ ۸ حل می‌شود.

۱۰. بنابر مسألهٔ ۶، دقیقاً $\left[\frac{n}{p}\right]$ از مضارب p، کوچک‌تر از یا مساوی با n هستند. هر یک از اینها به‌عنوان یکی از عوامل $n!$ ظاهر خواهد شد. از اینها، تعداد $\left[\left[\frac{n}{p}\right]/p\right]$ عدد، مضاربی هستند که بر خود p بخش‌پذیرند. بنابراین، اینها، مضارب $p^{\text{۲}}$ هستند، چون p، به عنوان یک عامل، حداقل دوبار ظاهر می‌شود. اکنون قرار دهید $n/p = q + (r/p)$، که در آن $\circ \le r \le p - \text{۱}$. آنگاه $n/p^{\text{۲}} = (q/p) + (r/p^{\text{۲}}) = q_{\text{۱}} + (r_{\text{۱}}/p) + (r/p^{\text{۲}})$، که در آن $\circ \le r_{\text{۱}} \le p - \text{۱}$. حالا

$$\circ \le (r_{\text{۱}}/p) + (r/p^{\text{۲}}) \le \left((p-\text{۱})/p\right) + \left((p-\text{۱})/p^{\text{۲}}\right)$$
$$= \text{۱} - (\text{۱}/p) + (\text{۱}/p) - (\text{۱}/p^{\text{۲}}) = \text{۱} - (\text{۱}/p^{\text{۲}}) < \text{۱}$$

بنابراین $[n/p^{\text{۲}}] = q_{\text{۱}} = [[n/p]/p]$. اگر به همین طریق ادامه دهیم، می‌بینیم که

$$[n/p^{\text{۳}}] = [[n/p^{\text{۲}}]/p]$$

از اینها درواقع مضارب $p^{\text{۳}}$ هستند؛ p، به عنوان یک عامل، سه بار ظاهر می‌شود. با تکرار، به بزرگ‌ترین توان p^k می‌رسیم که بعد از آن $\left[\frac{n}{p^j}\right] = \circ$ ، بنابراین

$$E(n,p) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^{\text{۲}}}\right] + \cdots + \left[\frac{n}{p^k}\right]$$

بخش ۲.۲

۲. راهنمایی: با قرار دادن (p_k, q_k)ها در معادلهٔ خط نشان دهید که هر کدام یک جواب است. برای اینکه نشان دهید هر جواب به همین شکل است، فرض کنید که (p, q) یک جواب دلخواه است و بنویسید

$$ap + bq = n$$

$$ap_\circ + bq_\circ = n$$

دو معادله را از هم کم کنید و از این واقعیت استفاده کنید که $\gcd(a, b) = ۱$.

۳. راهنمایی: از هر یک از معادلات مسألهٔ ۱ می‌توانید استفاده کنید.

۴. با توجه به شکل واضح است.

بخش ۳.۲

۱. سه حالت را باید بررسی کرد. (۱) P و Q، هر دو فرد؛ (۲) P (یا Q) زوج و Q (یا P) فرد؛ (۳) P و Q، هر دو زوج.

حالت ۱: پس $P - ۱$ و $Q - ۱$ هر دو زوج هستند، بنابراین $۲ \mid (P - ۱)(Q - ۱)$. چون همهٔ عامل‌های P و Q فرد هستند، d باید فرد باشد. بنابراین $d - ۱$ زوج است و $۲ \mid (d - ۱)$.

حالت ۲: پس $Q - ۱$ زوج است، بنابراین $۲ \mid (P - ۱)(Q - ۱)$. چون ۲ فقط یکی از P و Q را تقسیم می‌کند، d را تقسیم نمی‌کند. بنابراین، $d - ۱$ زوج است و $۲ \mid (d - ۱)$.

حالت ۳: بنابراین $P - ۱$ و $Q - ۱$ هر دو فردند، پس $[(P - ۱)(Q - ۱)]/۲$، نصف یک عدد صحیح و کسری با صورت فرد است. چون $۲ \mid P$ و $۲ \mid Q$، داریم $۲ \mid d$. بنابراین، $(d - ۱)/۲$ نیز، نصف یک عدد صحیح و کسری با صورت فرد است. بنابراین

$$\frac{[(P - ۱)(Q - ۱)]}{۲} + \frac{d - ۱}{۲} = \frac{[(P - ۱)(Q - ۱)] + (d - ۱)}{۲}$$

عددی صحیح است.

۳. اثبات قضیهٔ ۱.۲ با تغییرات زیر کار می‌کند: فرض کنید $P = dP_\circ$ و $Q = dQ_\circ$. پس، قطر مستطیل شامل $(d - ۱)$ نقطهٔ مشبکهٔ $(P_\circ, Q_\circ)$، $(۲P_\circ, ۲Q_\circ)$، ...، $((d - ۱)P_\circ, (d - ۱)Q_\circ)$ روی مرزش است. این نقاط متناظر به جمله‌هایی از جمع هستند که برای آنها $j = ۱, ۲, \ldots, (d - ۱)$، $[n(Q/P)] = [jP_\circ(Q_\circ/P_\circ)] = jQ_\circ$.

باقی جمله‌های جمع، نقاط مشبکهٔ زیر قطر را می‌شمارند. بنابر تقارن، دوبرابر حاصل‌جمع برابر است با تعداد کل نقاط مشبکهٔ مستطیل به‌علاوهٔ $(d-۱)$، زیرا نقاط قطری دو بار شمرده می‌شوند. بنابراین،

$$۲\sum_{n=۱}^{P-۱}\left[n\frac{Q}{P}\right]=(P-۱)(Q-۱)+(d-۱).$$

۴. در مستطیل $OABC$، یک‌چهارم مستطیل که در گوشهٔ سمت چپ و پایین قرار دارد با نقاط $(۰,۰)$، $(P/۲,۰)$، $(P/۲,Q/۲)$، و $(۰,Q/۲)$ مشخص می‌شود. چون $P/۲$ و $Q/۲$ صحیح نیستند، هیچ نقطهٔ مشبکه‌ای روی مرز بالایی یا مرز سمت راست مستطیلی که با نقاط مذکور مشخص می‌شود قرار نمی‌گیرد. قطر $y=(Q/P)x$، این مستطیل را به دو مثلث $T_۱$ و $T_۲$ تقسیم می‌کند که هیچ نقطهٔ مشبکه‌ای روی مرزشان نیست. تعداد نقاط درونی $T_۱$ با $\sum_{n=۱}^{P'}[n(Q/P)]$ و تعداد نقاط درونی $T_۲$ با $\sum_{n=۱}^{Q'}[n(Q/P)]$ به‌دست می‌آید. بنابراین، جمع آنها برابر است با تعداد نقاط درونی مستطیل کوچک:

$$P'Q'=\frac{P-۱}{۲}\frac{Q-۱}{۲}$$

بخش ۲.۳

۲. $A=\frac{۱}{۲}ab$. مرز پایینی شامل $(a+۱)$ نقطهٔ مشبکه است: $(۰,۰)$، $(۱,۰)$، $(۲,۰)$، ...، $(a,۰)$؛ مرز سمت راست شامل b نقطه است: $(a,۱)$، $(a,۲)$، ...، (a,b). چون a و b نسبت به‌هم اولند، وتر شامل هیچ نقطهٔ مشبکه‌ای نیست، بنابراین، $B=a+b+۱$. بنابر قضیهٔ پیک: $I=A-\frac{۱}{۲}B+۱=\frac{۱}{۲}ab-\frac{۱}{۲}(a+b+۱)=\frac{۱}{۲}(a-۱)(b-۱)$.

۳. $P_۱P_۲P_۳P_۴$ با دو مثلث ساخته شده است، $T_۱$ (با رئوس $P_۰$، $P_۴$ و $(۱,۲)$) و $T_۲$ (با رئوس $P_۳$، $P_۴$ و $(۱,۲)$). مجموع مساحت‌ها برابر است با $A=\frac{۹}{۲}$. نقاط مشبکهٔ درونی، $P_۱$، $P_۲$، $P_۳$، $P_۴$، $(۱,۲)$، $(۲,۴)$، $(۱,۴)$ و $(۲,۵)$ هستند، پس $B=۸$. بنابراین قضیهٔ پیک برقرار نیست. چندضلعی ساده نیست زیرا $\overline{P_۱P_۲}$ و $\overline{P_۳P_۴}$ در نقطهٔ $(۱,۲)$ مشترک‌اند که این نقطه رأس نیست.

۴. با استفاده از قضیهٔ پیک (یا به هر روش دیگر)، مساحت شکل بیرونی برابر است با $\frac{۴۱}{۲}$، در حالی‌که مساحت شکل درونی برابر است با ۲. بنابراین، مساحت ناحیهٔ بینی برابر است با $۱۸\frac{۱}{۲}=\frac{۳۷}{۲}=۲-\frac{۴۱}{۲}$. اما بنابر قضیهٔ پیک:

$$A=I+\frac{۱}{۲}B-۱=۱۱+\frac{۱}{۲}(۱۵)-۱=\frac{۳۵}{۲}=۱۷\frac{۱}{۲}$$

بنابراین قضیهٔ پیک در اینجا کار نمی‌کند.

۵. فرض کنید $A = I + \frac{1}{2}B - 1$ مساحت چندضلعی بیرونی و $A' = I' + \frac{1}{2}B' - 1$ مساحت چندضلعی درونی باشد. در این‌صورت $A_1 = A - A' = (I - I') + \frac{1}{2}(B - B')$. اما، $I_1 = I - (I' + B')$، در حالی که $B_1 = B + B'$. بنابر قضیهٔ پیک داریم: $A_1 = I_1 + \frac{1}{2}B_1 - 1 = I - I' - B' + \frac{1}{2}B + \frac{1}{2}B' - 1 = (I - I') + \frac{1}{2}(B - B') - 1$، که یک واحد کمتر از مساحت واقعی است.

۶. نقاط $(\pm b, 0)$ و $(0, \pm a)$ رئوس لوزی هستند. علاوه‌بر این نقاط مرزی، هر ضلع شامل $(d - 1)$ نقطهٔ مشبکهٔ غیررأسی است. مساحت برابر است؛ $A = 4\left(\frac{1}{2}ab\right) = 2ab$. بنابر قضیهٔ پیک، $A = I + \frac{1}{2}B - 1$، پس $2ab = I + \frac{1}{2}\left[4 + 4(d - 1)\right] - 1 = I + 2d - 1$ و $I = 2ab - 2d + 1$.

بخش ۳.۳

۱. گزارهٔ ۱.۳ همچنان برقرار است اگر $\sqrt{2}$ را با $\epsilon + 1$، برای $\epsilon > 0$، جایگزین کنیم. این به این دلیل است که در اینجا، فاصلهٔ بین دو نقطهٔ مشبکه مجاور که روی یک پاره‌خط عمودی قرار دارند ۱ واحد است. اما چون فاصلهٔ قطری بین دو نقطهٔ مشبکه $\sqrt{2}$ است، هیچ عدد کوچک‌تری قضیهٔ پوششی را به‌دست نمی‌دهد.

۳. الف) نه.

ب) راهنمایی: به مسئلهٔ ۴ نگاه کنید.

ج) راهنمایی: به مسئلهٔ ۴ نگاه کنید.

بخش ۳.۴

۱. فرض کنید $n = 4k + 3 = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. اگر هر $p_i = 4k_i + 1$، هر $p_i^{a_i}$ به همین شکل و حاصل‌ضرب $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ نیز به همین شکل است. به‌علاوه، اگر $p_i = 4k_i + 3$، اما a_i زوج باشد، آنگاه $p_i^{a_i} = 4m + 1$، برای mای. بنابراین، بعضی از اول‌ها، به شکل $4k + 3$ و توان آنها فرد است. بنابر قضیهٔ ۲.۴، n را نمی‌توان به شکل مجموع دو مربع نوشت و قضیهٔ ۱.۴ نتیجه می‌شود.

۲. فرض کنید $z = a - bi$ و $z' = c + di$. پس $|z|^2 = a^2 + b^2$ و $|z'|^2 = c^2 + d^2$. اما $|zz'|^2 = \left(|zz'|\right)^2 = \left(|z|\,|z'|\right)^2 = |z|^2|z'|^2 = (a^2 + b^2)(c^2 + d^2)$. $zz' = (a - bi)(c + di) = (ac + bd) + (ad - bc)i$. بنابراین،

$$|zz'|^2 = (ac + bd)^2 + (ad - bc)^2$$

بخش ۵.۴

۱. نه. $۶ + ۴(۱) = ۱۰$ و $R(۱۰) = R(۲ \times ۵) = ۴(۲ - ۰) = ۸$.

۲. $n = ۱۲k + ۹ = ۳(۴k + ۳)$. چون $۴k$ بر ۳ بخش‌پذیر نیست، $۴k + ۳$ هم بر ۳ بخش‌پذیر نیست. این یعنی، عدد ۳ فقط یک بار به‌عنوان عامل n ظاهر می‌شود. بنابر قضیهٔ ۲.۴، $R(n) = ۰$.

۳. مقسوم علیه‌های ۱۲۲۵ عبارتند از: ۱، ۵، ۲۵، ۷، ۳۵، ۱۷۵، ۴۹، ۲۴۵، ۱۲۲۵. $A = ۶$ و $B = ۳$. $R(n) = ۴(A - B) = ۴(۶ - ۳) = ۱۲$.

۴. محاسبه طولانی ولی سرراست است:

$$T(۱۲۲۵) = ۱ + ۴\sum_{k=۰}^{۳۵}\left[\sqrt{۱۲۲۵ - k^۲}\right] = ۳۸۵۳$$

بخش ۱.۵

۱. الف) اگر (x, y) روی نوار باشد، آنگاه $\alpha x - \frac{۱}{۲} < y < \alpha x + \frac{۱}{۲}$. بنابراین،

$$-\alpha x + \frac{۱}{۲} > -y > -\alpha x - \frac{۱}{۲}$$

بنابراین داریم $\alpha(-x) - \frac{۱}{۲} < -y < \alpha(-x) + \frac{۱}{۲}$. این نشان می‌دهد که $(-x, -y)$ نیز روی نوار است.

ب) $d = ۱/\sqrt{۱ + \alpha^۲}$.

ج) فرض کنید $\alpha > ۰$ گنگ است. در این‌صورت،

$$\left|\alpha - [\alpha]\right| < \frac{۱}{۲} \qquad \text{یا} \qquad \left|\alpha - \left([\alpha] + ۱\right)\right| < \frac{۱}{۲}$$

بسته به اینکه کدام نابرابری برقرار باشد، قرار دهید $q = [\alpha]$ یا $[\alpha + ۱]$. آنگاه $-\frac{۱}{۲} < q - \alpha < \frac{۱}{۲}$، پس $\alpha - \frac{۱}{۲} < q < \alpha + \frac{۱}{۲}$، نشان می‌دهد که $(۱, q)$ روی نوار محدود به خطوط $y = \alpha x \pm \frac{۱}{۲}$ است. این نقطه اولین نقطه در ربع اول نوار است که خطی عمود بر خطوط محدودکننده که به سمت بالای نوار حرکت می‌کند از آن می‌گذرد. (برای هر نقطهٔ $(p_۱, q_۱)$ دیگری، باید $p_۱ > ۱$ و در نتیجه $q > q_۱$). خط $y = -(۱/\alpha)x + (k/\alpha)$ از نقطهٔ $(۱, q)$ می‌گذرد اگر $k = \alpha q + ۱ = \alpha[\alpha] + ۱$ یا $\alpha[\alpha] + \alpha + ۱$.

۲. الف) اگر (x, y) در ناحیه باشد، آنگاه $-۱ < ۲\alpha x^۲ - ۲xy < ۱$. اما این معادل است با $-۱ < ۲\alpha(-x)^۲ - ۲(-x)(-y) < ۱$. بنابراین، $(-x, -y)$ در ناحیه است.

ب) به‌دلیل تقارن S، کافی است که فقط نقاط نامنفی x را در نظر بگیریم. با حل کردن برحسب y، نابرابری $-1 \le 2\alpha x^2 - 2xy \le 1$ به نابرابری $ax-(1/2x) \le y \le ax+(1/2x)$ تبدیل می‌شود. کران بالا، $\alpha x + (1/2x)$ را در نظر بگیرید. به‌وضوح، وقتی $x \to 0^+$، $y \to +\infty$ و وقتی $x \to +\infty$، $y \to \alpha x$ از بالا. بنابراین، $y = \alpha x + (1/2x)$، برای $x > 0$، شاخه‌ای از هذلولی با مجانب‌های $x = 0$ و $y = \alpha x$ است. برای کران پایین، $y = \alpha x - (1/2x)$، وقتی $x \to 0^+$، $y \to -\infty$ و وقتی $x \to +\infty$، $y \to \alpha x$ از پایین. بنابراین، $y = \alpha x - (1/2x)$، برای $x > 0$، یک شاخه از هذلولی مزدوج است که مجانب‌های آن $x = 0$ و $y = \alpha x$ هستند. تقارن نسبت به مبدأ، شاخه‌های دیگر را در هر حالت به‌دست می‌دهد.

بخش ۲.۵

۱. بنابر تعریف، مجموعهٔ محدبی که شامل دو نقطه است، پاره‌خط واصل آنها را هم شامل می‌شود.

۳. فرض کنید M_1 و M_2 دو مجموعهٔ محدب و $M_1 \cap M_2$ اشتراک آنها باشد. اگر A و B دو نقطه در $M_1 \cap M_2$ باشند، آنگاه A و B هر دو در M_1، و A و B هر دو در M_2 هستند. بنابراین، $\overline{AB} \subset M_1$ و $\overline{AB} \subset M_2$. این نشان می‌دهد که $\overline{AB} \subset M_1 \cap M_2$.

بخش ۳.۵

۱. $A = 6$؛ $A' = \frac{3}{2}$؛ $s = 5$. $(n+1)^2 A' > (n+10)^2$ به‌ازای $n \ge 40$.

۲. قرصی به شعاع ۲ و مرکز $(0,0)$ در نظر بگیرید. هشت شعاع رسم کنید که هر یک از نقطهٔ $(0,0)$ و یک یا دو نقطهٔ مشبکه می‌گذرد (شعاع‌های روی محورها از دو نقطهٔ مشبکه می‌گذرند). هشت نواری را که از مرز قرص به سمت خارج امتداد دارند ببرید؛ عرض هر نوار ϵ_1، طول آن $1 + \epsilon_2$ و هر یک نسبت به یکی از هشت شعاع متقارن است. شکل غیرمحدب حاصل دارای مساحت $4\pi - 8(1+\epsilon_2)\epsilon_1$ است که می‌تواند به اندازهٔ دلخواه به 4π نزدیک باشد، دارای تقارن مرکزی است و بجز $(0,0)$ دارای هیچ نقطهٔ مشبکهٔ دیگری نیست.

۳. الف) اگر $P = (x,y)$، آنگاه $P_1 = (x+n_1, y+m_1)$ و $P_2 = (x+n_2, y+m_2)$. بنابراین، $P_1 - P_2 = (n_1 - n_2, m_1 - m_2)$.

ب) چون C' محدب است، شامل نقطهٔ $-P_1 = (-x-n_1, -y-m_1)$ و همچنین پاره‌خطی است که $-P_1$ را به P_2 وصل می‌کند. بنابراین C' شامل نقطهٔ میانی $-P_1$ و P_2 با مختصات $((n_2-n_1)/2, (m_2-m_1)/2)$ است. بنابراین C شامل نقطهٔ مشبکهٔ (n_2-n_1, m_2-m_1) است که $(0,0)$ نیست زیرا $P_1 \ne P_2$.

بخش ۲.۶

۱. $\sqrt{|\Delta|} = \sqrt{۱۸۴۲۵۹} \approx ۴۲۹{,}۲۵۴$. طرحی از متوازی‌الاضلاع توصیف‌شده رسم کنید، قرار دهید $k = ۴۲۹ < \sqrt{|\Delta|}$. می‌بینیم که ناحیه شامل نقاط $(۱, ۰)$ و $(-۱, ۰)$ است. درواقع، $\sqrt{|\Delta|} > ۴۲۹ > ۲۰۱$، و $\sqrt{|\Delta|} > ۴۲۹ > ۴۰۰$، بنابراین قضیهٔ اول مینکوفسکی در نقاط $(۱, ۰)$ و $(-۱, ۰)$ برقرار است.

بخش ۳.۶

۱. $\Delta = \pi - e \approx ۰{,}۴۲۳۳$. $\sqrt{|D|} = \sqrt{۲|\Delta|} \approx ۰{,}۹۲$. با نگاه به متوازی‌الاضلاع

$$\begin{aligned}\xi + \eta &= ۲x - (\pi + e)y = \pm\sqrt{|D|}\\ \xi - \eta &= \qquad -(\pi - e)y = \pm\sqrt{|D|}\end{aligned}$$

می‌بینیم که $(۳, ۱)$ در درون آن است. با امتحان، داریم:

$$|\xi||\eta| = \left|۲(۳) - (\pi + e)(۱)\right| \approx |۶ - ۵{,}۸۶||۰{,}۴۲۳۳| = ۰{,}۰۵۹۲۶۲$$

چون

$$\frac{۱}{۲}|\Delta| = \frac{۱}{۲}|\pi - e| \approx ۲{,}۱۱۶۵$$

قضیهٔ دوم مینکوفسکی در $(۳, ۱)$ برقرار است.

بخش ۱.۷

۱. الف) فرض کنید $P = (x, y)$ نقطهٔ دلخواهی از صفحه باشد. در این‌صورت،

$$T(P) = (ax + by, cx + dy)$$

نیز نقطه‌ای از صفحه است.

الف و ج) فرض کنید

$$P_۱ = (x_۱, y_۱) \text{ و } P_۲ = (x_۲, y_۲)$$

شکل برداری معادلهٔ خط حاصل از این دو نقطه این چنین است:

$$\begin{aligned}P_t &= P_۱ + t(P_۲ - p_۱)\\ &= \left(x_۱ + t(x_۲ - x_۱), y_۱ + t(y_۲ - y_۱)\right)\end{aligned}$$

$T(P_i) = (ax_i + by_i, cx_i + dy_i)$، برای $i = ۱, ۲$. خط حاصل از $T(P_۱)$ و $T(P_۲)$ این چنین است:

$$\begin{aligned} Q_t &= T(P_۱) + t\big(T(P_۲) - T(P_۱)\big) \\ &= \big(ax_۱ + by_۱ + t(ax_۲ + by_۲ - ax_۱ - by_۱) \\ &\quad cx_۱ + dy_۱ + t(cx_۲ + dy_۲ - cx_۱ - dy_۱)\big) \end{aligned}$$

با اعمال تبدیل T روی P_t می‌بینیم که $T(P_t) = Q_t$.

ب) فرم کلی مقاطع مخروطی این چنین است: $Ax^۲+Bxy+Cy^۲+Dx+Ey+F = ۰$. قرار دهید $x = ax_۱ + by_۱$ و $y = cx_۱ + dy_۱$، محاسبات لازم را انجام دهید و عبارت را ساده کنید. آنچه به‌دست می‌آید به همان فرم قبلی ولی این‌بار با متغیرهای $x_۱$ و $y_۱$ است.

۲. الف) رأس‌های جدید عبارتند از $(۰, ۰)$، $(۱, ۱)$، $(۱, ۳)$، و $(۰, ۲)$.

ب) مساحت‌های جدید و قدیم با هم برابرند.

۳. $\det T = \det \begin{pmatrix} ۱ & ۱ \\ ۱ & ۲ \end{pmatrix} = ۲ - ۱ = ۱$. رأس‌های جدید عبارتند از $(۰, ۰)$، $(۱۰, ۱۰)$، و $(۲۰, ۳۰)$. مساحت جدید = مساحت قدیم = ۵۰.

۴. ب) $\det T = \det \begin{pmatrix} ۲ & ۳ \\ ۴ & ۶ \end{pmatrix} = ۱۲ - ۱۲ = ۰$. بنابراین $T^{-۱}$ وجود ندارد.

بخش ۳.۷

۱. اگر $ap+bq = ap'+bq'$ و $cp+dq = cp'+dq'$، آنگاه $a(p-p')+b(q-q') = ۰$ و $c(p-p')+d(q-q') = ۰$. این معادلهٔ آخری نشان می‌دهد که $(p-p', q-q')$ یک جواب دستگاه خطی همگن $ax+by = ۰$ و $cx+dy = ۰$ است. اما، چون $\Delta = ad-bc \neq ۰$ دستگاه دارای جواب یکتای $(۰, ۰)$ است. بنابراین، $p = p'$ و $q = q'$.

۲. T را چنان انتخاب کنید که $\Delta = \det T = \pm ۱$.

۳. می‌توان فرض کرد که یک رأس چنین چندضلعی‌ای نقطهٔ $(۰, ۰)$ است. فرض کنید $P = (x, y)$ و $Q = (u, v)$. آنگاه $R = (x+u, y+v)$. فرض کنید T تبدیل داده‌شده با $T = \begin{pmatrix} x & u \\ y & v \end{pmatrix}$

باشد. در این‌صورت، $OPRQ$ تصویر مربع اصلی $(\circ, \circ)$، $(\circ, ۱)$، $(۱, ۱)$، $(۱, \circ)$ با مساحت ۱ است. برای مساحت $OPRQ$، A، داریم $A = |\det T| = |xv - uy| \geq ۱$.

پیوست الف، بخش الف.۱

۱. $۱/(a+bi) = [۱/(a+bi)][(a-bi)/(a-bi)] = (۱-bi)/(a^۲+b^۲)$. چون $a+bi$ یکه نیست، $a^۲+b^۲ \neq -۱$ و $(a+bi)^{-۱}$ عدد صحیح گاوسی نیست.

۲. $a^۲+b^۲ > ۱^۲+\circ^۲ = ۱$، چون یا (۱) هر دوی a و b اعداد صحیح غیرصفر یا (۲) یکی از آنها صفر و دیگری دارای قدرمطلقی بزرگ‌تر از یا مساوی با ۲ است.

۳. چون a و b هر دو صحیح‌اند، مربع آنها صحیح و $a^۲+b^۲$ نیز صحیح است.

پیوست الف، بخش الف.۲

۱. فرض کنید $\overline{q} = fh$، در حالی‌که، نه f و نه h یکه است. بنابراین $\overline{\overline{q}} = q = \overline{fh} = \overline{f} \cdot \overline{h}$، در حالی‌که، نه $\overline{f}$ و نه $\overline{h}$ یکه است. این با فرض اول بودن q در تناقض است.

۲. به‌وضوح، $a+bi \neq (a-bi)(-۱)$. اگر $a+bi = (a-bi)(i) = ai+b = b+ai$، آنگاه باید داشته باشیم $a = b$. اما، در این‌صورت، $a+bi = a+ai = a(۱+i)$ که در آن a عامل غیربدیهی برای عدد اول $q = a+bi$ است مگر اینکه $a = \pm ۱$. استدلالی مشابه برای $u = -i$ کار می‌کند.

کتابنامه

Blichfeldt, H. F. "A New Principle in the Geometry of Numbers with Some Applications." *Transactions of the American Mathematical Society* 15:3 (July 1914): 227-35.

________. *Finite Groups of Linear Homogeneous Transformations.* Part 2 of *Theory and Applications of Finite Groups* by G. A. Miller, H. F. Blichfeldt, and L. E. Dickson. New York: Wiley, 1916. Reprinted, New York: Dover, 1961.

________. *Finite Collineation Groups.* Chicago: University of Chicago Press, 1917.

________. "The Minimum Values of Positive Quadratic Forms in Six, Seven, and Eight Variables." *Mathematische Zeitschrift* 39 (1934): 1-15.

Cassels, J. W. S. *Introduction to the Geometry of Numbers.* Classics of Mathematics Series. Corrected reprint of 1917 edition. Berlin: Springer, 1997.

Davenport, Harold. "The Geometry of Numbers." *Math. Gazette* 31 (1947): 206-10.

________. *The Higher Arithmetic,* New York: Dover, 1983. Dickson, L. E. *History of the Theory of Numbers, Vol. I: Divisibility and Primality.* Washington, D. C.: Carnegie Institute, 1919.

________. *History of the Theory of Numbers, Vol. II: Diophantine Analysis.* Washington, D. C.: Carnegie Institute, 1920.

________. *History of the Theory of Numbers, Vol. III: Quadratic and Higher Forms.* Washington, D. C.: Carnegie Institute, 1923.

Gauss, C. F. *Werke.* Göttingen: Gesellschaft der Wissenschaften, 1863-1933.

Grace, J. H. "The Four Square Theorem." *Journal of the London Mathematical Society* 2 (1927): 3-8.

Grossman, Howard D. "Fun with Lattice Points." *Scripta Mathematica* 16 (1950): 207-12.

Gruber, P. M., and C. G. Lekkerkerker. *Geometry of Numbers.* 2nd edition. Amsterdam and New York: North-Holland, 1987.

Hajós, G. "Ein neuer Beweis eines Satzes von Minkowski." *Acta Litt. Sci. (Szeged)* 6 (1934): 224-5.

Hardy, G. H., and E. M. Wright. *An Introduction to the Theory of Numbers.* 5th ed. Oxford: Oxford University Press, 1983.

Hermite, Charles. "Lettres de Hermite á M. Jacobi." *J. reine angew. Math.* 40 (1850): 261-315.

________. *Comptes Rendus Paris* 37 (1853).

________. *J. reine angew. Math.* 47 (1854): 343-5, 364-8.

________. "Sur une extension donnée á la théorie des fractions continues par M. Tchebychev." *J. reine angew. Math.* 88 (1879): 10-15.

________. *Oeuvres,* Vol. I. Paris: E. Picard, 1905.

________. *Oeuvres,* Vol III. Paris: Gauthier-Villars, 1912.

Hilbert, David, and S. Cohn-Vossen. *Geometry and the Imagination.* Translated by P. Nemenyi. New York: Chelsea, 1952.

Honsberger, Ross. *Ingenuity in Mathematics.* New Mathematical Library Series, Vol. 23. Washington, DC: MAA, 1970.

Hurwitz, A. "Über die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche." *Mathematische Annalen* 39 (1891): 279-84.

Koksma, J. F. *Diophantische Approximationen.* New York: Chelsea, 1936.

Korkine, A., and E. I. Zolotareff. "Sur les formes quadratiques positives quaternaires." *Mathematische Annalen* 5 (1872): 581-3.

———. "Sur les formes quadratiques." *Mathematische Annalen* 6 (1873): 366-89.

———. "Sur les formes quadratiques positives." *Mathematische Annalen* 11 (1877): 242-92.

Lyusternik, L. A. *Convex Figures and Polyhedra.* First Russian edition (1956) translated and adapted by Donald L. Barrett. Boston: D. C. Heath, 1966.

Minkowski, Hermann. "Über die positiven quadratischen Formen un über kettenbruchähnliche Algorithm." *J. reine agnew. Math.* 107 (1891): 209-12.

———. *Ausgewahlte Arbeiten zur Zahlentheorie und zur Geometrie. Mit D. Hilbert's Gedachtnisre auf H. Minkowski* (*Göttingen,* 1909). [*Selected Papers on Number Theory and Geometry. With D. Hilbert's Commemorative Address in Honor of H. Minkowski.*] Teubner-Archiv zur Mathematik, Vol 12. E. Kratzel and B. Weissbach, eds. Leipzig: Teubner, 1989.

———. *geometrie der Zahlen.* Bibliotheca Mathematic Teubneriana, Vol. 40. Leipzig: Teubner, 1910. First section of 240 pages appeared in 1896. Reprinted, New York and London: Johnson Reprint Corp., 1988.

———. *Diophantische Approximationen: Eine Einfuhrung in die Zahlentheorie.* Reprinted, New York: Chelsea, 1957.

Mitchell, H. L., III. *Numerical Experiments on the Number of Lattice Points in the Circle.* Stanford, CA: Stanford University, Applied Mathematics and Statistics Labs, 1961.

Mordell, L. J. "On Some Arithmetical Results in the Geometry of Numbers," *Compositio Math.* I (1934): 248-53.

Niven. Ivan. *Irrational Numbers.* Carus Mathematical Monographs, No. 11. Washington, DC: MAA, 1956.

———. *Numbers: Rational and Irrational.* New Mathematical Library Series, Vol. I. Washington, DC: MAA, 1961.

Niven. Ivan, and Herbert Zuckerman. "The Lattice Point Covering Theorem for Rectangles," *Mathematics Magazine* 42 (1969): 85-86.

Olds, Carl D. *Continued Fractions.* New Mathematical Library Series, Vol. 9. Washington, DC: MAA. 1963.

Ore. Oystein. *Number Theory and Its History.* New York: McGraw-Hill, 1948. Reprinted with supplement, New York: Dover, 1988.

Schaaf, William. *Bibliography of Recreational Mathematics,* Vol. I. Reston, VA: National Council of Teachers of Mathematics, 1959; reprinted, 1973.

Scott. W. T. "Approximation to Real Irrationals by Certain Classes of Rational Fractions." *Bulletin of the American Mathematical Society* 46 (1940): 124-9.

Sierpinski, W. *The Elementary Theory of Numbers.* 2nd edition. Andrzej Schinzel, ed. North-Holland Mathematical Library, Vol. 31. Amsterdam and New York: North-Holland; Warsaw: Polish Scientific Publishers, 1988.

Tchebychef, P. L. *Oeuvres de Tchebychef.* Translated into French by A. Markoff and N. Sonin. Reprinted, New York: Chelsea.

Uspensky, J. V., and M. A. Heaslet. *Elementary Number Theory.* New York: McGraw-Hill, 1939.