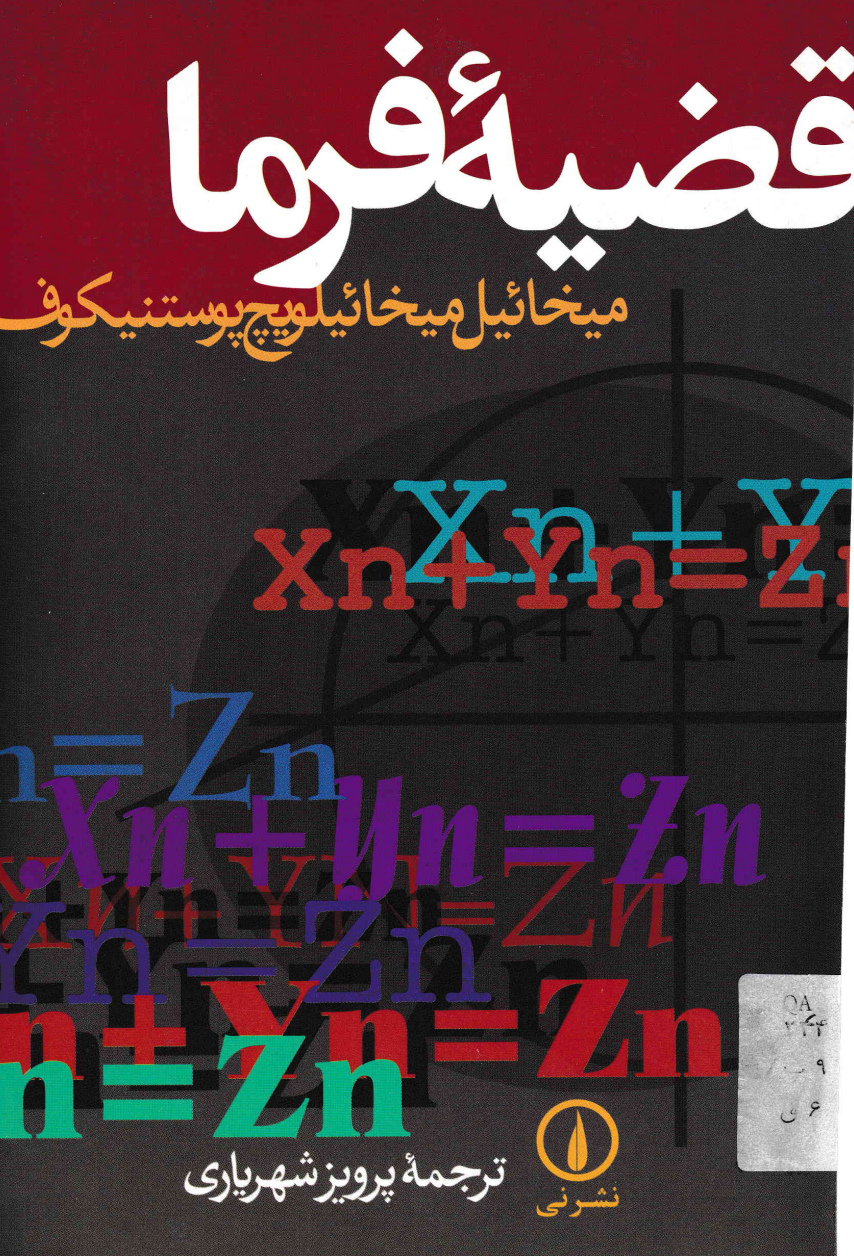
قضیهٔ فرما

میخائیل میخائیلویچ پوستنیکوف



ترجمهٔ پرویز شهریاری

نشر نی

میخائیل میخائیلویچ پوستنیکوف

قضیهٔ فرما

ترجمهٔ پرویز شهریاری

نشر نی

پوستنیکوف، میخائیل میخائیلویچ
Postnikov, Mikhail Mikhailovich
قضیه فرما / میخائیل میخائیلویچ پوستنیکوف؛ ترجمه پرویز شهریاری. ـ تهران: نشر نی، ۱۳۷۹.
۲۲۸ ص.
ISBN 964-312-544-0
فهرستنویسی براساس اطلاعات فیپا.
۱. قضیه فرما. الف. شهریاری، پرویز، ۱۳۰۵ـ ، مترجم.
ب. عنوان.
۶ ق ۹ پ / QA ۲۴۴ ۵۱۲/۷۴
۱۳۷۹
کتابخانه ملی ایران ۷۹ـ۱۷۷۴۵ م

نشر نی

نشانی: تهران، خیابان فاطمی، خیابان رهی معیری، شمارهٔ ۵۸
صندوق پستی ۵۵۶ ــ ۱۳۱۴۵، نشر نی تلفن ۵۹ و ۸۰۰۴۶۵۸

میخائیل میخائیلویچ پوستنیکوف

قضیهٔ فرما

ترجمهٔ پرویز شهریاری

ویراستاری و بخش آخر: شهریار شهریاری

• **چاپ اول** ۱۳۷۹ تهران • **تعداد** ۲۲۰۰ نسخه • **لیتوگرافی** باختر • **چاپ** اسلامیه

شابک ۰ـ۵۴۴ـ۳۱۲ـ۹۶۴ ISBN 964-312-544-0

فهرست مطالب

از پیش‌گفتار نویسنده ۵

پیش‌گفتار مترجم ۷

۱. سرگذشت قضیهٔ فرما ۹

۲. قضیهٔ ژرمن ۲۳

۳. قضیهٔ فرما، برای نمای ۴ ..... ۳۹

۴. قضیهٔ فرما، برای نمای ۳ ..... ۴۷

۵. حساب حلقهٔ D_3 ..... ۵۵

۶. میدان K_l و حلقهٔ K_l ۷۷

۷. واحدهای حلقهٔ D_l ۹۳

۸. حالت اول قضیهٔ فرما ۱۰۳

۹. نظریهٔ بخشیاب‌ها (دی‌وی زورها) ۱۱۳

۱۰. حالت دوم قضیهٔ فرما ۱۲۱

۱۱. نظریهٔ ایده‌آل‌ها ۱۳۱

۱۲. عددهای جبری درست ۱۶۵

۱۳. عددهای اول سامان‌پذیر ۱۷۹

۱۴. حل قطعی قضیهٔ فرما (ترجمهٔ دکتر شهریار شهریاری) ۱۹۳

فهرست منابع ۲۲۷

از پیش‌گفتار نویسنده

نظریهٔ عددهای جبری، یکی از زیباترین ساختمان‌های ریاضی است که در سدهٔ نوزدهم پایه‌گذاری شد. اندیشه‌های اصلی نظریهٔ عددهای جبری براساس جبر جدید، به‌مفهوم کلی آن، پدید آمد که، به‌نوبهٔ خود، تأثیر نیرومندی بر پیشرفت تمامی ریاضیات داشت. در دهه‌های اخیر، فرایند عکس هم دیده می‌شود؛ ساختارها و روش‌های ریاضیات انتزاعی امروز، هجوم بی‌وقفهٔ خود را به حوزهٔ نظریهٔ عددها، که پیش از این منطقهٔ ممنوع به‌حساب می‌آمد، آغاز کرده‌اند و به‌همین دلیل، چهرهٔ تازه‌ای از آن را نشان می‌دهند. این سمت‌گیری و پیشرفت تازهٔ نظریه، خیلی خوب در ادب ریاضی و از جمله در کتاب‌های درسی بازتاب داشته‌است؛ کافی است در این باره از دو کتاب **وِیل** و **لَنگ** نام ببریم. کتاب "نظریهٔ عددها" نوشته ز. ای **نوره‌ویچ** و ای. ر. **شافاره‌ویچ**، که چاپ دوم آن در سال ۱۹۷۲ منتشر شد، بیشر سمت‌گیری کلاسیک دارد. با وجود این، کتاب **بوره‌ویچ** و **شافاره‌ویچ** جامع‌تر است و می‌توان گفت یک دایرةالمعارف درسی است و بیشتر برای دانشجویان و استادیاران متخصص در نظریهٔ عددهای جبری سودمند است. این کتاب گرچه برای کسانی که می‌خواهند با اندیشه‌های اصلی و موقعیت نظریه آشنا شوند، کمتر سودمند است، در عوض خواننده‌ای را که به‌دنبال مطلب جدی و عمیق در ریاضیات است، راضی می‌کند.

کتاب حاضر که چندان بزرگ نیست، می‌تواند رضایت خواننده‌ای را که علاقه‌مند به آشنایی با مهم‌ترین اندیشه‌های نظریهٔ عددهای جبری است، به‌دست آورد و کمبود کتاب‌های ساده را در این زمینه، جبران کند. این کتاب، به همهٔ جنبه‌های نظریه عددهای جبری نپرداخته، و تنها بررسی یکی

از شاخه‌های آن، یعنی نظریهٔ بخش‌پذیری عددهای جبری درست را به‌عهده گرفته‌است. با همهٔ این‌ها، با خواندن این کتاب می‌توان با گام‌های استوارتری به‌سوی مسأله‌های دشوارتر حرکت کرد.

خواننده‌ای که کتاب را دنبال می‌کند، به‌تدریج با موضوع‌های دشوار و دشوارتری برخورد می‌کند. ولی کتاب طوری تنظیم شده‌است که بتواند در هر مرحله، خواننده را با آگاهی‌های تازه‌ای آشنا کند. بنابراین، خواننده‌ای هم که در ریاضیات آمادگی ضعیفی داشته‌باشد (ازجمله دانش‌آموزان)، بسیاری چیزها یاد می‌گیرد و انگیزه‌ای برای کار آیندهٔ او می‌شود.

هدف این کتاب این است که، در درجهٔ اول، خواننده را در هر گام با مطلب کاملی آشنا کند و سپس او را قانع کند که باید جلوتر برود.

از نظر تاریخی، نظریهٔ بخش‌پذیری عددهای جبریِ درست، در بستگی با قضیهٔ **فرما** پدید آمد. از آن‌جا که این انگیزه، هنوز تا اندازهٔ زیادی وجود دارد امکان بررسی تاریخی را هم به‌دست می‌آوریم.

پیش‌گفتار مترجم

وقتی پیر فرما در بیش از سیصدسال پیش، در حاشیهٔ کتاب دیوفانت قضیهٔ مشهور خود را مطرح کرد که معادلهٔ $x^n + y^n = z^n$ برای عددهای درست z، y، z و $n>2$ جواب ندارد و مدعی شد که راه ساده‌ای برای اثبات آن درنظر دارد (که چون در حاشیهٔ کتاب جایی برای طرح آن نیست، از آن می‌گذرد)، بسیاری از بزرگ‌ترین ریاضی‌دانان به آن پرداخته‌اند و اگر از افراد غیرحرفه‌ای که همیشه موجب آزار دیگران بوده‌اند، بگذریم، تنها پیشرفت اندکی در این راه حاصل شد.

یکی از اساسی‌ترین فایده‌های قضیهٔ فرما این بود که ریاضی‌دانان به‌خاطر حل آن بسیاری از مشکلات درونی ریاضیات را به‌ویژه در نظریهٔ عددها حل کردند و شاخه‌های تازه‌ای در این راه به‌وجود آمد که مهم‌ترین آن‌ها طرح عددهای جبری و حساب هندسی بود. با این همه قضیه فرما حل نشد تا این‌که در سال ۱۹۹۵ به‌وسیلهٔ آندرو واینر راه‌حلی دشوار در ۲۰۰ صفحه برای آن ارائه شد.

خیلی از ریاضی‌دانان از حل قضیهٔ فرما متأسف شدند، چرا که قضیهٔ فرما انگیزه‌ای بود برای کشف خیلی از ویژگی‌های عددها، ولی باید هنوز منتظر بود که راه‌حل ساده‌تری برای قضیهٔ فرما پیدا شود و از این لحاظ هنوز کار ریاضی‌دانان پایان نیافته است.

مقالهٔ پایانی کتاب را پسرم دکتر شهریار شهریاری نوشته است و کوشش کرده تا آن‌جا که ممکن است خط‌سیری را که راه‌حل قضیه فرما به‌وسیلهٔ وایـنر داده شده است، روشن کند.

۱

سرگذشت قضیهٔ فرما

پیر فرما (Pierre de Fermat) (۱۶۰۸-۱۶۶۵)، یکی از بزرگ‌ترین ریاضی‌دانان، در سدهٔ هفدهم می‌زیست. او پایه‌های هندسهٔ تحلیلی را طرح ریخت (کم‌وبیش هم‌زمان با **دکارت** (Descarte)) و روشی کلی برای جست‌وجوی ماکزیمم و می‌نیمم پیدا کرد (که بعدها به محاسبهٔ بی‌نهایت کوچک‌ها تکامل یافت). با همهٔ این‌ها، مشهورترین نتیجه‌گیری‌های **فرما** در زمینهٔ نظریهٔ عددها است.

نتیجه‌گیری‌های نظری-محاسبه‌ای **فرما** چاپ نشد. آن‌ها را در نامه‌ها و کاغذهای پراکندهٔ او، بعد از مرگش پیدا کردند. بیشتر استدلال‌هایی که **فرما** برای نتیجه‌گیری‌های خود داشته، به ما نرسیده‌است. این استدلال‌ها و اثبات‌ها، به‌وسیلهٔ ریاضی‌دانان بعد از او و به‌ویژه **اویلر** (Euler) تنظیم شد.

برخی از گزاره‌های **فرما** همراه با اشاره‌هایی است که روشن می‌کند، خودِ او نتوانسته است استدلال قانع‌کننده‌ای برای آن‌ها بیاورد. درضمن روشن شده‌است که برخی از گزاره‌های او، همراه با اشتباه هستند. ازجمله، **فرما** گمان می‌کرد، هر عدد به‌صورت $۲^{۲^n} + ۱$، برای هر عدد درست و نامنفی n، عددی اول است، در حالی‌که **اویلر** ثابت کرد، این عدد به‌ازای $n = ۵$، عددی مرکب است.

ولی در همهٔ حالت‌هایی که **فرما** مدعی اثبات گزاره‌ای شده‌است، ریاضی‌دانان توانسته‌اند اثبات درستیِ گزاره را در برخی حالت‌ها پیدا کنند.

جالب‌ترین و بی‌همتاترین گزارهٔ **فرما**، «قضیهٔ بزرگ **فرما**» یا «آخرین قضیهٔ **فرما**» است. این قضیه می‌گوید: وقتی n عدد درستی بزرگ‌تر از ۲ باشد، معادلهٔ

$$x^n + y^n = z^n$$

نمی‌تواند جواب درستی برای x، y و z، به‌جز صفر داشته‌باشد. درضمن می‌دانیم، برای $n = ۲$، چنین عددهایی وجود دارند؛ ازجمله ۳، ۴ و ۵.

در کاغذهای **فرما**، اثبات این قضیه برای $n = ۴$ پیدا شده‌است و جالب است که این، تنها اثبات کاملی است که از **فرما** باقی‌مانده‌است.

ولی برای حالت کلی و به‌ازای $n > ۲$، **فرما** در کنارهٔ کتاب «حساب» **دیوفانت** (Diophantus) نوشته است: «در واقع، اثبات جالبی» برای آن پیدا کرده‌است، ولی «کنارهٔ کتاب بسیار کوچک‌تر از آن است که بتوان این اثبات را در آن جا داد».

با وجود تلاش‌های بسیاری از ریاضی‌دانان، که به قول **دیکسون** (Dickson) در «تاریخ نظریهٔ عددها»، بیش از سیصد سال ریاضی‌دانان را به خود مشغول داشته‌است، این اثبات به‌دست نیامد، به‌نحوی که بسیاری، دربارهٔ وجود چنین اثباتی دچار تردید شدند.

به‌جز این، همان‌طور که خواهیم دید، به‌جز برای $n = ۴$، برای هیچ‌یک از مقدارهای n، نتوانسته‌اند درستیِ قضیهٔ **فرما** را با روش‌های مقدماتی ثابت کنند. به‌همین جهت، بسیاری از ریاضی‌دانان همهٔ تلاش خود را در این زمینه به‌کار بردند که ثابت کنند، قضیهٔ فرما را نمی‌توان با روش‌های مقدماتی ثابت کرد.

در سال ۱۹۰۸، **وُلف سکل** (Wolfskehl) آلمانی، که از علاقه‌مندان به دانش ریاضی بود، ۱۰۰۰۰۰ مارک جایزه برای کسی تعیین کرد که بتواند قضیهٔ **فرما** را حل کند. بلافاصله، صدها و هزاران نفر از کسانی که چشم به این جایزه دوخته بودند، سازمان‌ها و نشریه‌های علمی را با نوشته‌های خود بمباران کردند که، گویا توانسته‌اند قضیهٔ **فرما** را ثابت کنند. تنها در گوتینگن آلمان، در جریان سه سال بعد از اعلام جایزهٔ **وُلف سکل** بیش از هزار راه‌حل، به جامعهٔ ریاضی در گوتینگن فرستاده شد.

این بیماری، دست‌کم در سراسر اروپا به همه‌جا سرایت کرده‌بود و اغلب کسانی هم که آگاهی اندکی در ریاضیات داشتند، به این «مسابقه» پیوستند. همه‌جا راه‌حل خود را، که اغلب بی‌مایه و حتا خنده‌دار بود، ارائه می‌دادند و منتظر دریافت جایزه بودند.

بعد از جنگ جهانی اول که سراسر اروپا دچار تورم و بحران مالی شده‌بود، جایزهٔ **وُلف سکل** ارزش خود را از دست داد و «فرما کاران» (ریاضی‌دانان به کسانی که با امکان علمی ضعیف و از راه‌های بی‌ارزش و بی‌نتیجه، تلاش

می‌کردند به قضیهٔ **فرما** حمله و آن را حل کنند، این نام را داده بودند)، انگیزهٔ سودجویی را از دست دادند. به‌این دلیل و به‌طور طبیعی، سیل «اثبات‌های فرما کاران» از خروش خود افتاد، ولی البته به‌کلی قطع نشد. جریان انبوه نامه‌ها به‌طرف مرکزهای ریاضی و علمی، همچنان ادامه داشت. نویسندگان این نامه‌ها، امید داشتند دست‌کم شهرتی به‌دست آورند، اگرچه در نوشته‌های آن‌ها، اندکی حقیقت و استدلال درست هم پیدا نمی‌شد. برخی از نویسندگان این نامه‌ها، با خشم اعلام می‌کردند که به‌هیچ وجه به افتخار شخصی خود توجهی ندارند، بلکه تنها می‌خواهند خدمتی به دانش کرده‌باشند. و این، نمونهٔ مشخصی از گمراهی و بیهوده‌کاری در تاریخ دانش است.

قضیهٔ **فرما** برای ریاضی‌دانان از این جهت ارزش داشت که، ضمن تلاش برای اثبات آن، روش‌ها و مسیرهای تازه‌ای در ریاضیات پدید می‌آمد و به‌ویژه، به شاخه‌ای از ریاضیات به‌نام «نظریهٔ عددهای جبری» یاری می‌رسانید و آن را به جلو می‌برد. این حقیقت که قضیهٔ **فرما** تن به اثبات نمی‌داد، به‌معنای آن بود که وجود روش‌ها و مسیرهای دقیق‌تر و تازه‌تری در ریاضیات لازم است. به‌نظر می‌رسد، برای قضیهٔ **فرما** نمی‌توان راه‌حل مقدماتی پیدا کرد (یعنی با روش‌های شناخته‌شده نمی‌توان قضیهٔ **فرما** را ثابت کرد)، ولی تلاش برای پیدا کردن روش‌ها و مسیرهای تازه با هدف دستیابی به اثبات قضیهٔ **فرما**، برای ریاضیات ارزش داشت و به آن خدمت کرد.

به‌ظاهر باید از جست‌وجوی راه‌حل مقدماتی برای قضیهٔ **فرما** صرف‌نظر کرد. به‌هرحال، چه این نظر درست باشد و چه نادرست، وارد شدن در حل مقدماتی قضیهٔ **فرما**، به‌ویژه برای ریاضی‌دانان جوان و تازه‌کار، صلاح نیست.

یکی از هدف‌های این کتاب آن است که نشان دهد، قضیهٔ **فرما** با چه مساله‌های دشوار و عمیقی از نظریهٔ عددها بستگی دارد و چگونه هر کسی را که گمان می‌کرد کار این قضیه را به‌پایان رسانده‌است ناامید کرده و در ردیف «فرماکاران» قرار داده‌است (بگذریم از این‌که در بعضی حالت‌ها حتا به نتیجه‌ای ناقص یا جنبی هم نرسیده‌اند).

بد نیست یادآوری کنیم، «کورکورانه» به‌دنبال مثالی رفتن که قضیهٔ **فرما** را

نقض کند، باز هم ناامید کننده است. در سال ۱۸۵۶، هه‌یررنرت یادآوری کرد، اگر عددهای طبیعی x، y و z وجود داشته‌باشند که در برابری

$$x^n + y^n = z^n$$

صدق کنند، باید با این نابرابری‌ها سازگار باشند:

$$x > n,\ y > n,\ z > n$$

در واقع، اگر فرض کنیم $z = x + a (a \geq ۱)$، آن‌وقت

$$x^n + y^n = x^n + nx^{n-۱}a + \ldots + nxa^{n-۱} + a^n$$

که از آن نتیجه می‌شود $y^n > nx^{n-۱}a > nx^{n-۱}$. به‌همین ترتیب می‌توان ثابت کرد $x^n > ny^{n-۱}$. بنابراین

$$(y^n)^n > n^n x^{n(n-۱)} > n^n n^{n-۱}(y^{n-۱})^{n-۱}$$

یعنی $y^{۲n-۱} > n^{۲n-۱}$ و از آن‌جا $y > n$. به‌دلیل وجود تقارن، درضمن نتیجه می‌شود: $x > n$ و $z > n$. پایان اثبات.

در زمان ما، قضیهٔ فرما برای هر n که کوچک‌تر از ۱۰۰۰۰۰ باشد، ثابت شده‌است[۱]. بنابراین، برای مثال مربوط به آن، باید با عددهایی کار کرد که از $۱۰^{۵۰۰۰۰۰}$ تجاوز می‌کنند.

همان‌طور که گفتیم، *اثبات مقدماتی قضیهٔ فرما برای هیچ‌یک از عددهای* $n \neq ۴$ *وجود ندارد*. حتا در حالت $n = ۳$، که اویلر در سال ۱۷۶۸ به بررسی آن پرداخت، معلوم شد باید از عددهایی به‌صورت

$$a + b\sqrt{-۳} \qquad (۱)$$

۱- کتاب در سال ۱۹۷۸ چاپ شده‌است. م.

استفاده کرد (a و b، عددهایی درست‌اند). **فرما** با چنین عددهایی بیگانه بود و روشن است نمی‌توانست از آن‌ها استفاده کند.

در واقع، اثبات **اویلر** هم کمبودی دارد، زیرا بدون این‌که دربارهٔ عددهای مختلط بحث کند و پایه‌های آن‌ها را بیاورد، از عددهای به‌صورت (۱) در استدلال خود استفاده کرد و برای آن‌ها همان ویژگی‌های عددهای درست را درنظر گرفت. برای نمونه، برای عددهای (۱)، ساده‌ترین قانون‌ها را از نظریهٔ بخش‌پذیری عددهای درست بدون اثبات استفاده کرده‌است.

نخستین کسی که حساب عددهای (۱) را تنظیم کرد و برای، استدلال **اویلر** بنیانی مطمئن به‌وجود آورد، به‌ظاهر **گاوس** (Gauss) بود.

اثبات قضیهٔ **فرما** برای $n = ۵$، به‌تقریب در یک زمان، در سال ۱۸۲۵ به‌وسیله **دیریکله** (Dirichlet) و **لژاندر** (Legendre) داده شد. اثبات **دیریکله** در سال ۱۸۲۸ چاپ شد که بسیار پیچیده است. در سال ۱۹۲۱، **پله‌مِل** تا اندازه‌ای اثبات را ساده‌تر کرد.

برای عدد اول بعدی، یعنی $n = ۷$، قضیهٔ **فرما** تنها در سال ۱۸۳۹ به‌وسیلهٔ **لامه** (Lame) ثابت شد. کم‌وبیش بلافاصله بعد از **لامه**، اثبات او به‌وسیلهٔ لِه‌بِگ (Lebesgue) تکمیل و ساده شد.

در سال ۱۸۴۷، **لامه** اعلام کرد، توانسته است قضیهٔ **فرما** را برای همهٔ عددهای اول $n > ۳$ ثابت کند. روش **لامه** به‌کلی دور از اندیشهٔ **اویلر** بود و براساس ویژگی‌های حسابی عددهای به‌صورت

$$a_۰ + a_۱\zeta + \ldots + a_{n-۲}\zeta^{n-۲} \qquad (۲)$$

قرار داشت که در آن، $a_۰$، $a_۱$، ...، $a_{n-۲}$ عددهایی درست و

$$\xi = \cos\frac{۲\pi}{n} + i\sin\frac{۲\pi}{n}$$

ریشهٔ nام عدد ۱ است.

ولی **لیوویل** (Liouville) در استدلال **لامه**، یک نارسایی جدی پیدا کرد. نارسایی این استدلال در این بود که **لامه** بدون استدلال فرض کرده بود

که عددهای به‌صورت (۲)، شبیه عددهای درست معمولی، به‌صورت یگانه‌ای به ضرب عامل‌های اول تجزیه می‌شوند (به‌نحوی‌که این عامل‌ها، قابل تجزیه به ضرب عامل‌های دیگری نیستند). **لامه** به‌ناچار اشتباه خود را پذیرفت.

در همان زمانی که این پیش‌آمدها در فرانسه جریان داشت، در آلمان، ریاضی‌دان جوانی به‌نام **کومر** (Kummer)، به‌طور جدی به قضیهٔ **فرما** مشغول بود. در آغاز گمان کرد توانسته‌است اثبات کامل قضیهٔ **فرما** را پیدا کند و در سال ۱۸۴۳، رسالهٔ خود را در این‌باره به **دیریکله** سپرد. این اثبات هم براساس همان عددهای به‌صورت (۲) انجام گرفته‌بود و **کومر** هم با تکرار همان اشتباه **لامه**، فرض را بر این گرفته‌بود که این عددها، تنها به یک طریق، به عامل‌های اول تجزیه می‌شوند. **دیریکله** بلافاصله یادآوری کرد، این حقیقت نیاز به اثبات دارد و دست‌نویس **کومر** را به او برگرداند.

کومر خیلی زود متوجه شد، قضیهٔ مربوط به یگانه بودن تجزیه به عامل‌های اول، برای عددهای به‌صورت (۲) درست نیست و از جست‌وجوی خود برای اثبات آن دست برداشت. **کومر** بررسی‌های خود را کنار نگذاشت و راه خروجی پیدا کرد که هم او را مشهور کرد و هم موجب پدید آمدن شاخه‌های تازه‌ای در جبر امروزی شد. **کومر** به عددهای (۲)، عددهای تازه‌ای -عددهای انتزاعی- اضافه کرد و آن‌ها را «ایده‌آل‌ها» نامید، به‌نحوی‌که برای ایده‌آل‌ها، ویژگی یگانه بودن تجزیه به عامل‌های اول درست بود.

مثالی می‌آوریم. به‌سادگی روشن می‌شود (خودتان انجام دهید)، در حوزهٔ عددهای به‌صورت

$$a + b\sqrt{-۵} \qquad (۳)$$

که در آن a و b عددهایی درست‌اند، عدد ۲۱ با دو روش، به ضرب عامل‌های اول تجزیه می‌شود:

$$۲۱ = ۳ \times ۷ = (۱ + ۲\sqrt{-۵})(۱ - ۲\sqrt{-۵})$$

با این‌که عددهای به‌صورت (۳)، برای هر مقداری از n، عددهای به‌صورت (۲) نیستند (برای عددهای (۲)، مثال مشابه تنها به‌ازای $n \geq ۲۳$ ممکن

است)، ولی اندیشهٔ کومر را می‌توان دربارهٔ آن به‌کار برد. برای این منظور باید به عددهای (۳)، عددهای ایده‌آلی A، B، C و D را اضافه و فرض کرد:

$$۳ = AB,\ ۷ = CD,\ ۱ + ۲\sqrt{-۵} = AC,\ ۱ - ۲\sqrt{-۵} = BD$$

روشن است که در این‌صورت، تجزیهٔ منحصری برای عدد ۲۱ به ضرب عامل‌های اول (همان ایده‌آل‌ها) به‌دست می‌آید.

البته «ایده‌آل بودن» عددهای تازه دشواری‌هایی پدید می‌آورد، ولی، به‌سادگی می‌توان بر این دشواری‌ها مسلط شد. در سال ۱۸۴۷، کومر توانست قضیهٔ فرما را برای همهٔ عددهای اول $n = l$ که با شرط‌هایی به‌نام (A) و (B) سازگار باشند، ثابت کند. آن‌طور که از نامهٔ کومر به لیوویل برمی‌آید، کومر در این زمان گمان می‌کرد، این شرط برای همهٔ عددهای اول برقرار است، ولی خیلی زود متوجه شد که استثناهایی وجود دارد (ازجمله، برای عدد ۳۷). استدلال کومر در سال ۱۸۹۴ به‌وسیلهٔ داوید هیلبرت (Hilbert) ساده‌تر شد.

ولی این نتیجه‌گیری کومر هنوز به‌جای مطلوبی نرسیده بود، زیرا تا این‌جا، حتا یک عدد اول l هم پیدا نکرده‌بود که برای آن قضیهٔ فرما درست باشد. با وجود این، تا همین‌جا گامی اساسی به جلو بود و ما با تفصیل بیشتری دربارهٔ آن صحبت می‌کنیم.

کومر در سال ۱۸۵۱، با تجزیه‌وتحلیل بسیار ظریف و کم‌وبیش دشواری توانست نتیجه‌هایی را که در سال ۱۸۴۷ به‌دست آورده‌بود، به‌صورتی جدی تکمیل کند. او ثابت کرد، شرط (B) را می‌توان از شرط (A) نتیجه گرفت (این گزاره به «پیش‌قضیهٔ کومر» معروف است؛ بخش ۷ همین کتاب را ببینید)، و بنابراین، اضافی است. او شرط (A) را تا مرز امکان ساده کرد و به‌صورتی درآورد که به‌سادگی بتوان از آن استفاده کرد. این شرط در تنظیم نخستینِ خود، با این درخواست همراه بود که عدد اول l، بخشیابی از عدد h، که به‌سختی تعریف می‌شد، نیست. کومر، عدد h را به ضرب دو عامل تجزیه کرد:

$$h = h_۱h_۲$$

و دستورهای روشنی (که البته به‌اندازهٔ کافی دشوار بود) برای h_1 و h_2 به‌دست آورد؛ سپس ثابت کرد، عدد h وقتی، و تنها وقتی، بر l بخش‌پذیر است که عدد اول l، صورت $(l-3)$ عدد نخستین **برنولی** (Bernoulli) را نشمارد، یعنی بخشیابی از آن‌ها نباشد (البته با این شرط، که این کسرها، ساده‌نشدنی باشند). **کومر** چنین عددهایی را «سامان‌پذیر» (regular=منظم) نامید.

عددهای برنولی، این عددهای گویا هستند:

$$B_1 = \frac{1}{6},\ B_2 = \frac{1}{30},\ B_3 = 0,\ \ldots$$

که می‌توان آن‌ها را، یکی بعد از دیگری، بنابر قانون ساده‌ای به‌دست آورد (بخش ۱۳ را ببینید). به‌این ترتیب، شرط **کومر** را می‌توان، بدون دشواری خاصی، برای هر l آزمایش کرد.

به‌ویژه معلوم شد، بین عددهای اول $l < 100$، تنها عددهای ۳۷، ۵۹ و ۶۷ سامان‌پذیر نیستند.

این، پیشرفت بسیار جالبی بود که **کومر** در تکمیل بررسی‌های سال ۱۸۴۷ خود به‌دست آورد، ولی جای افسوس دارد که اثبات این نتیجه‌گیری‌ها، دشوارتر از آن است که بتوان در این‌جا از آن‌ها یاد کرد. در بخش ۱۳، تنها تلاش کرده‌ایم نشان دهیم، چرا با شرط سامان‌پذیر بودن، عددهای **برنولی** پدید می‌آیند.

کومر در تمامی زندگی خود گمان می‌کرد، تعداد عددهای سامان‌پذیر بی‌نهایت است، بسیاری از ریاضی‌دانان هم در این زمینه با او هم‌عقیده بودند. ولی این حقیقت، تا امروز ثابت نشده‌است.

از این گذشته، در سال ۱۹۱۵، **یِنسِن** (Jensen)، با روشی ساده، ثابت کرد، برعکس، تعداد عددهای اول «سامان‌ناپذیر»، بی‌نهایت است.

بعد از سال ۱۸۵۱، **کومر** تلاش خود را روی بررسی عددهای اولی گذاشت که سامان‌پذیر نیستند و کوشید **قضیهٔ فرما** را برای آن‌ها ثابت کند. او با دشواری بسیار، در سال ۱۸۵۸ **قضیهٔ فرما** را برای خانواده‌هایی از عددهای

اول سامان‌ناپذیر و ازجمله برای عددهای ۳۷، ۵۹ و ۶۷ ثابت کرد. به‌این ترتیب، درستی قضیهٔ فرما برای همهٔ عددهای اول $l < ۱۰۰$ ثابت شد. درست است که در سال‌های ربع اول سدهٔ بیستم، مِرتِنس و واندی‌وِر (Vandiver) کمبودهایی در استدلال‌های کومر پیدا کردند، ولی همهٔ آن‌ها به‌سادگی قابل اصلاح بود.

در سال ۱۸۹۳، می‌ری‌مانوف (Mirimanoff) توانست قضیهٔ فرما را با روشی ساده‌تر برای نمای $l = ۳۷$ ثابت کند.

در سال ۱۸۵۰، فرهنگستان علوم فرانسه، سه‌هزار فرانک جایزه برای اثبات قضیهٔ فرما تعیین کرد. اعطای جایزه چند بار عقب افتاد تا سرانجام در سال ۱۸۵۷ به کومر داده شد (به‌ظاهر، در آغاز، کومر حتا در بین نامزدها هم نبود).

بعد از کومر، گامی جدی در راه اثبات قضیهٔ فرما برداشته نشد تا این‌که در سال ۱۹۲۹، واندی‌وِر ثابت کرد، قضیهٔ فرما برای نماهای اول l وقتی درست است که

۱) عامل دوم $h_۲$ از عدد h بر l بخش‌پذیر نباشد؛

۲) صورت‌های $(l - ۳)$ جملهٔ برنولی، یعنی

$$B_{۲l},\ B_{۴l},\ \ldots,\ B_{۲l(l-۳)}$$

بر $l^۳$ بخش‌پذیر نباشند.

آزمایش شرط ۲)، باتوجه به رایانه‌های امروزی، دشوار نیست. ولی دربارهٔ شرط ۱)، با این‌که دربارهٔ همهٔ عددهای $l < ۱۰۰۰۰۰$ آزمایش شده‌است، هنوز نتوانسته‌اند عدد اولی برای l پیدا کنند که با این شرط سازگار نباشد. شرط ۲) هم برای عددهای $l < ۱۰۰۰۰۰$ برقرار است. به‌این ترتیب، **قضیهٔ فرما، برای همهٔ عددهای اول $l < ۱۰۰۰۰۰$ درست است.**

برای اویلر معلوم بود، برای بررسی معادلهٔ

$$x^l + y^l = z^l \quad (l، \text{عددی اول و بزرگ‌تر از } ۳) \qquad (۴)$$

باید حالتی را که هیچ‌یک از عددهای x، y یا z بر l بخش‌پذیر نیستند، از حالتی‌که دست‌کم یکی از این عددها بر l بخش‌پذیر است، جدا کرد.

اگر اجازهٔ اندکی بی‌دقتی را به خود بدهیم، می‌توان این گزاره را که، معادلهٔ (۴) نمی‌تواند برای عددهای بخش‌ناپذیر بر l برقرار باشد، **حالت اول قضیهٔ فرما**، و این گزاره را که معادلهٔ (۲) نمی‌تواند برای عددهایی که یکی از آن‌ها بر l بخش‌پذیر است برقرار باشد، **حالت دوم قضیهٔ فرما** نامید.

جدا از حالت کلی قضیهٔ فرما، حالت اول آن را می‌توان برای بسیاری از عددهای l، اثبات مقدماتی پیدا کرد. **سوفی ژرمن** (Sophie Germain) (۱۷۷۶-۱۸۳۱)، نخستین زن ریاضی‌دان دوران جدید، در همان آغاز سدهٔ نوزدهم، به این مساله پرداخت. او به‌ویژه ثابت کرد، **برای عددهای اول l، به‌شرطی‌که عدد $۲l + ۱$ هم عددی اول باشد، حالت اول قضیهٔ فرما درست است.**

با همهٔ این‌ها امیدی که **سوفی ژرمن** داشت برآورده نشد و راهی که برای پیدا کردن اثبات انتخاب کرده‌بود، ولو برای حالت اول قضیهٔ فرما به‌جایی نرسید.

ژرمن نتیجه‌گیری‌های خود را چاپ نکرد، ولی ضمن نامه‌ای آن‌ها را به **لژاندر**، ریاضی‌دان فرانسوی اطلاع داد. **لژاندر** در سال ۱۸۲۸، رسالهٔ مفصلی دربارهٔ قضیهٔ فرما منتشر و در آن قضیه‌های **ژرمن** را آورد و از آن‌ها یک رشته نتیجه گرفت. او ازجمله ثابت کرد، حالت اول قضیهٔ فرما، برای نماهای اول l، وقتی دست‌کم یکی از این پنج عدد

$$۴l + ۱,\ ۸l + ۱,\ ۱۰l + ۱,\ ۱۴l + ۱,\ ۱۶l + ۱$$

اول باشند، درست است. از این گذشته، حالت اول قضیهٔ فرما برای همهٔ

عددهای اول کوچک‌تر از ۱۹۷ درست است. برای نمای ۱۹۷، قضیه لژاندر جواب نمی‌دهد.

بعد از لژاندر، بسیاری از ریاضی‌دانان تلاش کردند نتیجه‌گیری‌های او را بهبود بخشند. به‌ظاهر، قضیهٔ قطعی را، وِنت ریاضی‌دان آلمانی در سال ۱۸۹۳ به‌دست آورد (این قضیه را بعدها نتوانستند با روش‌های مقدماتی بهبود بخشند).

وِنت برای هر $m > ۱$ عدد درستی با نماد D_m وارد کرد و با استفاده از روش کلی ژرمن ثابت کرد، حالت اول قضیهٔ فرما برای هر نمای اول l درست است، به‌شرطی‌که $m \geq ۱$ وجود داشته‌باشد، به‌نحوی‌که

۱) عدد $p = ۲ml + ۱$ عددی اول و بخش‌ناپذیر بر D_m باشد؛

۲) عدد $l^{۲m} - ۱$ بر p بخش‌پذیر نباشد.

عدد D_m سه تعریف هم‌ارز دارد:

الف) $D_m = (-۱)^m \prod_{j=۱}^{۲m-۱} [(۱ + \zeta^j)^{۲m} - ۱]$ با فرض

$$\zeta = \cos\frac{\pi}{n} + i\sin\frac{\pi}{n}$$

ب) D_m دترمینان این ماتریس است:

$$\begin{Vmatrix} \binom{۲m}{۱} & \binom{۲m}{۲} & \cdots & \binom{۲m}{۲m-۱} & \binom{۲m}{۲m} \\ \binom{۲m}{۲} & \binom{۲m}{۳} & \cdots & \binom{۲m}{۲m} & \binom{۲m}{۱} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \binom{۲m}{۲m} & \binom{۲m}{۱} & \cdots & \binom{۲m}{۲m-۲} & \binom{۲m}{۲m-۱} \end{Vmatrix}$$

ج) D_m عبارت است از به‌اصطلاح برآیند (resultant) چندجمله‌ای $x^{۲m} - ۱$ و $(x+۱)^{۲m} - ۱$.

یادآوری می‌کنیم، با وجود تلاش ده‌ها ریاضی‌دان، که در بین آن‌ها دانشمندان بسیار هوشمند و نکته‌سنج وجود داشت، هیچ‌گونه راه مقدماتی دیگری، برای اثبات قضیهٔ **فرما** و یا دست‌کم حالت اول آن ارائه نشده‌است (باوجود این، هنوز نتیجه‌گیری‌های **ژرمن**، تا پایان خود، روشن نشده‌است. برای نمونه، هنوز نمی‌دانیم، آیا تعداد نماهای اول l که می‌توان برای آن‌ها از این نتیجه‌ها استفاده کرد، بی‌نهایت است یا نه).

روش‌های غیرمقدماتی را، برای حالت اول قضیهٔ **فرما**، **کومر** مطرح کرد. او در کار خود در سال ۱۸۵۸، ثابت کرد: *حالت اول قضیهٔ فرما برای نماهای اول l، وقتی صورت دست‌کم یکی از دو عدد برنولی $B_{l-۳}$ و $B_{l-۵}$ بر l بخش‌پذیر نباشد، درست است.*

در سال ۱۹۰۵، **می‌ری مانوف** این نتیجه را تعمیم داد و ثابت کرد، کافی است یکی از صورت‌های چهار عدد **برنولی** $B_{l-۳}$، $B_{l-۵}$، $B_{l-۷}$ و $B_{l-۹}$ بر l بخش‌پذیر نباشد. و این، همهٔ مقدارهای $l < ۲۵۷$ را می‌پوشاند.

وی‌فه‌ریخ (Wieferich) با استفاده از روش **می‌ری مائوف**، در سال ۱۹۰۹ ثابت کرد، حالت اول قضیهٔ فرما برای همهٔ نماهای اول l درست است، به‌شرطی‌که $(۱ - ۲^{l-۱})$ بر $l^۲$ بخش‌پذیر نباشد. این نتیجه‌گیری، بسیار جالب است، زیرا به‌کمک آن می‌توان، به‌عنوان نمونه، دربارهٔ عددهای اول کوچک‌تر یا برابر ۲۰۰۱۸۳ داوری کرد که تنها دربارهٔ دو عدد ۱۰۹۳ و ۳۵۱۱ پاسخ نمی‌دهد.

بعدها اثبات **وی‌فه‌ریخ** به‌وسیلهٔ **می‌ری مانوف** و **فروبه‌نوس** (Frobenius) ساده‌تر شد، به‌این ترتیب که در شرط **وی‌فه‌ریخ**، می‌توان پایهٔ ۲ را به ۳ تغییر داد، به‌نحوی‌که حالت اول قضیهٔ **فرما** برای هر نمای اول l که برای آن، دست‌کم یکی از دو عدد $(۱ - ۲^{l-۱})$ و یا $(۱ - ۳^{l-۱})$ بر $l^۲$ بخش‌پذیر نباشد.

در سال ۱۹۱۲ **فورت وِن‌گلر** (Furtwangler)، با استفاده از روشی که به قانون دوجانبهٔ **اَی‌زِن‌شتاین** (Eisenstein) مشهور است، معیار **وی‌فه‌ریخ**

و **می‌ری‌مانوف** - **فروبه‌نوس** را، خیلی کوتاه و در چند سطر ثابت کرد. این کار آغازی برای یک رشته بررسی‌ها برای کسانی شد که موقعیت‌هایی در زمینهٔ تازه‌ترین‌ها در نظریهٔ عددها به‌دست آورده بودند (ازجمله دربارهٔ خانوادهٔ گروه‌ها) و توانستند در سال ۱۹۴۱ ثابت کنند، پایهٔ ۲ را در معیار **وی‌فه‌ریخ** می‌توان با هر عدد اولی که از ۴۳ بزرگ‌تر نباشد، عوض کرد. این نتیجه‌گیری توانست درستی حالت اول قضیهٔ **فرما** را برای هر نمایی از l که کوچک‌تر از ۲۵۳۷۴۷۸۸۹ باشد، ثابت کند.

در سال ۱۹۳۴، **واندی‌وِر** ثابت کرد، برای نمای اولی از l که عامل دوم آن $h_۲$، بر l بخش‌پذیر نباشد، حالت اول قضیهٔ **فرما** درست است. این قضیه از این جهت جالب است که، همان‌طور که پیش از این هم گفتیم، تاکنون نمای اولی شناخته نشده‌است که با این شرط سازگار نباشد. ولی از آن‌جاکه $h_۲$ بر l بخش‌پذیر نیست، تحقیق تنها برای $l < ۱۰۰۰۰۰$ انجام شده‌است.

۲

قضیهٔ ژرمن

چگونه می‌توان به سمت اثبات قضیهٔ فرما رفت؟

در آغاز باید یادآوری کرد، اگر سه عدد (x, y, z)، عددهای درستی باشند و در معادلهٔ

$$x^n + y^n = z^n \qquad (۱)$$

صدق کنند (حالت $n = ۲$ را، در حال حاضر کنار نمی‌گذاریم)، آن‌وقت هر سه عددی که به‌صورت $(\lambda x, \lambda y, \lambda z)$ باشند، برای عدد درست و دلخواه λ، در این معادله صدق می‌کنند. برعکس، اگر عددهای سه‌گانهٔ $(\lambda x, \lambda y, \lambda z)$ جوابی از معادلهٔ (۱) باشد، آن‌وقت (x, y, z) هم جوابی از معادله است. بنابراین، برای این‌که همهٔ جواب‌های معادلهٔ (۱) (به‌جز حالت بی‌مایهٔ $x = y = z = ۰$) را پیدا کنیم، کافی است جواب (x, y, z) را طوری به‌دست آوریم که عددهای x، y، z دوبه‌دو نسبت به هم اول باشند (یعنی بخشیاب مشترکی به‌جز واحد نداشته‌باشند)؛ و برای این‌که ثابت کنیم، معادلهٔ (۱) در مجموعهٔ عددهای درست جواب ندارد، کافی است از بُرهان خُلف استفاده کنیم و فرض را بر این بگیریم، جواب (x, y, z) که شامل عددهایی دوبه‌دو نسبت به هم اول است، وجود دارد.

درضمن روشن است، اگر در جواب (x, y, z) از معادلهٔ (۱)، دو عدد از بین عددهای x، y و z عامل مشترکی مثل $\lambda \neq \pm ۱$ داشته‌باشند، بی‌تردید عدد سوم هم بر λ بخش‌پذیر است. بنابراین، در هر معادلهٔ به‌صورت (۱)، می‌توان تنها به جوابی نظر داشت که در آن x، y و z دوبه‌دو نسبت به هم اول باشند. چنین جوابی را "جواب مقدماتی" (primitive=اولیه) می‌نامیم.

سپس روشن است، اگر قضیهٔ فرما برای نمایی مثل n درست باشد، برای هر نمای به‌صورت an، یعنی مضربی از n هم درست است، زیرا اگر معادلهٔ

$$x^{an} + y^{an} = z^{an}$$

در مجموعهٔ عددهای درست دارای جواب (x, y, z) باشد، آن‌وقت برای معادلهٔ (۱) جواب (x^a, y^a, z^a) به‌دست می‌آید. به‌این ترتیب کافی است قضیهٔ فرما را برای $n = ۴$ (همان‌طور که پیش از این گفته‌ایم، این حالت را

خود فرما هم ثابت کرده‌است) و برای $n = l$ ثابت کنیم، که در آن، l عددی است اول و بزرگ‌تر از ۲.

پیش‌قضیه‌ای که در این‌جا می‌آوریم، در همهٔ استدلال‌های مربوط به قضیهٔ فرما، نقشی اساسی داشته‌است.

پیش‌قضیه. a، b و c را عددهایی طبیعی (یعنی درست و مثبت) می‌گیریم، به‌نحوی که

۱) این برابری برقرار باشد:

$$ab = c^n$$

۲) عددهای a و b نسبت به هم اول باشند.

در این صورت، عددهای طبیعی x و y وجود دارند، به‌نحوی‌که داشته‌باشیم:

$$a = x^n,\ b = y^n$$

یعنی، اگر حاصل‌ضرب دو عدد طبیعیِ نسبت به هم اول، برابر توان nام یک عدد طبیعی باشد، آن‌وقت هریک از دو عامل ضرب هم، برابر توان nام یک عدد طبیعی‌اند.

اگر n عددی فرد باشد، روشن است که این پیش‌قضیه، حتا برای عددهای درست و غیرصفر (مثبت یا منفی) a، b و c درست است.

اثبات. پیش‌قضیه را به‌طور کامل می‌آوریم. فرض کنید

$$a = p_1^{k_1} \dots p_s^{k_s},\ b = q_1^{l_1} \dots q_t^{l_t}$$

تجزیه عددهای a و b به ضرب عامل‌های اول باشد. در این‌جا $k_1 \geq 1$، ...، $k_s \geq 1$ و p_1، ...، p_s عددهای اولِ مختلفی هستند. به‌همین ترتیب $l_1 \geq 1$، ...، $l_t \geq 1$ و q_1، ...، q_t عددهایی اول و مختلف‌اند. درضمن، از آن‌جا که عددهای a و b نسبت به هم اول‌اند، هیچ‌کدام از عددهای p_1، ...، p_s با عددی از عددهای q_1، ...، q_t برابر نیست.

بنابراین دستور

$$c^n = p_1^{k_1} \dots p_s^{k_s} q_1^{l_1} \dots q_t^{l_t} \qquad (۲)$$

تجزیهٔ عدد $c^n = ab$ را به‌صورت ضرب توان‌هایی از عددهای اول مختلف به‌ما می‌دهد. از طرف دیگر می‌دانیم (این، قضیهٔ اصلی حساب است)، تجزیهٔ هر عدد طبیعی به ضرب توان‌هایی از عددهای مختلف اول، تجزیه‌ای یگانه است (به‌شرطی‌که تغییر ردیف عامل‌ها را، دو تجزیهٔ مختلف به‌حساب نیاوریم)، یعنی تنها به یک طریق می‌توان یک عدد طبیعی را به ضرب توان‌هایی از عددهای اولِ مختلف به‌دست آورد. بنابراین، این تجزیه باید بر تجزیهٔ عدد c، وقتی آن را به توان n برسانیم، منطبق باشد. و این، ثابت می‌کند، همهٔ نماهای k_1، ...، k_s، l_1، ...، l_t بر n بخش‌پذیرند. به‌این ترتیب a و b برابر توان‌های nام یک عدد طبیعی‌اند.

این اثبات را (که بی‌شک برای خواننده شناخته شده‌است)، به‌این دلیل می‌آوریم که بر نقش قضیهٔ اصلی حساب تاکید کرده‌باشیم.

برای هر جواب مقدماتی (x, y, z) از معادلهٔ

$$x^l + y^l = z^l \quad (l \text{ عددی اول و بزرگ‌تر از } ۲) \qquad (۳)$$

عدد z^l برابر است با حاصل‌ضرب دو عدد درستِ

$$a = x + y$$

و

$$b = \frac{x^l + y^l}{x + y} = \frac{(a - y)^l + y^l}{x + y} =$$

$$= a^{l-1} - \binom{l}{1} a^{l-2} y + \dots + (-1)^k \binom{l}{k} a^{l-k-1} y^h +$$

$$+ \dots + \binom{l}{l-1} y^{l-1} \qquad (۴)$$

که در آن

$$\begin{pmatrix} l \\ k \end{pmatrix} = \frac{l!}{k!(l-k)!}$$

عبارت‌اند از ضریب‌های بسط دوجمله‌ای (که گاهی هم با نماد C_l^k نشان می‌دهند).

از برابری (۴) نتیجه می‌شود، هر بخشیاب اول مشترک p از عددهای a و b، باید بخشیابی از عدد

$$\begin{pmatrix} l \\ l-1 \end{pmatrix} y^{l-1}$$

باشد و بنابراین، به‌شرط $p \neq l$، بخشیابی از y است. ولی وقتی p بخشیابی از a و y باشد، آن‌وقت بخشیابی از $x = a - y$ است که ممکن نیست، زیرا بنابر شرط، عددهای x و y نسبت به هم اول‌اند. اکنون اگر z بر l بخش‌پذیر نباشد، آن‌وقت $z^l = ab$ هم بر l بخش‌پذیر نیست، یعنی l بخشیابی از a یا b هم نیست. بنابراین عددهای a و b، در این حالت، نسبت به هم اول‌اند و از آن‌جا، بنابر پیش‌قضیه (برای $c = z$ و $n = l$)، چنان عددهای درست u و v وجود دارد که برای آن‌ها داشته‌باشیم:

$$x + y = u^l, \frac{x^l + y^l}{x + y} = v^l,\ z = uv$$

اکنون توجه می‌کنیم که معادلهٔ (۳) را می‌توان به این صورت نوشت:

$$x^l + y^l + (-z)^l = 0$$

از آن‌جاکه عددهای x، y، $-z$ در این برابری نسبت به هم نقشی متقارن دارند، می‌توانیم برابری‌های شبیهی برای سه عدد $(y, -z, x)$ و برای سه عدد $(-z, x, y)$ هم بنویسیم. به‌این ترتیب، برای عددهای درست x، y، z، که دوبه‌دو نسبت به هم اول و بر l بخش‌ناپذیرند؛ درضمن در معادلهٔ

$$x^l + y^l = z^l \text{ (l، عددی فرد و اول)}$$

صدق می‌کنند، زوج عددهای درست (u,v)، $(u_۱,v_۱)$ و $(u_۲,v_۲)$ وجود دارند که هردو عدد یک زوج، نسبت به هم اول باشند و داشته‌باشیم:

$$\begin{cases} x+y=u^l,\ \dfrac{x^l+y^l}{x+y}=v^l,\ z=uv \\ z-y=u_۱^l,\ \dfrac{z^l-y^l}{z-y}=v_۱^l,\ x=u_۱v_۱ \\ z-x=u_۲^l,\ \dfrac{z^l-x^l}{z-x}=v_۲^l,\ y=u_۲v_۲ \end{cases} \qquad (۵)$$

این دستورها، به **دستورهای آبل** مشهورند، گرچه **ژرمن** هم از آن‌ها آگاه بود و برای نخستین بار به‌وسیلهٔ **لژاندر** چاپ شد.

شبیه همین دستورها را (البته اندکی پیچیده‌تر) می‌توان برای حالتی هم که یکی از عددهای x، y، z بر l بخش‌پذیر است، به‌دست آورد. ولی بعد از حدود پنجاه سال بررسی پیگیر این دستورها، هیچ نتیجهٔ واقعی به‌دست نیامد و بنابراین، از آوردن آن‌ها در این‌جا، صرف‌نظر می‌کنیم.

بررسی مساله‌های عددی-نظری که مربوط به بخش‌پذیری عددها است و به‌ویژه نمادگذاری‌های ساده و راحت را در این‌زمینه **گاوس** طرح کرده‌است.

n را عدد طبیعی دلخواهی می‌گیریم. بنابر بیان **گاوس**، a و b را نسبت به *پیمانهٔ (مُدول)* n **هم‌نهشت** گویند، وقتی‌که تفاضل آن‌ها $a-b$ بر n بخش‌پذیر باشد. در این حالت می‌نویسند:

$$a \equiv b (\mathrm{mod} n)$$

روشن است که، نسبت یا رابطهٔ هم‌نهشتی یک نسبت هم‌ارزی است و بنابراین، مجموعهٔ $\mathbf{Z}$ همهٔ عددهای درست را می‌توان به خانواده‌های عددهای هم‌نهشت با هم تقسیم کرد. مجموعهٔ همهٔ این خانواده‌ها را با نماد $\dfrac{\mathbf{Z}}{n}$ نشان می‌دهیم.

هم‌نهشتی‌ها را، شبیه برابری‌ها، می‌توان با هم جمع و یا در هم ضرب کرد. همچنین می‌توان هم‌نهشتی را به عامل مشترک خود ساده‌تر کرد، تنها

به‌شرطی که این عامل نسبت به n اول باشد. با زبان جبر امروزی، مجموعهٔ $\frac{\mathbf{Z}}{n}$ شامل همهٔ خانواده‌های عددهای هم‌نهشت یک حلقه است[۲]

(یعنی، شرکت‌پذیر، جابه‌جایی‌پذیر و دارای واحد است)؛ درضمن خانواده‌هایی که از عددهایی تشکیل شده‌اند که با n نسبت به هم اول‌اند و در این حلقه بخشیاب صفر نیستند.

از این‌گذشته به‌سادگی دیده می‌شود، این خانواده‌ها در حلقهٔ $\frac{\mathbf{Z}}{n}$ وارون‌پذیرند، یعنی برای هر عدد a که نسبت به n اول باشد، عددی مثل b وجود دارد، که «وارون عدد a نسبت به مدول n» است و برای آن داریم:

$$ab \equiv ۱ (\mathrm{mod} n) \qquad (۶)$$

در واقع، از آن‌جاکه عددهای a و n نسبت به هم اول‌اند، بنابر قضیهٔ مشهور نظریهٔ مقدماتی عددها (که در بخش ۵ آن را ثابت خواهیم کرد)، چنان عددهای درستی برای x و y وجود دارد که برای آن‌ها داشته‌باشیم:

$$nx + ay = ۱$$

ولی روشن است که این برابری با هم‌نهشتی (۶) هم‌ارز است و $b = y$.

به‌ویژه می‌بینیم، اگر $n = l$ (که در آن، l عددی اول است)، آن‌وقت همهٔ عضوهای غیرصفر حلقهٔ $\frac{\mathbf{Z}}{l}$ دارای وارون (inverse) هستند، یعنی این

۲- نویسنده فرض را بر این گرفته که خواننده با تعریف‌های پایه‌ای ساختمان‌های جبری آشنا است. برای کامل بودن مطلب، بعضی از این تعریف‌ها را این‌جا می‌آوریم.

تعریف گروه. مجموعه غیرتهی G را درنظر بگیرید. فرض کنید $*$ یک عمل دوتایی روی مجموعه G باشد به‌نحوی که

(a) برای هر $a, b \in G$ داشته‌باشیم $a * b \in G$ (بسته بودن نسبت به عمل $*$)، و

(b) برای هر $a, b, c \in G$ داشته‌باشیم $(a * b) * c = a * (b * c)$ (شرکت‌پذیری)، و

(c) عضو خاصی به‌نام یکه (یا واحد و یا خنثی) وجود داشته‌باشد که با نماد e و یا ۱ نشان داده می‌شود، به‌نحوی‌که برای هر $a \in G$ داشته‌باشیم $e * a = a * e = a$ (وجود یکه)، و (d) برای هر $a \in G$، عضوی دیگری به‌نام $a^{-۱}$ در G وجود داشته‌باشد

حلقه، یک میدان است.

به‌زبان دیگر، مجموعهٔ $\frac{\mathbf{Z}^*}{l}$ همهٔ عضوهای غیرصفر حلقهٔ $\frac{\mathbf{Z}}{l}$، نسبت به ضرب، یک گروه است.

از طرف دیگر روشن است که، هر عدد نسبت به مدول l، با یکی و تنها یکی از عددهای

$$۰, ۱, ۲, \ldots, l-۱ \qquad (۷)$$

هم‌نهشت است و بنابراین معلوم می‌شود، میدان $\frac{\mathbf{Z}}{l}$ دارای l عضو و گروه $\frac{\mathbf{Z}^*}{l}$ شامل $l-۱$ عضو است، یعنی مرتبهٔ این گروه، برابر $(l-۱)$ است.

ولی از نظریهٔ مقدماتی گروه‌ها می‌دانیم، اگر عضوی از یک گروه متناهی را به توانی برابر مرتبهٔ گروه برسانیم، واحد گروه را به‌دست می‌آوریم. دربارهٔ

به‌نحوی‌که $a * a^{-۱} = a^{-۱} * a = ۱$ (وجود وارون)،

آن‌گاه مجموعه G با عمل $*$ را، که به‌صورت $(G, *)$ نشان می‌دهیم، یک گروه (group) گوییم. اگر عمل $*$ خاصیت جابه‌جایی‌پذیری هم داشته‌باشد، یعنی برای هر $a, b \in G$ داشته‌باشیم $a * b = b * a$، آن‌گاه گوییم G یک گروه آبلی است. در این کتاب فقط از گروه‌های آبلی استفاده شده‌است.

تعریف حلقه. حلقه (ring) یک مجموعه غیرتهی R با دو عمل دوتایی $+$ و $\cdot$ است به‌نحوی‌که

(a) $(R, +)$ یک گروه آبلی است. یکه عمل جمع را با ۰ نشان می‌دهیم، و

(b) برای هر $a, b \in R$ داریم $a \cdot b \in R$ (بسته بودن نسبت به ضرب)، و

(c) برای هر $a, b, c \in R$ داریم $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (شرکت‌پذیری درضرب)،و

(d) برای هر $a, b, c \in R$ داریم $a \cdot (b + c) = a \cdot b + a \cdot c$ و

$(a + b) \cdot c = a \cdot c + b \cdot c$ (خاصیت پخشی).

معمولاً درست در تعریف حلقه به خاصیت‌های بالا اکتفا می‌کنند، ولی در بسیاری حالت‌ها (و از جمله در این کتاب) حلقه‌ها خاصیت‌های دیگری هم دارند:

اگر عضوی به‌نام ۱ در حلقه R وجود داشته‌باشد به‌نحوی‌که برای هر $a \in R$ داشته‌باشیم $a \cdot ۱ = ۱ \cdot a = a$، آن‌گاه گوییم که R حلقه با یکه است. اگر R نسبت به ضرب هم جابه‌جایی‌پذیر باشد، یعنی برای هر $a, b \in R$ داشته‌باشیم $a \cdot b = b \cdot a$، آن‌گاه گوییم R

گروه $\frac{Z^*}{l}$، این مطلب به‌معنای آن است که هم‌نهشتی

$$a^{l-1} = 1 (\mathrm{mod} l) \qquad (۸)$$

برای هر عدد درست a که بر l بخش‌پذیر نباشد، برقرار است. این گزاره را، **قضیهٔ کوچک فرما** هم می‌نامند.

اگر هم‌نهشتی (۸) را در a ضرب کنیم، به‌دست می‌آید:

$$a^l \equiv a (\mathrm{mod} l) \qquad (۹)$$

روشن است این هم‌نهشتی برای $a \equiv 0 (\mathrm{mod} l)$ هم برقرار است. بنابراین، هم‌نهشتی (۹)، برای هر عدد درست a برقرار است؛ و اویلر قضیهٔ کوچک فرما را به‌همین‌ترتیب تنظیم کرده‌است.

به‌زبان جبری، هم‌نهشتی (۹) به این معنی است که هر عضو میدان $\frac{\mathbf{Z}}{l}$، ریشه‌ای از دوجمله‌ای $x^l - x$ است.

هم‌نهشتی (۹) را می‌توان، بدون استفاده از نظریهٔ گروه‌ها و به این ترتیب هم ثابت کرد.

حلقه‌ای جابه‌جایی‌پذیر است.

در این کتاب همه حلقه‌ها جابه‌جایی‌پذیر و دارای یکه هستند.

بخشیاب صفر و حلقهٔ صحیح. R را حلقه‌ای جابه‌جایی‌پذیر بگیرید. $0 \neq a \in R$ را بخشیاب صفر (zero-divisor) گوییم، اگر عضو $0 \neq b \in R$ وجود داشته‌باشد به‌نحوی که $ab = 0$. حلقهٔ جابه‌جایی‌پذیر و با یکه را حلقهٔ صحیح یا حوزهٔ کامل (integral domain) گوییم اگر بخشیاب صفر نداشته‌باشد.

تعریف میدان. حلقهٔ جابه‌جایی‌پذیر و با یکه R را میدان گویند اگر R بیش از یک عضو داشته‌باشد، و هر عضو $0 \neq a \in R$ وارون‌پذیر باشد، یعنی عضو $a^{-1} \in R$ وجود داشته‌باشد به‌نحوی‌که $a \cdot a^{-1} = a^{-1} \cdot a = 1$. (ویراستار).

از آن‌جا که عدد اول l عدد $l!$ را می‌شمارد (یعنی $l!$ بر l بخش‌پذیر است)، و برای $0 < k < l$، عدد $k!(l-k)!$ را نمی‌شمارد، نتیجه می‌گیریم که همهٔ ضریب‌های دوجمله‌ای، یعنی

$$\begin{pmatrix} l \\ k \end{pmatrix} = \frac{l!}{k!(l-k)!},\ 0 < k < l$$

بر l بخش‌پذیرند. بنابراین، برای هر دو عدد درست x_1 و x_2 داریم:

$$(x_1 + x_2)^l \equiv x_1^l + x_2^l (\mathrm{mod} l)$$

با استفاده از روش استقرای ریاضی می‌توان همین نتیجه را برای هر تعداد جمله گرفت:

$$(x_1 + x_2 + \ldots + x_n)^l \equiv x_1^l + x_2^l + \ldots + x_n^l (\mathrm{mod} l) \quad (10)$$

اگر در این دستور $x_1 = x_2 = \ldots = x_n = 1$ بگیریم، دستور (۹) (برای $a = n$) به‌دست می‌آید.

اکنون دیگر می‌توانیم به‌طور مستقیم به طرح بررسی‌های ژرمن بپردازیم.

(x, y, z) را جوابی مقدماتی از معادلهٔ (۳)، شامل عددهایی بخش‌ناپذیر بر l می‌گیریم. عدد اول و دلخواه p را طوری انتخاب می‌کنیم که نسبت به مُدول l هم‌نهشت با واحد باشد؛ یعنی به‌صورت

$$p = 2ml + 1$$

که در آن، m عددی درست است. فرض می‌کنیم، از عددهای x، y و z، هیچ‌کدام بر p بخش‌پذیر نباشند. چون $x \not\equiv 0 (\mathrm{mod} p)$، بنابراین عدد درستی مثل x' وجود دارد، به‌نحوی که داشته‌باشیم:

$$xx' \equiv 1 (\mathrm{mod} p)$$

اگر برابری (۳) را در x''^{l} ضرب کنیم و آن را به‌صورت یک هم‌نهشتی درآوریم، به‌دست می‌آید: $(yx')^{l} \equiv (zx')^{l} + ۱ \pmod{p}$، یعنی

$$۱ + a^{l} = b^{l} \pmod{p}$$

که در آن $a = yx'$ و $b = zx'$ بر p بخش‌پذیر نیستند.

عدد درست ξ را درجهٔ l نسبت به مدول p می‌نامیم، به‌شرطی‌که عددی مثل $a \neq ۰ \pmod{p}$ وجود داشته‌باشد که

$$\xi \equiv a^{l} \pmod{p}$$

درضمن، دو عدد ξ و η از درجهٔ l را، **نسبت به مدول p همسایه** می‌نامیم، وقتی‌که

$$\xi - \eta \equiv \pm ۱ \pmod{p}$$

هم‌نهشتی که در بالا ثابت کردیم، باتوجه به این نام‌گذاری، به معنی آن است که، اگر هیچ‌یک از عددهای x، y و z بر p بخش‌پذیر نباشند، آن‌وقت همسایگی‌های درجهٔ l نسبتِ به مدول p وجود دارند.

اکنون فرض می‌کنیم یکی از عددهای x، y و z (و باتوجه به مقدماتی بودن این عددها، تنها یکی از آن‌ها) بر p بخش‌پذیر باشد. برای مشخص بودن وضع، z را بخش‌پذیر بر p می‌گیریم. در این‌صورت، یکی (و تنها یکی) از عامل‌های شرکت‌کننده در دستور آبل $z = uv$ (رابطه‌های (۵) را ببینید)، یعنی u و v که نسبت به هم اول‌اند، بر p بخش‌پذیر است.

فرض کنید، v بر p بخش‌پذیر باشد. در این صورت u بر p بخش‌پذیر نیست و

$$uu' \equiv ۱ \pmod{p}$$

از طرف دیگر، از دستورهای (۵) آبل نتیجه می‌شود:

$$۲z = u^{l} + u_{۱}^{l} + u_{۲}^{l}$$

بنابراین

$$u^l + u_1^l \equiv (-u_2)^l (\mathrm{mod} p)$$

یعنی

$$1 + (u_1 u')^l \equiv (-u_2 u')^l (\mathrm{mod} p)$$

به‌این ترتیب، اگر $u \not\equiv 0 (\mathrm{mod} p)$، آن‌وقت باز هم همسایگی‌های درجهٔ l نسبت به مدول p وجود دارد.

سرانجام فرض کنید u بر p بخش‌پذیر باشد. در این‌صورت در رابطهٔ (۴) (که در آن به‌یاد بیاوریم $a = u^l$، $b = v^l$)، همه جمله‌های سمت راست، به‌جز جملهٔ آخری $\binom{l}{l-1} y^{l-1} = l y^{l-1}$، بر p بخش‌پذیرند و بنابراین، داریم

$$v^l \equiv l y^{l-1} (\mathrm{mod} p)$$

ولی بنابه همان دستور آبل

$$y = z - u_1^l$$

یعنی

$$y \equiv (-u_1)^l (\mathrm{mod} p)$$

بنابراین

$$v^l \equiv l(-u_1)^{l(l-1)} (\mathrm{mod} p)$$

و درنتیجه

$$l \equiv (v u_1')^l (\mathrm{mod} p)$$

که در آن u_1' عددی است که برای آن داشته‌باشیم:

$$u_1^{l-1} u_1' \equiv 1 (\mathrm{mod} p)$$

(روشن است که u_1 و بنابراین u_1^{l-1} بر p بخش‌پذیر نیست).

به‌این ترتیب ثابت می‌شود، به‌ازای $u \equiv ۰ (\mathrm{mod} p)$، عدد l، نسبت به مدول p، از درجهٔ l است.

درستی این قضیه هم ثابت می‌شود:

قضیهٔ سوفی ژرمن. فرض کنید برای عدد اول $l \geq ۳$، عدد درستی مثل m وجود داشته‌باشد که

۱) عدد $p = ۲ml + ۱$، عددی اول باشد؛

۲) بین عددهای از درجهٔ l، نسبت به مدول p، همسایگی‌هایی وجود نداشته‌باشد؛

۳) عدد l، نسبت به مُدول p، از درجهٔ l نباشد.

در این صورت، برای نمای l، حالت اول قضیهٔ فرما درست است.

برای آزمایش در موقعیت‌های مشخص شرط‌های ۲) و ۳) این قضیه، سودمند است که به‌یاد داشته‌باشیم، برای هر ξ با درجهٔ l نسبت به مُدول $p = ۲ml + ۱$، این هم‌نهشتی برقرار است:

$$\xi^{۲m} \equiv ۱ (\mathrm{mod} p) \qquad (۱۱)$$

در واقع، اگر $\xi \equiv a^l (\mathrm{mod} p)$، که در آن $a \not\equiv ۰ (\mathrm{mod} p)$، آن‌وقت بنابر قضیهٔ کوچک فرما داریم:

$$\xi^{۲m} \equiv a^{۲ml} \equiv a^{p-۱} \equiv ۱ (\mathrm{mod} p)$$

مساله. عکس این قضیه را ثابت کنید: هر جواب ξ از هم‌نهشتی (۱۱)، نسبت به مُدول p، از درجهٔ lام است.

به‌سادگی دیده می‌شود، برای هر عدد اول p، تنها دو عدد نابرابر برای ξ وجود دارد که در هم‌نهشتی

$$\xi^{۲} \equiv ۱ (\mathrm{mod} p)$$

صدق می‌کند، یعنی ۱ و $-۱ \equiv p - ۱ (\mathrm{mod} p)$.

این حقیقت که عددهای ۱ و $p-1$ در این هم‌نهشتی صدق می‌کنند، روشن است؛ ولی این‌که هم‌نهشتی ریشهٔ دیگری ندارد، ساده‌تر از همه، با تکیه بر این قضیهٔ جبر ثابت می‌شود که: یک چندجمله‌ای درجهٔ n در هر میدانی نمی‌تواند بیش از n ریشه داشته‌باشد. همچنین می‌توان از این مطلب استفاده کرد که عدد

$$\xi^{۲}-۱=(\xi-۱)(\xi+۱)$$

تنها وقتی بر عدد اول p بخش‌پذیر است که $\xi-۱$ یا $\xi+۱$ بر p بخش‌پذیر باشد.

چون عددهای ۱ و $p-1$، به‌روشنی همسایهٔ درجهٔ lام نسبت به مُدول $p=۲l+۱$ نیستند، به این نتیجه می‌رسیم که شرط ۲) از قضیهٔ ژرمن به‌ازای $m=۱$، به‌خودی خود، برقرار است.

از آن‌جاکه عدد $l^{۲}-۱=(l-۱)(l+۱)$ نمی‌تواند بر عدد اول $۲l+۱>l+۱$ بخش‌پذیر باشد، بنابراین، به‌ازای $m=۱$، شرط ۳) هم برقرار است.

به‌این ترتیب، اگر نمای l (که عددی اول و فرد است)، این ویژگی را داشته‌باشد که عدد $۲l+۱$ هم عددی اول باشد، آن‌وقت برای l، حالت اول قضیهٔ فرما درست است.

همان‌طور که در بخش ۱ گفتیم، این نتیجه را خودِ ژرمن به‌دست آورد. بسیاری از مولفان هم، آن را قضیهٔ ژرمن نامیده‌اند.

به‌همین ترتیب، از قضیهٔ کلی ژرمن می‌توان قضیهٔ لژاندر را، که در بخش ۱ آوردیم نتیجه گرفت. به‌یاد آورید که قضیهٔ لژاندر می‌گوید که برای نماد اول l، اگر $۲ml+۱$، که در آن m یکی از پنج عدد ۲، ۴، ۵، ۷ و یا ۸ است، عددی اول باشد، آن‌گاه حالت اول قضیهٔ فرما درست است.

در این‌جا، آن را تنها برای $m=۲$ ثابت می‌کنیم، زیرا با بزرگ شدن m، استدلال به سرعت رو به بغرنجی می‌رود.

فرض کنید، به‌ازای $m=۲$، شرط ۱) از قضیهٔ ژرمن برقرار باشد، یعنی

عدد $p = ۴l + ۱$، عددی اول باشد.

آزمایش می‌کنیم که، شرط ۲) از این قضیه هم برقرار است. باتوجه به آن‌چه پیش از این آوردیم، کافی است ثابت کنیم بین ریشه‌های هم‌نهشتی

$$\xi^۴ \equiv ۱(\mathrm{mod}p) \qquad (۱۲)$$

همسایگی‌هایی وجود ندارد.

چون $\xi^۴ - ۱ = (\xi^۲ + ۱)(\xi^۲ - ۱)$، بنابراین ریشه‌های هم‌نهشتی (۱۲)، ریشه‌های این دو هم‌نهشتی‌اند:

$$\xi^۲ \equiv ۱(\mathrm{mod}p)$$
$$\xi^۲ \equiv -۱(\mathrm{mod}p)$$

می‌دانیم، هم‌نهشتی اول دارای دو ریشهٔ ۱ و $p - ۱ \equiv -۱$ است. دربارهٔ هم‌نهشتی دوم دو حالت ممکن است: یا ریشه‌ای ندارد و یا درست دو ریشه دارد: $\xi_۰$ و $p - \xi_۰ = -\xi_۰$.

در حالت اول، هم‌نهشتی (۱۲) دارای دو ریشهٔ ۱ و $p - ۱$ است که به‌روشنی همسایه نیستند. بنابراین شرط ۲) از قضیهٔ ژرمن در این حالت برقرار است. در حالت دوم، هم‌نهشتی (۱۲)، چهار ریشه دارد:

$$۱, p - ۱, \xi_۰, p - \xi_۰$$

دوتا از این ریشه‌ها، تنها به‌ازای

$$\xi_۰ = \pm ۲ \text{ یا } \xi_۰ = \pm\frac{p-۱}{۲} = \pm ۲l$$

می‌توانند همسایه باشند. اگر $\xi_۰ = \pm ۲$، آن‌وقت $۲^۲ + ۱ = ۵$ بر $p = ۴l + ۱$ بخش‌پذیر است که برای $l > ۱$ ممکن نیست. به‌همین‌ترتیب، اگر $\xi_۰ = \pm ۲l$، آن‌وقت

$$(۲l)^۲ + ۱ = ۴l^۲ + ۱ = (۴l + ۱)l - (l - ۱)$$

بر $p = ۴l + ۱$ بخش‌پذیر می‌شود، یعنی $(l - ۱)$ بر $(۴l + ۱)$ بخش‌پذیر است که باز هم برای $l > ۱$ ممکن نیست. بنابراین، شرط ۲) از قضیهٔ ژرمن در حالت دوم هم برقرار است.

اکنون به شرط ۳) می‌پردازیم. اگر این شرط برقرار نباشد، آن‌وقت $l^۴ \equiv ۱ (\mathrm{mod} p)$، یعنی $(۴l)^۴ \equiv ۱ (\mathrm{mod} p)$ که از آن‌جا نتیجه می‌شود:

$$۴^۴ \equiv ۱ (\mathrm{mod} p)$$

یعنی $۴^۴ - ۱ = ۲۵۵ = ۳ \times ۵ \times ۱۷$ بر p بخش‌پذیر است. چون می‌دانیم $p \neq ۵$، این امکان تنها برای $p = ۱۷$ وجود دارد. ولی معادلهٔ $۴l + ۱ = ۱۷$ جواب $l = ۴$ را دارد که عددی اول نیست و، بنابراین، این حالت هم ناممکن است؛ یعنی شرط ۳) از قضیهٔ ژرمن هم برقرار است.

قضیهٔ ونت هم (بخش ۱ را ببینید)، به قضیهٔ ژرمن منجر می‌شود. تنها باید ثابت کرد، اگر عدد اول $p = ۲ml + ۱$، عدد ونت یعنی D_m را نشمارد، آن‌وقت شرط ۳) از قضیهٔ ژرمن برقرار است.

این اثبات را، به‌عنوان تمرین کم‌وبیش ساده‌ای، به‌عهدهٔ خواننده می‌گذاریم.

۳

قضیهٔ فرما، برای نمای ۴

حالت $n = ۴$، تنها حالتی از قضیهٔ فرما است که با روشی مقدماتی ثابت شده‌است. همان‌طور که پیش از این هم گفتیم، این اثبات را خودِ فرما هم پیدا کرده‌بود. او از دستورهای مربوط به جواب کلی معادلهٔ

$$x^۲ + y^۲ = z^۲ \qquad (۱)$$

استفاده می‌کند. این دستورها را ریاضی‌دانان هندی هم می‌شناختند. در این‌جا، از اثبات همین دستورها آغاز می‌کنیم.

می‌دانیم که برای معادلهٔ (۱) کافی است جواب‌های مقدماتی آن را پیدا کنیم. روشن است، اگر (x, y, z) جوابی از معادلهٔ (۱) باشد، (y, x, z) هم جواب آن است. از طرف دیگر، برای هر جواب (x, y, z)، دست‌کم یکی از عددهای x یا y زوج است. در واقع، اگر هر دو عدد x و y فرد باشند، آن‌وقت $x^۲ + y^۲$ به‌صورت $۴k + ۲$ درمی‌آید که نمی‌تواند برابر توان دوم یک عدد درست باشد (زیرا همه توان دوم، $z^۲$، یا به‌صورت $۴k$ است و یا به‌صورت $۴k + ۱$). همچنین روشن است همراه با جواب (x, y, z)، $(\pm x, \pm y, \pm z)$ هم جوابی از معادله است.

باتوجه به این نکته‌ها، می‌توان بلافاصله نتیجه گرفت، کافی است تنها جوابی مقدماتی از معادلهٔ (۱) را که هر سه عدد x، y و z مثبت و عدد x زوج باشد، پیدا کرد.

پیش‌قضیه. برای هر دو عدد درست و مثبت m و n، که $n < m$، که نسبت به هم اول باشند، با فرض این‌که از m و n یکی زوج و دیگری فرد باشد، دستورهای

$$\begin{aligned} x &= ۲mn \\ y &= m^۲ - n^۲ \\ z &= m^۲ + n^۲ \end{aligned} \qquad (۲)$$

شامل سه عدد درست مثبت‌اند که جوابی مقدماتی از معادله با شرط زوج بودن x است. برعکس، هر سه عدد درست و مثبت (x, y, z) که جوابی

مقدماتی از معادلهٔ (۱) باشند، با فرض زوج بودن عدد x، می‌تواند به‌صورت دستورهای (۲) بیان شود که در آن m و $n < m$ دو عدد نسبت به هم اول‌اند و درضمن یکی زوج و دیگری فرد است.

اثبات. اتحاد

$$(۲mn)^۲ + (m^۲ - n^۲) = (m^۲ + n^۲)^۲$$

نشان می‌دهد، عددهای (۲) (که به‌روشنی عددهایی مثبت‌اند) جوابی از معادلهٔ (۱) هستند که درضمن، x عددی زوج است. اگر این عددها بخشیاب مشترکی مثل $\lambda \geq ۲$ داشته‌باشند، آن‌وقت باید عددهای

$$۲m^۲ = (m^۲ + n^۲) + (m^۲ - n^۲)$$
$$۲n^۲ = (m^۲ + n^۲) - (m^۲ - n^۲)$$

هم بر λ بخش‌پذیر باشند؛ یعنی $\lambda = ۲$، زیرا بنابرفرض، m و n نسبت به هم اول‌اند. ولی اگر $\lambda = ۲$، آن‌وقت عدد $y = m^۲ - n^۲$ زوج است و درنتیجه، $m^۲$ و $n^۲$ یا هردو زوج و یا هردو فردند که ممکن نیست، زیرا بنابرفرض، از m و n باید یکی زوج و دیگری فرد باشد. و این، ثابت می‌کند جواب (۲) یک جواب مقدماتی است.

برعکس، فرض می‌کنیم (x, y, z) جوابی مقدماتی شامل عددهای مثبت و درضمن عدد زوج $x = ۲a$ باشد. چون y و z عددهایی فردند، بنابراین عددهای $z + y$ و $z - y$ زوج می‌شوند. فرض کنید

$$z + y = ۲b,\ z - y = ۲c$$

که در آن، عددهای b و c به‌روشنی مثبت‌اند.

هر بخشیاب مشترک b و c، بخشیابی از $z = b + c$ و $y = b - c$ هم خواهد بود. بنابراین $\lambda = \pm ۱$، یعنی عددهای b و c نسبت به هم اول‌اند. از طرف دیگر

$$۴a^۲ = x^۲ = z^۲ - y^۲ = ۴bc$$

یعنی

$$a^۲ = bc$$

بنابراین، باتوجه به پیش‌قضیه بخش ۲ (که برای حالت $n = ۲$ آوردیم)، چنان عددهای مثبت m و n (که به‌روشنی نسبت به هم اول‌اند و یکی زوج و دیگری فرد است) وجود دارند، به‌نحوی که داشته‌باشیم:

$$b = m^۲,\ c = n^۲$$

در این‌صورت $a^۲ = m^۲n^۲$، یعنی $a = mn$ و

$$x = ۲a = ۲mn, \quad y = b - c = m^۲ - n^۲,$$
$$z = b + c = m^۲ + n^۲$$

برای تکمیل اثبات، کافی است توجه کنیم که $n < m$. پایان اثبات پیش‌قضیه.

اکنون می‌توانیم به اثبات قضیهٔ فرما برای $n = ۴$ بپردازیم. درستی گزارهٔ کلی‌تری را ثابت می‌کنیم.

قضیه. معادلهٔ

$$x^۴ + y^۴ = z^۲ \qquad (۳)$$

در مجموعهٔ عددهای درست، جوابی غیرصفر ندارد.

اثبات. از بُرهان خُلف استفاده و فرض می‌کنیم، برای معادلهٔ (۳)، در مجموعهٔ عددهای درست جوابی مخالف صفر وجود داشته‌باشد. روشن است، بدون این‌که به کلی بودن مطلب لطمه‌ای وارد شود، می‌توان این جواب را شامل عددهای مثبتی درنظر گرفت که دوبه‌دو نسبت به هم اول‌اند. چون در هر مجموعهٔ عددهای درست مثبت، کوچک‌ترین عدد وجود دارد، بنابراین در میان این‌گونه جواب‌ها برای معادلهٔ (۳)، جواب (x, y, z) وجود دارد که در آن، z کم‌ترین مقدار ممکن باشد. به این جواب بیشتر دقت می‌کنیم.

همان‌طور که برای جواب معادلهٔ (۱) ثابت کردیم، یکی از عددهای x یا y باید زوج باشد، در این‌جا هم فرض می‌کنیم، x عددی زوج است. روشن است که این فرض، به کلی بودن مطلب لطمه‌ای نمی‌زند. چون

$$(x^۲)^۲ + (y^۲)^۲ = z^۲$$

از آن‌جاکه عددهای $x^۲$، $y^۲$ و z مثبت و دوبه‌دو نسبت به هم اول‌اند و $x^۲$ عددی زوج است، بنابراین باتوجه به پیش‌قضیه، دو عدد نسبت به هم اولِ m و $n < m$ وجود دارند که یکی زوج و دیگری فرد باشد، به‌نحوی‌که داشته‌باشیم:

$$\begin{aligned} x^۲ &= ۲mn, \\ y^۲ &= m^۲ - n^۲, \\ z &= m^۲ + n^۲ \end{aligned}$$

اگر $m = ۲k$ و $n = ۲l + ۱$، آن‌وقت

$$y^۲ = ۴(k^۲ - l^۲ - l - ۱) + ۳$$

که ممکن نیست، زیرا همان‌طور که پیش از این هم یادآوری کردیم، توان دوم هر عدد فرد باید به‌صورت $۴k + ۱$ باشد. بنابراین عدد m فرد و عدد n زوج است.

$n = ۲q$ می‌گیریم. در این‌صورت $x^۲ = ۴mq$ و بنابراین

$$mq = \left(\frac{x}{۲}\right)^۲$$

چون عددهای m و q نسبت به هم اول‌اند، نتیجه می‌گیریم که

$$m = z_۱^۲, \; q = t^۲$$

که در آن‌ها، z_1 و t عددهای مثبت درست و نسبت به هم اول‌اند.
به‌ویژه، می‌بینیم که

$$y^2 = (z_1^2)^2 - (2t^2)^2$$

یعنی

$$(2t^2)^2 + y^2 = (z_1^2)^2$$

چون دو عدد t و z_1 نسبت به هم اول‌اند، می‌توان برای این برابری دوباره از پیش‌قضیه استفاده کرد. بنابراین دو عدد نسبت به‌هم اولِ a و $b < a$ وجود دارند که یکی فرد و دیگری زوج باشد، به‌نحوی‌که

$$2t^2 = 2ab \Rightarrow t^2 = ab,$$
$$y^2 = a^2 - b^2,$$
$$z_1^2 = a^2 + b^2$$

چون a و b نسبت به‌هم اول‌اند، از برابری اول (بنابه پیش‌قضیه بخش ۲) نتیجه می‌شود: دو عدد درست x_1 و y_1 وجود دارند که برای آن‌ها

$$a = x_1^2,\ b = y_1^2$$

بنابراین، برابری سوم را می‌توان این‌طور نوشت:

$$x_1^4 + y_1^4 = z_1^2$$

و این، به‌معنی آن است که (x_1, y_1, z_1) جوابی مقدماتی از معادلهٔ (۳) است که درضمن شامل عددهایی مثبت است. به‌این ترتیب، باتوجه به جواب (x, y, z) باید داشته‌باشیم:

$$z_1 \geq z$$

از آن‌جا

$$z_1^2 \geq z$$

که درنتیجه، به نابرابری بی‌معنی زیر می‌رسیم:

$$m \geq m^2 + n^2$$

به‌این ترتیب، فرض وجود جواب برای معادلهٔ (۳)، ما را به تناقض می‌کشاند. یعنی این معادله، در مجموعهٔ عددهای درست، جوابی مخالف صفر ندارد.

۴

قضیهٔ فرما، برای نمای ۳

پیش از این هم گفته‌ایم، قضیهٔ **فرما** را برای حالت $l = ۳$، نخستین بار **اویلر** در سال ۱۷۶۸ ثابت کرد. در این‌جا، این اثبات را بازسازی می‌کنیم. **اویلر** در آغاز این پیش‌قضیه را می‌آورد.

پیش‌قضیه. اگر دو عدد a و b که نسبت به هم اول‌اند، دارای این ویژگی باشند که عدد $a^۲ + ۳b^۲$ توان سوم یک عدد درست باشد، آن‌وقت دو عدد درست s و t وجود دارند، به‌نحوی‌که داشته‌باشیم:

$$a = s(s^۲ - ۹t^۲),\ b = ۳t(s^۲ - t^۲)$$

در آغاز روشن می‌کنیم، چگونه می‌توان از این پیش‌قضیه، برای اثبات قضیهٔ **فرما** استفاده کرد.

فرض می‌کنیم، به‌ازای $l = ۳$ قضیهٔ **فرما** درست نباشد، یعنی عددهای درستی مثل x، y و z وجود داشته‌باشند، به‌نحوی‌که داشته‌باشیم:

$$x^۳ + y^۳ = z^۳ \qquad (۱)$$

می‌دانیم، عددهای x، y و z را می‌توان دوبه‌دو نسبت به هم اول، درنظر گرفت. در این‌صورت، تنها یکی از این سه عدد، می‌تواند عددی زوج باشد. از طرف دیگر، روشن است، هر سه عدد نمی‌توانند عددهایی فرد باشند (زیرا مجموع یا تفاضل دو عدد فرد، عددی زوج است). بنابراین یک، و تنها یکی از سه عدد x، y و z زوج است.

بی آن‌که به کلی بودن مطلب لطمه‌ای وارد شود، می‌توان x را عددی زوج گرفت. در واقع، اگر y عددی زوج باشد، می‌توان نقش x و y را با هم عوض کرد؛ اگر z عددی زوج باشد، می‌توان نقش x و z را با تغییر علامت عوض کرد، زیرا

$$(-z)^۳ + y^۳ = (-x)^۳$$

بین همهٔ عددهای درست و سه‌گانهٔ (x, y, z) که در معادلهٔ (۱) صدق کند، با فرض زوج بودن x، می‌توان آن را انتخاب کرد که $|x|$ کم‌ترین مقدار

ممکن را داشته‌باشد. چنین عددهای سه‌گانهٔ «حداقل» وجود دارد، زیرا در هر مجموعه از عددهای درست مثبت، کوچک‌ترین عدد وجود دارد.

چون y و z عددهایی فردند، بنابراین عددهای

$$p = \frac{z+y}{۲},\ q = \frac{z-y}{۲}$$

عددهایی درست‌اند. از آن‌جاکه

$$z = p+q,\ y = p-q \qquad (۲)$$

بنابراین، یکی از عددهای p و q زوج و دیگری فرد است. درضمن این عددها به‌روشنی نسبت به هم اول‌اند.

باتوجه به (۱) و (۲) داریم:

$$x^۳ = z^۳ - y^۳ = (p+q)^۳ - (p-q)^۳ =$$
$$= ۶p^۲q + ۲q^۳ = ۲q(q^۲ + ۳p^۲)$$

اگر در این‌جا فرض کنیم $x = ۲u$، به‌دست می‌آید:

$$u^۳ = \frac{q}{۴}(q^۲ + ۳p^۲) \qquad (۳)$$

چون از دو عدد p و q، یکی زوج و دیگری فرد است، $q^۲ + ۳p^۲$ عددی فرد می‌شود. درنتیجه، از (۳) می‌توان نتیجه گرفت، عدد q بر ۴ بخش‌پذیر است (یعنی q عددی زوج و p عددی فرد است).

باتوجه به پیش‌قضیه‌ای که در بخش ۲ ثابت کردیم، حاصل‌ضرب دوعددی که نسبت به‌هم اول‌اند، وقتی و تنها وقتی می‌تواند توان سوم یک عدد درست باشد که هریک از آن‌ها، توان سوم عددی درست باشد. از طرف دیگر، عددهای $\frac{q}{۴}$ و $q^۲ + ۳p^۲$، تنها وقتی نسبت به هم اول‌اند که عددهای q و

$۳p^۲ = (q^۲ + ۳p^۲) - q^۲$ نسبت به‌هم اول باشند؛ و این، وقتی و تنها وقتی پیش می‌آید که (باتوجه به این‌که p و q نسبت به‌هم اول‌اند) q بر ۳ بخش‌پذیر نباشد. به‌این ترتیب، اگر فرض کنیم q بر ۳ بخش‌پذیر نیست، آن‌وقت از (۳) نتیجه می‌شود که هریک از عددهای $\frac{q}{۴}$ و $q^۲ + ۳p^۲$ توان سوم یک عدد درست است.

ولی باتوجه به پیش‌قضیه، اگر $q^۲ + ۳p^۲$ توان سوم یک عدد درست باشد، آن‌وقت داریم:

$$q = s(s^۲ - ۹t^۲),\ p = ۳t(s^۲ - t^۲)$$

که در آن‌ها، s و t، عددهایی درست‌اند. چون p عددی فرد است، پس از برابری $p = ۳t(s^۲ - t^۲)$ نتیجه می‌شود t عددی فرد و s عددی زوج است. به‌جز این، چون p و q نسبت به‌هم اول‌اند، عددهای t و s هم، نسبت به هم اول می‌شوند.

از آن‌جاکه $\frac{q}{۴}$ برابر توان سوم یک عدد درست است، بنابراین

$$۲q = ۸ \times \frac{q}{۴}$$

هم باید برابر توان سوم یک عدد درست باشد. این، ثابت می‌کند که عدد

$$۲s(s^۲ - ۹t^۲) = ۲s(s - ۲t)(s + ۳t)$$

هم برابر توان سوم یک عدد درست است.

عددهای $۲s$، $s - ۳t$ و $s + ۳t$ نسبت به‌هم اول‌اند. در واقع، اگر $۲s$ و $s \pm ۳t$ دارای بخشیاب اول و مشترک λ باشند، آن‌وقت $\lambda \neq ۲$، زیرا $s \pm ۳t$، عددی فرد است. بنابراین باید λ بخشیاب مشترک s و $\pm ۳t = (s \pm ۳t) - s$ باشد. ولی چون t و s نسبت به هم اول‌اند، این امکان تنها به‌ازای $\lambda = ۳$ پیش می‌آید. به‌همین ترتیب، اگر عددهای $s + ۳t$

و $s-۳t$ دارای عامل اول مشترک λ باشند، $\lambda \neq ۲$، زیرا هریک از این دو عدد فرد هستند؛ درضمن عددهای

$$۲s=(s+۳t)+(s-۳t),\ ۶t=(s+۳t)-(s-۳t)$$

بر λ بخش‌پذیرند که دوباره تنها به‌ازای $\lambda=۳$ ممکن است. به‌این ترتیب، در هر دو حالت، عدد s و درنتیجه عدد q، برخلاف فرض، بر $\lambda=۳$ بخش‌پذیر می‌شوند.

چون حاصل‌ضرب عددهای $۲s$، $s-۳t$ و $s+۳t$ که نسبت به‌هم اول‌اند، توان سوم یک عدد درست است، بنابراین باید هریک از آن‌ها برابر توان سوم عددی درست باشد. و این، به‌معنی آن است که سه عدد درست $x_۱$، $y_۱$ و $z_۱$ وجود دارد، به‌نحوی‌که داشته‌باشیم:

$$\begin{aligned} x_۱^۳ &= ۲s,\\ y_۱^۳ &= -(s+۳t),\\ z_۱^۳ &= s-۳t \end{aligned}$$

و از آن‌جا

$$x_۱^۳+y_۱^۳=z_۱^۳$$

به‌این ترتیب، با آغاز از سه عدد (x,y,z)، توانستیم سه عدد جدید $(x_۱,y_۱,z_۱)$ به‌دست آوریم که در معادلهٔ (۱) صدق می‌کنند و درضمن، دارای این ویژگی‌اند که نخستین عدد آن‌ها، یعنی $x_۱$، عددی زوج است.

چون داریم: $x^۳=۲q(q^۲+۳p^۲)$، بنابراین $|q|<\frac{|x^۳|}{۲}$؛ و چون داریم $q=s(s^۲-۹t^۲)$، بنابراین $|s|\leq|q|$ و درنتیجه

$$|x_۱^۳|=۲|s|<|x^۳|$$

به‌این ترتیب $|x_۱|<|x|$ که با فرض «حداقل» یا «می‌نیمال» بودن عددهای سه‌گانهٔ (x,y,z) متناقض است. این تناقض ثابت می‌کند، عدد q باید بر ۳

بخش‌پذیر باشد، یعنی داشته‌باشیم:

$$q = ۳r$$

که در آن، r عددی است درست (و بخش‌پذیر بر ۴). در این‌صورت باتوجه به (۳)

$$u^۳ = \frac{۳}{۴}r(۹r^۲ + ۳p^۲) = \frac{۹}{۴}r(۳r^۲ + p^۲) \qquad (۴)$$

اگر عددهای درست $\frac{۹}{۴}r$ و $۳r^۲ + p^۲$ بر عدد اولی مثل λ بخش‌پذیر باشند، آن‌وقت $\lambda \neq ۳$، زیرا در غیر این‌صورت عدد p بر λ بخش‌پذیر می‌شود، یعنی با q بخشیابی مشترک دارد. ولی اگر $\lambda \neq ۳$، آن‌وقت باید عددهای

$$r,\ p^۲ = (۳r^۲ + p^۲) - ۳r^۲$$

یعنی p و q بر λ بخش‌پذیر باشند که ممکن نیست. بنابراین، عددهای $\frac{۹}{۴}r$ و $۳r^۲ + p^۲$ نسبت به‌هم اول‌اند.

به‌این ترتیب، از (۴) نتیجه می‌گیریم، این دو عدد، هرکدام توان سوم یک عدد درست است و بنابراین باتوجه به پیش‌قضیه (اگر دربارهٔ عدد $p^۲ + ۳r^۲$ به‌کار ببریم)، به‌این برابری‌ها می‌رسیم:

$$p = s(s^۲ - ۹r^۲),\ r = ۳t(s^۲ - t^۲) \qquad (۵)$$

که در آن‌ها، s و t، عددهایی درست و نسبت به‌هم اول‌اند. درضمن، روشن است، t عددی زوج است (زیرا r زوج است) و درنتیجه، s عددی فرد می‌شود. به‌جز این می‌بینیم، عدد درست

$$\frac{۸}{۲۷} \cdot \frac{۹}{۴}r = \frac{۲}{۳}r = ۲t(s^۲ - t^۲) = ۲t(s+t)(s-t)$$

برابر توان سوم یک عدد درست است.

از آن‌جاکه عددهای s و t نسبت به‌هم اول‌اند و، درضمن، یکی زوج و دیگری فرد است، بنابراین عددهای $۲t$، $s+t$ و $s-t$ دوبه‌دو نسبت به‌هم اول‌اند. درنتیجه، هریک از آن‌ها توان سوم یک عدد درست است، به‌نحوی‌که عددهای درست $x_۱$، $y_۱$ و $z_۱$ وجود دارند که

$$x_۲^۳ = ۲t,$$
$$y_۱^۳ = s - t,$$
$$z_۱^۳ = s + t$$

ولی در این‌صورت

$$x_۱^۳ + y_۱^۳ = z_۱^۳$$

و

$$|x_۱^۳| = ۲|t| \leq \frac{۲}{۳}|r| = \frac{۲}{۹}|q| < ۲|q| < |x^۳|$$

یعنی $|x_۱| < |x|$.

به‌این ترتیب، در این حالت هم به تناقض می‌رسیم («حداقل بودن» عددهای سه‌گانهٔ (x, y, z) نقض می‌شود). پایان اثبات.

۵

حساب حلقهٔ D_3

به‌این ترتیب، برای اثبات کامل قضیهٔ **فرما** دربارهٔ نمای $l = ۳$، تنها این می‌ماند که درستی پیش‌قضیهٔ آغاز بند پیش را ثابت کنیم.

اویلر، برای اثبات پیش‌قضیه، از این‌جا آغاز می‌کند که [۳]

$$a^۲ + ۳b^۲ = (a + b\sqrt{-۳})(a - b\sqrt{-۳})$$

سپس می‌نویسد، چون سمت چپ برابری، توان سوم یک عدد است، بنابراین هردو عامل سمت راست برابری هم باید توان سوم باشند. به‌ویژه

$$a + b\sqrt{-۳} = (s + t\sqrt{-۳})^۳$$

که در آن، s و t عددهایی درست‌اند. اگر پرانتز سمت راست این برابری را باز کنیم، به‌دست می‌آید:

$$a + b\sqrt{-۳} = s^۳ - ۹st^۲ + (۳s^۲t - ۳t^۳)\sqrt{-۳}$$

و بنابراین

$$a = s^۳ - ۹st^۲ = s(s^۲ - ۹t^۲),$$
$$b = ۳s^۲t - ۳t^۳ = ۳t(s^۲ - t^۲)$$

نمی‌توان به تیزهوشی و شجاعت **اویلر** آفرین نگفت که با دلیری از بحث دربارهٔ عددهای درست، خود را به عددی به‌صورت $a + b\sqrt{-۳}$ رساند. ولی برای این‌که اثبات ممتاز او را بیاوریم، در آغاز باید حساب چنین عددهایی را بشناسیم. به‌ویژه از آن‌جاکه گزارهٔ مربوط به حاصل‌ضرب‌هایی که توان سوم‌اند ناشی از قضیهٔ اصلی حساب است، باید درستی این قضیه را برای عددهای

۳- در این‌جا و بعد از این، $\sqrt{-۳}$ را ریشه‌ای از معادلهٔ $x^۲ + ۳ = ۰$ می‌گیریم که در نیم‌صفحهٔ بالا قرار دارد.

به‌صورت $a+b\sqrt{-۳}$ هم ثابت کنیم (دیگر در این‌باره صحبت نمی‌کنیم که باید ثابت کرد، عددهای $a+b\sqrt{-۳}$ و $a-b\sqrt{-۳}$ «نسبت به‌هم اول‌اند»).

باوجود این، به‌نظر می‌رسد، برای عددهای به‌صورت $a+b\sqrt{-۳}$، قضیهٔ اصلی حساب درست نیست: برای عددهای به‌صورت $a+b\sqrt{-۳}$ تجزیهٔ یگانه به‌ضرب عددهای «اول» (که دیگر قابل‌تجزیه نباشند) وجود ندارد. برای نمونه

$$۴ = ۲ \times ۲ = (۱+\sqrt{-۳})(۱-\sqrt{-۳})$$

درضمن، عددهای ۲ و $۱ \pm \sqrt{-۳}$ غیرقابل تجزیه‌اند.

اثبات. داریم:

$$(a+b\sqrt{-۳})(c+d\sqrt{-۳}) = ac - ۳bd + (ad+bc)\sqrt{-۳}$$

بنابراین، اگر داشته‌باشیم:

$$۲ = (a+b\sqrt{-۳})(c+d\sqrt{-۳})$$

آن‌وقت

$$\begin{cases} ac - ۳bd = ۲ \\ ad + bc = ۰ \end{cases}$$

به‌طور مستقیم می‌توان ثابت کرد، این معادله‌ها در مجموعهٔ عددهای درست جواب ندارند، ولی بهتر است روش دیگری را انتخاب کنیم. به این نکته توجه می‌کنیم که با تغییر علامت‌های b و d (به‌شرطی‌که علامت هردو را عوض کنیم)، این معادله‌ها تغییر نمی‌کنند. بنابراین

$$۲ = (a-b\sqrt{-۳})(c-d\sqrt{-۳})$$

و این، به‌معنی آن است که

$$۲ \times ۲ = (a+b\sqrt{-۳})(a-b\sqrt{-۳}) \cdot (c+d\sqrt{-۳})(c-d\sqrt{-۳})$$

یعنی

$$۴ = (a^۲ + ۳b^۲)(c^۲ + ۳d^۲) \qquad (۱)$$

به‌همین ترتیب، اگر

$$۱ + \sqrt{-۳} = (a + b\sqrt{-۳})(c + d\sqrt{-۳})$$

آن‌وقت

$$۱ - \sqrt{-۳} = (a - b\sqrt{-۳})(c - d\sqrt{-۳})$$

و بنابراین، دوباره به معادلهٔ (۱) می‌رسیم.

چون تنها عددهای طبیعی در این معادله شرکت دارند، بنابراین، یا یکی از عامل‌های سمت راست برابر ۴ و دیگری برابر ۱ است، یعنی برای نمونه

$$a^۲ + ۳b^۲ = ۴,$$
$$c^۲ + ۳d^۲ = ۱$$

و یا هریک از این عامل‌ها برابر است با ۲، یعنی

$$a^۲ + ۳b^۲ = ۲$$
$$c^۲ + ۳d^۲ = ۲$$

ولی روشن است، معادلهٔ $a^۲ + ۳b^۲ = ۲$ در مجموعهٔ عددهای درست جواب ندارد. بنابراین، حالت دوم ممکن نیست. در حالت اول، معادلهٔ

$$a^۲ + ۳b^۲ = ۴$$

تنها به‌ازای $a = \pm ۱$، $b = \pm ۱$ و $a = \pm ۲$، $b = ۰$ و معادلهٔ

$$c^۲ + ۳d^۲ = ۱$$

تنها به‌ازای $c = \pm ۱$، $d = ۰$ برقرار است.

و در همین‌جا ثابت می‌شود، عددهای ۲ و $1 \pm \sqrt{-3}$ قابل تجزیه نیستند.

اگر اندکی عمیق‌تر وارد موضوع بشویم، می‌توان استدلال اویلر را نجات داد.

آیا اویلر آگاهانه و قانون‌مند عددهای به‌صورت $a + b\sqrt{-3}$ را انتخاب کرده‌است، یا به‌تصادف؟

اگر قرار باشد از عددی استفاده شود که غیر از عددهای درست باشد، طبیعی است در نوبت اول به عددهایی توجه شود که از تجزیهٔ عبارت سمت چپ معادلهٔ فرما به ضرب عامل‌های خطی به‌دست می‌آید. این تجزیه چنین است:

$$x^3 + y^3 = (x + y)(x + \zeta y)(x + \overline{\zeta} y)$$

که در آن ζ و $\overline{\zeta}$ عددهایی مختلط‌اند که همراه با ۱، ریشه‌های معادلهٔ

$$z^3 = 1 \qquad (۲)$$

را تشکیل می‌دهند. این ملاحظه، به‌طور طبیعی تلقین می‌کند، دامنه‌ای که باید معادلهٔ فرما برای $l = 3$ در آن بررسی شود، عبارت است از عددهای به‌صورت

$$a + b\zeta + c\overline{\zeta} \qquad (۳)$$

که در آن a، b و c، عددهایی درست‌اند.

از طرف دیگر، همراه با ζ، عدد ζ^2 هم ریشه‌ای از معادلهٔ (۲) است، زیرا

$$(\zeta^2)^3 = (\zeta^3)^2 = 1^2 = 1$$

بنابراین $\overline{\zeta} = \zeta^2$، یعنی عدد (۳) را می‌توان به‌این صورت نوشت:

$$a + b\zeta + c\zeta^2 \qquad (۳')$$

به‌جز این، عدد ζ (همراه با عدد $\overline{\zeta} = \zeta^۲$)، ریشه‌ای از این معادله است:

$$\frac{x^۳ - ۱}{x - ۱} = x^۲ + x + ۱ = ۰$$

که از آن نتیجه می‌شود:

$$\zeta^۲ = -۱ - \zeta \qquad (۴)$$

بنابراین، هر عدد به‌صورت $(۳')$، در واقع، به‌این صورت است:

$$A + B\zeta \qquad (۵)$$

که در آن $A = a - c$ و $B = b - c$.

به‌این ترتیب، نتیجه می‌گیریم که باید مجموعهٔ عددهای به‌صورت (۵) را بررسی کنیم که در آن، A و B عددهای درست دلخواهی‌اند. این مجموعه را با نماد $D_۳$ نشان می‌دهیم.

روشن است، مجموع و حاصل‌ضرب دو عدد از $D_۳$، باز هم عددی است از $D_۳$. در واقع، باتوجه به برابری (۴) داریم:

$$(A+B\zeta)(A_۱+B_۱\zeta) = (AA_۱-BB_۱)+(AB_۱+BA_۱-BB_۱)\zeta$$

همهٔ این‌ها، به زبان جبر امروزی، به این معنی است که $D_۳$ یک حلقهٔ عددی است.

برای ساده‌تر شدن محاسبه، بهتر است عددهای به‌صورت (۵) را، با ضریب‌های گویای A و B هم درنظر بگیریم. مجموعهٔ چنین عددهایی را $K_۳$ [۴] می‌نامیم.

روشن است، مجموع، تفاضل و حاصل‌ضرب عددهایی از $K_۳$، باز هم عددی از $K_۳$ است. ولی در این‌جا، همچنین از بخش دوعددی که

۴- دیگران به‌جای $D_۳$ و $K_۳$ از نمادهای $Z[\xi_۳]$ و $Q[\xi_۳]$، که در آن $\xi_۳$ ریشه‌ای از $x^۲ + x + ۱$ است، استفاده کرده‌اند. (ویراستار).

در مجموعهٔ عددهای K_3 هستند، عددی از K_3 به‌دست می‌آید. در واقع، اگر عدد $\frac{C+D\zeta}{A+B\zeta}$ را با فرض $A+B\zeta \neq 0$ درنظر بگیریم، می‌توانیم آن را به‌این صورت تبدیل کنیم (این عمل، در جبر مقدماتی، به‌نام «گویا کردن مخرج کسر» معروف است):

$$\frac{C+D\zeta}{A+B\zeta}=\frac{(C+D\zeta)(A+B\bar{\zeta})}{(A+B\zeta)(A+B\bar{\zeta})}=\frac{(C+D\zeta)(A+B\bar{\zeta})}{A^2+AB(\zeta+\bar{\zeta})+B^2\zeta\bar{\zeta}}$$
$$=\frac{CA+DA\zeta+CB\zeta^2+DB\zeta^3}{A^2-AB+B^2}=$$
$$=\frac{CA+DB-CB}{A^2-AB+B^2}+\frac{DA-CB}{A^2-AB+B^2}\zeta$$

همهٔ این‌ها، به‌معنای آن است که K_3 یک میدان را تشکیل می‌دهد و آن را میدان دایره بُری می‌نامند (این نام‌گذاری به‌این مناسبت است که ریشه‌های معادلهٔ (۲) بستگی تنگاتنگی با مسالهٔ تقسیم دایره به سه بخش برابر دارد). عددهای D_3 را، عددهای درست میدان K_3 و خود D_3 را حلقهٔ عددهای درست از میدان K_3 می‌نامند. این حلقه شامل همهٔ عددهای درست عادی هم می‌شود (که به‌ازای $B=0$، به‌دست می‌آیند).

یادآور می‌شویم، عددهای D_3 (یا K_3) را تنها به یک طریق می‌توان به‌صورت (۵) نوشت. در واقع اگر

$$A+B\zeta=A_1+B_1\zeta$$

و $B\neq B_1$، آن‌وقت

$$\zeta=\frac{A-A_1}{B-B_1}$$

که ممکن نیست، زیرا ζ عددی حقیقی و، بالاتر از آن، عددی گویا نیست. بنابراین $B=B_1$ و درنتیجه $A=A_1$.

ضمن محاسبهٔ خارج‌قسمت در K_3، در واقع برای هر عدد

$$\alpha = A + B\zeta \subset K_3$$

به‌دست می‌آوریم:

$$N\alpha = \lambda\overline{\alpha} = A^2 - AB + B^2 = \frac{(2A - B)^2 + 3B^2}{4}$$

که عددی گویا و نامنفی است (و عددی درست، وقتی $\alpha \in D_3$). این عدد را هَنج (یا نُرم) α گویند. نُرم α تنها برای $\alpha = 0$ برابر صفر است.

ویژگی جالب نُرم‌ها در این است که، نُرم حاصل‌ضرب، برابر است با حاصل‌ضرب نُرم‌ها:

$$N(\alpha\beta) = N\alpha \cdot N\beta,\ (\alpha, \beta \in K_3) \qquad (۶)$$

در واقع

$$N(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\beta \cdot \overline{\alpha}\overline{\beta} = \alpha\overline{\alpha} \cdot \beta\overline{\beta} = N\alpha \cdot N\beta$$

اگر رابطهٔ (۶) را باز کنیم به‌دست می‌آید:

$$\begin{aligned}(AA_1 - BB_1)^2 - (AA_1 - BB_1)(AB_1 + BA_1 - BB_1) + \\ + (AB_1 + BA_1 - BB_1)^2 = \\ = (A^2 - AB + B^2)(A_1^2 - A_1B_1 + B_1^2)\end{aligned}$$

این، ساده‌ترین نمونه از اتحادهای جبری است که از رابطهٔ (۶) برای هر میدان عددهای جبری به‌دست می‌آید.

عددهای K_3 (و D_3) را می‌توان به‌صورت روشن‌تری نوشت، اگر توجه کنیم که معادلهٔ درجه دوم

$$x^2 + x + 1 = 0$$

ریشه‌هایی برابر

$$\frac{-1 \pm \sqrt{-3}}{2}$$

دارد. هریک از این ریشه‌ها، می‌تواند به‌عنوان ζ درنظر گرفته شود. برای روشن بودن وضع فرض می‌کنیم:

$$\zeta = \frac{-1 + \sqrt{-3}}{2}$$

در این‌صورت

$$A + B\zeta = \frac{(2A - B) + B\sqrt{-3}}{2}$$

به‌این ترتیب، روشن می‌شود که عددهای K_{-3} به‌صورت $a + b\sqrt{-3}$ هستند که در آن a و b عددهایی گویا و عددهای D_{-3} (عددهای درست K_{-3}) به‌صورت

$$\frac{p + q\sqrt{-3}}{2} \qquad (7)$$

درمی‌آیند؛ درضمن p و q، عددهایی درست و هردو فرد یا هردو زوج‌اند.

در حالت خاص، اگر هر دو عدد p و q زوج باشند، عددهای اویلر به‌دست می‌آید:

$$a + b\sqrt{-3}$$

به‌این ترتیب، محدود کردن کار به این‌گونه عددها، از دیدگاه کلی، دلیلی ندارد و بنابراین می‌توان امید داشت، اگر به عددهای (۷)، که به‌صورت طبیعی‌تری به‌دست آمده‌اند، بپردازیم، همهٔ دشواری‌ها از بین می‌رود. به‌نظر می‌رسد که در واقع امر هم، چنین است.

برای این‌که در بررسی مطلب به دشواری برنخوریم، بهتر است درآغاز به ساده‌ترین مفهوم‌های اصلی حساب حلقه‌ها بپردازیم. گرچه در این‌جا تنها

به حلقهٔ $D_۳$ و برای بعد هم تنها به تعمیم مستقیم آن D_l، برای $l \geq ۳$، نیازمندیم، تعریف این مفهوم‌ها را به‌صورت کلی و طبیعی خود می‌آوریم. خواننده‌ای که به جنبه‌های نظری دقیق علاقه‌ای ندارد و نمی‌خواهد خود را درگیر تعریف‌های انتزاعی کند، می‌تواند از چند سطر بعد صرف‌نظر کند و از این‌جا به‌بعد، D را به‌معنای حلقه $D_۳$ بگیرد.

فرض را بر این می‌گیریم که مفهوم حلقه (جابه‌جایی‌پذیر، شرکت‌پذیر و با واحد ۱) برایمان روشن باشد. به‌یاد می‌آوریم، چنین حلقه‌ای را «حلقهٔ صحیح» (ویا گاهی «حوزهٔ کامل») گویند، وقتی که بخشیابی برای صفر نداشته‌باشد، یعنی حاصل‌ضرب هردو عضو مخالف صفر از آن، مخالف صفر باشد. از این به‌بعد، هرجا از حلقه صحبت می‌کنیم، منظورمان حلقهٔ صحیح است.

ویژگی اصلی حلقه‌های صحیح، که همه‌جا از آن استفاده می‌کنیم، این است که در آن‌ها (و تنها در آن‌ها) قاعدهٔ ساده کردن درست است، یعنی از برابری $(\alpha \neq ۰)\alpha\beta = \alpha\gamma$ نتیجه می‌شود: $\beta = \gamma$.

عضو ε از حلقهٔ D را واحد می‌نامند، وقتی که عضوی به‌نام $\varepsilon^{-۱} \in D$ وجود داشته‌باشد، به‌نحوی‌که داشته‌باشیم:

$$\varepsilon\varepsilon^{-۱} = ۱$$

(عضو واحد را، عضو وارون‌دار هم می‌گویند.)

روشن است که حاصل‌ضرب و خارج‌قسمت دو واحد، عبارت است از واحد.

مثال ۱. حلقهٔ $\mathbf{Z}$ از عددهای درست شامل دو واحد است: $+۱$ و -۱.

مثال ۲: عضو $\varepsilon \in D$ را ریشهٔ مرتبهٔ n از یک گویند، وقتی‌که

$$\varepsilon^n = ۱$$

روشن است، هر ریشهٔ یک (که در D وجود دارد)، واحدی از حلقهٔ D است (که برای آن $\varepsilon^{-۱} = \varepsilon^{n-۱}$).

مثال ۳. واحدهای D_{-3} را پیدا می‌کنیم. ثابت می‌شود، عدد $\alpha \in D_{-3}$ وقتی، و تنها وقتی، واحد است که داشته‌باشیم: $N\alpha = 1$. درواقع، اگر $\alpha\alpha^{-1} = 1$، آن‌وقت

$$N\alpha \cdot N\alpha^{-1} = N(\alpha\alpha^{-1}) = N1 = 1$$

و بنابراین $N\alpha = 1$. برعکس، اگر $N\alpha = 1$، یعنی $\alpha\overline{\alpha} = 1$، آن‌وقت α واحد است ($\alpha^{-1} = \overline{\alpha}$).

چون برای عدد $\alpha = A + B\zeta$، نُرم $N\alpha$ با این دستور بیان می‌شود:

$$N\alpha = A^2 - AB + B^2 = \frac{(2A - B)^2 + 3B^2}{4}$$

بنابراین وقتی و تنها وقتی $N\alpha = 1$، که داشته‌باشیم:

$$B = = 0, A = \pm 1, \text{ یا } B = \pm 1 \text{ و } (2A - B)^2 = 1 \Rightarrow$$
$$\Rightarrow A = B = \pm 1, \text{ یا } A = 0, B = \pm 1$$

به‌این ترتیب، حلقهٔ D_{-3} دارای شش واحد است:

$$+1,\ +\zeta,\ 1 + \zeta = -\zeta^2,$$
$$-1,\ -\zeta,\ -1 - \zeta = \zeta^2$$

که عبارت‌اند از ریشه‌های مرتبهٔ ششم «یک». درضمن، هر واحد، توانی است از واحد

$$1 + \zeta = \frac{1 + \sqrt{-3}}{2}$$

(ریشهٔ اولیه از ریشه‌های ششم یک). در واقع

$$(1 + \zeta)^1 = 1 + \zeta,\ (1 + \zeta)^2 = \zeta,\ (1 + \zeta)^3 = -1,$$
$$(1 + \zeta)^4 = -1 - \zeta,\ (1 + \zeta)^5 = -\zeta,\ (1 + \zeta)^6 = 1$$

D^* را، مجموعهٔ $D - \{0\}$، شامل همهٔ عضوهای غیرصفر حلقهٔ D فرض می‌کنیم.

دو عضو α و β از D^* را، هم‌پیوند (associate=وابسته) گویند (و به‌صورت $\alpha \sim \beta$ نشان می‌دهند) وقتی که عضو واحدی مثل ε وجود داشته‌باشد، به‌نحوی‌که داشته‌باشیم: $\beta = \varepsilon\alpha$. روشن است که، نسبت هم‌پیوندی، یک نسبت هم‌ارزی است و بنابراین، مجموعهٔ D^*، به خانواده‌هایی از عضوهای هم‌ارز تجزیه می‌شود.

$D' \subset D^*$ را مجموعهٔ همهٔ عضوهای غیرصفر حلقهٔ D می‌گیریم که واحد نباشند.

$\alpha \in D'$ را تجزیه‌پذیر می‌نامیم، وقتی عضوهای β و γ از D' وجود داشته‌باشند، به‌نحوی‌که داشته‌باشیم: $\alpha = \beta\gamma$. عضو تجزیه‌ناپذیر $\alpha \in D'$ را هم، «عضو اول[۵]» می‌نامند.

تابع $\alpha \to \|\alpha\|$ را که روی D^* تعریف شده‌است و مقدارهای درست مثبت در مجموعهٔ $\mathbf{N}$ می‌دهد، هنج‌نما (یا شبه‌نُرم) می‌نامند، وقتی‌که، اگر $\alpha \in D^*$ بر $\beta \in D^*$ بخش‌پذیر باشد، نتیجه شود $\|\beta\| \geq \|\alpha\|$. (بخش‌پذیری α بر β، یعنی $\alpha = \beta\gamma$، که در آن $\gamma \in D$.)

اگر γ واحد باشد، آن‌وقت $(\gamma^{-1} \in D)\beta = \alpha\gamma^{-1}$ و بنابراین $\|\beta\| \geq \|\alpha\|$. به‌این ترتیب، اگر α و β هم‌پیوند باشند، آن‌وقت داریم: $\|\beta\| = \|\alpha\|$. اگر عکس این حکم هم درست باشد، یعنی اگر $\|\alpha\| < \|\beta\|$، وقتی α بر β بخش‌پذیر باشد، ولی خارج‌قسمت γ غیر از واحد باشد، آن‌وقت هنج‌نما (یا شبه‌نُرم) را اکید می‌گویند.

۵- در این کتاب نویسنده دو اصطلاح «عضو تجزیه‌ناپذیر» و «عضو اول» را معادل هم تعریف کرده‌است. در اکثر کتاب‌ها، این دو اصطلاح تعریف‌های مستقل از هم دارند. آن‌چه را در این‌جا تعریف شده معمولاً «عضو تجزیه‌ناپذیر» گویند و عضو $\alpha \in D$ را عضو اول گویند، اگر α صفر و یا عضو واحد نباشد و هرگاه α بخشیابی از $\beta\gamma$ باشد آن‌گاه α بخشیابی از β و یا بخشیابی از γ باشد. همان‌طور که در کتاب ثابت شده‌است، اگر در حلقه‌ای قضیه اصلی حساب برقرار باشد، آن‌گاه دو اصطلاح بالا معادل هم خواهند بود. (ویراستار).

مثال روشنی از هَنج‌نمای اکید، عبارت است از هَنج (یا نُرم) D_3.

گزارهٔ ۱. اگر در حلقهٔ D، هنج‌نمای اکید وجود داشته‌باشد، آن‌وقت هر عضو $\alpha \in D'$ را می‌توان به‌صورت ضربِ عضوهای اول تجزیه کرد، یعنی

$$\alpha = \pi_1 \pi_2 \dots \pi_k \qquad (۸)$$

که در آن، π_1، π_2، ...، π_k، عضوهای اول‌اند.

اثبات. مقدارهای شبه‌نُرم (یا هَنج‌نما) برای عضوهای $\alpha \in D'$ عددهای درست مثبت‌اند. بنابراین، بین آن‌ها کوچک‌ترین وجود دارد. p_0 را کوچک‌ترین مقدار می‌گیریم. روشن است، هر عضو $\alpha \in D'$ که برای آن داشته‌باشیم $\|\alpha\| = p_0$، عضوی اول است. بنابراین، تجزیهٔ (۸) برای آن برقرار است (که در آن $k = 1$ و $\pi_1 = \alpha$). اکنون فرض کنید $p > p_0$؛ درضمن فرض کنید، برای همهٔ عضوهای $\alpha \in D'$، به‌شرط $\|\alpha\| < p$، وجود تجزیهٔ (۸) ثابت شده‌باشد. عضو دلخواه $\alpha \in D'$ را درنظر می‌گیریم که برای آن داشته‌باشیم: $\|\alpha\| = p$. اگر α اول باشد، چیزی برای اثبات نمی‌ماند. $\alpha = \alpha_1 \alpha_2$ می‌گیریم که در آن α_1 و α_2 عضوهایی از D' هستند. در این‌صورت $\|\alpha_1\| < \|\alpha\| = p$ و $\|\alpha_2\| < \|\alpha\| = p$. بنابراین، برای عضوهای α_1 و α_2 تجزیهٔ (۸) وجود دارد، که از ضرب آن‌ها در یکدیگر، تجزیهٔ عضو α به‌دست می‌آید. به‌این ترتیب، گزارهٔ ۱، با استقرای ریاضی به‌طور کامل ثابت شد.

در حالت کلی، تجزیهٔ (۸) یگانه نیست. می‌توان ردیف عامل‌های اول را عوض کرد و به‌جای هرکدام یکی از عضوهای هم‌پیوندش را قرار داد. (البته به‌این‌ترتیب که حاصل‌ضرب همهٔ عامل‌های واحد اضافی، برابر ۱ باشد). دو تجزیهٔ

$$\alpha = \pi_1 \dots \pi_r, \ \alpha = \pi'_1 \dots \pi'_s$$

از عضو $\alpha \in D'$ به ضرب عامل‌های اول را «هم‌پیوند» گوییم، وقتی‌که $r = s$، و درضمن، بعد از هرگونه تجدید شماره‌گذاری ممکن، عضو π'_i (برای هر i از ۱ تا r) هم‌پیوند با هر عضو π_i باشد. اگر هر عضو

$\alpha \in D'$ به ضرب عامل‌های اول تجزیه شود و اگر هر دو تجزیه‌ای از این‌گونه «هم‌پیوند» باشند، می‌گویند: در حلقهٔ D قضیهٔ اصلی حساب برقرار است و یا، با اندکی عدم دقت، D حلقه‌ای است با تجزیهٔ یگانه به عامل‌ها (unique factoriation domain).

در چنین حلقه‌ای همهٔ مفهوم‌های اصلی نظریهٔ بخش‌پذیری در عددهای درست، برقرار است، و ویژگی‌های آن‌ها شبیه همان ویژگی‌هایی است که از حساب مقدماتی می‌دانیم.

ازجمله، شبیه آن‌چه دربارهٔ عددهای طبیعی داریم، عضوهای حلقهٔ D را وقتی نسبت به هم اول گوییم که عامل اول مشترکی نداشته‌باشند. دراین‌صورت، شبیه تجزیهٔ عددهای طبیعی (پیش‌قضیهٔ بخش ۲ را ببینید) ثابت می‌شود، اگر قضیهٔ اصلی حساب در حلقهٔ D برقرار باشد، آن‌وقت عددهای α و β هم، که نسبت به هم اول‌اند، به‌شرطی که حاصل‌ضرب آن‌ها توان nام یک عدد باشد، برابر توان nام خواهند بود.

عضو $\delta \in D^*$ را بزرگ‌ترین بخشیاب مشترک عضوهای α و β (از D^*) گویند، وقتی بخشیابی از این عضوها باشد و، درضمن، بر هر بخشیاب مشترک دیگری از α و β بخش‌پذیر باشد. روشن است، بزرگ‌ترین بخشیاب مشترک، با دقت تا هم‌پیوندی، یگانه است. ولی، در حالت کلی، این حکم ممکن است برای یک حلقهٔ دلخواه درست نباشد. اما در حلقه‌ای که تجزیهٔ عضوهای آن به عامل‌ها یگانه باشد، روشن است که بزرگ‌ترین بخشیاب مشترک برای هر دو عضو α و β وجود دارد. برای پیدا کردن بزرگ‌ترین بخشیاب مشترک دو عضو، باید هریک از آن‌ها را به ضرب عامل‌های اول تجزیه کرد و در هر دو تجزیه عامل‌های مشابه (هم‌پیوند) را درنظر گرفت. اگر چنین عامل‌هایی وجود نداشته‌باشد (یعنی عضوهای α و β نسبت به هم اول باشند)، آن‌وقت بزرگ‌ترین بخشیاب مشترک برابر است با ۱ (و یا هر واحد دلخواهی).

از قضیهٔ اصلی حساب، این گزاره هم بلافاصله نتیجه می‌شود:

(*) اگر عضو اول π بخشیابی از حاصل‌ضرب $\alpha\beta$ باشد، آن‌وقت بخشیابی از α و یا بخشیابی از β است.

عکس این گزاره هم درست است: اگر در حلقهٔ D هر عضو $\alpha \in D'$ به ضرب عامل‌های اول تجزیه شود (ازجمله، اگر در D، هَنج‌نمای اکید ـیا شبه نُرم اکیدـ وجود داشته‌باشد) و اگر D دارای ویژگی (*) باشد، آن‌وقت قضیهٔ اصلی حساب در D برقرار است.

در واقع، اگر داشته‌باشیم:

$$\pi_1 \dots \pi_r = \pi'_1 \dots \pi'_s$$

که در آن π_1، ...، π_r، π'_1، ...، π'_s عضوهایی اول‌اند، آن‌وقت π_1 بخشیابی از $\pi'_1 \dots \pi'_s$ است. بنابراین π_1 بخشیاب یکی از این عامل‌ها است (که نتیجه‌ای است از (*) به‌کمک استقرا). می‌توان π_1 را بخشیابی از π'_1 دانست، یعنی $\pi'_1 = \pi_1\varepsilon_1$ که در آن، چون π'_1 اول است، ε_1 عضو واحد است. اکنون اگر دوطرف برابری بالا را به π_1 ساده کنیم، به‌دست می‌آید:

$$\pi_2 \dots \pi_r = \varepsilon_1\pi'_2 \dots \pi'_s$$

به‌همین ترتیب، ثابت می‌شود، π_2 (بعد از شماره‌گذاری مناسب) بخشیابی از π'_2 و سپس (بعد از ساده کردن به π_2)، π_3 بخشیابی از π'_3 است و غیره. بعد از r گام معلوم می‌شود $r \le s$. ولی، اگر $r < s$، به‌این برابری می‌رسیم:

$$1 = \varepsilon_1 \dots \varepsilon_r\pi'_{r+1} \dots \pi'_s$$

از آن‌جاکه این برابری ممکن نیست (عضوهای π'_{r+1}، ...، π'_s بنابر شرط واحد نیستند)، بنابراین $r = s$ و برای هر $i = 1, \dots, r$، عضو π'_i با عضو π_i هم‌پیوند است.

می‌دانیم (و ما آن را ثابت خواهیم کرد)، در حلقهٔ عددهای درست، بزرگ‌ترین بخشیاب مشترک d را، برای هر دو عدد a و b، می‌توان به‌صورت

$$ax + by = d \qquad (۹)$$

نشان داد که در آن، x و y عددهایی درست‌اند (به‌زبان دیگر، معادلهٔ (۹) همیشه جواب درست دارد). این ویژگی را نمی‌توان برای هر حلقه‌ای، از قضیهٔ اصلی حساب نتیجه گرفت. بنابراین، باید خانوادهٔ دیگری از حلقه‌ها را وارد کرد.

حلقهٔ D را، «حلقهٔ با ایده‌آل‌های اصلی» (principal ideal domain) گویند (سرچشمهٔ این نام‌گذاری را در بخش ۱۲ خواهید دید)، به‌شرطی‌که برای هر دو عضو α و β از D^*:

الف) بزرگ‌ترین بخشیاب مشترک δ وجود داشته‌باشد؛

ب) بتوان عضوهای x و y از D را طوری پیدا کرد که داشته‌باشیم:

$$ax + by = \delta$$

به‌سادگی روشن می‌شود، هر حلقهٔ ایده‌آل‌های اصلی، ویژگی (*) را دارد.

در واقع، اگر π بخشیابی از α نباشد، آن‌وقت π و α نسبت به هم اول‌اند، بنابراین چنین عضوهای $x, y \in D$ وجود دارند که برای آن‌ها داشته‌باشیم. $\alpha x + \pi y = ۱$. اگر این برابری را در β ضرب کنیم، به‌دست می‌آید:

$$\beta = (\alpha\beta)x + \pi(y\beta) \ .$$

هر دو جملهٔ سمت راست برابری بر π بخش‌پذیر است. بنابراین π بخشیابی از عضو β است.

می‌گویند در حلقهٔ D با شبه‌نُرم، اَلگوریتم تقسیم با باقی‌مانده برقرار است (چنین حلقه‌ای را، حلقهٔ اقلیدسی (Euclidean domain) گویند)، وقتی

برای هر دو عضو α و β از D^*، عضوهایی مثل γ و ρ وجود داشته‌باشد که برای آن‌ها داشته‌باشیم: $\alpha = \beta\gamma + \rho$؛ درضمن یا $\rho = 0$ و یا $\|\rho\| < \|\beta\|$.

جالب است که در حلقهٔ اقلیدسی، شبه‌نُرم بی‌شک اکید است. در واقع، اگر $\alpha = \beta\gamma$ و $\|\beta\| = \|\alpha\|$، آن‌وقت از تقسیم (با باقی‌ماندهٔ) β بر α، برابریِ به‌صورت

$$\beta = \alpha\delta + \rho$$

به‌دست می‌آید که در آن $\delta \in D$، و یا $\|\rho\| < \|\alpha\|$. ولی $\rho = \beta(1-\gamma\delta)$ و بنابراین برای $\rho \neq 0$، نابرابری $\|\rho\| \geq \|\beta\| = \|\alpha\|$ برقرار است؛ درنتیجه $\rho = 0$ و $\beta = (\beta\gamma)\delta$، یعنی $\beta\gamma = 1$.

از طرف دیگر، هر حلقهٔ اقلیدسی، حلقهٔ با ایده‌آل‌های اصلی است (و بنابراین، دارای ویژگی (*) است). در واقع برای هر دو عضو α و β از D^*، در مجموعهٔ همهٔ عضوهای مخالف صفر و به‌صورت

$$\alpha x + \beta y, \quad x, y \in D \qquad (10)$$

عضوهایی با کم‌ترین شبه‌نُرم وجود دارند. $\delta = \alpha x_0 + \beta y_0$ را یکی از این عضوها می‌گیریم. اگر ثابت کنیم، δ بزرگ‌ترین بخشیاب مشترک α و β است، همه‌چیز ثابت خواهد شد. ولی روشن است که δ بر هر بخشیاب مشترک α و β بخش‌پذیر است. بنابراین تنها باید ثابت کرد δ بخشیابی از α و β است. ثابت می‌کنیم δ بخشیابی از α است (اثبات برای β، شبیه α انجام می‌شود).

$\alpha = \delta\gamma + \rho$ می‌گیریم که در آن $\rho = 0$ یا $\|\rho\| < \|\delta\|$. در این‌صورت

$$\rho = \alpha - \delta\gamma = \alpha - (\alpha x_0 + \beta y_0)\gamma = \alpha(1 - x_0\gamma) + \beta(-y_0\gamma)$$

به‌نحوی‌که ρ باز هم به‌صورت (۱۰) درمی‌آید. بنابراین، نابرابری $\|\rho\| < \|\delta\|$ ممکن نیست، یعنی $\rho = 0$.

با جمع‌بندی همهٔ آن‌چه گفتیم، به‌درستی این گزاره می‌رسیم.

گزارهٔ ۲. هر حلقهٔ اقلیدسی، حلقهٔ ایده‌آل‌های اصلی است که دربارهٔ آن، قضیهٔ اصلی حساب صدق می‌کند.

یادآوری می‌کنیم، حلقه‌هایی وجود دارند که برای آن‌ها قضیهٔ اصلی حساب برقرار است، ولی اَلگوریتم تقسیم با باقی‌مانده برای آن‌ها برقرار نیست. برای این‌گونه حلقه‌ها، ازجمله می‌توان حلقهٔ همهٔ عددهای به‌صورت

$$\frac{a+b\sqrt{-۱۹}}{۲}$$

را نام برد که در آن a و b عددهایی درست و یکی زوج و دیگری فرد باشد. ولی اثبات این مطلب، چندان ساده نیست.

همان‌طور که پیش از این هم گفتیم، برای این‌که پایهٔ استواری در اثبات **اویلر** داشته‌باشیم، کافی است ثابت کنیم، در حلقهٔ $D_۳$، قضیهٔ اصلی حساب برقرار است. باتوجه به گزارهٔ ۲، برای این منظور کافی است به اثبات درستی گزارهٔ ۳، که در این‌جا می‌آوریم، بپردازیم.

گزارهٔ ۳. نسبت به نُرم حلقهٔ $D_۳$، الگوریتم تقسیم با باقی‌مانده برقرار است.

اثبات. باید ثابت کنیم، برای عضوهای دلخواه α و $\beta \neq ۰$ از حلقهٔ $D_۳$، چنان عضوهای γ و ρ وجود دارد که داشته‌باشیم:

$$\alpha = \beta\gamma + \rho \quad و \quad N\rho < N\beta$$

پیش‌قضیه. برای هر عدد $\xi \in K_۳$، عدد $\gamma \in D_۳$ وجود دارد که

$$N(\xi - \gamma) \leq \frac{۳}{۴}$$

گزارهٔ ۳، نتیجهٔ مستقیمی است از این پیش‌قضیه. در واقع، اگر پیش‌قضیه را برای عدد $\xi = \frac{\alpha}{\beta}$ به‌کار بریم و فرض کنیم $\rho = \alpha - \beta\gamma$، بلافاصله

به‌دست می‌آید $\alpha = \beta\gamma + \rho$ و

$$N\rho = N(\alpha - \beta\gamma) = N\beta \cdot N(\xi - \gamma) \leq \frac{3}{4} N\beta < N\beta$$

به‌این ترتیب، تنها باید پیش‌قضیه را ثابت کنیم.

اثبات پیش‌قضیه. فرض کنید

$$\xi = A + B\zeta$$

و فرض کنید a و b عددهای درستی باشند که برای آن‌ها داشته‌باشیم:

$$|A - a| \leq \frac{1}{2},\ |B - b| \leq \frac{1}{2}$$

در این‌صورت برای عدد

$$\gamma = a + b\zeta \in D_{-3}$$

به‌دست می‌آید:

$$\begin{aligned} N(\xi - \gamma) &= (A-a)^2 - (A-a)(B-b) + (B-b)^2 \leq \\ &\leq |A-a|^2 + |A-a| \cdot |B-b| + |B-b|^2 \leq \\ &\leq \left(\frac{1}{2}\right)^2 + \frac{1}{2} \cdot \frac{1}{2} + \left(\frac{1}{2}\right)^2 = \frac{3}{4} \end{aligned}$$

نتیجه. برای حلقهٔ D_{-3}، قضیهٔ اصلی حساب برقرار است.

وجود دو تجزیهٔ

$$4 = 2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

با این نتیجه متناقض نیست، زیرا در D_{-3} عددهای ۲ و $1 + \sqrt{-3}$ هم‌پیوندند (عدد $\frac{1 + \sqrt{-3}}{2}$ به D_{-3} تعلق دارد و در D_{-3} واحد است).

اکنون برای کامل کردن اثبات اویلر، تنها این می‌ماند که وجود دو رخنهٔ کوچک موجود در آن را پر کنیم.

اول، باید ثابت کرد، برای عددهای درست a و b که نسبت به‌هم اول‌اند، عضوهای $a+b\sqrt{-۳}$ و $a-b\sqrt{-۳}$ از حلقهٔ $D_۳$ هم، نسبت به‌هم اول‌اند. این اثبات بسیار ساده است. در واقع، اگر این عضوها بر عضو $r\in D_۳$ بخش‌پذیر باشند، آن‌وقت باید عضوهای

$$۲a=(a+b\sqrt{-۳})+(a-b\sqrt{-۳}),$$
$$۲b\sqrt{-۳}=(a+b\sqrt{-۳})-(a-b\sqrt{-۳})$$

هم بر γ بخش‌پذیر باشند. اگر به نُرم‌ها مراجعه کنیم، معلوم می‌شود $N\gamma$ بخشیابی از عددهای $N(۲a)=۴a^۲$ و $N\gamma=۱۲b^۲$ است. چون عددهای a و b، بنابر شرط، نسبت به هم اول‌اند، نتیجه می‌گیریم، عدد درست و مثبت $N\gamma$ بخشیابی از عدد ۴ است.

اگر $N\gamma=۴$، آن‌وقت $N\left(\frac{\gamma}{۲}\right)=۱$، یعنی $\gamma=۲\varepsilon$، که در آن، ε واحد است. به‌این ترتیب در این حالت، بادقت هم‌پیوندی، جواب منحصرِ $\gamma=۲$ به‌دست می‌آید. ولی این جواب به درد ما نمی‌خورد، زیرا عدد $a+b\sqrt{-۳}$، وقتی و تنها وقتی در $D_۳$ بر ۲ بخش‌پذیر است که هر دو عدد a و b بر ۲ بخش‌پذیر باشند.

حالت $N\gamma=۲$ به‌طور کلی ممکن نیست، زیرا معادلهٔ

$$x^۲-xy+y^۲=۲$$

در مجموعهٔ عددهای درست جواب ندارد.

به‌این ترتیب، به‌ناچار $N\gamma=۱$، یعنی γ واحد است. بنابراین عضوهای $a+b\sqrt{-۳}$ و $a-b\sqrt{-۳}$ نسبت به هم اول‌اند.

رخنهٔ دوم، که برای اویلر وجود نداشت، ولی وقتی دربارهٔ حلقهٔ $D_۳$ صحبت می‌کردیم، از این‌جا ناشی می‌شد که در برابری

$$a+b\sqrt{-۳}=(s+t\sqrt{-۳})^۳ \qquad (۱۱)$$

ممکن است عددهای s و t، در حالت کلی، عددهایی درست نباشند، زیرا، همان‌طور که می‌دانیم، عددهای D_{-3} به‌این صورت‌اند:

$$\frac{p+q\sqrt{-3}}{2} \qquad (12)$$

که در آن p و q عددهای درست و هردو فرد یا هردو زوج‌اند.

برای این‌که این دشواری را برطرف کنیم، توجه می‌کنیم، اگر عدد (۱۲) را به‌صورت $A+B\zeta$ بنویسیم، به این برابری‌ها می‌رسیم:

$$p=2A-B, \quad q=B$$

بنابراین، عددهای p و q، وقتی و تنها وقتی زوج‌اند (یعنی عدد (۱۲) به‌صورتی که لازم داریم، به‌صورت $s+t\sqrt{-3}$ با عددهای درست s و t درمی‌آید)، که عدد B زوج باشد. ولی دستورهای

$$(A+B\zeta)\zeta=-B+(A-B)\zeta,\ (A+B\zeta)\zeta^2=(B-A)-A\zeta$$

نشان می‌دهند، دست‌کم در یکی از سه عدد هم‌پیوند $A+B\zeta$، $(A+B\zeta)\zeta$، $(A+B\zeta)\zeta^2$، ضریب ζ زوج است. بنابراین، اگر در برابری (۱۱)، عدد $s+t\sqrt{-3}$ را در ζ یا در ζ^2 ضرب کنیم (که البته، برابری را به‌هم نمی‌زند)، همیشه می‌توانیم برای s و t به عددهای درستی برسیم.

به‌این ترتیب، پیش‌قضیهٔ اویلر به‌طور کامل ثابت می‌شود که، در واقع، قضیهٔ فرما را برای نمای ۳ هم ثابت می‌کند.

ضمیمه. دربارهٔ حساب چندجمله‌ای‌ها

K را میدانی دلخواه و $K[x]$ را حلقهٔ چندجمله‌ای‌های با یک متغیر روی میدان K می‌گیریم (یعنی $K[x]$ شامل چندجمله‌ای‌های با ضرب‌هایی از K است). از جبر مقدماتی می‌دانیم، برای چندجمله‌ای‌ها، الگوریتم

تقسیم با باقی‌مانده وجود دارد[۶]. بنابراین، قضیهٔ اصلی حساب، دربارهٔ حلقهٔ $K[x]$ صادق است. درضمن روشن است، واحدها در حلقهٔ $K[x]$، تنها چندجمله‌ای‌های از درجهٔ صفرند، یعنی عضوهای غیرصفر میدان K.

عضوهای اول حلقهٔ $K[x]$ به‌صورتی که معمول است، به چندجمله‌ای‌های تجزیه‌ناپذیر گفته می‌شود. بنابراین می‌توان گفت، هر چندجمله‌ای، با دقت تا ضریب‌های ثابت، به ضرب چندجمله‌ای‌های تجزیه‌ناپذیر قابل‌تجزیه است.

به‌جز این، باتوجه به این‌که $K[x]$ یک حلقهٔ اقلیدسی است، حلقهٔ ایده‌آل‌های اصلی هم خواهد بود. بنابراین، برای هر دو چندجمله‌ای $f(x)$ و $g(x)$ که نسبت به هم اول باشند، چندجمله‌ای‌های $u(x)$ و $v(x)$ وجود دارند، به‌نحوی که داشته‌باشیم:

$$f(x)u(x) + g(x)v(x) = ۱$$

درنتیجه، به‌ازای هیچ مقداری از x، چندجمله‌ای‌های $f(x)$ و $g(x)$، نمی‌توانند با هم برابر صفر باشند. از این‌جا ثابت می‌شود، چندجمله‌ای‌هایی که ریشهٔ مشترک دارند، نسبت به هم اول نیستند.

از آن‌جاکه چندجمله‌ای تجزیه‌ناپذیر، نسبت به هر چندجمله‌ای با درجهٔ پایین‌تر، اول است، می‌توان نتیجه گرفت که، هیچ ریشه‌ای از چندجمله‌ای تجزیه‌ناپذیر، نمی‌تواند ریشه‌ای از چندجمله‌ای با درجهٔ پایین‌تر باشد.

۶- برای وجود الگوریتم تقسیم با باقی‌مانده در حلقه $K[x]$، کافی است که K یک میدان باشد. برای مثال حلقه $Z[x]$ دارای الگوریتم تقسیم با باقی‌مانده نیست (ویراستار).

۶

میدان K_l و حلقهٔ D_l

تنها روش کلیِ اثبات قضیهٔ فرما که تاکنون برای عددهای اول $l \geq ۳$ شناخته‌شده، روش کومر است که براساس تکامل و تعمیم روش اویلر شکل گرفته‌است (که البته، هنوز کار به‌پایان نرسیده‌است، زیرا از این روش نمی‌توان برای همهٔ مقدارهای اول l استفاده کرد). در این روش، نقش اساسی به‌عهدهٔ میدانی به‌نام میدان K_l است که با میدان $K_۳$ شباهت دارد. به‌همین جهت، کار را از آشنایی با این میدان آغاز می‌کنیم.

این چندجمله‌ای را درنظر می‌گیریم:

$$x^l - ۱ \qquad (۱)$$

و یا بهتر از آن، این چندجمله‌ای را:

$$\varphi(x) = x^{l-۱} + x^{l-۲} + \ldots + x + ۱ \qquad (۲)$$

که از تقسیم چندجمله‌ای (۱) بر $x - ۱$ به‌دست می‌آید. ریشه‌های چندجمله‌ای (۱)، با این دستور بیان می‌شوند:

$$\cos \frac{۲k\pi}{l} + i \sin \frac{۲k\pi}{l} \qquad (۳)$$

که در آن، k یکی از عددهای ۰، ۱، ...، $l - ۱$ است. این ریشه‌ها، روی صفحهٔ عددهای مختلط، مُعرف راس‌های lضلعی منتظم محاط در دایرهٔ واحد است. بر همین اساس است که چندجمله‌ای (۱)، همچنین چندجمله‌ای (۲) را، چندجمله‌ای دایره‌بُر (cyclotomic) lام گویند.

حقیقتی که عبور از چندجمله‌ای (۱) به چندجمله‌ای (۲) را توجیه می‌کند، این است که چندجمله‌ای (۲) (در میدان عددهای گویای $\mathbf{Q}$) تجزیه‌ناپذیر است. اثبات این گزاره را در چند مرحله می‌آوریم.

۱. کافی است، برای اثبات ساده نشدن چندجمله‌ای (۲)، ثابت کنیم چندجمله‌ای

$$p(y) = \frac{(y+۱)^l - ۱}{y} =$$

$$= y^{l-1} + \binom{l}{1} y^{l-2} + \ldots + \binom{l}{l-2} y + \binom{l}{l-1}$$

که از چندجمله‌ای (۲) و با تبدیل x به $y+1$ به‌دست می‌آید، ساده‌نشدنی است.

۲. همان‌طور که یادآوری کرده‌بودیم، همهٔ ضریب‌های بسط دوجمله‌ای

$$\binom{l}{k} = \frac{l!}{k!(l-k)!},\ k = 1, \ldots, l-1 \qquad (۴)$$

بر l بخش‌پذیرند.

۳. فرض می‌کنیم، چندجمله‌ای $p(y)$ تجزیه‌پذیر باشد، یعنی بتوان چندجمله‌ای‌های $a(y)$ و $b(y)$ را پیدا کرد که ضریب‌هایی گویا و توان‌هایی مثبت داشته‌باشند (یعنی عضوهای واحدی از حلقهٔ $\mathbf{Q}[y]$ نباشند)، به‌نحوی‌که داشته‌باشیم:

$$p(y) = a(y) \cdot b(y)$$

در حالت کلی، چندجمله‌ای‌های $a(y)$ و $b(y)$ با تقریب ضریب‌های عددی معین‌اند، یعنی هریک از آن‌ها را می‌توان در عدد گویایی مخالف صفر ضرب و دیگری را بر همان عدد تقسیم کرد. باتوجه به این نکته، می‌توان ترتیبی داد که همهٔ ضریب‌های یکی از چندجمله‌ای‌ها، و در مثل چندجمله‌ای $a(y)$، عددهایی درست و (درمجموع) نسبت به هم اول[۷] و درضمن ضریب جملهٔ با درجهٔ بزرگ‌تر مثبت باشد. پس، برای هر $a(y)$ که به‌این ترتیب معین شود، تنها یک چندجمله‌ای $b(y)$ به‌دست می‌آید.

۴. اگر ضریب‌های چندجمله‌ای $b(y)$ را به یک مخرج تبدیل کنیم، می‌توانیم این چندجمله‌ای را به‌صورت

$$b(y) = \frac{b_0}{N} y^s + \frac{b_1}{N} y^{s-1} + \ldots + \frac{b_s}{N}$$

۷- عددهای درست a_0، a_1، ...، a_k نسبت به هم اول‌اند (درمجموع) اگر به‌جز ± 1 عدد درست دیگری بخشیاب همهٔ آن‌ها نباشد (ویراستار).

بنویسیم که در آن، b_0، b_1، ...، b_s و $N > 0$ عددهایی درست‌اند، درضمن هیچ بخشیاب اولی از عدد N، بخشیابی از همهٔ عددهای b_0، ...، b_s نیست. بنابر شرط داریم:

$$a(y) = a_0 y^r + a_1 y^{r-1} + \ldots + a_r$$

که در آن a_0، a_1، ...، a_r نسبت به هم اول‌اند (درمجموع) و درضمن $r = l - 1 - s$ بنابراین، برای ضریب‌های $\binom{l}{k}$ از چندجمله‌ای $p(y)$، این برابری‌ها برقرارند:

$$\begin{aligned}
&\binom{l}{0} = 1 = \frac{a_0 b_0}{N},\\
&\binom{l}{1} = l = \frac{a_0 b_1 + a_1 b_0}{N},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
&\binom{l}{k} = \frac{a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0}{N}\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
&\binom{l}{l-1} = l = \frac{a_r b_s}{N}
\end{aligned} \qquad (۵)$$

(در واقع، برای $i > r$، مقدار a_i را و برای $j > s$ مقدار b_j را برابر صفر گرفته‌ایم). این، به‌ویژه به‌این معناست که همهٔ عددهای

$$a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0, \quad (k = 0, 1, \ldots, l-1) \qquad (۶)$$

بر N بخش‌پذیرند.

۵. با فرض $N > 1$، بخشیاب اول دلخواه p از عدد N را درنظر می‌گیریم. از آن‌جاکه، بنابر شرط، ضریب‌های a_0، ...، a_r نسبت به هم اول‌اند، بین آن‌ها ضریب‌هایی وجود دارند که بر p بخش‌پذیر نیستند.

فرض کنید a_{i_0}، نخستین عدد از این‌گونه باشد (به‌نحوی‌که یا $i_0 = 0$ و یا همهٔ ضریب‌های a_0، ...، a_{i_0-1} بر p بخش‌پذیر باشند). به‌همین ترتیب، چون p بخشیابی از همهٔ ضریب‌های b_0، ...، b_s نیست، بنابراین ضریب b_{j_0} وجود دارد که بر p بخش‌پذیر نیست و درضمن، برای $j_0 \geq 1$، همهٔ ضریب‌های b_0، ...، b_{j_0-1} بر p بخش‌پذیرند.

اکنون عدد (۶) را به‌ازای $k = i_0 + j_0$ درنظر می‌گیریم. این عدد شامل جملهٔ $a_{i_0}b_{j_0}$ است که بر p بخش‌پذیر نیست. همهٔ جمله‌های دیگر به‌صورت a_ib_j که، برای آن‌ها، $i < i_0$ یا $j < j_0$، به‌روشنی بر p بخش‌پذیرند. بنابراین، عددی کـــه درنظـر گرفته‌ایم، بر p، و بنابراین، بر N بخش‌پذیر نیست.

چون این نتیجه، با نتیجه‌گیری مرحلهٔ ۴ متناقض است، ثابت می‌شود که $N = 1$، یعنی همهٔ ضریب‌های چندجمله‌ای $b(y)$ (باتوجه به شرطی که برای چندجمله‌ای $a(y)$ داشتیم)، در مجموعهٔ عددهای درست نسبت به هم اول‌اند.

به‌ویژه، عددهای (۶)، ضریب‌های $\binom{l}{k}$ از چندجمله‌ای $p(y)$ هستند.

۶. از آن‌جاکه همهٔ ضریب‌های چندجمله‌ای $a(y)$ (و بنابر آن‌چه ثابت کردیم، ضریب‌های چندجمله‌ای $b(y)$) عددهایی درست و نسبت به هم اول‌اند، بنابراین بین آن‌ها، ضریب‌هایی پیدا می‌شود که بر عدد اول l بخش‌پذیر نباشند. فرض کنید a_{i_0}، ضریب چندجمله‌ای $a(y)$ دارای این دو ویژگی باشد و درضمن i_0 بزرگ‌ترین اندیس در بین ضریب‌ها باشد؛ به‌همین ترتیب، ضریب مشابه را در چندجمله‌ای $b(y)$، b_{j_0} می‌گیریم.

چون $a_rb_s = l$، بنابراین یا $i_0 < r$ و یا $j_0 < s$. برای مشخص بودن وضع، فرض می‌کنیم $i_0 < r$، به‌نحوی‌که $a_r = \pm l$ و $b_s = \pm 1$. در این‌صورت، عدد $\binom{l}{i_0+s}$ ضریب چندجمله‌ای $p(y)$ است، یعنی

برای آن داریم:

$$\binom{l}{i_\circ + s} = a_{i_\circ} b_s + a_{i_\circ+1} b_{s-1} + \ldots + a_r b_{s-(r-i_\circ)}$$

ولی همهٔ جمله‌های این دستور، به‌جز نخستین عدد $a_{i_\circ} b_s = \pm a_{i_\circ}$، بر l بخش‌پذیرند (زیرا عددهای $a_{i_\circ+1}$، ...، a_r بر l بخش‌پذیرند) و جملهٔ $a_{i_\circ} b_s$ بر l بخش‌پذیر نیست که در واقع، مرحلهٔ ۲ را نقض می‌کند.

به‌این ترتیب، وقتی فرض کنیم $p(y)$ حاصل‌ضرب دو چندجمله‌ای است، به تناقض برمی‌خوریم؛ یعنی این چندجمله‌ای تجزیه‌پذیر نیست.

یادآوری می‌کنیم در این‌جا، در واقع، دو قضیهٔ کلی را ثابت کردیم: قضیهٔ اول می‌گوید، هر چندجمله‌ای با ضریب‌های درست که روی $\mathbf{Q}$ تجزیه‌پذیر باشد، به عامل‌هایی با ضریب‌های درست تجزیه می‌شود (این قضیه، به‌نام پیش‌قضیهٔ گاوس مشهور است)؛ قضیهٔ دوم حکم می‌کند، چندجمله‌ای با ضریب‌های درست روی $\mathbf{Q}$ تجزیه‌پذیر نیست، به‌شرطی‌که ضریب بزرگ‌تر بر عدد اولی مثل l بخش‌پذیر نباشد و بقیهٔ ضریب‌ها بر l بخش‌پذیر باشند، ولی جملهٔ ثابت آن بر l^2 بخش‌پذیر نباشد (معیار اَیزِنْشتین).

اکنون ζ را ریشهٔ دلخواه ولی معینی از چندجمله‌ای (۲) می‌گیریم. برای مشخص بودن وضع می‌توان فرض کرد:

$$\zeta = \cos\frac{2\pi}{l} + i\sin\frac{2\pi}{l}$$

ولی این انتخاب در واقع اهمیتی ندارد (برای عدد اول l) و از این به بعد کاربردی پیدا نمی‌کند.

به‌جز این، به عبارت‌های (۳) هم، که مُعرف ریشه‌های چندجمله‌ای‌های (۱) و (۲) است، نیازی نداریم. کافی است بدانیم، ζ عدد مختلطی است

که در رابطهٔ

$$\zeta^{l-1} = -1 - \zeta - \ldots - \zeta^{l-2} \qquad (7)$$

صدق می‌کند؛ قبول این رابطه هم‌ارز آن است که ζ را ریشهٔ چندجمله‌ای (۲) بدانیم. تنها از همین ویژگی آن استفاده خواهیم‌کرد.

شبیه حالت $l = 3$، در این‌جا هم، مجموعهٔ همهٔ عددهای به‌صورت

$$\alpha = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2} \qquad (8)$$

که در آن a_0، a_1، ...، a_{l-2}، عددهای گویای دلخواهی‌اند، K_l می‌نامیم.

به‌سادگی دیده می‌شود که نمایش هر عدد $\alpha \in K_l$ به‌صورت (۸) یگانه است، یعنی هر عضو K_l را تنها به یک طریق می‌توان به‌صورت (۸) نشان داد. در واقع، اگر چنین نباشد، آن‌وقت باید داشته‌باشیم:

$$a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2} = 0$$

که در آن، همهٔ عددهای a_0، a_1، ...، a_{l-2} مخالف صفر نیستند. به‌زبان دیگر، عدد ζ ریشهٔ یک چندجمله‌ایِ با ضریب‌های گویا و از درجه‌ای کمتر از $(l-1)$ است، که ممکن نیست، زیرا چندجمله‌ای (۲) تجزیه‌ناپذیر بود.

چون بنابر (۷) داریم:

$$1 = -\zeta - \zeta^2 - \ldots - \zeta^{l-1}$$

بنابراین هر عضو $\alpha \in K_l$ می‌تواند (تنها به یک صورت)، این‌طور نمایش داده شود:

$$\alpha = b_1\zeta + b_2\zeta^2 + \ldots + b_{l-1}\zeta^{l-1}$$

که در آن b_1، b_2، ...، b_{l-1} عددهایی گویا هستند (و عددهایی درست‌اند، به‌شرطی‌که عددهای a_1، ...، a_{l-2} درست باشند).

این نکته، گاهی سودمند است.

روشن است، مجموع دو عددِ به‌صورت (۸)، باز هم عددی به‌صورت (۸) است. همین مطلب دربارهٔ ضرب دو عدد هم درست است، زیرا نماهایی را که در نتیجهٔ ضرب، بزرگ‌تر از $(l-۲)$ برای ζ به‌دست می‌آید، می‌توان به‌یاری (۷) برحسب توان‌های کوچک‌تر نوشت. و این، به‌معنای آن است که K_l، یک حلقه است. ولی در واقع، K_l را یک میدان هم می‌توان دانست، زیرا از تقسیم دو عدد به‌صورت (۸)، باز هم عددی به‌همان صورت به‌دست می‌آید.

در واقع، برابری (۸) به‌این معنی است که عدد $\alpha \in K_l$، عبارت است از مقدار $f(\zeta)$ به‌ازای $x = \zeta$ از چندجمله‌ایِ

$$f(x) = a_۰ + a_۱x + \ldots + a_{l-۲}x^{l-۲}$$

(که به‌ازای $\alpha \neq ۰$، مخالف صفر است). از آن‌جاکه درجهٔ این چندجمله‌ای کمتر از $(l-۱)$، یعنی کمتر از درجهٔ چندجمله‌ای دایره بُری $\varphi(x)$ است. درضمن، چندجمله‌ای $\varphi(x)$ تجزیه‌ناپذیر است، بنابراین چندجمله‌ای‌های $f(x)$ و $\varphi(x)$ نسبت به هم اول‌اند. درنتیجه، چندجمله‌ای‌های $u(x)$ و $v(x)$ وجود دارند، به‌نحوی‌که

$$f(x)u(x) + \varphi(x)v(x) = ۱$$

اگر در این‌جا فرض کنیم $x = \zeta$ و درنظر بگیریم $\varphi(\zeta) = ۰$، به‌دست می‌آید:

$$f(\zeta)u(\zeta) = ۱$$

یعنی

$$\frac{۱}{\alpha} = u(\zeta) \in K_l$$

به‌این ترتیب، در حلقهٔ K_l، هر عضو $\alpha \neq ۰$، وارون‌پذیر است؛ یعنی K_l یک میدان است.

به این نکته توجه کنیم، همین حقیقت را برای $l = ۳$ (که K_l یک میدان است)، بر پایه‌های دیگری ثابت کردیم. برای این‌که از این پایه‌ها برای هر l استفاده کنیم، باید به برخی ملاحظه‌های مقدماتی توجه کنیم.

ریشهٔ ζ، تنها یکی از $(l-۱)$ ریشهٔ

$$\zeta^{(۱)} = \zeta, \zeta^{(۲)}, \zeta^{(۳)}, \ldots, \zeta^{(l-۱)} \qquad (۹)$$

از چندجمله‌ای (۲) است. معلوم می‌شود، همهٔ این ریشه‌ها را می‌توان خیلی ساده برحسب ریشهٔ ζ بیان کرد.

روشن است، همراه با ζ از معادلهٔ $x^l = ۱$، همهٔ عددهای به‌صورت ζ^k هم صدق می‌کنند که در آن k عدد درست دلخواهی است؛ درضمن، $\zeta^{k_۱} = \zeta^{k_۲}$ وقتی، و تنها وقتی که داشته‌باشیم:

$$k_۱ \equiv k_۲ (\mathrm{mod} l)$$

و این ثابت می‌کند، برای شماره‌گذاری‌های ریشه‌های (۹)، می‌توان نوشت:

$$\zeta^{(۱)} = \zeta,\ \zeta^{(۲)} = \zeta^۲,\ \zeta^{(۳)} = \zeta^۳, \ldots,\ \zeta^{(l-۱)} = \zeta^{l-۱} \qquad (۱۰)$$

به‌ویژه می‌بینیم، همهٔ ریشه‌های (۹)، به میدان K_l تعلق دارند.

بنابراین، اگر در عبارت (۸)، به‌جای $\zeta = \zeta^{(۱)}$، ریشهٔ دلخواه $\zeta^{(k)}$ را قرار دهیم (برای $k = ۱, ۲, \ldots, l-۱$)، باز هم عددی از میدان K_l به‌دست می‌آید. این عدد را با نماد $\alpha^{(k)}$ نشان می‌دهیم. به‌این ترتیب، بنابر تعریف

$$\alpha^{(k)} = a_۰ + a_۱\zeta^{(k)} + a_۲(\zeta^{(k)})^۲ + \ldots + a_{l-۲}(\zeta^{(k)})^{l-۲} =$$
$$= a_۰ + a_۱\zeta^k + a_۲\zeta^{۲k} + \ldots + a_{l-۲}\zeta^{(l-۲)k}$$

اکنون، این حاصل‌ضرب را درنظر می‌گیریم:

$$N\alpha = \alpha^{(۱)}\alpha^{(۲)} \ldots \alpha^{(l-۱)}$$

این حاصل‌ضرب، یک چندجمله‌ای نسبت به $\zeta^{(1)}$، ...، $\zeta^{(l-1)}$ است که ضریب‌های آن عبارت‌اند از a_0، a_1، ...، a_{l-2} با ضریب‌هایی درست. هر جایگشتی از عددهای $\zeta^{(1)}$، ...، $\zeta^{(l-1)}$، همان جایگشت را از عددهای $\alpha^{(1)}$، ...، $\alpha^{(l-1)}$ به‌همراه دارد و بنابراین $N\alpha$ را تغییر نمی‌دهد. و این، به‌معنای آن است که $N\alpha$ یک چندجمله‌ای متقارن نسبت به $\zeta^{(1)}$، ...، $\zeta^{(l-1)}$ است. ولی می‌دانیم (برای نمونه، کتاب «تقارن در جبر» ترجمهٔ پرویز شهریاری را ببینید)، هر چندجمله‌ای متقارن F، یک چندجمله‌ای به‌صورت $G(\sigma_1, \ldots, \sigma_{l-1})$ است، از چندجمله‌ای‌های متقارن مقدماتی σ_1، ...، σ_{l-1}؛ درضمن، ضریب‌های چندجمله‌ای G برحسب ضریب‌های چندجمله‌ای F، با عمل‌های جمع، تفریق و ضرب بیان می‌شوند، یعنی در حالت ما (برای $F = N\alpha$) مثل قبل عبارت‌اند از چندجمله‌ای‌هایی از a_0، a_1، ...، a_{l-2} با ضریب‌های درست. این چندجمله‌ای‌های متقارن مقدماتی به‌این صورت‌اند.

$$\begin{aligned}
\sigma_1 &= \zeta^{(1)} + \zeta^{(2)} + \ldots + \zeta^{(l-1)},\\
\sigma_2 &= \zeta^{(1)}\zeta^{(2)} + \ldots + \zeta^{(l-2)}\zeta^{(l-1)},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
\sigma_{l-1} &= \zeta^{(1)}\zeta^{(2)}\ldots\zeta^{(l-1)}
\end{aligned}$$

که باتوجه به دستورهای ویت در چندجمله‌ای (۲)، برابرند با $(-1)^k$. و این ثابت می‌کند، عدد

$$N\alpha = G(-1, 1, \ldots)$$

یک چندجمله‌ای از a_0، a_1، ...، a_{l-2} با ضریب‌های درست است، یعنی عددی گویا است (وقتی عددی درست است که a_0، a_1، ...، a_{l-2}، همگی عددهای درست باشند).

استدلالی که در این‌جا آوردیم، خصلتی عام دارد و می‌تواند به‌همین ترتیب، نه‌تنها دربارهٔ $N\alpha$، که دربارهٔ هر چندجمله‌ای متقارن نسبت به $\alpha^{(1)}$، ...، $\alpha^{(l-1)}$ که ضریب‌های درستی داشته‌باشد، به‌کار رود؛ ازجمله دربارهٔ ضریب‌های چندجمله‌ای

$$(x-\alpha^{(1)})\dots(x-\alpha^{(l-1)})$$

به‌این ترتیب، به‌ویژه می‌بینیم، برای هر عضو

$$\alpha = a_0 + a_1\zeta + \dots + a_{l-2}\zeta^{l-2} \in K_l$$

ضریب‌های چندجمله‌ای $(x-\alpha^{(1)})\dots(x-\alpha^{(l-1)})$ عددهایی گویا هستند (و درست‌اند وقتی‌که همهٔ عددهای a_0، a_1، ...، a_{l-2} درست باشند).

عدد گویای $N\alpha$ را نُرمِ عضو $\alpha \in K_l$ گویند، که دارای این ویژگی‌ها است:

۱) $N\alpha \geq 0$؛ درضمن وقتی و تنها وقتی $N\alpha = 0$ که $\alpha = 0$؛

۲) برای هر دو عدد α و β که عضو K_l باشند، این برابری برقرار است.

$$N(\alpha\beta) = N\alpha \cdot N\beta \qquad (11)$$

۳) اگر $\alpha \in K_l$ عددی گویا باشد (یعنی $a_1 = \dots = a_{l-2} = 0$ و بنابراین $\alpha = a_0$)، آن‌وقت

$$N\alpha = a_0^{l-1}$$

این ویژگی‌ها روشن‌اند (با حالت $l = 3$ مقایسه کنید)، به‌احتمالی به‌جز ویژگی $N\alpha \geq 0$ که برای اثبات آن، باید به‌یاد آورد، عددهای

(۹) (ریشه‌های موهومی معادله‌ای با ضریب‌های حقیقی)، عددهای مختلطی دوبه‌دو مزدوج‌اند (برای نمونه، می‌توان به‌حساب آورد: $\zeta^{(l-k)} = \overline{\zeta}^{(k)}$؛ دستور (۱۰) را ببینید). بنابراین، عددهای $\alpha^{(1)}$، ...، $\alpha^{(l-1)}$ هم، عددهایی مختلط و دوبه‌دو مزدوج‌اند (برای مثل $\alpha^{(l-k)} = \overline{\alpha}^{(k)}$)، یعنی $N\alpha \geq 0$؛ درواقع، با توجه به شماره‌گذاری ریشه‌ها داریم:

$$N\alpha = |\alpha_1|^2 \dots |\alpha_s|^2,\ s = \frac{l-1}{2}$$

به‌یاری نُرم، اثبات میدان بودن K_l، مثل حالت $l = 3$، منجر به برآورد سادهٔ زیر می‌شود:

$$\frac{\beta}{\alpha} = \frac{\beta\alpha^{(2)}\alpha^{(3)} \dots \alpha^{(l-1)}}{\alpha^{(1)}\alpha^{(2)} \dots \alpha^{(l-1)}} = \frac{\beta\alpha^{(2)}\alpha^{(3)} \dots \alpha^{(l-1)}}{N\alpha} \in K_l$$

عدد (۸) از میدان K_l را درست گویند، وقتی همهٔ ضریب‌های a_0، a_1، ...، a_{l-2} عددهای گویای درست باشند (متعلق به حلقهٔ Z). همان‌طور که دیدیم، نُرم $N\alpha$ از عدد درست α، عددی گویا و درست (و نامنفی) است. روشن است که، همهٔ عددهای درست K_l، تشکیل حلقه می‌دهند. این حلقه را با نماد D_l نشان می‌دهیم.

مثل حالت $l = 3$، در این‌جا هم عدد $\alpha \in D_l$ وقتی، و تنها وقتی، واحد حلقهٔ D_l است که داشته‌باشیم: $N\alpha = 1$.

در واقع، اگر $\alpha\alpha^{-1} = 1$، آن‌وقت $N\alpha \cdot N\alpha^{-1} = 1$ و بنابراین $N\alpha = 1$. برعکس، اگر داشته‌باشیم $N\alpha = 1$، آن‌وقت $\alpha\alpha^{-1} = 1$ که در آن $\alpha^{-1} = \alpha^{(2)} \dots \alpha^{(l-1)}$.

از این‌جا (و از (۱۱)) نتیجه می‌شود، تابع $\alpha \to N\alpha$ (روی D_l^*) نُرم‌نما (یا شبه‌نُرم) اکید است. بنابراین (بخش ۵، گزارهٔ ۱ را ببینید) در حلقهٔ D_l، هر عضو غیرواحد، به ضرب عضوهای اول تجزیه می‌شود.

با وجود این، با نمونه‌هایی می‌توان ثابت کرد، حلقهٔ D_l همیشه حلقه‌ای با تجزیهٔ یگانه به عامل‌ها نیست. ازجمله، می‌توان ثابت کرد، حلقهٔ $D_{۲۳}$، حلقه‌ای نیست که تنها به یک طریق به ضرب عامل‌ها تجزیه شود، درحالی‌که در حلقه‌های D_l، برای $l < ۲۳$، تجزیهٔ به عامل‌ها، یگانه است.

مساله. حلقهٔ $D_۵$ را بررسی کنید. واحدهای آن را به‌دست آورید. ثابت کنید، $D_۵$ حلقه‌ای اقلیدسی است و بنابراین هر عضو آن به یک صورت به ضرب عامل‌های تجزیه‌ناپذیر تجزیه می‌شود.

بررسی مشابه حلقهٔ D_l برای $۵ < l < ۲۳$، مساله‌ای بسیار دشوار است.

چون عددهای $\zeta = \zeta^{(۱)}$، $\zeta^{(۲)} = \zeta^۲$، ...، $\zeta^{(l-۱)} = \zeta^{l-۱}$ ریشه‌های چندجمله‌ای (۲) هستند، بنابراین

$$x^{l-۲} + \ldots + ۱ = (x-\zeta)(x-\zeta^۲)\ldots(x-\zeta^{l-۱})$$

که با فرض $x = ۱$، به‌دست می‌آید:

$$l = (۱-\zeta)(۱-\zeta^۲)\ldots(۱-\zeta^{l-۱}) \qquad (۱۲)$$

یعنی $l = \lambda^{(۱)}\ldots\lambda^{(l-۱)}$ که در آن $\lambda = ۱ - \zeta$. و این، به‌معنای آن است که

$$N\lambda = l,\ \lambda = ۱ - \zeta \qquad (۱۳)$$

از این‌جا نتیجه می‌گیریم، عدد $\lambda = ۱ - \zeta$، عضو اول حلقهٔ D_l است. در واقع، اگر فرض کنیم $\lambda = \alpha\beta$ آن‌وقت $l = N\lambda = N\alpha \cdot N\beta$ و بنابراین، یا $N\alpha = ۱$ و یا $N\beta = ۱$.

به‌جز این، اگر در حلقهٔ D_l، عدد گویا و درست a بر λ بخش‌پذیر باشد، به‌معنای آن است که بر l هم بخش‌پذیر است. در واقع، اگر $a = \lambda\alpha$ را به‌صورت نُرم آن بنویسیم، به‌دست می‌آید: $a^{l-۱} = l \cdot N\alpha$ که در

آن، $N\alpha$ عددی گویا و درست است. بنابراین، l بخشیابی از a^{l-1}، یعنی بخشیابی از a است.

نقش ζ را می‌توان به‌عهدهٔ هر ریشهٔ $\zeta^k = \zeta^{(k)}$ گذاشت. بنابراین، شبیه برابری (۱۳)، برای هر k وجود دارد:

$$N(1-\zeta^k) = l,\ k = 1,\ldots,l-1$$

اثباتی دیگر:

$$N(1-\zeta^k) = \prod_{s=1}^{l-1}(1-\zeta^{sk}) = \prod_{s=1}^{l-1}(1-\zeta^s) = N(1-\zeta) = l$$

زیرا از تقسیم عددهای k، $2k$، ...، $(l-1)k$ بر l همان عددهای ۱، ۲، ...، $l-1$ با ترتیبی دیگر به‌دست می‌آید.

ولی $1-\zeta^k = (1-\zeta)\varepsilon_k,\ \varepsilon_k = 1+\zeta+\ldots+\zeta^{k-1}$

که از آن‌جا نتیجه می‌شود:

$$N(1-\zeta^k) = N(1-\zeta)\cdot N\varepsilon_k$$

یعنی $l = l\cdot N\varepsilon_k$. بنابراین $N\varepsilon_k = 1$، به‌نحوی‌که عدد ε_k عضو واحد است و درنتیجه عدد $1-\zeta^k$ (برای k از ۱ تا $l-1$) با عدد $\lambda = 1-\zeta$ هم‌پیوند است.

باتوجه به (۱۲)، آن‌چه گفتیم به‌معنای این است که در حلقهٔ D_l این برابری برقرار است:

$$l = \varepsilon\lambda^{l-1} \qquad (۱۴)$$

که در آن، ε عبارت است از یک واحد.

به‌این ترتیب، با دقت تا هم‌پیوندی، عدد l در حلقهٔ D_l، $(l-1)$اُمین درجهٔ عضو اول $\lambda = 1-\zeta$ است.

از این به‌بعد، سودمند است اگر درنظر داشته‌باشیم که هر عضو $\alpha \in D_l$ را می‌توان به‌صورت ترکیبی از توان‌های عضو λ نوشت:

$$\alpha = b_0 + b_1\lambda + \ldots + b_{l-2}\lambda^{l-2} \qquad (۱۵)$$

اگر به حالت حلقهٔ D_l برگردیم، علامت‌گذاری گاوس را (بخش ۲ را ببینید)، به‌صورت $\alpha \equiv \beta(\mathrm{mod}\lambda)$ می‌نویسیم (α و β عضو D_l)، به‌شرطی‌که $\alpha - \beta$ بر λ بخش‌پذیر باشد. شبیه عددهای گویای درست، این هم‌نهشتی‌ها هم نسبت به عمل‌های جمع و ضرب، رفتاری مثل برابری‌های عادی دارند (آن‌ها را می‌توان با هم جمع و یا در هم ضرب کرد، به‌ویژه می‌توان به توان هر عدد طبیعی رساند).

از دستور (۱۵) بلافاصله نتیجه می‌شود، برای هر $\alpha \in D_l$، چنان عدد گویا و درست b_0 وجود دارد که داشته‌باشیم:

$$\alpha = b_0(\mathrm{mod}\lambda) \qquad (۱۶)$$

۷

واحدهای حلقهٔ D_l

استدلال کومر بر پایهٔ بررسی ظریفی از ساختار گروه واحدهای حلقهٔ D_l قرار دارد. به چهار گزاره دربارهٔ این گروه نیاز داریم؛ سه گزاره از این گزاره‌ها را ثابت می‌کنیم، ولی ناچاریم از اثبات گزارهٔ چهارم بگذریم.

در آغاز، همهٔ عضوهای حلقهٔ D_l را، که ریشه‌های یک هستند، پیدا می‌کنیم. نمونهٔ چنین عضوی عدد ζ است، که عبارت است از ریشهٔ مرتبهٔ l یک. نمونهٔ دیگر، ما را به عدد $-\zeta$ می‌رساند که عبارت است از ریشهٔ مرتبهٔ $2l$ یک. همهٔ درجه‌های ممکن عدد $-\zeta$ هم (که به‌صورت $\pm\zeta^a$ هستند؛ و a می‌تواند عددهای ۰، ۱، ...، $l-1$ را اختیار کند) ریشه‌های یک از مرتبهٔ $2l$ هستند (و روشن است که شامل همهٔ این‌گونه ریشه‌ها می‌شوند). این‌ها، همهٔ ریشه‌های یک را، که در حلقهٔ D_l قرار دارند، تشکیل می‌دهند.

گزارهٔ ۱. هر ریشهٔ یک که در حلقهٔ D_l باشد، ریشهٔ مرتبهٔ $2l$ است، یعنی می‌توان آن را به‌این صورت نشان داد:

$$\pm\zeta^a,\ a = 0, 1, \ldots, l-1$$

اثبات. باید ثابت کنیم، اگر در حلقهٔ D_l، برابری $\alpha^N = 1$، به‌شرط درست و مثبت بودن N، برقرار باشد؛ درضمن $\alpha^{N_1} \neq 1$ برای هیچ‌کدام از عددهای N_1 $(N_1 < N)$ برقرار نباشد، آن‌وقت N بخشیابی از $2l$ است، یعنی بر l^2 یا بر ۴ یا بر عدد اول $p \neq l$ بخش‌پذیر نیست.

فرض کنید $N = l^2 n$. عدد $\beta = \alpha^n$ را درنظر می‌گیریم. همان‌طور که می‌دانیم (دستور (۱۶) را در بخش ۶ ببینید)، عدد گویای درستی مثل b_0 وجود دارد، به‌نحوی‌که داشته‌باشیم:

$$\beta \equiv b_0 (\mathrm{mod}\lambda)$$

و این به‌معنای آن است که $\beta = b_0 + \lambda\gamma$ که در آن $\gamma \in D_l$. ولی در این صورت، باتوجه به ویژگی ضریب‌های بسط دوجمله‌ای باید داشته‌باشیم:

$$\beta^l \equiv b_0^l + (\lambda\gamma)^l (\mathrm{mod}l)$$

و بنابراین (دستور ۱۴ بخش ۶ را ببینید):

$$\beta^l = c_\circ (\mathrm{mod} l)$$

که در آن $c_\circ = b_\circ^l$.

از طرف دیگر روشن است که $\beta^l \neq ۱$، ولی $(\beta^l)^l = ۱$، یعنی β^l مخالف ۱، به‌عنوان ریشهٔ مرتبهٔ l از یک است. ولی همهٔ این‌گونه ریشه‌ها در D_l قرار دارند و به‌صورت ζ^a هستند $(\circ < a \leq l - ۱)$. بنابراین ثابت می‌شود، به‌ازای مقداری از a $(\circ < a \leq l - ۱)$ داریم: $\beta^l = \zeta^a$.

به‌این ترتیب، می‌بینیم، در حلقهٔ D_l، این هم‌نهشتی برقرار است:

$$\zeta^a \equiv c_\circ (\mathrm{mod} l)$$

که در آن $\circ < a \leq l - ۱$ و $c_\circ \in \mathbf{Z}$. ولی این ممکن نیست، زیرا عضو به‌صورت $\dfrac{\zeta^a - c_\circ}{l}$ نمی‌تواند متعلق به D_l باشد. بنابراین، برابری $N = l^۲ n$ ممکن نیست، یعنی N بر $l^۲$ بخش‌پذیر نیست.

فرض کنید $N = ۴n$ یا $N = pN$ (p عددی است فرد و اول مخالف با l). دوباره عدد $\beta = \alpha^n$ را درنظر می‌گیریم. روشن است برای $N = ۴n$ داریم $\beta = \pm i$، یعنی $\beta^۲ = -۱$ و برای $N = pn$ داریم $\beta^p = ۱$. در هر دو حالت

$$\beta^p \equiv ۱ (\mathrm{mod} p)$$

یعنی

$$\beta^p \equiv -\zeta - \zeta^۲ - \ldots - \zeta^{l-۱} (\mathrm{mod} p) \qquad (۱)$$

که در آن برای $N = ۴n$ داریم $p = ۲$.

عدد β را به‌این صورت نشان می‌دهیم:

$$\beta = b_۱\zeta + b_۲\zeta^۲ + \ldots + b_{l-۱}\zeta^{l-۱}$$

در این‌صورت، بنابر ویژگی معلوم ضریب‌های چندجمله‌ای

$$\beta^p \equiv b_1^p \zeta^p + b_2^p \zeta^{2p} + \ldots + b_{l-1}^p \zeta^{(l-1)p} (\mathrm{mod} p)$$

یعنی (اگر از قضیهٔ اویلر استفاده کنیم):

$$\beta^p \equiv b_1 \zeta^p + b_2 \zeta^{2p} + \ldots + b_{l-1} \zeta^{(l-1)p} (\mathrm{mod} p)$$

ولی روشن است، برای هر عدد اول $p \geq 2$ که غیر از l باشد، عددهای ζ^p، ζ^{2p}، ...، $\zeta^{(l-1)p}$، بدون توجه به دریف آن‌ها، بر عددهای ξ، ζ^2، ...، ζ^{l-1} منطبق‌اند. از این‌جا و باتوجه به هم‌نهشتی (۱) (و یگانه بودن تجزیهٔ عضوهای حلقهٔ D_l برحسب توان‌های ζ، ζ^2، ...، ζ^{l-1}) نتیجه می‌شود:

$$b_1 \equiv b_2 \equiv \ldots \equiv b_{l-1} \equiv -1 (\mathrm{mod} p)$$

بنابراین

$$\beta \equiv -\zeta - \zeta^2 - \ldots - \zeta^{l-1} (\mathrm{mod} p)$$

یعنی

$$\beta \equiv 1 (\mathrm{mod} p)$$

این، به‌معنای آن است که، عضو β را می‌توان به‌صورت $\beta = 1 + p^k \gamma$ نشان داد که در آن، $k \geq 1$ و $\gamma \in D_l$ بخش‌ناپذیر بر p. از این‌جا، با استفاده از دستور دوجمله‌ای نیوتُن و توجه به این‌که برای $k \geq 1$ داریم $2k + 1 \geq k + 2$، بلافاصله به‌دست می‌آید:

$$\beta^p \equiv 1 + p^{k+1} \gamma (\mathrm{mod} p^{k+2})$$

اکنون اگر $p > 2$ (یعنی با حالت $N = pn$ سروکار داشته‌باشیم)، آن‌وقت $\beta^p = 1$، و بنابراین

$$p^{k+1} \gamma \equiv 0 (\mathrm{mod} p^{k+2})$$

یعنی $\gamma \equiv ۰ (\mathrm{mod} p)$، که نوع انتخاب γ را نقض می‌کند. به‌این ترتیب، فرضِ بخش‌پذیر بودن N بر p، منجر به تناقض می‌شود.

اگر هم $p = ۲$ (یعنی با حالت $N = ۴n$ سروکار داشته‌باشیم)، آن‌وقت $\beta^p = -۱$ و درنتیجه

$$۰ \equiv ۲ + ۲^{k+۱} (\mathrm{mod} ۲^{k+۲}) \Rightarrow ۲^k \gamma \equiv ۱ (\mathrm{mod} ۲^{k+۱})$$

که ناممکن بودن آن روشن است. بنابراین، N نمی‌تواند بر ۴ بخش‌پذیر باشد.

یادداشت: در متن گزاره‌ای که تنظیم کردیم، می‌توان به‌جای «در حلقهٔ D_l» گفت «در میدان K_l»، زیرا می‌توان ثابت کرد، هر ریشهٔ یک که در میدان K_l باشد، به‌خودی خود متعلق به حلقهٔ D_l هم هست (بخش ۱۳ را ببینید). البته ما از این مطلب، استفاده‌ای نخواهیم کرد.

هر ریشهٔ یک مثل $\alpha \in D_l$ دارای این ویژگی است که برای هر مقدار k از ۱ تا $l - ۱$ داریم: $|\alpha^{(k)}| = ۱$، زیرا $(\alpha^{(k)})^{۲l} = ۱$. درضمن، عکس این حکم هم درست است.

گزارهٔ ۲. اگر برای عضو $\alpha \in D_l$ داشته‌باشیم

$$|\alpha^{(k)}| = ۱, \ k = ۱, ۲, \ldots, l - ۱ \qquad (۲)$$

آن‌وقت α، ریشه‌ای از یک است.

اثبات. A_l را مجموعهٔ همهٔ عضوهای $\alpha \in D_l$ می‌گیریم که با شرط (۲) سازگار باشند.

برای هر عضو دلخواه $\alpha \in A_l$، این چندجمله‌ای را درنظر می‌گیریم:

$$(x - \alpha^{(۱)}) \ldots (x - \alpha^{(l-۱)}) = x^{l-۱} + c_۱ x^{l-۲} + \ldots + c_{l-۱} \qquad (۳)$$

که ریشهٔ آن، عدد $\alpha = \alpha^{(۱)}$ است. روشن است قدرمطلق $|c_k|$ از هر ضریب c_k $(k = ۱, \ldots, l - ۱)$ در این چندجمله‌ای، از ضریب متناظر آن در چندجمله‌ای

$$(x + |\alpha^{(۱)}|) \ldots (x + |\alpha^{(l-۱)}|) = (x + ۱)^{l+۱}$$

یعنی از $\begin{pmatrix} l-1 \\ k \end{pmatrix}$ تجاوز نمی‌کند.

ولی در بخش ۶ ثابت کردیم (برای هر $\alpha \in D_l$)، چندجمله‌ای (۳) ضریب‌های درستی دارد. چون از عددهای درست c_k، که در نابرابری

$$|c_k| \leq \begin{pmatrix} l-1 \\ k \end{pmatrix}, \quad k = 1, \ldots, l-1$$

صدق کنند، برای l مفروض، تنها تعداد محدودی وجود دارد، به‌این نتیجه می‌رسیم که مجموعهٔ چندجمله‌ای‌های به‌صورت (۳) (برای همهٔ αهای ممکن عضو A_l)، مجموعه‌ای محدود است. از آن‌جاکه تعداد محدودی چندجمله‌ای با درجهٔ مفروض، تعداد محدودی ریشه دارد و از آن‌جاکه هر عضو $\alpha \in A_l$، ریشه‌ای از چندجمله‌ای متناظر (۳) است، نتیجه می‌شود که مجموعهٔ A_l، مجموعه‌ای محدود است.

از طرف دیگر روشن است، اگر $\alpha \in A_l$، آن‌وقت $\alpha^n \in A_l$ (برای هر $n \in \mathbf{Z}$). بنابراین، باتوجه به محدود بودن A_l، می‌توان نماهای مختلف m و n را طوری پیدا کرد که داشته‌باشیم $\alpha^m = \alpha^n$. ولی در این‌صورت $\alpha^{n-m} = 1$، یعنی α ریشه‌ای از یک است.

باوجودی‌که همهٔ‌ریشه‌های‌چندجمله‌ای (۲) (در بخش ۶)، عددهایی مختلط (موهومی) هستند، در میدان K_l (و در حلقهٔ D_l) عددهای حقیقی به‌اندازهٔ کافی زیادی وجود دارد.

به‌ویژه معلوم می‌شود، واحدهای به‌صورت $\pm\zeta^a$ و واحدهای حقیقی، در واقع همهٔ واحدهای حلقهٔ D_l هستند.

گزارهٔ ۳. هر واحدی از حلقهٔ D_l، به‌این صورت است:

$$\pm\zeta^a\varepsilon_0$$

که در آن ε_0 واحد حقیقی است.

اثبات. فرض کنید

$$\varepsilon = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$$

واحد دلخواهی از حلقهٔ D_l باشد. چون $\zeta = \zeta^{-1} = \zeta^{l-1}$، بنابراین عدد مختلط مزدوج، یعنی

$$\overline{\varepsilon} = a_0 + a_1\overline{\zeta} + \ldots + a_{l-2}\overline{\zeta}^{l-2}$$

هم در D_l قرار دارد و به‌روشنی، واحد است. درنتیجه، این عدد هم واحد است:

$$\mu = \frac{\overline{\varepsilon}}{\varepsilon} \in D_l$$

این واحد، همان ویژگی $|\mu| = 1$ را دارد.

از این گذشته، برای هر k (۱، ۲، ...، $l-1$)، عدد

$$\varepsilon^{(k)} = a_0 + a_1\zeta^{(k)} + \ldots + a_{l-2}(\zeta^{(k)})^{l-2}$$

هم یک واحد است؛ همچنین

$$\mu^{(k)} = \frac{\overline{\varepsilon}^{(k)}}{\varepsilon^{(k)}}$$

بنابراین برای هر k (برابر ۱، ۲، ...، $l-1$) داریم: $|\mu^{(k)}| = 1$.

به‌این ترتیب، باتوجه به گزارهٔ ۲، عدد μ ریشهٔ یک است. از آن‌جاکه، باتوجه به گزارهٔ ۱، هر ریشهٔ یک به‌صورت $\pm\zeta^c$ است، ثابت می‌شود که، عدد درست $c \geq 0$ وجود دارد، به‌نحوی‌که

$$\overline{\varepsilon} = \pm\zeta^c\varepsilon$$

باتوجه به آن‌چه در پایان بخش ۶ گفتیم، چنان عدد گویا و درست b_0 وجود دارد که داشته‌باشیم:

$$\varepsilon \equiv b_0 (\mathrm{mod}\lambda)$$

درضمن، چون $\overline{\lambda} \equiv ۰ (\mathrm{mod}\lambda)$، بنابراین همچنین

$$\overline{\varepsilon} \equiv b_۰ (\mathrm{mod}\lambda)$$

درنتیجه، اگر داشته‌باشیم:

$$\overline{\varepsilon} = -\zeta^c \varepsilon$$

آن‌وقت خواهیم داشت:

$$b_۰ \equiv -b_۰ (\mathrm{mod}\lambda)$$

زیرا $\zeta \equiv ۱ (\mathrm{mod}\lambda)$. بنابراین

$$۲b_۰ = ۰ (\mathrm{mod}\lambda)$$

یعنی $۲b_۰$ بر λ بخش‌پذیر است. ولی می‌دانیم (بخش ۶ را ببینید)، اگر عدد گویای درستی در حلقهٔ D_l، بر λ بخش‌پذیر باشد، آن‌وقت بر l هم بخش‌پذیر است. درنتیجه $۲b_۰$، یعنی $b_۰$ بر l بخش‌پذیر است. وقتی $b_۰$ بر λ بخش‌پذیر باشد، ازجمله ε بر λ بخش‌پذیر است که ممکن نیست (زیرا $N\varepsilon = ۱$ بر $N\lambda = l$ بخش‌پذیر نیست).

تناقضی که به‌دست آمد، نشان می‌دهد که

$$\overline{\varepsilon} = \zeta^c \varepsilon$$

فرض می‌کنیم

$$\varepsilon_۰ = \zeta^{-sc}\varepsilon,\ s = \frac{l-۱}{۲}$$

در این‌صورت

$$\varepsilon = \zeta^a \varepsilon_۰,\ a = sc$$

درضمن (به‌یاد داشته‌باشیم: $\zeta = \zeta^{-1}$).

$$\begin{aligned}\overline{\varepsilon}_\circ &= \overline{\zeta}^{-sc}\varepsilon = \zeta^{sc}\zeta^{c}\varepsilon = \zeta^{(s+1)c}\varepsilon \\ &= \zeta^{(l-s)c}\varepsilon = \zeta^{-sc}\varepsilon = \varepsilon_\circ\end{aligned}$$

پایان اثبات.

برای بررسی حالت اول قضیهٔ فرما با روش اویلر-کومر، که در بخش بعد به آن می‌پردازیم، گزارهٔ ۳ کافی است. باوجود این، برای حالت دشوارتر دوم، به ویژگی دیگری از واحدهای حلقهٔ D_l نیاز داریم که دربارهٔ عدد اول l است، وقتی که سامان‌پذیر باشد (بخش ۱ را ببینید). این ویژگی که به «پیش‌قضیهٔ کومر» معروف است، شرط‌های کافی را، برای این‌که واحدهای از حلقهٔ D_l، درجهٔ lاُم واحد دیگر باشد، به‌دست می‌دهد.

پیش‌قضیهٔ کومر. اگر عدد اول l سامان‌پذیر باشد، آن‌وقت هر واحد ε از حلقهٔ D_l، که برای آن عدد گویای درست e وجود داشته‌باشد، به‌نحوی‌که داشته‌باشیم:

$$\varepsilon \equiv e(\mathrm{mod} l)$$

lامین توان واحد دیگری مثل $\eta \in D_l$ است:

$$\varepsilon = \eta^l$$

در این‌جا حتا تلاشی برای اثبات این پیش‌قضیه نمی‌کنیم. به‌طور صوری، می‌توان این گزاره را در تعریف عدد سامان‌پذیر وارد کرد (کومر هم، در آغاز، همین فرض را پذیرفت).

۸

حالت اول قضیهٔ فرما

برای این‌که دشواری تلاش‌هایی را که برای اثبات قضیهٔ فرما شده‌است، نشان دهیم، اثبات کومر را دربارهٔ حالت اول قضیهٔ فرما (وقتی نماها سامان‌پذیرند)، به دو مرحله تقسیم می‌کنیم. در این بخش، قضیه‌ای از یک گزارهٔ کمکی را می‌آوریم و در بخش‌های بعد، دربارهٔ روش اثبات آن صحبت می‌کنیم.

گزارهٔ کمکی. اگر داشته‌باشیم:

$$x^l + y^l = z^l,\ l \geq ۳ \qquad (۱)$$

که در آن x، y و z، عددهای گویا و درستی‌اندکه‌دوبه‌دو نسبت‌به هم اول‌اند و درضمن بر عدد اول l بخش‌پذیر نیستند، آن‌وقت در حلقهٔ D_l، برابری

$$x + \zeta y = \varepsilon \alpha^l \qquad (۲)$$

برقرار است که در آن $\alpha \in D_l$، و ε، واحد حلقهٔ D_l است.

برای این‌که این گزاره را، در حالت اول قضیهٔ فرما، به تناقض برسانیم، کافی است ثابت کنیم برابری (۲) در حلقهٔ D_l (با پذیرفتن برابری (۱))، تنها وقتی ممکن است که دست‌کم یکی از عددهای x، y و z بر l بخش‌پذیر باشد. درضمن، می‌توانیم فرض کنیم $l \geq ۵$، زیرا برای حالت $l = ۳$، قضیهٔ فرما را ثابت کرده‌ایم.

همان‌طور که می‌دانیم (بخش ۲ را ببینید)، برای هر $x_۱$، $x_۲$، ...، x_n داریم:

$$(x_۱ + x_۲ + \ldots + x_n)^l \equiv x_۱^l + \ldots x_n^l + x_n'(\mathrm{mod} l) \qquad (۳)$$

پیش‌قضیه. اگر داشته‌باشیم:

$$x + \zeta y = \varepsilon \alpha^l$$

که در آن x و y عددهای گویای درست، $\alpha \in D_l$ و ε واحد حلقهٔ D_l است، آن‌وقت به‌ازای $l \geq ۵$، یا x و یا y بر l بخش‌پذیر است و یا $x \equiv y(\mathrm{mod} l)$.

اثبات. فرض می‌کنیم:

$$\alpha = b_0 + b_1\lambda + \ldots + b_{l-2}\lambda^{l-2}$$

که در آن b_0، b_1، ...، b_{l-2} عددهای گویای درست‌اند (بخش ۶، دستور (۱۵) را ببینید). در این‌صورت، بنابر دستور (۳)

$$\alpha^l \equiv b_0^l + b_1^l\lambda^2 + \ldots + b_{l-2}^l\lambda^{l(l-2)} (\mathrm{mod} l)$$

از آن‌جا، باتوجه به دستور (۱۴) بخش ۶، نتیجه می‌شود:

$$\alpha^l \equiv b_0^l (\mathrm{mod} l)$$

بنابراین، باتوجه به قضیهٔ کوچک فرما

$$\alpha^l \equiv b_0 (\mathrm{mod} l)$$

باتوجه به گزارهٔ ۳ بخش ۷، واحد ε به‌این صورت است:

$$\varepsilon = \zeta^a \varepsilon_0$$

که در آن ε_0 واحد حقیقی است. بنابراین، بافرض

$$\eta = b_0 \varepsilon_0$$

به‌دست می‌آید که

$$x + \zeta y \equiv \zeta^a \eta (\mathrm{mod} l)$$

و یا

$$\zeta^{-a}(x + \zeta y) \equiv \eta (\mathrm{mod} l)$$

اکنون یادآوری می‌کنیم، اگر $\alpha \equiv \beta (\mathrm{mod} l)$، یعنی اگر $\alpha = \beta + l\gamma$، که در آن $\gamma \in D_l$، آن‌وقت $\overline{\alpha} = \overline{\beta} + l\overline{\gamma}$ که در آن $\overline{\gamma} \in D_l$ و بنابراین $\overline{\alpha} \equiv \overline{\beta} (\mathrm{mod} l)$. ازجمله

$$\overline{\zeta^{-a}(x + \zeta y)} \equiv \overline{\eta} (\mathrm{mod} l)$$

ولی η عددی حقیقی است $(\overline{\eta} = \eta)$ و $\overline{\zeta} = \zeta^{-1}$. بنابراین

$$\zeta^a(x + \zeta^{-1}y) \equiv \eta(\mathrm{mod}\, l)$$

که می‌توان آن را این‌طور نوشت:

$$\zeta^a(x + \zeta^{-1}y) \equiv \zeta^{-a}(x + \zeta y)(\mathrm{mod}\, l)$$

یعنی

$$x\zeta^a + y\zeta^{a-1} - x\zeta^{-a} - y\zeta^{1-a} \equiv 0(\mathrm{mod}\, l)$$

اگر نماد $< k >$ را برای باقی‌ماندهٔ نامنفیِ تقسیم عدد درست k بر l انتخاب کنیم، می‌توانیم این رابطه را چنین بنویسیم

$$x\zeta^{<a>} + y\zeta^{<a-1>} - x\zeta^{<-a>} - y\zeta^{<1-a>} \equiv 0(\mathrm{mod}\, l) \quad (۴)$$

روشن است، عدد $a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$ از حلقهٔ D_l، وقتی و تنها وقتی بر l بخش‌پذیر است که همهٔ ضریب‌های آن، یعنی a_0، a_1، ...، a_{l-2}، بر l بخش‌پذیر باشند. بنابراین، اگر در (۴)، همهٔ نماها مختلف و مخالف $l - 1$ باشند، آن‌وقت y هم بر l بخش‌پذیر است. به‌این ترتیب، در این حالت، همه‌چیز ثابت شد.

فرض کنید بین نماها در (۴)، عدد $l - 1$ وجود داشته‌باشد. این، وقتی و تنها وقتی ممکن است که داشته‌باشیم:

$$< a >= 0, 1, 2, l - 1$$

و متناظر با آن

$$< a - 1 >= l - 1, 0, 1, l - 2,$$
$$< -a >= 0, l - 1, l - 2, 1,$$
$$< 1 - a >= 1, 0, l - 1, 2$$

چون بنابه فرض $l \geq ۵$، بنابراین در هریک از این چهار حالت، تنها یکی از نماها در (۴)، برابر $(l-۱)$ است. جملهٔ مربوط به این نما را باید با این دستور تبدیل کنیم:

$$\zeta^{l-۱} = -۱ - \zeta - \ldots - \zeta^{l-۲}$$

بعد از چنین تبدیلی، این جمله به مجموع جمله‌های ۱، ζ، ...، $\zeta^{l-۲}$ با ضریب‌های $\pm x$ یا $\pm y$ منجر می‌شود. از آن‌جاکه تعداد این تک‌جمله‌ای‌ها، یعنی $l-۱$، کمتر از چهار نیست (زیرا $l \geq ۵$)، بنابراین ضمن ساده‌کردن جمله‌های متشابه، دست‌کم برخی از آن‌ها با سه جملهٔ دیگر سمت چپ هم‌نهشتی (۴) ساده نمی‌شوند (برای نمونه، اگر $< a >= l-۱$، آن‌وقت جملهٔ $x\zeta$ باقی می‌ماند). چون درنتیجهٔ تبدیل جمله‌های متشابه در سمت چپ هم‌نهشتی (۴)، عدد حلقهٔ D_l به‌دست می‌آید که به‌صورت نُرمالِ

$$a_۰ + a_۱\zeta + \ldots + a_{l-۲}\zeta^{l-۲}$$

نوشته شده‌است، ضریب این جملهٔ باقی‌مانده باید بر l بخش‌پذیر باشد.

بنابراین، در این حالت هم، یا x بر l بخش‌پذیر است و یا y.

فرض کنید، همهٔ نماها در (۴)، کمتر از $l-۱$ باشد، ولی در بین آن‌ها، نماهای برابر وجود داشته‌باشد. چون برابری‌های $< a >=< a-۱ >$ و $< a >=< ۱-a >$ نمی‌توانند برقرار باشند (دو عدد مجاور، نمی‌توانند در تقسیم بر l، به یک باقی‌مانده برسند)، تنها چهار حالتِ

$$< a >=< -a >, \qquad < a >=< ۱-a >,$$
$$< a-۱ >=< ۱-a >, \quad < a-۱ >=< -a >$$

را باید بررسی کرد، یعنی حالت‌های

$$a \equiv -a(\mathrm{mod} l), \qquad a \equiv ۱-a(\mathrm{mod} l),$$
$$a-۱ \equiv ۱-a(\mathrm{mod} l), \quad a-۱ = -a(\mathrm{mod} l)$$

در حالت اول $۲a \equiv ۰(\mathrm{mod} l)$، یعنی $۲a = Al$ (A عددی است درست و زوج). بنابراین

$$a - ۱ = (l - ۱) + \left(\frac{A}{۲} - ۱\right) l$$

و از آن‌جا $l - ۱ =< a - ۱ < a$ که باتوجه به شرط ممکن نیست.

به‌همین ترتیب، در حالت دوم $۲a \equiv ۲(\mathrm{mod} l)$، یعنی به‌شرط درست و زوج بودن A : $۲a = ۲ + Al$ و بنابراین

$$-a = (l - ۱) - \left(\frac{A}{۲} + ۱\right) l$$

و دوباره به برابری ناممکنِ $l - ۱ =< -a < a$ می‌رسیم.

در حالت‌های سوم و چهارم هم $۲a \equiv ۱(\mathrm{mod} l)$، یعنی بافرض درست و فرد بودن A، به‌دست می‌آید: $۲a = ۱ + Al$. بنابراین

$$a = \frac{l + ۱}{۲} + \frac{A - ۱}{۲} l$$

از آن‌جا $< a >= \frac{l + ۱}{۲}$، یعنی

$$< a - ۱ >=< -a >= \frac{l - ۱}{۲}$$

و

$$< ۱ - a >=< a >= \frac{l + ۱}{۲}$$

به‌این ترتیب، در این حالت‌ها، هم‌نهشتی (۴) به‌این صورت درمی‌آید:

$$(x - y)\zeta^{\frac{l+۱}{۲}} + (y - x)\zeta^{\frac{l-۱}{۲}} \equiv ۰(\mathrm{mod} l) \qquad (۵)$$

از آن‌جاکه سمت چپ هم‌نهشتی (۵) به‌صورت نرمال است (نماهای $\frac{l+1}{2}$ و $\frac{l-1}{2}$ مختلف و از عدد $l-1$ کوچکترند)، می‌توان از آن نتیجه گرفت که $(x-y)$ بر l بخش‌پذیر است، یعنی

$$x \equiv y (\mathrm{mod} l)$$

به‌این ترتیب، پیش‌قضیه، به‌طور کامل ثابت شد.
از این پیش‌قضیه و گزارهٔ کمکی نتیجه می‌شود، اگر داشته‌باشیم:

$$x^l + y^l = z^l \qquad (۶)$$

که در آن x و y نسبت به هم اول و بر l بخش‌ناپذیرند، آن‌وقت به‌ناچار باید داشته‌باشیم: $x \equiv y (\mathrm{mod} l)$. ولی به‌جای برابری (۶)، می‌توان این برابری را درنظر گرفت:

$$x^l + (-z)^l = (-y)^l$$

که با همان استدلال به هم‌نهشتی $x \equiv -z (\mathrm{mod} l)$ می‌رسیم. بنابراین

$$x + y - z \equiv ۳x (\mathrm{mod} l)$$

از طرف دیگر، از برابری (۶) و باتوجه به قضیهٔ کوچک فرما نتیجه می‌شود:

$$z \equiv x + y (\mathrm{mod} l)$$

بنابراین

$$۳x \equiv ۰ (\mathrm{mod} l)$$

که ممکن نیست، زیرا $l > ۳$ و درضمن، x بر l بخش‌پذیر نیست.
به‌این ترتیب، اگر فرض کنیم برای عددهای x، y و z که دوبه‌دو نسبت به هم اول‌اند و بر l بخش‌پذیر نیستند، برابری (۶) برقرار باشد، با استفاده از گزارهٔ کمکی، به تناقض می‌رسیم.

ثابت شد، حالت اول قضیهٔ فرما، برای مقدارهایی از l، که برای آن‌ها گزارهٔ کمکی برقرار باشد، درست است.

چون

$$x^l + y^l = (x+y)(x+\zeta y)\dots(x+\zeta^{l-1}y)$$

می‌توان برابری

$$x^l + y^l = z^l \qquad (۷)$$

را به‌این صورت نوشت:

$$(x+y)(x+\zeta y)\dots(x+\zeta^{l-1}y) = z^l \qquad (۸)$$

به‌شرطی‌که

الف) همهٔ عامل‌ها در سمت چپ برابری (۸)، دوبه‌دو نسبت به هم اول باشند؛

ب) برای حلقهٔ D_l، قضیهٔ اصلی حساب برقرار باشد؛

آن‌وقت، هریک از عامل‌های (۸)، بادقت تا هم‌پیوندی، از درجهٔ l خواهند بود (زیرا، باتوجه به (۸)، حاصل‌ضرب آن‌ها، از درجه l است). به‌زبان دیگر، در حلقهٔ D_l، عضوی مثل α و واحدی مثل ε پیدا می‌شود، به‌نحوی‌که داشته‌باشیم:

$$x + \zeta y = \varepsilon\alpha^l$$

گزارهٔ کمکی از بخش ۸، به‌این ترتیب ثابت می‌شود، البته با دو «اگر» (دو «شرط»). ولی «اگر» اول به‌سادگی برطرف می‌شود.

گزارهٔ ۱. اگر عددهای گویا و درست x و y نسبت به هم اول باشند، درضمن مجموع آن‌ها بر l بخش‌پذیر نباشد، آن‌وقت همهٔ عددهای

$$x+y,\ x+\zeta y,\dots,x+\zeta^{l-1}y \qquad (۹)$$

دوبه‌دو نسبت به هم اول‌اند (در حلقهٔ D_l).

اثبات. فرض کنید، عامل اول π در D_l وجود داشته‌باشد، به‌نحوی‌که دو عدد از عددهای (۹)، یعنی $x+\zeta^m y$ و $x+\zeta^n y$ بر آن بخش‌پذیر باشند ($0 \le m,n < l-1$ و $m \neq n$).

چون

$$-\zeta^{n-m}(x+\zeta^m y)+(x+\zeta^n y)=(1-\zeta^{n-m})x,$$
$$\zeta^{-m}(x+\zeta^m y)-\zeta^{-m}(x+\zeta^n y)=(1-\zeta^{n-m})y$$

و چون $1-\zeta^{n-m} \sim 1-\zeta$ (بخش ۶ را ببینید)، آن‌وقت π باید بخشیابی از عددهای $x(1-\zeta)$ و $y(1-\zeta)$ باشد.

از آن‌جاکه x و y نسبت به هم اول‌اند، عددهای درستِ a و b را می‌توان پیدا کرد، به‌نحوی‌که $xa+yb=1$. بنابراین، π بخشیابی از عدد

$$(1-\zeta)xa+(1-\zeta)yb=1-\zeta$$

یعنی بخشیابی از عدد $(1-\zeta)^{l-1} \sim l$ است.

چون عدد π بخشیابی از عدد $1-\zeta$ است، درضمن باید بخشیابی از عدد $1-\zeta \sim 1-\zeta^m$ هم باشد. بنابراین

$$x+y=x+\zeta^m y+(1-\zeta^m)y$$

ولی بنابر شرط، عددهای l و $x+y$ نسبت به هم اول‌اند، بنابراین عددهای u و v وجود دارند، به‌نحوی که

$$lu+(x+y)v=1$$

و این نشان می‌دهد که π، بخشیاب عدد ۱ است.

تناقض حاصل، ثابت می‌کند که عددهای (۹)، دوبه‌دو نسبت به هم اول‌اند.

گزارهٔ ۱ شرط الف) را تامین می‌کند. زیرا در برابری (۱)، عددهای x و y نسبت به هم اول‌اند؛ درضمن عدد z، باتوجه به قضیهٔ کوچک فرما، نسبت به مُدول l، با $x+y$ هم‌نهشت است و، بنابر شرط، بر l بخش‌پذیر نیست.

آن‌چه به شرط ب) مربوط می‌شود، می‌دانیم تنها برای برخی از مقدارهای l برقرار است؛ و بنابراین، تا این‌جا، باید خود را به همین مقدارهای l محدود کنیم.

اگر مطلب را خلاصه کنیم، می‌بینیم روش اویلر، تا این‌جا به ما این امکان را می‌دهد که، قضیهٔ فرما را به‌این صورت ثابت کنیم:

قضیهٔ ۱. فرض کنیم $l \geq ۳$، عددی اول باشد به‌نحوی که در حلقهٔ D_l، قضیهٔ اصلی حساب برقرار باشد. در این‌صورت، اگر برای عددهای گویا و درستِ x، y، z، این برابری را داشته‌باشیم:

$$x^l + y^l = z^l$$

آن‌وقت، دست‌کم باید یکی از عددهای x، y، z بر l بخش‌پذیر باشد.

می‌توان ثابت کرد (بخش ۱۳ را ببینید)، شرط این قضیه، در این عددهای اول صدق می‌کند:

$$l = ۳, ۵, ۷, ۱۱, ۱۳, ۱۷, ۱۹ \qquad (۱۰)$$

عددهای اول دیگری که با شرط قضیهٔ ۱ سازگار باشند، در محدودهٔ صد عدد نخست وجود ندارد.

باوجود این، تاکید می‌کنیم، این آزمایش که برای عددهای (۱۰) در حلقهٔ D_l، قضیهٔ اصلی حساب به‌ازای $l > ۵$ صادق است، مسالهٔ چندان ساده‌ای نیست. بنابراین، درواقع هنوز حق نداریم ادعا کنیم، حالت اول قضیهٔ فرما را برای عددهای (۱۰) ثابت کرده‌ایم.

۹

نظریهٔ بخشیاب‌ها (دی‌وی زورها)

ببینیم، وقتی تجزیهٔ به ضرب عامل‌های اول در حلقهٔ D_l، یگانه نیست (یعنی با روش‌های مختلف می‌توان عددی از حلقهٔ D_l را به‌صورت ضرب عامل‌های اول تجزیه کرد)، گزارهٔ کمکی چه وضعی پیدا می‌کند؟ می‌توان ثابت کرد، در این حالت هم، همه‌چیز به اعتبار خود باقی است (دست‌کم، برای برخی از مقدارهای l). اندیشهٔ کومر، همان‌طور که پیش از این هم گفتیم، این بود که برای بازسازی و پذیرش تجزیهٔ یگانه به عامل‌های اول در D_l، باید برخی عددهای «ایده‌آلی» تازه را اضافه کرد. این اندیشهٔ کومر، تمامی نظریهٔ عددهای جبری را دگرگون کرد و به‌وسیلهٔ دِدِکیند، کِرونه‌کر و زُولوتاریف، منجر به ساختارهای به‌کلی تازه‌ای شد که تاثیر ژرفی بر همهٔ شاخه‌های ریاضیات داشت.

عددهای ایده‌آلی کومر را بخشیاب (دی‌وی‌زُور divisor) نامیده‌اند. موقعیت دی‌وی‌زورها را، به‌صورت انتزاعی، به‌این ترتیب می‌توان شرح داد.

مجموعهٔ $\mathcal{D}$ را درنظر می‌گیریم که در آن، عمل ضرب جابه‌جایی‌پذیر و شرکت‌پذیر باشد؛ درضمن مجموعه دارای یکه باشد (در جبر انتزاعی، این‌گونه مجموعه‌ها را «تک‌واره‌های جابه‌جایی‌پذیر می‌نامند). عضوهای تک‌واره (مُونُوئید Monoid) $\mathcal{D}$ را با حرف‌های خاصی نشان می‌دهیم. به‌ویژه، یکهٔ تکه‌وارهٔ $\mathcal{D}$ را با نماد $\breve{o}$ مشخص می‌کنیم.

گویند عضو $\sigma \in \mathcal{D}$ بخشیابی از عضو $\varsigma \in \mathcal{D}$ است، به‌شرطی‌که عضوی مثل $\natural \in \mathcal{D}$ وجود داشته‌باشد، به‌نحوی‌که داشته‌باشیم: $\varsigma = \sigma\natural$. عضو $\wp \neq \breve{o}$ را اول گویند، وقتی‌که تنها بر خودش و یکهٔ $\breve{o}$ بخش‌پذیر باشد. تکه‌وارهٔ $\mathcal{D}$ را تکه‌واره‌ای آزاد (و جابه‌جایی‌پذیر)، تک‌واره‌ای یگانه در تجزیهٔ به عامل‌های اول، گویند وقتی‌که هر عضو $\sigma \in \mathcal{D}$ از آن بتواند به‌صورت ضرب عامل‌های اول نشان داده شود:

$$\sigma = \wp_1 \dots \wp_r,\ r \geq 0$$

و چنین تجزیه‌ای، به‌شرطی‌که ردیف عامل‌ها را درنظر نگیریم، یگانه باشد (در

حالت $r = 0$، ضرب را برابر $\check{0}$ به‌حساب می‌آورند). به‌این ترتیب، تک‌وارهٔ آزاد، عضو معکوسی ندارد، به‌جز برای واحد $\check{0}$.

نمونهٔ تک‌وارهٔ آزاد، عبارت است از مجموعهٔ $\mathbf{N}$ عددهای طبیعی نسبت به ضرب.

در تک‌وارهٔ آزاد، برای هر چند عضو، بزرگ‌ترین بخشیاب مشترکِ یگانه و کوچک‌ترین مضرب مشترکِ یگانه وجود دارد. اگر بزرگ‌ترین بخشیاب مشترک برابر $\check{0}$ باشد، آن‌وقت عضوها را نسبت به هم اول گویند.

روشن است، در هر تک‌وارهٔ آزاد، ویژگی‌های معروف مربوط به بخش‌پذیری، که در تک‌وارهٔ آزادِ عددهای طبیعی وجود دارد، حفظ می‌شود. ازجمله، اگر $\sigma\natural$ بر ς بخش‌پذیر و σ نسبت به ς اول باشد، آن‌وقت $\natural$ بر ς بخش‌پذیر است؛ اگر σ و $\natural$ نسبت به هم اول و $\sigma\natural = \varsigma^n$، آن‌وقت عضوهایی مثل σ و $\natural$ وجود دارند، به‌نحوی‌که $\sigma = \sigma_1^n$ و $\natural = \natural_1^n$ و غیره.

برای حلقهٔ دلخواه D، مجموعهٔ D^*، شامل همهٔ عضوهای غیرصفر آن، به‌روشنی تک‌واره است (حلقه‌ای مثال بزنید که برای آن، این تک‌واره آزاد باشد). فرض می‌کنیم نگاشتی از این تک‌واره در تک‌وارهٔ آزاد $\mathcal{D}$ داده شده‌باشد. اگر تصویر $\alpha \in D^*$ را با نماد (α) نشان دهیم، می‌خواهیم برای α و β (عضوهای D^*)، این برابری برقراز باشد:

$$(\alpha\beta) = (\alpha)(\beta)$$

یعنی این‌که، نگاشت $\alpha \to (\alpha)$، همسانی یا همریختی (هومُومُورفیسم) تک‌واره‌ها باشد. در این‌صورت، اگر α بر β در D بخش‌پذیر باشد، آن‌وقت (α) هم در $\mathcal{D}$ بر (β) بخش‌پذیر خواهد بود. به‌عکسِ این حکم هم نیاز داریم:

اصل موضوع ۱. عضو $\alpha \in D^*$، وقتی و تنها وقتی بر عضو $\beta \in D^*$ بخش‌پذیر است که عضو $(\alpha) \in \mathcal{D}$ بر عضو $(\beta) \in \mathcal{D}$ بخش‌پذیر باشد.

در حالت خاص، از این‌جا نتیجه می‌شود، وقتی و تنها وقتی (α) با (β) برابر است که عضوهای α و β هم‌پیوند باشند. به‌همین مناسبت، واحدهای

ε از حلقهٔ D با برابری $(\varepsilon) = \check{o}$ مشخص می‌شوند.

اگر عضو σ بخشیابی از عضو (α) باشد، آن‌وقت، می‌گوییم σ بخشیابی از α است. مجموعهٔ همهٔ عضوهای $\alpha \in D^*$ را که بر عضو $\sigma \in \mathcal{D}$ بخش‌پذیر باشند، به‌اضافهٔ $\mathcal{D}\circ \in D$ (که بنابر تعریف، بخش‌پذیر بر هر عضو $\sigma \in \mathcal{D}$ می‌گیریم)، با نماد $[\sigma]$ نشان می‌دهیم. طبیعی است، این را هم بخواهیم که، اگر دو عضو حلقهٔ D بر عضو $\sigma \in \mathcal{D}$ بخش‌پذیر باشند، مجموع و تفاضل آن‌ها هم بر σ بخش‌پذیر شود.

اصل موضوع ۲. اگر $\alpha, \beta \in [\sigma]$، آن‌وقت $\alpha \pm \beta \in [\sigma]$.

سرانجام، این شرط را هم لازم داریم که در $\mathcal{D}$، عضوهای «اضافی» وجود نداشته‌باشد، یعنی بتوان هر دو عضو $\mathcal{D}$ را با ویژگی‌های بخش‌پذیریشان نسبت به عضوهای حلقهٔ D تمیز داد.

اصل موضوع ۳. اگر $[\natural] = [\sigma]$، آن‌وقت $\sigma = \natural$.

اگر برای حلقهٔ D، تک‌وارهٔ آزاد جابه‌جایی‌پذیر $\mathcal{D}$ و همسانی (هوموморفیسم) $\alpha \to (\alpha)$ که با اصل موضوع‌های ۱ تا ۳ سازگار باشد، داده شده‌باشد، آن‌وقت می‌گویند در D **نظریهٔ بخشیاب‌ها** (دی‌وی‌زورها) داده شده‌است. عضوهای تک‌وارهٔ $\mathcal{D}$ را بخشیاب‌ها (دی‌وی‌زورها)، و بخشیاب‌های به‌صورت (α) را، به شرط $\alpha \in D$، **بخشیاب‌های اصلی** گویند. یکهٔ $\check{o}$ از تک‌وارهٔ $\mathcal{D}$ را هم **بخشیاب یکه** گویند.

یادآوری می‌کنیم، در این تعریف، صحبتی از یگانه بودن نظریهٔ بخشیاب‌ها نشده‌است. باوجود این، می‌توان بدون دشواری ثابت کرد که، به مفهومی، نظریهٔ بخشیاب‌ها برای حلقهٔ مفروض D، تنها یکی می‌تواند باشد. ما به این حکم نیازی نداریم و در این‌جا هم، به اثبات آن نمی‌پردازیم.

برعکس، وجود نظریهٔ بخشیاب‌ها، برای حلقهٔ D محدودیت‌های زیادی ایجاد می‌کند که البته، در این‌جا، به‌صورت کلی آن نخواهیم پرداخت، زیرا این بحث، ما را از راه اصلی خود به‌کلی دور می‌کند.

ولی به‌سادگی دیده می‌شود، اگر در حلقهٔ D قضیهٔ اصلی حساب صدق

کند، دارای نظریهٔ بخشیاب‌ها است؛ درضمن در این نظریه، همهٔ بخشیاب‌ها، بخشیاب اصلی‌اند.

در واقع، فرض کنید $\mathcal{D}$ مجموعهٔ خانواده‌های عضوهای هم‌پیوند مجموعهٔ D باشد (بخش ۵ را ببینید). اگر خانواده‌ای را که شامل عضو α است با نماد (α) نشان دهیم و فرض کنیم $(\alpha)(\beta) = (\alpha\beta)$، به‌طور مستقیم قابل تحقیق است که نسبت به ضرب، تعریف شده در مجموعهٔ $\mathcal{D}$ یک تک‌وارهٔ جابه‌جایی‌پذیر آزاد است. درضمن نگاشت $\alpha \to (\alpha)$، نگاشتی همسان و با اصل موضوع‌های ۱ تا ۳ سازگار است. درضمن بخشیاب (α) تنها وقتی اول است که عضو α اول باشد.

برعکس، اگر برای حلقهٔ D، نظریهٔ بخشیاب‌ها وجود داشته‌باشد و در آن همهٔ بخشیاب‌ها اصلی باشند، آن‌وقت قضیهٔ اصلی حساب در D صدق می‌کند.

در واقع، کافی است به این نکته توجه کنیم که، در چنین حلقه‌ای، بخشیاب (π) تنها وقتی اول است که عضو π اول باشد (اگر $\pi = \pi_1\pi_2$، آن‌وقت $(\pi_1)(\pi_2) = (\pi)$ و اگر $(\pi_1)(\pi_2) = (\pi)$، آن‌وقت π با حاصل‌ضرب $\pi_1\pi_2$ هم‌پیوند است؛ توجه کنیم، در این‌جا از این فرض استفاده کرده‌ایم که همهٔ بخشیاب‌ها اصلی‌اند)، و بنابراین تجزیهٔ هر بخشیاب (α) به ضرب عامل‌های اول، با دقت تا هم‌پیوندی، یگانه است.

به‌این ترتیب، هرچه تعداد بخشیاب‌های غیراصلی بیشتر باشد، ویژگی‌های بخش‌پذیری عضوهای حلقهٔ D کمتر است، یعنی ویژگی‌های نظریهٔ بخشیاب‌ها، از ویژگی‌های بخش‌پذیری در عددهای طبیعی دورتر می‌شوند. برای این‌که این مطلب را با مفهوم دقیق‌تری بیان کنیم، دو بخشیاب σ و $\natural$ را هم‌ارز می‌نامیم (و به‌صورت $\sigma \sim \natural$ نشان می‌دهیم) وقتی که تنها در بخشیاب‌های اصلی با هم اختلاف داشته‌باشند، یعنی عضوهای $\alpha, \beta \in D^*$ وجود داشته‌باشند، به‌نحوی‌که

$$(\alpha)\sigma = (\beta)\natural$$

روشن است که این رابطه، به‌واقع یک رابطهٔ هم‌ارزی است (این رابطه، دارای ویژگی‌های انعکاسی، تقارنی و سرایت‌پذیری است)؛ بنابراین، تک‌وارهٔ $\mathcal{D}$ به خانواده‌های $\{\sigma\}$ از بخشیاب‌های هم‌ارز با یکدیگر تقسیم می‌شود. روشن است، دستور $\{\sigma\}\{\natural\} = \{\sigma\natural\}$، ضرب خانواده‌های بخشیاب‌ها را تعریف می‌کند. این ضرب، شرکت‌پذیر و جابه‌جایی‌پذیر است، به‌نحوی‌که مجموعهٔ $\mathcal{H}$ همهٔ خانواده‌های بخشیاب‌ها، نسبت به ضرب، یک تک‌واره است. این تک‌واره (دقیق‌تر، تعداد عضوهای آن)، انحراف حساب D از حساب عددهای طبیعی را اندازه‌گیری می‌کند.

یادآوری می‌کنیم، هر بخشیاب اصلی با بخشیاب یکه هم‌ارز است، یعنی خانوادهٔ آن عبارت است از یکهٔ تک‌وارهٔ $\mathcal{H}$. عکس این حکم هم درست است: اگر $\sigma \sim \check{\mathrm{o}}$، یعنی $(\alpha)\sigma = (\beta)$، آن‌وقت، باتوجه به اصل موضوع ۱، عضوی مثل γ وجود دارد که داشته‌باشیم $\alpha\gamma = \beta$ که به‌معنای $(\alpha)(\gamma) = (\beta)$ یا $\sigma = (\gamma)$ است. به‌این ترتیب، بخشیاب وقتی و تنها وقتی با بخشیاب یکه هم‌ارز است که بخشیاب اصلی باشد:

$$\sigma \sim \check{\mathrm{o}} \Leftrightarrow \sigma = (\alpha)$$

درحالتی‌که تک‌واره $\mathcal{H}$ محدود باشد، تعداد عضوهای آن، یعنی تعداد خانواده‌های بخشیاب‌های حلقهٔ D را، با نماد h نشان می‌دهیم. بنابر اثباتی که در بالا آوردیم، در حلقهٔ D وقتی و تنها وقتی قضیهٔ اصلی حساب صدق می‌کند که تک‌وارهٔ $\mathcal{H}$ شامل تنها یک عضو باشد، یعنی عدد h معین و برابر ۱ باشد.

به نظریهٔ بخشیاب‌ها، دو اصل موضوع دیگر را هم اضافه می‌کنیم.

اصل موضوع ۴. تک‌وارهٔ $\mathcal{H}$، یک گروه (و آبلی) است، یعنی هر عضو آن وارن‌پذیر است.

اصل موضوع ۵. در گروه $\mathcal{H}$، عضوهای مرتبهٔ l وجود ندارد.

در اصل موضوع اخیر، مثل جاهای دیگر، عدد معین و مفروض اول را با l نشان می‌دهیم.

از اصل موضوع‌های ۴ و ۵ نتیجه می‌شود، اگر $\sigma^l = \natural^l$، آن‌وقت $\sigma \sim \natural$. در واقع، هم‌ارزی $\sigma^l \sim \natural^l$، به این معنا است که برای خانواده‌ها برابری $\{\sigma\}^l = \{\natural\}^l$ برقرار است، یعنی (چون $\mathcal{H}$ گروه است)، داریم: $(\{\sigma\}\{\natural\}^{-1})^l = \{\check{o}\}$. ولی چون در گروه $\mathcal{H}$، عضو مرتبهٔ l وجود ندارد، برابری اخیر تنها وقتی ممکن است که داشته‌باشیم: $\{\sigma\}\{\natural\}^{-1} = \{\check{o}\}$، یعنی وقتی‌که $\{\sigma\} = \{\natural\}$ یا $\sigma \sim \natural$.

به‌یاد بیاوریم، اگر گروه $\mathcal{H}$ محدود باشد، آن‌وقت اصل موضوع ۵ به این معنا است که عدد اول l بخشیابی از تعداد خانواده‌های h (یعنی مرتبهٔ گروه) نیست.

اکنون دوباره به قضیهٔ فرما برمی‌گردیم.

عدد اول l را «سامان‌پذیر» گوییم، وقتی حلقهٔ D_l دارای نظریهٔ بخشیاب‌ها باشد، به‌نحوی که اصل موضوع‌های ۴ و ۵ در آن صدق کند. توجه کنیم که در اصل موضوع ۵، عدد l که در ساختمان حلقهٔ D_l وجود دارد، شرکت کرده‌است.

گزارهٔ ۱. برای هر عدد اول سامان‌پذیر l، گزارهٔ کمکی بخش ۸، درست است.

اثبات. اگر

$$x^l + y^l = z^l$$

آن‌وقت

$$(x+y)(x+\zeta y)\dots(x+\zeta^{l-1}y) = z^l$$

اگر از این برابری به بخشیاب برویم، می‌بینیم که اثبات گزارهٔ ۱ از بخش ۸ را می‌توان جزء‌به‌جزء، دربارهٔ آن به‌کار برد، به‌شرطی که π را، به‌جای عضو اول، بخشیاب اول درنظر بگیریم. بنابراین، همه بخشیاب‌های به‌صورت

$$(x+\zeta^m y),\ 0 \le m < l-1$$

دوبه‌دو نسبت به هم اول‌اند. به‌این ترتیب، از آن‌جاکه حاصل‌ضرب این بخشیاب‌ها از درجهٔ lاُم است (این حاصل‌ضرب برابر است با بخشیاب $(z)^l$)، نتیجه می‌شود، هرکدام از آن‌ها از درجهٔ l است. بنابراین، به‌ویژه چنان بخشیابی مثل $\sigma \in \mathcal{D}$ وجود دارد که داشته‌باشیم:

$$(x + \zeta y) = (\sigma^l)$$

این برابری به‌معنای $\sigma^l \sim \check{o}$ است که از آن‌جا باید داشته‌باشیم $\sigma \sim \check{o}$، یعنی $\sigma = (\alpha)$ (برای برخی عضوهای $\alpha \in D_l$). به‌این ترتیب

$$(x + \zeta y) = (\alpha^l)$$

و بنابراین، عددهای $x + \zeta y$ و α^l هم‌پیوندند، یعنی واحدی مثل $\varepsilon \in D_l$ وجود دارد که داشته‌باشیم:

$$x + \zeta y = \varepsilon \alpha^l$$

به‌این ترتیب، باتوجه به بخش ۸، برای عددهای اول سامان‌پذیر، حالت اول قضیهٔ فرما ثابت می‌شود:

قضیه. اگر عدد اول $l \geq 3$ سامان‌پذیر باشد، آن‌وقت برابری

$$x^l + y^l = z^l$$

به‌شرط گویا و درست بودن عددهای x، y و z، تنها وقتی ممکن است که دست‌کم یکی ازاین عددها بر عدد l بخش‌پذیر باشد.

البته این قضیه باید برای تکمیل خود، بررسی‌هایی به‌دنبال داشته‌باشد: کدام عددهای اول سامان‌پذیرند و چگونه می‌توان تشخیص داد، عدد اول مفروضی که در اختیار داریم، سامان‌پذیر است یا سامان‌ناپذیر؟ و طبیعی است، بدون این بررسی، قضیهٔ ما هیچ‌گونه ارزش عملی ندارد. ولی اکنون در این‌جا این پرسش را کنار می‌گذاریم و به‌حالت دوم قضیهٔ فرما می‌پردازیم.

۱۰

حالت دوم قضیهٔ فرما

در این بخش ثابت می‌کنیم، برای نماهای اول سامان‌پذیر l، حالت دوم قضیهٔ فرما باز هم درست است، یعنی برابری

$$x^l + y^l = z^l \qquad (۱)$$

وقتی هم که یکی از عددهای غیرصفر x، y و z بخش‌پذیر بر l باشد، ممکن نیست.

چون عددهای x، y و z را دوبه‌دو نسبت به هم اول گرفته‌ایم، تنها یکی از آن‌ها می‌تواند بر l بخش‌پذیر باشد. فرض می‌کنیم عدد z بر l بخش‌پذیر است. این فرض به کلی بودن مطلب لطمه‌ای نمی‌زند، زیرا اگر در مثل y بر l بخش‌پذیر باشد، کافی است برابری (۱) را به‌این صورت بنویسیم:

$$x^l + (-z)^l = (-y)^l$$

فرض کنید $z = l^k z_۰$ که در آن، $z_۰$ بر l بخش‌پذیر نیست و $k \geq ۱$. از آن‌جاکه در حلقهٔ D_l داریم:

$$l = \varepsilon_۰ \lambda^{l-۱},\ \lambda = ۱ - \zeta$$

که در آن $\varepsilon_۰$ یک واحد است (بخش ۶، دستور (۱۴) را ببینید)، می‌توان برابری (۱) را به‌صورت زیر نوشت (دوباره $z_۰$ را z نامیده‌ایم و فرض کرده‌ایم: $m = k(l-۱)$):

$$x^l + y^l = \varepsilon \lambda^{lm} z^l \qquad (۲)$$

که در آن، ε واحد است. در این‌جا x، y، z نسبت به l و بنابراین (اگر به‌عنوان عضوهای حلقهٔ D_l درنظر گرفته شوند) نسبت به λ اول‌اند.

ثابت می‌کنیم، برابریِ از نوع (۲) ممکن نیست، حتا وقتی x، y، z عددهای دلخواهی از حلقهٔ D_l و نسبت به λ اول (و بنابراین مخالف صفر) باشند. به‌زبان دیگر، ثابت می‌کنیم حالت دوم قضیهٔ فرما (برای lهای سامان‌پذیر) در حلقهٔ D_l برقرار است.

یادآوری می‌کنیم، حالت اول قضیهٔ فرما (و درنتیجه قضیهٔ کامل فرما) هم در حلقهٔ D_l درست است. برای این اثبات، کافی است استدلال‌های دو بخش پیشین را اندکی پیچیده‌تر کنیم.

برخلاف حالت اول، نمی‌توانیم حالت دوم قضیهٔ فرما را تنها برای عددهای گویای درست ثابت کنیم: باید گزارهٔ نیرومندتری را که مربوط به عددهای D_l است، ثابت کرد (این شیوهٔ استدلال، در بسیاری از موقعیت‌های ریاضی پیش می‌آید: گزاره‌ای که بررسی می‌کنیم، وقتی ثابت می‌شود که ابتدا گزاره‌ای کلی‌تر و نیرومندتر از آن را ثابت کنیم).

ضمن اثبات گزاره، از این موضوع استفاده می‌کنیم که بخشیاب اصلیِ $(\lambda) = (\lambda = ۱ - \zeta)l$، بخشیاب اول است. خود این حقیقت را، بعد و در بخش ۱۱ ثابت خواهیم کرد و در این‌جا، برای این‌که رشتهٔ بحث پاره نشود، آن را بدون اثبات می‌پذیریم.

عدد α از حلقهٔ D_l را «نیم‌مقدماتی» می‌نامیم (و در این‌جا به سرچشمهٔ این نام‌گذاری نمی‌پردازیم) که بر l (و درنتیجه بر λ) بخش‌پذیر نباشد و درضمن، چنان عدد گویا و درست $b_۰$ (که البته مخالف صفر است) وجود داشته‌باشد، به‌نحوی‌که تفاضل $\alpha - b_۰$ بر $l^۲$ بخش‌پذیر باشد (یعنی $\alpha \equiv b_۰ (\mathrm{mod}\lambda^۲)$).

به‌زبان دیگر، عدد α وقتی نیم‌مقدماتی است که در تجزیهٔ (۱۵) آن از بخش ۶، عدد $b_۰$ بر l بخش‌ناپذیر و $b_۱ = ۰$ باشد.

به‌سادگی دیده می‌شود، برای هر $\alpha \in D_l$ که بر l بخش‌ناپذیر است، چنان عدد گویای درستی مثل a وجود دارد که حاصل‌ضرب $\zeta^a \alpha$ نیم‌مقدماتی باشد.

در واقع، باتوجه به دستور (۱۵) از بخش ۶

$$\alpha \equiv b_۰ + b_۱\lambda (\mathrm{mod}\lambda^۲)$$

که در آن، بنابر شرط $b_۰ \not\equiv ۰ (\mathrm{mod}l)$. فرض کنید $a_۰$ همان عدد گویای درستی باشد که برای آن $a_۰ b_۰ \equiv ۱ (\mathrm{mod}l)$ و فرض کنید $a = a_۰ b_۱$. چون

$$\zeta^a = (۱ - \lambda)^a \equiv ۱ - a\lambda (\mathrm{mod}\lambda^۲)$$

بنابراین

$$\zeta^a\alpha = (1-a\lambda)(b_0+b_1\lambda) \equiv b_0 + (b_1 - a_1 b_0)\lambda (\mathrm{mod}\lambda^2)$$

ولی، بنابر ساختمان، $b_1 - ab_0 \equiv b_1(1-a_0b_0)$ بر l و بنابراین بر λ بخش‌پذیر است.

درنتیجه $\zeta^a\alpha \equiv b_0 (\mathrm{mod}\lambda^2)$.

چون $\zeta^l = 1$، اگر عددهای x، y، z را در توانی از عدد ζ ضرب کنیم، برابری (۲) تغییر نمی‌کند. بنابراین، بی‌آن‌که به کلی بودن مطلب لطمه‌ای وارد شود، می‌توان همهٔ عددهای x، y و z را در برابری (۲)، نیم مقدماتی به‌حساب آورد. یادآوری می‌کنیم که، با این فرض، نمای m بی‌تغییر می‌ماند.

بعد از این مقدمه‌ها، می‌توانیم به‌طور مستقیم، ناممکن بودن برابریِ از نوع (۲) را ثابت کنیم.

از برهان خُلف استفاده و فرض می‌کنیم، برابری‌هایی از نوع (۲) وجود داشته‌باشد. از بین این‌گونه برابری‌ها، آن را انتخاب می‌کنیم که نمای m در آن، کوچک‌ترین باشد (عددهای x، y و z نیم‌مقدماتی و نسبت به l اول‌اند). برای این‌که به نام‌گذاری‌های تازه‌ای متوسل نشویم، برابریِ انتخابی را، همان برابری (۲) می‌گیریم.

یادآوری می‌کنیم، اکنون دیگر m، در حالت کلی، به‌صورت $k(l-1)$ نیست. باوجود این، دست‌کم، پیش‌قضیه‌ای که می‌آوریم، درست است:

پیش‌قضیهٔ ۱. نمای m، از واحد بزرگ‌تر است:

$$m > 1$$

اثبات. برابری (۲) را، با تجزیهٔ سمت چپ آن به عامل‌ها، به‌این صورت می‌نویسیم:

$$(x+y)(x+\zeta y)\dots(x+\zeta^{l-1}y) = \varepsilon\lambda^{lm}z^l \qquad (۳)$$

چون $\downarrow = \downarrow(\lambda)$ اول است، بنابراین دست‌کم یکی از عامل‌ها باید بر $\downarrow$ بخش‌پذیر باشد. ولی از آن‌جاکه همهٔ این عامل‌ها، نسبت به مدول λ، با

یکدیگر هم‌نهشت‌اند (زیرا $(x+\zeta^a y)-(x+\zeta^b y)=\zeta^a(1-\zeta^{b-a})\ y$ بر $\lambda=1-\zeta$ بخش‌پذیر است)، بنابراین هرکدام از آن‌ها بر $\downarrow$ بخش‌پذیر است؛ به‌ویژه، $x+y$ هم بر $\downarrow$ بخش‌پذیر است.

چون عددهای x و y نیم‌مقدماتی‌اند، عدد گویای درستی مثل a وجود دارد که

$$x+y\equiv a(\mathrm{mod}\lambda^2)$$

(عدد $x+y$، نیم‌مقدماتی نیست، زیرا بر λ بخش‌پذیر است). این هم‌نهشتی نشان می‌دهد که عدد گویا و درست a بر λ بخش‌پذیر است. ولی در این‌صورت، بر l، یعنی λ^{l-1} بخش‌پذیر می‌شود. بنابراین a به‌روشنی بر λ^2 بخش‌پذیر می‌شود، یعنی عدد $x+y$ هم بر λ^2 بخش‌پذیر است.

به‌این ترتیب، در برابری (۳)، همهٔ عامل‌های سمت چپ بر λ، حتا نخستینِ آن‌ها بر λ^2، بخش‌پذیرند. از این‌جا نتیجه می‌شود، سمت چپ این برابری بر λ^{l+1} بخش‌پذیر است؛ بنابراین، سمت راست برابری هم بر λ^{l+1} بخش‌پذیر می‌شود. چون z و λ نسبت به هم اول‌اند، این نتیجه تنها وقتی ممکن است که داشته‌باشیم: $m>1$.

آن‌چه را دربارهٔ بخش‌پذیری عامل‌های سمت چپ برابری (۳) بر λ گفتیم، می‌توان دقیق‌تر کرد:

پیش‌قضیهٔ ۲. عددهای

$$x+\zeta y,\ldots,x+\zeta^{l-1}y \qquad (۴)$$

بر λ بخش‌پذیر و بر λ^2 بخش‌ناپذیرند. عدد

$$x+y$$

بر $\lambda^{l(m-1)+1}$ بخش‌پذیر و بر $\lambda^{l(m-1)+2}$ بخش‌ناپذیر است.

اثبات. کافی است ثابت کنیم، هیچ‌کدام از عددهای (۴) بر λ^2 بخش‌پذیر نیست. فرض کنیم، عدد $x+\zeta^k y$ بر λ^2 بخش‌پذیر باشد. در این‌صورت، عدد

$$(1-\zeta^k)y=(x+y)-(x+\zeta^k y)$$

هم باید بر $\lambda^۲$ بخش‌پذیر باشد؛ یعنی عدد $\zeta^k - ۱$ بر $\lambda^۲$ بخش‌پذیر است که ممکن نیست، زیرا می‌دانیم عدد $\zeta^k - ۱$ با $\lambda = ۱ - \zeta$ هم‌پیوند است.

اکنون فرض کنید، $\mathfrak{m}$ بزرگ‌ترین بخشیاب مشترک بخشیاب‌های اصلی (x) و (y) باشد. چون x و y بر $(\lambda) = \downarrow$ بخش‌پذیر نیستند، بنابراین m هم بر $\downarrow$ بخش‌ناپذیر است. به‌این ترتیب، باتوجه به پیش‌قضیهٔ ۲، بخشیاب‌های به‌صورت $(x + \zeta^k y)$ با شرط $k \neq ۰$، بر $\mathfrak{m} \downarrow$ و بخشیاب $(x + y)$ حتا بر $\mathfrak{m} \downarrow^{l(m-۱)+۱}$ بخش‌پذیر می‌شود. فرض کنید

$$(x + y) = \downarrow^{l(m-۱)+۱} \mathfrak{m}\varsigma_۰$$
$$(x + \zeta^k y) = \downarrow \mathfrak{m}\varsigma_k,\ k = ۱, \ldots, l - ۱ \qquad (۵)$$

بنابر پیش‌قضیهٔ ۲، هیچ‌یک از بخشیاب‌های $\varsigma_۰$، $\varsigma_۱$، $\varsigma_{l-۱}$ بر $\downarrow$ بخش‌پذیر نیست.

پیش‌قضیهٔ ۳. بخشیاب‌های $\varsigma_۰$، $\varsigma_۱$، ...، $\varsigma_{l-۱}$ دوبه‌دو نسبت به هم اول‌اند.

اثبات. فرض کنید، بخشیاب‌های ς_i و σ_k $(۰ \leq i < k \leq l - ۱)$، دارای بخشیاب مشترک $\wp$ باشند. در این‌صورت عددهای $x + \zeta^i y$ و $x + \zeta^k y$ بر $\mathfrak{m}\wp \downarrow$ بخش‌ناپذیرند و بنابراین عددهای

$$(x + \zeta^k y)\zeta^i - (x + \zeta^i y)\zeta^k = \zeta^i(۱ - \zeta^{k-i})x,$$
$$-(x + \zeta^k y) + (x + \zeta^i y) = \zeta^i(۱ - \zeta^{k-i})y$$

هم بر $\mathfrak{m}\wp \downarrow$ بخش‌پذیر می‌شوند. چون عامل $\zeta^i(۱-\zeta^{k-i})$ با $\lambda = ۱-\zeta$ هم‌پیوند است؛ نتیجه می‌شود که عددهای x و y بر $\mathfrak{m}\wp$ بخش‌پذیرند، که تعریف بزرگ‌ترین بخشیاب مشترک را نقض می‌کند.

اگر در (۳) به بخشیاب‌ها برویم و عبارت‌های (۵) را برای آن‌ها درنظر بگیریم (بعد از ساده کردن به $\downarrow^{lm}$) به این برابری می‌رسیم:

$$\mathfrak{m}^l \varsigma_۰ \varsigma_۱ \ldots \varsigma_l = \Im^l$$

که در آن $\mathfrak{F} = (z)$. چون بخشیاب‌های ς_0، ς_1، ... ς_l دوبه‌دو نسبت به هم اول‌اند، این برابری تنها وقتی برقرار است که این بخشیاب‌ها از درجهٔ lام، یعنی به‌این صورت باشند:

$$\varsigma_i = \sigma_i^l,\ i = 0, 1, \ldots, l-1 \qquad (۶)$$

که در آن σ_i یک بخشیاب است (و البته بخشیابی که بر $\downarrow$ بخش‌پذیر نیست).

پیش‌قضیهٔ ۴. بخشیاب‌های σ_0، σ_1، ...، σ_{l-1} هم‌ارزند (و متعلق به یک حلقه).

اثبات. اگر عبارت‌های (۶) را در (۵) قرار دهیم، به‌دست می‌آید:

$$(x+y) = \downarrow^{l(m-1)+1} \mathrm{m}\sigma_0^l,$$
$$(x+\zeta^k y) = \downarrow \mathrm{m}\sigma_k^l,\ k = 1, \ldots, l-1$$

اگر این برابری‌ها را «به‌صورت چلیپایی» در هم ضرب و به $\downarrow \mathrm{m}$ ساده کنیم، به این رابطه می‌رسیم:

$$(x+y)\sigma_k^l = (x+\zeta^k y)(\downarrow^{m-1} \sigma_0)^l, k = 1, \ldots, l-1 \qquad (۷)$$

که به‌معنای $\sigma_k^l \sim (\downarrow^{m-1} \sigma_0)^l$ است. چون عدد l سامان‌پذیر است، بنابراین از این‌جا نتیجه می‌شود: $\sigma_k \sim \downarrow^{m-1} \sigma_0$. ولی بخشیاب $\downarrow = (\lambda)$ اصلی و بنابراین $\downarrow^{m-1} \sigma_0 \sim \sigma_0$. به‌این ترتیب، برای هر k (۱، ...، $l-1$) داریم: $\sigma_k = \sigma_0$.

باتوجه به پیش‌قضیهٔ ۴، عددهای $\alpha_k, \beta_k \in D_l$ وجود دارند به‌نحوی‌که

$$(\alpha_k)\sigma_0 = (\beta_k)\sigma_k, k = 1, \ldots, l-1 \qquad (۸)$$

چون بخشیاب‌های $\sigma_i (i = 0, 1, \ldots, l-1)$ بر $\downarrow = (\lambda)$ بخش‌پذیر نیستند، بنابراین بدون این‌که به کلی بودن مطلب لطمه‌ای وارد شود، می‌توان عددهای α_k و β_k را بخش‌ناپذیر بر λ درنظر گرفت.

اگربرابری‌های (۷)رادر $(\alpha_k\beta_k)^l$ ضرب و از رابطهٔ (۸) استفاده کنیم، به‌این رابطه بین بخشیاب‌های اصلی می‌رسیم:

$$(x+y)(\alpha_k)^l = (x+\zeta^k y)(\lambda^{m-1}\beta_k)^l,\ k = 1,\dots,l-1$$

ولی برابری بخشیاب‌های اصلی با برابری متناظر عددها، با دقت تا عامل‌هایی که واحدند، یگانه است. بنابراین

$$(x+\zeta^k y)\lambda^{l(m-1)}\beta_k^l = (x+y)\varepsilon_k\alpha_k^l \qquad (۹)$$

که در آن، ε_k واحدی از حلقهٔ D_l است. ما به این برابری، تنها برای $k=1$ و $k=2$ نیاز داریم.

پیش‌قضیهٔ ۵. در حلقهٔ D_l عددهای x_1، β و z_1 که بر λ بخش‌پذیر نیستند (و بنابراین مخالف صفرند) و واحدهای ε_0 و ε وجود دارند، به‌نحوی‌که

$$x_1^l + \varepsilon_0\beta^l = \varepsilon\lambda^{l(m-1)}z_1^l \qquad (۱۰)$$

اثبات. ثابت می‌کنیم، برابری (۱۰) به‌ازای

$$x_1 = \alpha_1\beta_2,\ \beta = \alpha_2\beta_1,\ z_1 = \beta_1\beta_2,$$
$$\varepsilon_0 = \frac{\varepsilon_2}{\varepsilon_1(1+\zeta)},\ \varepsilon = \frac{\zeta}{\varepsilon_1(1+\zeta)}$$

برقرار است (روشن است، عدد $\zeta+1$، واحد است).
از آن‌جا

$$(x+\zeta y)(1+\zeta) - (x+\zeta^2 y) = (x+y)\zeta$$

بنابراین، اگر این برابری را در $\lambda^{l(m-1)}$ ضرب و از رابطهٔ (۹) به‌ازای $k=1$ و $k=2$ استفاده کنیم، به‌دست می‌آید:

$$(x+y)\left(\frac{\alpha_1}{\beta_1}\right)^l\varepsilon_1(1+\zeta) - (x+y)\left(\frac{\alpha_2}{\beta_2}\right)^l\varepsilon_2 =$$
$$= (x+y)\zeta\lambda^{l(m-1)}$$

اگر این برابری را به $(x+y)$ ساده و سپس در $(\beta_1\beta_2)^l\varepsilon_1^{-1}(1+\zeta)^{-1}$ ضرب کنیم، به (۱۰) می‌رسیم.

اکنون دیگر، بدون هیچ دشواری می‌توانیم تناقض را آشکار کنیم.

همان‌طور که می‌دانیم، برای عدد x_1، عدد گویای درستی مثل b_0 وجود دارد (که بر λ و بنابراین بر l بخش‌پذیر نیست)، به‌نحوی که $x_1 - b_0$ بر λ بخش‌پذیر باشد. ولی در این‌صورت $(x_1 - b_0)^l$ بر λ^l و درنتیجه بر $l \sim \lambda^{l-1}$ بخش‌پذیر می‌شود. از طرف دیگر، چون

$$(x_1 - b_0)^l \equiv x_1^l - b_0^l (\mathrm{mod} l)$$

نتیجه می‌گیریم که، به شرط $a = b_0^l$:

$$x_1^l \equiv a (\mathrm{mod} l)$$

به‌همین ترتیب، ثابت می‌شود، عدد گویای درست b (بخش‌ناپذیر بر λ) وجود دارد، به‌نحوی‌که

$$\beta^l \equiv b (\mathrm{mod} l)$$

از طرف دیگر، چون $l(m-1) \geq l > l-1$ (پیش‌قضیهٔ ۱ را ببینید)، بنابراین سمت راست رابطهٔ (۱۰) بر $l \sim \lambda^{l-1}$ بخش‌پذیر است؛ بنابراین، سمت چپ این رابطه هم بر l بخش‌پذیر می‌شود. به‌زبان دیگر

$$a + \varepsilon_0 b \equiv 0 (\mathrm{mod} l)$$

ولی b بر l بخش‌پذیر نیست و عدد درستی مثل b' وجود دارد که داشته‌باشیم: $bb' \equiv 1 (\mathrm{mod} l)$. درنتیجه

$$\varepsilon_0 \equiv b'b\varepsilon_0 \equiv -b'a (\mathrm{mod} l)$$

و از این‌جا ثابت می‌شود، واحد ε_0 در شرط پیش‌قضیهٔ کومر از بخش ۷ صدق می‌کند. بنابراین از درجهٔ lام واحد دیگری مثل η است:

$$\varepsilon_0 = \eta^l$$

به‌این ترتیب، در حلقهٔ D_l، چنان عددهای $x_1, y_1 = \eta\beta$ و z_1 (که مخالف صفرند) وجود دارند که بر λ بخش‌پذیر نیستند، و همراه با واحد ε در این رابطه صدق می‌کنند:

$$x_1^l + y_1^l = \varepsilon\lambda^{l(m-1)} z_1^l$$

می‌بینیم با آغاز از برابری (۲) با نمای m، به برابری دیگری با نمای کوچک‌تر $m-1$ رسیدیم. ولی این، ممکن نیست، زیرا نمای m را کوچک‌ترین مقدار ممکن گرفته‌بودیم؛ به‌این ترتیب، ثابت می‌شود که برابری (۲) ممکن نیست.

کوتاه سخن، قضیهٔ فرما، برای همهٔ نماهای اول سامان‌پذیر ثابت شد.

قضیه. اگر عددهای اول $l \geq 3$ سامان‌پذیر باشند، برای عددهای گویا و درست x، y و z (به‌شرطی‌که غیر از صفر باشند)، برابری

$$x^l + y^l = z^l$$

ممکن نیست.

اکنون، تنها این مطلب باقی می‌ماند، ببینیم بین عددهای اول، کدام سامان‌پذیر و کدام سامان‌ناپذیرند، یعنی به بررسی مفهوم عدد اول سامان‌پذیر بپردازیم.

برای عددهای اول سامان‌پذیر تعریفی لازم است که در همهٔ عددهای اول صدق کند و درضمن بتوان عددهای اول سامان‌پذیر را از بین همهٔ عددهای اول جدا کرد. به‌ویژه معلوم می‌شود، باید به سراغ هر حلقه‌ای از D_l رفت که نظریهٔ بخشیاب‌ها را امکان دهد و درضمن، اصل موضوع ۴ در آن صدق کند.

این گزاره، حالت خاصی است از قضیهٔ کلیِ مربوط به حلقه‌های با عضوهای درست در میدان دلخواهی از عددهای جبری (پایان بخش ۱۲ را ببینید). این قضیهٔ کلی را، اول‌بار دِدِ کیند ثابت کرد (و به‌عنوان گزاره‌ای دربارهٔ حلقهٔ D_l، به‌وسیلهٔ کومر) و سپس به‌وسیلهٔ بسیاری از ریاضی‌دانان اثبات‌های دیگری پیدا کرد.

در این‌جا، همین قضیه را، با دنبال کردن اندیشهٔ دِدِ کیند ثابت می‌کنیم.

۱۱

نظریهٔ ایده‌آل‌ها

D را حلقه‌ای دلخواه می‌گیریم. زیرمجموعهٔ A از حلقهٔ D را ایده‌آل (ideal) می‌نامیم[۸] (این اصطلاح را دِدِ کیند، در رابطه با ایده‌آل‌های کومر انتخاب کرد)، وقتی‌که

۱) برای عضوهای دلخواه α و β از A، داشته‌باشیم: $\alpha \pm \beta \in A$؛

۲) برای هر $\alpha \in A$ و $\beta \in D$، داشته‌باشیم: $\alpha\beta \in A$.

نمونه‌ای از ایده‌آل، ایده‌آل صفر است که تنها شامل صفرِ حلقهٔ D باشد. از این به بعد، همهٔ ایده‌آل‌ها را غیرصفر درنظر می‌گیریم.

نمونهٔ ایده‌آل را یکانی گویند و ما گاهی آن را با نماد (۱) نشان می‌دهیم.

این مثال را می‌توان تعمیم داد. $\alpha \in D$ را عضو غیرصفر دلخواهی از حلقهٔ D فرض می‌کنیم. روشن است، همهٔ عضوهای حلقهٔ D که بر α بخش‌پذیرند، تشکیل ایده‌آل می‌دهند. این ایده‌آل را با نماد (α) نشان می‌دهیم و آن را ایده‌آل اصلیِ (principal ideal) مولدِ α می‌نامیم. به‌ازای $\alpha = ۱$ (همچنین وقتی α، واحد دلخواه دیگری باشد)، آن‌وقت به ایده‌آل یکانی می‌رسیم.

روشن است، اشتراک هر خانواده از ایده‌آل‌ها، خود یک ایده‌آل است. بنابراین، برای هر مجموعهٔ $X \subset D$، کوچک‌ترین ایده‌آل وجود دارد که شامل این مجموعه است (و عبارت است از اشتراک همهٔ ایده‌آل‌های شامل X). این ایده‌آل را با نماد (X) نشان می‌دهیم و آن را ایده‌آلِ با مولد مجموعهٔ X می‌نامیم.

به‌روشنی دیده می‌شود، ایده‌آل (X) از همهٔ عضوهای به‌صورت

$$\alpha_۱\xi_۱ + \alpha_۲\xi_۲ + \ldots + \alpha_n\xi_n$$

تشکیل شده‌است که در آن $\alpha_۱$، $\alpha_۲$، ...، α_n عضو D و $\xi_۱$، $\xi_۲$، ...، ξ_n عضو X هستند (ثابت کنید!).

اگر X شامل تعداد محدودی عضوهای $\xi_۱$، ...، ξ_n باشد، ایده‌آل (X) را با نماد $(\xi_۱, \ldots, \xi_n)$ نشان می‌دهند. به‌ویژه، به‌ازای $n = ۱$،

۸- این تعریف ایده‌آل تنها برای حلقه‌های جابه‌جایی‌پذیر است. (ویراستار).

ایده‌آل اصلی (ξ_1) به‌دست می‌آید.

حلقهٔ D، حلقهٔ ایده‌آل‌های اصلی نامیده می‌شود، به‌شرطی که هر ایده‌آل آن اصلی باشد. چون برابری $(\alpha,\beta)=(\delta)$، به‌صورتی دقیق هم‌ارز با این بیان است که δ بزرگ‌ترین بخشیاب مشترک عضوهای α و β و به‌صورت $\alpha x_0+\beta y_0$ است، می‌بینیم، در حالتی‌که هر ایده‌آل به‌وسیلهٔ دو عضو (یا دست‌کم، تعداد محدودی عضو) تولید می‌شود، این مفهوم ایده‌آل‌های اصلی، بر مفهومی که در بخش ۵ دادیم، منطبق می‌شود.

وقتی حلقهٔ D، اجازهٔ نظریهٔ بخشیاب‌ها را بدهد، مفهوم ایده‌آل اصلی را می‌توان با روش دیگری تعمیم داد. باتوجه به اصل موضوع ۲ از بخش ۹، برای هر بخشیاب σ در مجموعهٔ $[\sigma]$ از همهٔ عضوهای حلقهٔ D (با به‌حساب آوردن صفر) که بر σ بخش‌پذیرند، ویژگی ۱) ایده‌آل‌ها وجود دارد. ویژگی ۲) هم به‌روشنی در آن صدق می‌کند. بنابراین σ یک ایده‌آل است.

به‌این ترتیب، رابطهٔ $\sigma\to[\sigma]$ هر بخشیاب را به یک ایده‌آل تبدیل می‌کند و به‌روشنی، دارای این ویژگی است که، برای هر بخشیاب اصلی (α)، ایده‌آل متناظر $[(\alpha)]$ وجود دارد؛ و این، درست همان ایده‌آل اصلی (α) است که در بالا آوردیم. از همین‌جا، وجود یک نماد برای بخشیاب اصلی و ایده‌آل اصلی متناظر با آن تامین می‌شود؛ اگر دقت کافی داشته‌باشیم، این مطلب نمی‌تواند منجر به سوءتفاهم شود.

باتوجه به اصل موضوع ۳ از بخش ۹، نگاشت $\sigma\to[\sigma]$ از تک‌وارهٔ بخشیاب‌ها به مجموعهٔ ایده‌آل‌ها، یک‌به‌یک است، یعنی بخشیاب‌های مختلفِ آن، منجر به ایده‌آل‌های مختلف می‌شود. از این‌جا به‌نظر می‌رسد که بتوان بخشیاب‌ها را با ایده‌آل‌ها متحد کرد و نظریهٔ بخشیاب‌ها را با آغاز از ایده‌آل‌ها ساخت. اندیشهٔ دِدِکیند هم از همین‌جا سرچشمه می‌گیرد. از دیدگاه او، بخشیاب‌ها و ایده‌آل‌ها، یکی هستند.

باوجود این معلوم شد حلقه‌هایی وجود دارند که اجازهٔ نظریهٔ بخشیاب‌ها را می‌دهند، ولی در آن‌ها ایده‌آل‌هایی وجود دارد که به‌صورت $[\sigma]$ نیستند

(ازجمله می‌توان از حلقهٔ چندجمله‌ای‌های شامل دو متغیر نام برد و در آن، ایده‌آل همهٔ چندجمله‌ای‌های بدون مقدار ثابت را درنظر گرفت). بنابراین، در این حلقه‌ها، «تعداد زیادی» ایده‌آل است. از طرف دیگر، حلقه‌هایی یافت می‌شوند که تک‌وارهٔ ایده‌آل‌های اصلی آن‌ها، در تک‌وارهٔ آزاد نشانده نمی‌شود. در چنین حلقه‌هایی، در حالت کلی، نظریهٔ بخشیاب‌ها ممکن نیست. چنین است که در زمان ما، اختلاف جدی بین ایده‌آل‌ها و بخشیاب‌ها را پذیرفته‌اند.

برنامهٔ دِدِ کیند را به این دلیل دنبال می‌کنیم که، در حلقه‌های مربوط به عددهای جبری درست، ایده‌آل‌ها، تکه‌وارهٔ آزاد تشکیل می‌دهند و، در این حلقه‌ها، ایده‌آل‌های «اضافی» وجود ندارد.

آغاز اندیشهٔ دِدِ کیند را باید از تعریف ضرب ایده‌آل‌ها دانست.

A و B را دو ایده‌آلِ یک حلقهٔ D می‌گیریم. مجموعهٔ X از همهٔ عضوهای به‌صورت $\alpha\beta$ را (با فرض $\alpha \in A$، $\beta \in B$) درنظر می‌گیریم. این مجموعه، در حالت کلی یک ایده‌آل نیست. به‌عنوان AB ایده‌آلی را به‌حساب می‌آوریم که از ضرب ایده‌آل‌های A و B و به‌وسیلهٔ مولد X تولید شده‌باشد. باتوجه به آن‌چه گفته‌ایم، ایده‌آل AB از همهٔ عضوهای به‌صورت

$$\alpha_1\beta_1 + \alpha_2\beta_2 + \ldots + \alpha_n\beta_n$$

تشکیل شده‌است که در آن α_1، ...، α_n عضو A و β_1، ...، β_n عضو B هستند.

روشن است، این ضرب شرکت‌پذیر، جابه‌جایی‌پذیر و دارای واحد است (این واحد، عبارت است از $D = (1)$). به‌این ترتیب، نسبت به این ضرب، مجموعهٔ $Id(D)$ از همهٔ ایده‌آل‌های غیرصفر حلقهٔ D، یک تک‌واره است.

به‌سادگی روشن می‌شود، ایده‌آل اصلی که از ضرب عضوهای حلقهٔ D تولید می‌شود، عبارت است از حاصل‌ضرب ایده‌آل‌های اصلی متناظر:

$$(\alpha\beta) = (\alpha)(\beta) \qquad (1)$$

و این به‌معنای آن است که نگاشت $\alpha \to (\alpha)$ تک‌وارهٔ D^* در تک‌وارهٔ $Id(D)$، یک نگاشت همسانی (هوموومورفیسم) است.

اگر حلقهٔ D با نظریهٔ بخشیاب‌ها سازگار باشد، آن‌وقت نگاشت یک‌به‌یک $[\sigma] \to \sigma$ دارای همان ویژگی $[\sigma][\natural] \subset [\sigma\natural]$ برای بخشیاب‌های دلخواه σ و $\natural$ خواهد بود. باوجود این، وقتی تک‌واره $\mathcal{D}$ را در تک‌وارهٔ $Id(D)$ همسان می‌نامیم، به این معنی است که برای بخشیاب‌های σ و $\natural$، برابری $[\sigma][\natural] = [\sigma\natural]$ در حالت کلی برقرار نیست. این برابری تنها وقتی برقرار است که σ و $\natural$، ایده‌آل‌های اصلی باشند.

از دستور (۱) این نتیجه به‌دست می‌آید که، اگر عضو α بخشیابی از عضو γ باشد، آن‌وقت ایده‌آل (α) بخشیابی از ایده‌آل (γ) است. عکس این حکم هم درست است: اگر (α) بخشیابی از (γ) باشد، آن‌وقت α بخشیابی از γ است. در واقع، روشن است، هر ایده‌آل به‌صورت $(\alpha)B$ شامل همهٔ عضوهای به‌صورت $\alpha\beta$ است که در آن $\beta \in B$. بنابراین، اگر $(\alpha)B = (\gamma)$، آن‌وقت $\alpha\beta_\circ = \gamma$ $(\beta_\circ \in B)$، یعنی γ بر α بخش‌پذیر است.

به‌این ترتیب، برای نگاشت $\alpha \to (\alpha)$، اصل موضوع ۱ از نظریهٔ بخشیاب‌ها، صادق است.

توجه به این نکته هم سودمند است که، اگر $(\gamma)A = (\gamma)B$، آن‌وقت $A = B$ (امکان ساده کردن به ایده‌آل اصلی). در واقع، وقتی با برابری $\gamma(A) = (\gamma)B$ سروکارداریم، به این معنی است که هر عضو به‌صورت $\gamma\alpha$ $(\alpha \in A)$، می‌تواند به‌صورت $\gamma\beta$ $(\beta \in B)$ باشد و برعکس. اگر به γ ساده کنیم، معلوم می‌شود، هر عضو $\alpha \in A$ در B قرار دارد و برعکس.

چون $AB \subset A$، پس، اگر ایده‌آل C بر ایده‌آل A بخش‌پذیر باشد، آن‌وقت $C \subset A$ (توجه داشته‌باشید که، ایده‌آل بخشیاب «بزرگ‌تر» از ایده‌آل بخشی است).

عکس این حکم در همهٔ حالت‌هایی که ایده‌آل A اصلی باشد، درست است، یعنی اگر $C \subset (\alpha)$، آن‌وقت ایده‌آلی مثل B وجود دارد که برای آن

داشته‌باشیم: $C = (\alpha)B$. در واقع $C \subset (\alpha)$ به این معنی است که هر عضو $\gamma \in C$ به‌صورت $\alpha\beta$ است که در آن $\beta \in D$. فرض کنید، B مجموعهٔ چنان عضوهای $\beta \in D$ باشد که $\alpha\beta \in C$. بلافاصله قابل تحقیق است که B ایده‌آل است و $(\alpha)B = C$.

برای این‌که جلوتر برویم، باید برای D شرط‌های معینی را درنظر بگیریم. در این سمت تلاش نمی‌کنیم که کمترین تعداد شرط‌ها را جست‌وجو کنیم، بلکه شرط‌هایی را برای D درنظر می‌گیریم که ما را زودتر به هدف برساند و، درضمن، ما را از حلقه‌های D_l که همه‌جا به آن نیاز داریم، جدا نکند.

در آغاز، این شرط را درنظر می‌گیریم که در D، n عضو

$$\omega_1, \omega_2, \ldots, \omega_n$$

(n، عددی طبیعی است) وجود داشته‌باشد، به‌نحوی‌که هر عضو $\alpha \in D$، به‌طور یگانه به‌صورت

$$\alpha = a_1\omega_1 + a_2\omega_2 + \ldots + a_n\omega_n \qquad (2)$$

نشان داده شود (a_1، a_2، ...، a_n عددهایی گویا و درست‌اند). با زبان نظریهٔ گروه‌ها، این ویژگی به‌معنای آن است که، گروه جمع حلقهٔ D، شبکه‌ای (lattice) است (گروه آبلی آزاد) از مرتبهٔ n با پایهٔ ω_1، ω_2، ...، ω_n. حلقهٔ D_l، برای $n = l - 1$ و $\omega_1 = 1$، $\omega_2 = \zeta$، ...، $\omega_n = \zeta^{l-2}$، دارای این ویژگی است.

در نظریهٔ گروه‌ها ثابت می‌شود، هر زیرگروه A شبکهٔ D مرتبهٔ n، شبکه‌ای با مرتبهٔ $r \leq n$ است.

اثبات این گزاره را می‌آوریم.

A_k $(k = 1, \ldots, n+1)$ را زیرگروهی از گروه A فرض می‌کنیم که از عضوهای (۲) تشکیل شده‌باشد و برای آن داشته‌باشیم:

$$a_1 = \ldots = a_{k-1} = 0$$

(بنابراین $A_1 = A$ و $A_{n+1} = 0$). روشن است، برای هر مقدار k از ۱ تا n، مجموعهٔ همهٔ ضریب‌های a_k مربوط به عضوهای A_k، ایده‌آلی در حلقهٔ عددهای درست $\mathbf{Z}$ تشکیل می‌دهد (که درضمن، ممکن است برابر صفر باشد). ولی در این حلقه، همهٔ ایده‌آل‌ها اصلی‌اند (زیرا برای آن‌ها، الگوریتم تقسیمِ با باقی‌مانده وجود دارد) و بنابراین ضریب $a_k^{(0)}$ وجود دارد که این ایده‌آل را تولید می‌کند (در این‌جا، حالت $a_k^{(0)} = 0$ استفاده نمی‌شود). ξ_k را عضو دلخواهی از گروه A_k با این ضریب می‌گیریم (اگر $A_k^{(0)} = 0$، آن‌وقت فرض می‌کنیم $\xi_k = 0$).

ثابت می‌کنیم عضوهای ξ_1، ...، ξ_n، گروه A را تولید کنند، یعنی هر عضو $\alpha \in A$ به‌این صورت باشد:

$$\alpha = b_1\xi_1 + \ldots + b_n\xi_n \qquad (۳)$$

که در آن، b_1، ...، b_n عددهایی گویا و درست‌اند.

چون $A_{n+1} = 0$، بنابراین برای عضوهای A_{n+1}، دستور (۳) برقرار است. اگر از استقرای ریاضی استفاده کنیم، با فرض این‌که برای مقداری از $k \leq n$ ثابت شده‌باشد، که هر عضو A_{k+1} به‌صورت (۳) است (با $b_1 = \ldots = b_k = 0$)، ثابت می‌کنیم که در این‌صورت هر عضو $\alpha \in A_k$ هم به‌صورت (۳) است (با $b_1 = \ldots = b_{k-1} = 0$).

فرض کنید:

$$\alpha = a_k\omega_k + \ldots + a_n\omega_n$$

ضریب‌های a_k بر $a_k^{(0)}$ بخش‌پذیرند (اگر $a_k^{(0)} = 0$، آن‌وقت برای همهٔ عضوهای $\alpha \in A_k$ داریم $\alpha_k = 0$)، یعنی عدد درست b_k وجود دارد، به‌نحوی‌که داشته‌باشیم: $a_k = a_k^{(0)}b_k$. در این‌صورت $\alpha - b_k\xi_k \in A_{k+1}$ و درنتیجه

$$\alpha - b_k\xi_k = b_{k+1}\xi_{k+1} + \ldots + b_n\xi_n$$

و بنابراین $\alpha = b_k\xi_k + b_{k+1}\xi_{k+1} + \ldots + b_n\xi_n$.

در حالت کلی، ممکن است بین عضوهای ξ_1، ...، ξ_n، صفر وجود داشته‌باشد. اگر لازم باشد، با شماره‌گذاری این عضوها، می‌توانیم فرض کنیم:

$$\xi_1 \neq 0, \ldots, \xi_r \neq 0, \xi_{r+1} = 0, \ldots, \xi_n = 0$$

متناظر آن‌ها، با شماره‌گذاری پایهٔ ω_1، ...، ω_n، می‌توانیم فرض کنیم، برای k از ۱ تا n، مثل قبل $\xi_k \in A_k$، یعنی در عبارت‌های ξ_k برحسب پایهٔ ω_1، ...، ω_n، ضریب‌های ω_1، ...، ω_{k-1} برابر صفر باشند. ولی به‌جز آن، اکنون می‌توانیم حکم کنیم، برای k از ۱ تا r، ضریب $a_k^{(0)}$ از عضو ξ_k مخالف صفر است، زیرا بنابرساختمان، تنهابه‌ازای $\xi_k = 0$ داریم $a_k^{(0)} = 0$.

از این‌جا نتیجه می‌شود، عضوهای ξ_1، ...، ξ_r به هم بستگی ندارند و مستقل‌اند، یعنی برابری $a_1\xi_1 + \ldots + a_r\xi_r = 0$ (a_1، ...، a_r عددهایی گویا و درست‌اند)، تنها برای $a_1 = 0$، ...، $a_r = 0$ برقرار است. در غیر این‌صورت، کوچک‌ترین مقدار i را درنظر بگیرید که برای آن عدد a_i مخالف صفر باشد. در این‌صورت، در تجزیهٔ عضو

$$a_1\xi_1 + \ldots + a_r\xi_r = 0$$

برحسب پایهٔ ω_1، ...، ω_n، عدد $a_i a_i^{(0)}$ مخالف صفر می‌شود که ممکن نیست.

ثابت شد، هر عضو $\alpha \in A$، به‌طور یگانه، برحسب ξ_1، ...، ξ_r بیان می‌شود، یعنی A شبکه‌ای است با پایهٔ ξ_1، ...، ξ_r (و بنابراین از مرتبهٔ r است).

سپس، می‌دانیم، مرتبهٔ n شبکه، به انتخاب پایه بستگی ندارد و برابر است با حداکثر تعداد عضوهای مستقلِ شبکه.

درواقع، عضوهای پایه، بنابر تعریف، مستقل‌اند و هر $n+1$ عضو به هم وابسته‌اند (زیرا هر دستگاه شامل n معادلهٔ خطی همگن با $(n+1)$ مجهول و ضریب‌های درست، دارای جوابی غیرصفر در مجموعهٔ عددهای درست است).

یادآوری می‌کنیم، برخلاف حالت معمولی فضاهای خطی، نمی‌توان هر n عضو مستقل شبکه را به‌عنوان پایهٔ آن درنظر گرفت. برای این منظور، لازم و کافی است، دترمینان شامل ضریب‌های تجزیهٔ این عضوها برحسب عضوهای پایه، برابر ± 1 باشد (ضمیمه را در پایان همین بخش ببینید).

به‌جز این، از نظریهٔ گروه‌ها می‌دانیم، برای هر زیرشبکهٔ A از مرتبهٔ n، گروه بهری (یا گروه عامل =factor group) D/A، متناهی است.

در واقع، به‌ازای $r=n$، پایهٔ ξ_1، ...، ξ_n در A، به‌این صورت است:

$$\begin{aligned}
\xi_1 &= a_1^{(0)}\omega_1 + a_1^{(1)}\omega_2 + \ldots + a_1^{(n-1)}\omega_n,\\
\xi_2 &= a_2^{(0)}\omega_2 + \ldots + a_2^{(n-2)}\omega_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\xi_n &= a_n^{(0)}\omega_n
\end{aligned}$$

که در آن $a_1^{(0)} \neq 0$، ...، $a_n^{(0)} \neq 0$، و از آن‌جا بلافاصله نتیجه می‌شود، عضو به‌صورت

$$a_1\omega_1 + a_2\omega_2 + \ldots + a_n\omega_n$$

که در آن

$$0 \leq a_1 < |a_1^{(0)}|,\ 0 \leq a_2 < |a_2^{(0)}|, \ldots, 0 \leq a_n < |a_n^{(0)}|$$

دستگاه کاملی از همرده‌های زیرگروه A نسبت به گروه D را تشکیل می‌دهد. بنابراین D/A گروهی متناهی است از مرتبهٔ $|a_1^{(0)} \ldots a_n^{(0)}|$.

از این‌جا نتیجه می‌گیریم، تنها تعداد محدودی زیرگروه از گروه‌های D وجود دارد که شامل زیرگروه A هستند.

در واقع، در همسانی طبیعی $D \to D/A$، چنین زیرگروه‌هایی، در تناظر یک‌به‌یک با همهٔ زیرگروه‌های ممکن از گروه D/A هستند، و تعداد این زیرگروه‌ها محدود است.

همهٔ این گزاره‌ها را می‌توان دربارهٔ ایده‌آل دلخواه A از حلقهٔ D به‌کار برد، زیرا بنابر تعریف، ایده‌آل به‌ویژه عبارت است از زیرگروهِ گروه جمع حلقه. به‌این ترتیب، می‌بینیم، هر ایده‌آل A، یک شبکه‌است.

دوم، چون برای هر عضو $\alpha \in A$، عضوهای $\alpha\omega_1$، ...، $\alpha\omega_n$ از ایده‌آل A، مستقل‌اند، بنابراین هر ایده‌آل حلقهٔ D (که به‌عنوان یک شبکه درنظر گرفته می‌شود) از مرتبهٔ n است، یعنی ایده‌آل A، پایه‌ای شامل n عضو دارد.

این عضوها به‌روشنی ایده‌آل A را تولید می‌کنند، به‌نحوی که هر ایده‌آل A از حلقهٔ D به‌وسیلهٔ تعداد محدودی عضو تولید می‌شود، یعنی به‌صورت $A = (\alpha_1, \ldots, \alpha_m)$ است که در آن α_1، ...، α_m عضو D هستند (در حالت کلی، تعداد m ممکن است از مرتبهٔ n کمتر باشد).

سوم، از آن‌جاکه هر بخشیاب ایده‌آل A، زیرگروهی است شامل A، برای هر ایده‌آل حلقهٔ D، تنها محدودی از ایده‌آل مختلف و به‌ویژه، تنها تعداد محدودی بخشیاب وجود دارد. از این‌جا، با استقرا نتیجه می‌شود، هر ایده‌آل حلقهٔ D به ضرب ایده‌آل‌های اول تجزیه می‌شود (که البته، خود این ایده‌آل‌های اول قابل تجزیه نیستند).

به‌جز این، اکنون دیگر می‌توانیم ثابت کنیم، در برخی حالت‌ها، ساده کردن برابری ایده‌آل‌ها به‌وسیلهٔ ایده‌آل غیراصلی هم ممکن است. برای این منظور، به یک پیش قضیه نیاز داریم (که در آن، زیر نام «عددها»، می‌توان عضوهای حلقه‌ای دلخواه را درنظر گرفت):

پیش‌قضیهٔ ۱. فرض کنید:

$$\begin{Vmatrix} \beta_{11} & \ldots & \beta_{1n} \\ \ldots & \ldots & \ldots \\ \beta_{n1} & \ldots & \beta_{nn} \end{Vmatrix} \qquad (۴)$$

ماتریسی دلخواه، و ρ یک عدد باشد. اگر عددهایی مثل ξ_1، ...، ξ_n وجود داشته‌باشند، به‌نحوی که دست‌کم یکی از آن‌ها مخالف صفر و درضمن، برابری‌های

$$\begin{aligned}\rho\xi_1 &= \beta_{11}\xi_1 + \ldots + \beta_{1n}\xi_n\\ &\cdots\cdots\cdots\cdots\cdots\\ \rho\xi_n &= \beta_{n1}\xi_1 + \ldots + \beta_{nn}\xi_n\end{aligned} \qquad (۵)$$

برقرار باشد، آن‌وقت، عدد ρ ریشهٔ معادلهٔ

$$x^n + \beta_1 x^{n-1} + \ldots + \beta_n = 0 \qquad (۶)$$

است، که در آن، ضریب‌های β_1، ...، β_n برحسب درایه‌های ماتریس (۴) و به‌وسیلهٔ عمل‌های جمع، تفریق و ضرب بیان می‌شوند.

به‌یاری این پیش‌قضیه به‌سادگی ثابت می‌شود، برای ایده‌آل‌های دلخواه A و B، از برابری

$$AB = A$$

نتیجه می‌شود: $B = (1)$.

در واقع، فرض کنید ξ_1، ...، ξ_n پایهٔ ایده‌آل A باشد. در این‌صورت، هر عضو ایده‌آل AB را می‌توان به‌صورت $\xi_1\beta_1 + \ldots + \xi_n\beta_n$ نشان داد که در آن β_1، ...، β_n عضوهایی از B هستند. چون $AB = B$، معلوم می‌شود که برای ξ_1، ...، ξ_n، برابری‌های

$$\begin{aligned}\xi_1 &= \xi_1\beta_{11} + \ldots + \xi_n\beta_{1n}\\ &\cdots\cdots\cdots\cdots\cdots \quad \beta_{ij} \in B\\ \xi_n &= \xi_1\beta_{n1} + \ldots + \xi_n\beta_{nn}\end{aligned}$$

برقرار است، یعنی به‌ازای $\rho = 1$ برابر (۴) است. بنابراین عدد $\rho = 1$، ریشهٔ معادلهٔ به‌صورت (۶) است، یعنی برابری $\beta_n - \ldots - \beta_1 = -1$ برقرار است که در آن، β_1، ...، β_n برحسب β_{ij} از ایده‌آل B به‌وسیلهٔ عمل‌های جمع، تفریق و ضرب بیان می‌شوند و، بنابراین، متعلق به این ایده‌آل‌اند. ولی در این صورت $1 \in B$، یعنی $B = (1)$.

خودِ پیش‌قضیهٔ ۱، نتیجه مستقیمی از ساده‌ترین حقیقت‌های جبر خطی است. در واقع، برابری (۵) به این معنا است که

$$(\xi_1, \ldots, \xi_n) \neq (0, \ldots, 0)$$

جوابی از دستگاه معادله‌های خطی و همگن

$$\begin{aligned}
&(\beta_{11} - \rho)\xi_1 + \ldots + \beta_{1n}\xi_n = 0 \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&\beta_{n1}\xi_1 + \ldots + (\beta_{nn} - \rho)\xi_n = 0
\end{aligned}$$

است. ولی از جبر خطی می‌دانیم، اگر دستگاه n معادلهٔ خطی همگن با n مجهول، جوابی مخالف $(0, \ldots, 0)$ داشته‌باشد، آن‌وقت دترمینان ضریب‌های آن برابر صفر است:

$$\begin{vmatrix} \beta_{11} - \rho & \ldots & \beta_{1n} \\ \ldots & \ldots & \ldots \\ \beta_{n1} & \ldots & \beta_{n1} - \rho \end{vmatrix} = 0$$

که اگر دترمینان را باز کنیم، برای ρ، معادله‌ای به‌صورت (۶) به‌دست می‌آید.

برای این‌که جلوتر برویم، خانوادهٔ حلقه‌هایی را که در بررسی ما قرار دارد، باز هم تنگ‌تر ومحدودترمی‌کنیم. برای این منظور، برای حلقهٔ D، n نگاشت یک‌به‌یک $\alpha \to \alpha^{(i)}$ (برای i از ۱ تا n) را در میدان عددهای مختلط $\mathbf{C}$ با حفظ جمع و ضرب درنظر می‌گیریم (یعنی نگاشت‌هایی همسان و یک‌به‌یک و، درضمن به‌نحوی که برای هر $\alpha \in D$، چندجمله‌ای‌های متقارن مقدماتی نسبت به $\alpha^{(1)}$، ...، $\alpha^{(n)}$، عددهای گویا و درستی باشند (به زبان دیگر، چندجمله‌ای

$$(x - \alpha^{(1)})(x - \alpha^{(2)}) \ldots (x - \alpha^{(n)})$$

ضریب‌های درستی داشته‌باشد).

چنین نگاشت‌هایی را در بخش ۶، برای حلقهٔ D_l ساخته‌ایم.

برای حلقهٔ دلخواه D، هَنج (نُرم) $N\alpha$ از عضو $\alpha \in D$ را با این دستور وارد می‌کنیم:

$$N\alpha = \alpha^{(1)} \dots \alpha^{(n)}$$

این نُرم عددی گویا و درست است، ولی در حالت کلی ممکن است غیرمنفی نباشد (و بنابر آن‌چه گفته‌ایم، وقتی و تنها وقتی $N\alpha = 0$، که داشته‌باشیم: $\alpha = 0$). شبیه حالت حلقهٔ D_l، برای عضوهای α و β از حلقهٔ D هم، این برابری برقرار است.

$$N(\alpha\beta) = N\alpha \cdot N\beta$$

(زیرا برای هر $i = 1, \dots, n$، بنابر شرط داریم: $((\alpha\beta)^{(i)} = \alpha^{(i)}\beta^{(i)})$.

به‌جز این، برای هر عدد گویای a داریم:

$$Na = a^n$$

راحت‌تر است (ولی البته اجباری نیست)، حلقهٔ D را درون میدان $\mathbf{C}$ و به‌یاری نگاشت $\alpha \to \alpha^{(1)}$ «ملحق» کنیم، یعنی فرض کنیم $D \subset \mathbf{C}$ و $\alpha^{(1)} = \alpha$ برای هر $\alpha \in D$ (توجه کنیم که در حالت حلقهٔ D_l، وضع به همین گونه است).

اگر حلقهٔ D را مُلحق به میدان $\mathbf{C}$ درنظر بگیریم، می‌توانیم میدان کسرهای (field of fractions) K از حلقهٔ D را، خیلی ساده و به‌عنوان کوچک‌ترین زیرگروه میدان $\mathbf{C}$ تعریف کنیم که شامل حلقهٔ D باشد، یا به زبان دیگر، به‌عنوان مجموعهٔ همهٔ عددهایی از $\mathbf{C}$ که به‌صورت $\frac{\beta}{\alpha}$ باشند ($\alpha, \beta \in D$ و $\alpha \neq 0$)؛ و به‌این ترتیب، از مفهوم، اگرچه ساده، ولی همراه با فرایند انتزاعی دقیق ساختمان این میدان برای حلقهٔ D، که درون $\mathbf{C}$ ملحق نشده‌است، پرهیز کنیم.

در حالت حلقهٔ D_l، برای هر $i = ۱, \ldots, n$ $(n = l - ۱)$، فرض $a^{(i)} \in D$ را درنظر گرفته بودیم. اکنون، این فرض در حالت کلی، برقرار نیست. با وجود این، به‌سادگی دیده می‌شود که $\alpha^{(۲)} \ldots \alpha^{(n)}$ عضو D است (برای هر $\alpha \in D$)، یعنی $N\alpha$ بر α در D بخش‌پذیر است. در واقع، بنابر شرط، عدد $\alpha = \alpha^{(۱)}$ در معادلهٔ به‌صورت

$$\alpha^n + c_۱\alpha^{n-۱} + \ldots + c_{n-۱}\alpha + c_n = ۰$$

صدق می‌کند. ضریب‌های معادله درست‌اند، درضمن $N\alpha = (-۱)^n c_n$. بنابراین

$$\frac{N\alpha}{\alpha} = \frac{(-۱)^n c_n}{\alpha} = (-۱)^{n+۱}\frac{\alpha^n + c_۱\alpha^{n-۱} + \ldots + c_{n-۱}\alpha}{\alpha} =$$
$$= (-۱)^{n+۱}(\alpha^{n-۱} + c_۱\alpha^{n-۲} + \ldots + c_{n-۱}) \in D$$

از این‌جا و باتوجه به آن‌چه در بخش ۶ دیده‌ایم، نتیجه می‌شود، هر عضو $\xi = \frac{\beta}{\alpha}$ از میدان K را می‌توان به‌این صورت (و تنها به یک صورت از این‌گونه) نوشت:

$$\xi = x_۱\omega_۱ + \ldots + x_n\omega_n \qquad (۷)$$

که در آن $x_۱$، ...، x_n عددهایی گویا هستند (و البته، هر عدد ξ از این‌گونه، در K واقع است).

پیش‌قضیهٔ ۲. عدد طبیعیِ $T = T(D)$ وجود دارد که بستگی آن با حلقهٔ D به نحوی است که برای هر عضو $\xi \in K$، می‌توان $\alpha \in D$ و عدد طبیعی $s < T$ را پیدا کرد که برای آن‌ها داشته‌باشیم:

$$N(s\xi - \alpha) < ۱$$

اثبات. با درنظر گرفتن پایهٔ ω_1، ...، ω_n برای D، عدد طبیعی دلخواهی را به‌عنوان T انتخاب می‌کنیم که در این نابرابری صدق کند:

$$T > Q^n > \prod_{i=1}^{n}(|\omega_1^{(i)}| + \ldots + |\omega_n^{(i)}|)$$

که در آن، Q یک عدد طبیعی است.

روشن است، برای هر عضو (۷) از میدان K و هر عدد طبیعی i، می‌توان عضوی مثل $\alpha_i \in D$ به‌گونه‌ای انتخاب کرد که برای عضو

$$i\xi - \alpha_i = y_1\omega_1 + \ldots + y_n\omega_n \qquad (۸)$$

این نابرابری را داشته‌باشیم:

$$0 \leq |y_1| < 1, \ldots, 0 \leq |y_n| < 1$$

بازهٔ $[0, 1)$ در Q را، به بازه‌های به‌صورت زیر افراز می‌کنیم:

$$\left[\frac{J}{Q}, \frac{J+1}{Q}\right), J = 0, \ldots, Q-1 \qquad (۹)$$

هریک از مختصات y_1، ...، y_n از عددهای (۸)، در یکی از این بازه‌ها قرار دارد. بنابراین، روی‌هم Q^n امکان برای جا دادن این مختصات در بازه‌های (۹) وجود دارد. درنتیجه، اگر همهٔ عددهای (۸) را برای همهٔ مقدارهای i از ۰ تا Q^n درنظر بگیریم (یعنی روی‌هم $Q^n + 1$ عدد)، آن‌وقت دست‌کم دو عدد، ترکیب مشابهی در تقسیم مختصاتشان، در بازه‌های (۹) پیدا می‌کنند. اختلاف این عددها، به‌صورت $s\xi - \alpha$ است که در آن $s \in \mathbf{N}$ و $\alpha \in D$ است و مختصات آن در این نابرابری‌ها صدق می‌کند:

$$|y_1| < \frac{1}{Q}, \ldots, |y_n| < \frac{1}{Q}$$

بنابراین

$$|(s\xi-\alpha)^{(i)}|<\frac{1}{Q}(|\omega_1^{(i)}|+\ldots+|\omega_n^{(i)}|),\ i=1,\ldots,n$$

یعنی

$$|N(s\xi-\alpha)|<\frac{1}{Q^n}\prod_{i=1}^{n}(|\omega_1^{(i)}|+\ldots+|\omega_n^{(i)}|<1$$

برای کامل شدن اثبات، کافی است توجه کنیم که، عدد طبیعی ξ، تفاضل دو عدد طبیعی است که از Q^n تجاوز نمی‌کنند و درنتیجه ξ هم از Q^n تجاوز نمی‌کند و بنابراین از T کوچک‌تر است.

شبیه بخشیاب‌ها (دی‌وی‌زورها)، دو ایده‌آل A و B را هم‌ارز گوییم، وقتی ایده‌آل‌های اصلیِ (α) و (β) وجود داشته‌باشند، به‌نحوی‌که

$$(\alpha)A=(\beta)B$$

روشن است، مجموعهٔ همهٔ ایده‌آل‌ها، به خانواده‌هایی از ایده‌آل‌های هم‌ارز تقسیم می‌شود.

گزارهٔ ۱. برای هر حلقهٔ D، که با شرط‌های بالا سازگار باشد، تعداد خانواده‌های ایده‌آل‌ها، متناهی است.

اثبات. A را ایده‌آلی دلخواه می‌گیریم.

بین عددهای غیرصفر ایده‌آل A، عدد α_0 وجود دارد که، برای آن، عدد طبیعی $|N\alpha_0|$ کم‌ترین مقدار ممکن را دارد، به‌نحوی‌که، برای هر عضو غیرصفر $\alpha\in A$ داشته‌باشیم:

$$|N\alpha_0|\le|N\alpha|$$

α را عضو A می‌گیریم. با استفاده ازپیش‌قضیهٔ ۲ دربارهٔ عضو

$$\xi=\frac{\alpha}{\alpha_0}\in K$$

عدد طبیعی $s < T$ و عضو $\gamma \in D$ را پیدا می‌کنیم که در این رابطه صدق کنند:

$$\left| N\left(s\frac{\alpha}{\alpha_0} - \gamma\right)\right| < 1$$

یعنی

$$|n(s\alpha - \gamma\alpha_0)| < |N\alpha_0|$$

چون $s\alpha - \gamma\alpha_0 \in A$، این نابرابری تنها برای $s\alpha = \gamma\alpha_0$ برقرار است، و این، ثابت می‌کند که α_0 بخشیابی از $s\alpha$ است.

به‌این ترتیب، برای هر عضو $\alpha \in A$، عضو $\beta \in D$ وجود دارد که

$$\alpha_0\beta = S\alpha \qquad (10)$$

B را مجموعهٔ همهٔ این‌گونه βها (به‌ازای همهٔ αهای ممکن از A) می‌گیریم. روشن است، اگر β_1 و β_2 عضو B باشند، آن‌وقت $\beta_1 \pm \beta_2$ هم‌عضو B است (اگر $\alpha_0\beta_1 = S\alpha_1$ و $\alpha_0\beta_2 = S\alpha_2$، که در آن‌ها α_1 و α_2 عضوهایی از A هستند، آن‌وقت

$$\alpha_0(\beta_1 \pm \beta_2) = S(\alpha_1 \pm \alpha_2)$$

که در آن $(\alpha_1 \pm \alpha)_2 \in A$). به‌جز این، اگر $\alpha_0\beta = S\alpha$، آن‌وقت برای هر $\gamma \in D$ داریم: $\alpha_0(\beta\gamma) = S(\alpha\gamma)$، و بنابراین، $\beta\gamma \in B$ (زیرا $\alpha\gamma \in A$). از این‌جا ثابت می‌شود، B یک ایده‌آل است.

اکنون برابری (۱۰) به‌این معنی است که

$$(\alpha_0)B = (S)A$$

یعنی ایده‌آل B با ایده‌آل A هم‌ارز است.

به‌جز این، چون $\alpha_0 \in A$، بنابراین $(S)(\alpha_0) \subset (\alpha_0)B$، یعنی $(S) \subset B$.

ولی می‌دانیم، تعداد ایده‌آل‌هایی که شامل یک ایده‌آل ثابت (و در این‌جا، ایده‌آل (S)) باشند، محدود است. به‌این ترتیب، هر ایده‌آل A هم‌ارز ایده‌آل B -متعلق به مجموعهٔ محدودی از ایده‌آل‌ها- است.
بنابراین، تعداد خانواده‌های ایده‌آل‌ها، محدود است.

دوباره فرض کنید، A ایده‌آل دلخواهی (غیرصفر) از حلقهٔ D باشد. تلاش می‌کنیم ثابت کنیم، توانی از آن مثل A^m $(m \geq 0)$، یک ایده‌آل اصلی است.
از آن‌جاکه تعداد ایده‌آل‌های ناهم‌ارز محدود است، باید دو عدد مثل $p > 0$ و $q > 0$ وجود داشته‌باشند، به‌نحوی‌که داشته‌باشیم: $A^p \sim A^{p+q}$.
بنابر تعریف، این رابطه به‌معنای آن است که عضوهای $\alpha, \beta \in D^*$ وجود دارند که

$$(\alpha)A^p = (\beta)A^{p+q} \qquad (11)$$

ξ_1، ...، ξ_n را پایهٔ ایده‌آل A^p می‌گیریم. در این‌صورت، هر عضو ایده‌آل $A^{p+q} \subset A^p$ را می‌توان به‌صورت

$$a_1\xi_1 + \ldots + a_n\xi_n$$

نشان داد (a_1، ...، a_n عددهایی گویا و درست‌اند)، یعنی هر عضو ایده‌آل $(\beta)\ A^{p+q}$ را به‌صورت

$$\beta(a_1\xi_1 + \ldots + a_n\xi_n)$$

به‌ویژه، برای عضوهای

$$\alpha\xi_1, \ldots, \alpha\xi_n \in (\alpha)A^p = (\beta)A^{p+q}$$

چنین نمایشی به‌دست می‌آید. به‌این ترتیب، می‌بینیم با فرض

$$\rho = \frac{\alpha}{\beta} \in K$$

این برابری‌ها برقرارند:

$$\rho\xi_1 = a_{11}\xi_1 + \ldots + a_{1n}\xi_n$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\rho\xi_n = a_{n1}\xi_1 + \ldots + a_{nn}\xi_n$$

که در آن $a_{ij}(i,j = 1,\ldots,n)$ عددهایی گویا و درست‌اند. اگر در این برابری‌ها، از پیش‌قضیهٔ ۱ استفاده کنیم، معلوم می‌شود، ρ ریشه‌ای از یک معادلهٔ جبری درجهٔ n است:

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \qquad (12)$$

که در آن ضریب‌های a_1، ...، a_n عددهایی درست‌اند و ضریب بزرگ‌ترین درجه برابر واحد است.

D را «حلقهٔ بسته درست» (integrally closed ring) می‌نامیم، وقتی هر عضو ρ از میدان کسرهای K، که در معادله‌ای به‌صورت (۱۲) صدق می‌کند، متعلق به D باشد.

به‌این ترتیب، اگر D، حلقه بستهٔ درست باشد، آن‌وقت $\rho = \frac{\alpha}{\beta} \in D$، یعنی β بخشیابی از α است.

بنابراین، برابری (۱۱) را می‌توانیم به β ساده کنیم و آن را به‌این صورت بنویسیم:

$$(\rho)A^p = A^{p+q}$$

اکنون γ_1، ...، γ_n را پایهٔ ایده‌آل A^q می‌گیریم. چون

$$\gamma_i\xi_j \in A^{p+q} = (\rho)A^p; i,j = 1,\ldots,n$$

بنابراین، برای هر $i = 1,\ldots,n$، برای عدد

$$\rho_i = \frac{\gamma_i}{\rho}$$

این برابری‌ها برقرارند:

$$\rho_i\xi_1 = a_{11}^{(i)}\xi_1 + \ldots + a_{1n}^{(i)}\xi_n$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\rho_i\xi_n = a_{n1}\xi_1 + \ldots + a_{nn}\xi_n$$

از این‌جا، مثل قبل نتیجه می‌شود، ρ_i ریشهٔ معادله‌ای به‌صورت (۱۲) است، یعنی (باتوجه به این‌که D، حلقهٔ بستهٔ درست است)، در D قرار دارد و این، به‌معنای آن است که γ_i بر ρ بخش‌پذیر است.

بنابراین، همهٔ عددهای ایده‌آل A^q بر ρ بخش‌پذیرند. اگر آن‌ها را به ρ ساده کنیم، به‌روشنی به یک ایده‌آل تازهٔ B می‌رسیم (با پایهٔ ρ_1، ...، ρ_n). بنابر ساختمان $(\rho)B = A^q$، یعنی

$$(\rho)A^p = (\rho)A^pB$$

ولی می‌دانیم، در تک‌وارهٔ ایده‌آل‌ها، می‌توان برابری‌ها را به ایده‌آل اصلی ساده کرد. بنابراین

$$A^p = A^pB$$

از این‌جا، باتوجه به آن‌چه می‌دانیم، نتیجه می‌شود: $B = (1)$. به‌این ترتیب

$$A^p = (\rho)$$

در واقع، توانستیم این گزاره را ثابت کنیم:

گزارهٔ ۲. اگر حلقهٔ D، با شرط‌هایی که آوردیم سازگار و درضمن حلقهٔ بستهٔ درست باشد، آن‌وقت توانی از هر ایده‌آل، یک ایده‌آل اصلی است.

نتیجه. برای هر ایده‌آل A، ایده‌آلی مثل A' وجود دارد، به‌نحوی که حاصل‌ضرب AA' ایده‌آل اصلی باشد.

در واقع، کافی است فرض کنیم: $A' = A^{q-1}$.

از این‌جا، یک رشته نتیجه‌های مهم به‌دست می‌آید.

ازجمله، به‌سادگی ثابت می‌شود، قانون ساده کردن، برای هر ایده‌آلی درست است، یعنی اگر $CA = CB$، آن‌گاه $A = B$. در واقع، اگر C' را ایده‌آلی بگیریم که برای آن داشته‌باشیم: $C'C = (\gamma)$، آن‌وقت

$$(\gamma)A = C'(CA) = C'(CB) = (\gamma)B$$

و بنابراین $A = B$.

سپس، اگر $C \subset A$، آن‌وقت A بخشیابی از C است، یعنی ایده‌آلی مثل B وجود دارد، به‌نحوی‌که $C = AB$. درواقع، اگر $C \subset A$، آن‌وقت برای هر ایده‌آل A' داریم: $CA' \subset AA'$. اگر AA' به‌ویژه ایده‌آل اصلی باشد، آن‌وقت همان‌طور که ثابت کردیم، ایده‌آلی مثل B وجود دارد، به‌نحوی‌که داشته‌باشیم: $CA' = AA'B$، که با ساده کردن به A' به‌دست می‌آید: $C = AB$.

به‌ویژه از این‌جا نتیجه می‌شود که هر ایده‌آل اول P، ایده‌آل بیشین (ماکسیمال)[۹] است، یعنی اگر $A \supset P$، آن‌وقت $A = (1)$.

سرانجام، به‌سادگی دیده می‌شود، عضو $\alpha \in D$، وقتی و تنها وقتی بر ایده‌آل A بخش‌پذیر است (یعنی ایده‌آل (α) بر A بخش‌پذیر است) که داشته‌باشیم: $\alpha \in A$. در واقع، اگر (α) بر A بخش‌پذیر باشد، آن‌وقت $(\alpha) \subset A$ و بنابراین $\alpha \in A$. برعکس، اگر $\alpha \in A$، آن‌وقت $(\alpha) \subset A$ و بنابر آن‌چه ثابت کردیم، (α) بر A بخش‌پذیر است.

حکم اخیر، بادقت، به این معنی است که برای تک‌وارهٔ ایده‌آل‌ها (با نگاشت $\alpha \to (\alpha)$)، اصل موضوع ۳ از نظریهٔ بخشیاب‌ها صدق می‌کند (بخش ۹ را ببینید). اصل موضوع ۲ هم برقرار است (اگر α و β بر A

۹- ایده‌آل P از حلقهٔ R را ایده‌آل اول (prime ideal) خوانیم اگر $P \neq R$ و اگر هرگاه برای $a, b \in R$ داشته‌باشیم: $ab \in P$، آن‌گاه $a \in P$ یا $b \in P$. ایده‌آل M از حلقهٔ R را بیشین (maximal ideal) خوانیم اگر $M \neq R$ و اگر ایده‌آل N با شرط $M < N < R$ وجود نداشته‌باشد. (ویراستار).

بخش‌پذیر باشند، آن‌وقت $\alpha \in A$ و $\beta \in A$ و بنابراین $\alpha \pm \beta \in A$، یعنی $\alpha \pm \beta$ بر A بخش‌پذیر است). به برقراری اصل موضوع ۱ هم، پیش از این اشاره کردیم.

به‌این ترتیب، برای این‌که ثابت کنیم تک‌وارهٔ ایده‌آل‌های $\dot{Id}(D)$ به‌همراه نگاشت $\alpha \to (\alpha)$، نظریهٔ بخشیاب‌ها را برای حلقهٔ D تشکیل می‌دهد، تنها این می‌ماند که ثابت کنیم، این تک‌واره آزاد است، یعنی تجزیهٔ هر ایده‌آل به ایده‌آل‌های اول، یگانه است (البته، به‌شرط درنظر نگرفتن ردیف عامل‌ها).

ولی اکنون دیگر، این اثبات هم به‌سادگی به‌دست می‌آید.

در آغاز ثابت می‌کنیم، برای هر دو ایده‌آل A و B، بزرگ‌ترین بخشیاب مشترک وجود دارد، یعنی ایده‌آلی که بخشیاب A و B است و، درضمن، بر هر ایده‌آلی که ایده‌آل‌های A و B را می‌شمارد، بخش‌پذیر است. به‌سادگی معلوم می‌شود، چنین ایده‌آلی، ایده‌آل $(A \cup B)$ است، که ایده‌آل پدید آمده از اجتماع ایده‌آل‌های A و B است. در واقع روشن است که $A \subset (A \cup B)$ و $B \subset (A \cup B)$، یعنی $(A \cup B)$ بخشیابی از A و B است. اگر C بخشیابی از A و B باشد، یعنی $C \supset A$ و $C \supset B$، آن‌وقت $C \supset A \cup B$ و بنابراین $C \supset (A \cup B)$، یعنی C بخشیابی از $A \cup B$ است. از این‌به‌بعد، ایده‌آل $(A \cup B)$ را با نماد (A, B) نشان می‌دهیم.

از این‌جا ثابت می‌شود، هر ایده‌آل $A = (\alpha_1, \ldots, \alpha_k)$، بزرگ‌ترین بخشیاب مشترک ایده‌آل‌های اصلی (α_1)، ...، (α_k) است.

سپس، به‌سادگی دیده می‌شود، برای هر سه ایده‌آل A، B و C، این برابری برقرار است:

$$(A, B)C = (AC, BC)$$

(قانون پخشی بزرگ‌ترین بخشیاب مشترک، نسبت به ضرب).

اکنون می‌توانیم بلافاصله، یگانه بودنِ تجزیهٔ ایده‌آل‌ها را به ضرب ایده‌آل‌های اول ثابت کنیم. برای این منظور، کافی است ثابت کنیم، اگر ایده‌آل اول P بخشیابی از حاصل‌ضرب AB باشد، ولی بخشیابی از ایده‌آل

A نباشد، آن‌وقت بخشیابی از ایده‌آل B است (با ویژگی $(*)$ در بخش ۵ مقایسه کنید). ولی وقتی P بخشیابی از A نباشد، آن‌وقت $(A,P)\neq P$ و بنابراین $(A,P)=۱$ (زیرا P اول، یعنی ایده‌آل بیشین است). بنابراین

$$B=(۱)B=(A,P)B=(AB,PB)$$

و چون P بخشیابی از AB و PB است، بنابراین P بخشیابی از B است.

به‌این ترتیب، ثابت کردیم، ایده‌آل‌های غیرصفر در حلقهٔ D، همهٔ ویژگی‌هایی را دارند که از بخشیاب‌ها انتظار داریم. و این، به‌معنای درست بودن قضیهٔ زیر است:

قضیهٔ ۱. اگر

الف) گروه جمع حلقهٔ D، شبکه‌ای با رتبهٔ محدود n باشد؛

ب) n همسانی یک‌به‌یک $(i=۱,\dots,n)\alpha\to\alpha^{(i)}$ از حلقهٔ D در میدان $\mathbf{C}$ وجود داشته‌باشد که دارای همان ویژگی‌هایی باشند که برای هر $\alpha\in D$ همهٔ چندجمله‌ای‌های مقدماتی متقارن نسبت به $\alpha^{(۱)}$، ...، $\alpha^{(n)}$ (عددهای درست گویا) وجود دارد؛

ج) D، حلقهٔ بسته درست باشد؛

آن‌وقت، این حلقه، دارای نظریهٔ بخشیاب‌ها است.

در این نظریه، بخشیاب‌ها عبارتند از ایده‌آل‌های غیرصفر حلقهٔ D، و بنابر $\alpha\to(\alpha)$ نسبت به هر عضو $\alpha\in D^*$، ایده‌آل اصلی تولید می‌شود.

درضمن، تک‌وارهٔ خانواده‌های بخشیاب‌ها (ایده‌آل‌ها)، یک گروه (آبلی) محدود است.

حکم اخیر، تغییرشکل یافتهٔ ساده‌ای از گزارهٔ ۱ و نتیجهٔ گزارهٔ ۲ است. این حکم به این معنی است که ایده‌آل‌های حلقهٔ D نه‌تنها با اصل موضوع‌های ۱ تا ۳ از بخش ۹، بلکه با اصل موضوع ۴ هم سازگارند (خواست بیشتر و نیرومندتری برای محدود کردن گروه $\mathcal{H}$ از خانواده‌های ایده‌آل‌ها).

از آن‌جاکه حلقهٔ D دارای ویژگی‌های الف) و ب) است، اگر ثابت کنیم که ویژگی ج) را هم به‌همراه دارد، از نیازهایی که در بخش ۹ برای عددهای اول سامان‌پذیر درنظر گرفتیم، تنها اصل موضوع ۵ باقی می‌ماند. درضمن، با استفاده از محدود بودن گروه $\mathcal{H}$، می‌توانیم این اصل موضوع را به‌صورت ضعیف‌تری بازسازی کنیم و تنها به این بسنده کنیم که عدد l، بخشیاب مرتبهٔ h از گروه $\mathcal{H}$ نیست. البته همهٔ این‌ها، در جهت شناخت ویژگی‌های عددهای اول سامان‌پذیر، به ما یاری می‌رساند.

بستهٔ درست بودن حلقهٔ D را در بخش بعد ثابت می‌کنیم، در این‌جا تنها یادآور می‌شویم، شرط ج) دربارهٔ بستهٔ درست بودن، با شرط‌های الف) و ب) (که به‌طور کلی، برای وجود نظریهٔ بخشیاب‌ها در حلقهٔ D لازم نیستند) از این لحاظ اختلاف دارد که شرط ضروری است و از آن نمی‌توان گذشت. به زبان دیگر، در حلقهٔ D، اگر بستهٔ درست نباشد، نظریهٔ بخشیاب‌ها نمی‌تواند وجود داشته‌باشد.

حلقهٔ D حلقه‌ای با نظریهٔ بخشیاب‌ها، و K میدان کسرهای آن را درنظر بگیرید. اگر $\xi = \frac{\beta}{\alpha}$ عضو K باشد ولی عضو D نباشد، آن‌وقت بخشیاب اول $\wp$ وجود دارد که α را در درجه‌ای بالاتر از β می‌شمارد، یعنی اگر β بر $\wp^k$ بخش‌پذیر و بر $\wp^{k+1}$ بخش‌ناپذیر باشد، آن‌وقت α بر $\wp^{k+1}$ بخش‌پذیر است. بنابراین، اگر

$$\xi^n + a_1\xi^{n-1} + \ldots + a_n = 0$$

(a_1، ...، a_n عددهایی درست‌اند)، یعنی اگر

$$\beta^n = -a_1\beta^{n-1}\alpha - \ldots = a_n\alpha^n$$

آن‌وقت ρ^n بر $\wp^{kn+1}$ بخش‌پذیر است، زیرا برای هر مقدار s از ۱ تا n داریم:

$$kn + 1 \leq (n-s)k + s(k+1)$$

و بنابراین، هر جملهٔ به‌صورت $\beta^{n-s}\alpha^s$ بر $\wp^{kn+1}$ بخش‌پذیر می‌شود. بنابراین β بر $\wp^i$ $\left(i > k + \frac{1}{n}\right)$ بخش‌پذیر است که فرض ما را نقض می‌کند.

به‌این ترتیب، از تنها شرط قضیهٔ ۱، که برای حلقهٔ D_l با دشواری قابل‌تحقیق است، نمی‌توان صرف‌نظر کرد.

ضمیمه. نُرم ایده‌آل

در این ضمیمه، به برخی ویژگی‌های تکمیلیِ ایده‌آل‌ها در حلقه می‌پردازیم، ویژگی‌هایی که با شرط‌های قضیهٔ بخش ۱۱ سازگارند. از آن‌جاکه بنا بر این قضیه، ایده‌آل‌ها به‌عنوان بخشیاب‌ها تفسیر می‌شوند، آن‌ها را با همان نمادهای خاصی که برای بخشیاب انتخاب کردیم، نشان می‌دهیم.

نماد D را برای حلقهٔ دلخواهی می‌گیریم که شرط‌های قضیهٔ بخش ۱۱ در آن صدق کند. وقتی D را به‌عنوان ایده‌آل (بخشیاب) درنظر می‌گیریم، آن را با نماد (۱) یا نماد $\breve{0}$ نشان می‌دهیم.

σ را ایده‌آلی از حلقهٔ D و α و β را عضوهایی از D می‌گیریم. می‌نویسیم $\alpha \equiv \beta(\mathrm{mod}\sigma)$ و می‌خوانیم α نسبت به مدول σ با β هم‌نهشت است، وقتی عضو $\alpha - \beta$ بر σ بخش‌پذیر باشد. این هم‌نهشتی‌ها دارای ویژگی‌های معمولِ برابری‌ها هستند (می‌توان آن‌ها را با هم جمع یا در هم ضرب کرد و غیره؛ ولی دو طرف هم‌نهشتی را همیشه نمی‌توان به عامل مشترک آن‌ها ساده کرد: برای این‌که امکان ساده کردن وجود داشته‌باشد، باید این عامل نسبت به σ اول باشد).

گزاره‌ای که در این‌جا می‌آوریم، مربوط به نظریهٔ مقدماتی عددها است و به «قضیهٔ چینی دربارهٔ باقی‌مانده‌ها» شهرت دارد.

گزارهٔ ۱. برای ایده‌آل‌های دلخواه و دوبه‌دو نسبت به هم اولِ

$$\sigma_1, \ldots, \sigma_s \qquad (1)$$

و عضوهای دلخواه $\alpha_1, \ldots, \alpha_s$ از حلقهٔ D، عضوی مثل $\xi \in D$ وجود دارد، به‌نحوی‌که داشته‌باشیم:

$$\xi \equiv \alpha_1 (\mathrm{mod} \sigma_1)$$

$$\ldots\ldots\ldots\ldots$$

$$\xi \equiv \alpha_n (\mathrm{mod} \sigma_n)$$

اثبات. $\mathfrak{h}_i$ $(i = 1, \ldots, s)$ را حاصل‌ضرب همهٔ ایده‌آل‌های (۱)، به‌جز ایده‌آل σ_i فرض می‌کنیم. روشن است، ایده‌آل‌های $\mathfrak{h}_1$، $\mathfrak{h}_2$، ...، $\mathfrak{h}_s$ نسبت به هم اول‌اند، یعنی

$$(\mathfrak{h}_1, \mathfrak{h}_2, \ldots, \mathfrak{h}_s) = (1) \qquad (2)$$

برابری (۲) به این معنی است که چنان عضوهایی مثل

$$\beta_1 \in \mathfrak{h}_1, \beta_2 \in \mathfrak{h}_2, \ldots, \beta_s \in \mathfrak{h}_s$$

وجود دارند، به‌نحوی‌که داشته‌باشیم:

$$\beta_1 + \beta_2 + \ldots + \beta_s = 1 \qquad (3)$$

طبق ساختمان ما، هر ایده‌آل σ_i $(i = 1, \ldots, s)$، بخشیابی از همهٔ ایده‌آل‌های $\mathfrak{h}_j$ $(j \neq i)$ است، یعنی همهٔ عضوهای $\beta_j (j \neq i)$ را می‌شمارد. بنابراین، از برابری (۳) نتیجه می‌شود:

$$\beta_i \equiv 1 (\mathrm{mod} \sigma_i), \; i = 1, \ldots, s$$

فرض می‌کنیم:

$$\xi = \alpha_1 \beta_1 + \ldots + \alpha_s \beta_s$$

چون $\beta_j \equiv 0 (\mathrm{mod} \sigma_i) (j \neq i)$، ولی $\beta_i \equiv 1 (\mathrm{mod} \sigma_i)$، پس

$$\xi \equiv \alpha_i (\mathrm{mod} \sigma_i), i = 1, \ldots, s$$

گزارهٔ ۲. برای ایده‌آل‌های دلخواه σ و $\natural$، عضوی مثل $\gamma \in D$ وجود دارد، به‌نحوی‌که داشته‌باشیم:

$$(\sigma\natural, \gamma) = \sigma$$

اثبات. فرض کنید:

$$\sigma\natural = \wp_1^{k_1} \dots \wp_s^{k_s},\ k_1 \geq 1, \dots, k_s \geq 1$$

که در آن $\wp_1$، ...، $\wp_s$، ایده‌آل‌هایی اول و مختلف‌اند. در این‌صورت

$$\sigma = \wp_1^{l_1} \dots \wp_s^{l_s}$$

با شرط

$$0 \leq l_1 \leq k_1, \dots, 0 \leq l_s \leq k_s$$

چون $\wp_i^{l_i+1} \subset \wp_i^{l_i}$ و $\wp_i^{l_i+1} \neq \wp_i^{l_i}$ (اگر $\wp_i^{l_i+1} = \wp_i^{l_i}$، آن‌وقت به $\wp^{l_i}$ ساده می‌شود و به برابری ناممکن $\wp_i = \check{0}$ می‌رسیم؛ به‌ازای $l_i = 0$، به‌طور طبیعی فرض می‌کنیم: $\wp_i^{l_i} = \check{0}$)، بنابراین عضوی مثل $\alpha_i \in D$ وجود دارد، به‌نحوی که

$$\alpha_i \in \wp_i^{l_i} \text{ و } \alpha_i \notin \wp_i^{l_i+1}$$

یعنی $\alpha_i \equiv 0 (\mathrm{mod} \wp_i^{l_i})$ و $\alpha_i \not\equiv 0 (\mathrm{mod} \wp_i^{l_i+1})$.

بنابراین، عضو $\gamma \in D$، که برای آن داریم:

$$\gamma \equiv \alpha_i (\mathrm{mod} \wp_i^{l_i+1}), i = 1, \dots, s$$

(چنین عضوی، باتوجه به گزارهٔ ۱ وجود دارد)، دارای چنان ویژگی است که

$$\gamma \equiv 0 (\mathrm{mod} \wp^{l_i}),\ i = 1, \dots, s$$
$$\gamma \not\equiv 0 (\mathrm{mod} \wp^{l_i+1}), i = 1, \dots, s$$

ولی در این‌صورت، روشن است که

$$(\sigma\natural, \gamma) = \wp^{l_1} \dots \wp_s^{l_s} = \sigma$$

نتیجه. هر ایده‌آل σ از حلقهٔ D، به‌وسیلهٔ دو عضو تولید می‌شود:

$$\sigma = (\alpha, \beta)$$

اثبات. باتوجه به گزارهٔ ۲ بخش ۱۱، عضوی مثل $\alpha \in D$ و ایده‌آلی مثل $\natural$ وجود دارد، به‌نحوی‌که داشته‌باشیم: $\sigma\natural = (\alpha)$. باتوجه به گزارهٔ ۲، عضوی مثل $\beta \in D$ وجود دارد که داشته‌باشیم: $\sigma = (\sigma\natural, \beta)$.

از آن‌جاکه $\alpha - \beta$، وقتی و تنها وقتی بر σ بخش‌پذیر است که داشته‌باشیم $\alpha - \beta \in \sigma$، بنابراین خانواده‌های عضوهایی که، نسبت به مُدول ایده‌آل σ، هم‌نهشت با یکدیگرند، چیزی جز همرده‌های زیرشبکه σ نسبت به شبکهٔ D نیستند (عضوهای D/α)؛ و ما ثابت کرده‌ایم، تعداد این همرده‌ها محدود است. این تعداد را با نماد $N\sigma$ نشان می‌دهند و به آن، نُرم ایده‌آل σ گویند.

ثابت می‌شود، نُرم $N\sigma$ از ایده‌آل دلخواه σ، بر σ بخش‌پذیر است. در واقع، فرض کنید

$$\alpha_1, \dots, \alpha_N,\ N = N\sigma \qquad (۴)$$

دستگاه کامل معرف همرده‌های ایده‌آل σ نسبت به حلقهٔ D باشد (و این به‌معنی آن است که هر عضو حلقهٔ D، با یکی و تنها یکی از عضوهای (۴) هم‌نهشت است). روشن است، عضوهای

$$\alpha_1 + 1, \dots, \alpha_N + 1 \qquad (۴')$$

هم یک دستگاه کامل را تشکیل می‌دهند (اگر $\alpha_i + 1 \equiv \alpha_j + 1 (\mathrm{mod}\sigma)$، آن‌وقت $\alpha_i \equiv \alpha_j (\mathrm{mod}\sigma)$، یعنی $i = j$؛ اگر $\alpha - 1 \equiv \alpha_i (\mathrm{mod}\sigma)$، آن‌وقت $\alpha \equiv \alpha_i + 1 (\mathrm{mod}\sigma)$). این به‌معنای آن است که، هریک از عضوهای (۴')، نسبت به مدول σ، با یکی و تنها یکی از عضوهای (۴)

هم‌نهشت است. بنابراین، مجموع همهٔ عضوهای (۴′)، با مجموع همهٔ عضوهای (۴) هم‌نهشت است، یعنی تفاضل این مجموع‌ها بر σ بخش‌پذیر است. ولی روشن است که، این تفاضل، برابر است با $N = N\sigma$.

عبور از یک پایهٔ ایده‌آل (یا کلی‌تر، یک شبکهٔ دلخواه) به دیگری، به‌وسیلهٔ ماتریسی با درایه‌های درست شرح داده می‌شود. چون عمل عکس هم ممکن است، این ماتریس دارای وارون است. ولی به‌سادگی روشن می‌شود که، دترمینان ماتریسی که درایه‌های آن و درایه‌های ماتریس وارون آن عددهای درست باشند، باید برابر ۱ ± باشد. بنابراین، ماتریسِ عبور از یک پایهٔ ایده‌آل به پایه‌ای دیگر، دترمینانی برابر ۱ ± دارد.

اگر $\sigma \subset \mathfrak{h}$، آن‌وقت پایهٔ ایده‌آل $\mathfrak{h}$ هم برحسب پایهٔ ایده‌آل σ، به‌وسیلهٔ ماتریسی صحیح بیان می‌شود. روشن است (با حالت فضاهای خطی مقایسه کنید)، با تغییر پایه‌ها، این ماتریس (از راست یا از چپ)، در ماتریس‌های متناظر انتقال ضرب می‌شود. بنابراین قدرمطلق دترمینان آن تغییر نمی‌کند. و این، به‌معنای آن است که، این قدرمطلق، به انتخاب پایه‌ها بستگی ندارد و تنها به‌وسیلهٔ ایده‌آل‌های σ و $\mathfrak{h}$ معین می‌شود و ما آن را با نماد $[\mathfrak{h}; \sigma]$ نشان می‌دهیم.

از این حقیقت که دترمینان حاصل‌ضرب ماتریس‌ها، برابر است با حاصل‌ضرب دترمینان‌های حاصل‌های ضرب، بلافاصله نتیجه می‌شود، اگر $\mathfrak{s} \subset \mathfrak{h} \subset \sigma$، آن‌وقت

$$[\sigma : \mathfrak{s}] = [\sigma : \mathfrak{h}] \cdot [\mathfrak{h} : \mathfrak{s}] \qquad (۵)$$

همان‌طور که پیشتر دیدیم، برای زیرشبکهٔ دلخواه A با مرتبهٔ n از شبکهٔ D و پایهٔ دلخواه شبکهٔ D، پایه زیرشبکهٔ A وجود دارد که با پایهٔ شبکهٔ D به‌وسیلهٔ ماتریس مثلثی بستگی دارد که درایه‌های قطری آن $a_1^{(0)}$، ...، $a_n^{(0)}$ مخالف صفرند. درضمن قدرمطلق $|a_1^{(0)} \dots a_n^{(0)}|$ حاصل‌ضربِ این درایه‌ها برابر است با مرتبهٔ گروه بهری D/A.

در حالتی که شبکهٔ D ایده‌آل σ و زیرشبکهٔ A، ایده‌آل $\mathfrak{h}$ باشد، حاصل‌ضرب $a_1^{(\circ)} \dots a_n^{(\circ)}$، باتوجه به مثلثی بودن ماتریس انتقال، برابر دترمینان آن است و (با دقت تا یک علامت) بر عدد $[\sigma : \mathfrak{h}]$ منطبق می‌شود. بنابراین، ویژگی بی‌تغییر این عدد به‌دست می‌آید: برای ایده‌آل‌های دلخواه $\mathfrak{h} \subset \sigma, \sigma$، عدد $[\sigma : \mathfrak{h}]$ برابر است با مرتبهٔ گروه عامل $\sigma/\mathfrak{h}$ (البته در این‌جا، ایده‌آل‌های σ و $\mathfrak{h}$ همچون شبکه در نظر گرفته شده‌اند). متناظر با اصطلاح‌های کلی نظریهٔ گروه‌ها، در این‌جا هم عدد $[\sigma : \mathfrak{h}]$ را اندیس ایده‌آل $\mathfrak{h}$ در ایده‌آل σ می‌نامیم.

در حالت خاص، برای هر ایده‌آل σ داریم: $[(\mathfrak{1}) : \sigma] = N\sigma$.

اکنون ایده‌آل‌های σ و $\mathfrak{h}$ را، ایده‌آل‌هایی دلخواه می‌گیریم. با مقایسهٔ تعریف‌ها، بلافاصله متوجه می‌شویم، بزرگ‌ترین بخشیاب مشترک، یعنی $(\sigma, \mathfrak{h}) = (\sigma \cup \mathfrak{h})$، چیزی جز آن‌چه از نظریهٔ گروه‌ها، به‌عنوان مجموع $\sigma + \mathfrak{h}$ برای زیرگروه‌های σ و $\mathfrak{h}$ از شبکهٔ $D = (\mathfrak{1})$ می‌دانیم، نیست. ولی در نظریهٔ گروه‌ها ثابت می‌شود، برای زیرگروه‌های دلخواه σ و $\mathfrak{h}$ از یک گروه دلخواه، این یکسانی (ایزومورفیسم) وجود دارد:

$$(\sigma + \mathfrak{h})/\sigma \approx \mathfrak{h}/(\sigma \cap \mathfrak{h})$$

در واقع، هر خانوادهٔ مجاور $\beta + (\sigma \cap \mathfrak{h})$، $\beta \in \mathfrak{h}$ از $\mathfrak{h}/(\sigma \cap \mathfrak{h})$، به‌طور یگانه خانوادهٔ مجاور $\beta + \sigma$ از $(\sigma + \mathfrak{h})/\sigma$ را معین می‌کند. روشن است که این، نگاشتی هم‌سان (هوموومورف) است. درضمن اگر $\beta + \sigma = \circ$، یعنی $\beta \in \sigma$، آن‌وقت $\beta \in \sigma \cap \mathfrak{h}$، یعنی $\beta + (\sigma \cap \mathfrak{h}) = \circ$. چون هر عضو از $\sigma + \mathfrak{h}$ به‌صورت $\alpha + \beta$ است ($\alpha \in \sigma$ و $\beta \in \mathfrak{h}$)، یعنی هر خانوادهٔ مجاور از $(\sigma + \mathfrak{h})/\sigma$ به‌صورت $(\alpha + \beta) + \sigma = \beta + \sigma$ است، ثابت می‌کند که نگاشت $\beta + (\sigma \cap \mathfrak{h}) \to \beta + \sigma$، نگاشتی یکسان است.

باتوجه با این یکسانی برای ایده‌آل‌های σ و $\mathfrak{h}$، این برابری برقرار است:

$$[(\sigma, \mathfrak{h}) : \sigma] = [\mathfrak{h} : (\sigma \cap \mathfrak{h})] \qquad (۶)$$

جالب است، ایده‌آل $\sigma \cap \mathfrak{h}$ در این برابری مفهوم خاصی دارد: در تک‌وارهٔ ایده‌آل‌ها، $\sigma \cap \mathfrak{h}$ عبارت است از کوچک‌ترین مضرب مشترک ایده‌آل‌های σ و $\mathfrak{h}$. در واقع $\sigma \cap \mathfrak{h} \subset \sigma$ و $\sigma \cap \mathfrak{h} \subset \mathfrak{h}$، یعنی $\sigma \cap \mathfrak{h}$ هم بر σ و هم بر $\mathfrak{h}$ بخش‌پذیر است. اگر ς بر σ و بر $\mathfrak{h}$ بخش‌پذیر باشد، یعنی $\sigma \subset \varsigma$ و $\mathfrak{h} \subset \varsigma$، آن‌وقت $\mathfrak{h} \cap \sigma \subset \varsigma$ و بنابراین ς بر $\sigma \cap \mathfrak{h}$ بخش‌پذیر است.

از آن‌جا که هر ایده‌آل به‌صورتی یگانه به ضرب ایده‌آل‌های اول تجزیه می‌شود، آن‌وقت شبیه حکمی که برای عددهای طبیعی وجود دارد، در این‌جا هم، حاصل‌ضرب $\sigma\mathfrak{h}$ از دو ایده‌آل دلخواه σ و $\mathfrak{h}$، برابر است با حاصل‌ضرب بزرگ‌ترین بخشیاب مشترک در کوچک‌ترین مضرب مشترک آن‌ها:

$$\sigma\mathfrak{h} = (\sigma, \mathfrak{h}) \cdot (\sigma \cap \mathfrak{h}) \qquad (۷)$$

اکنون، بدون برخورد به دشواری خاصی، می‌توان ثابت کرد: برای ایده‌آل‌های دلخواه σ و $\mathfrak{h}$، اندیس $[\sigma : \sigma\mathfrak{h}]$ به σ بستگی ندارد و برابر است با نُرم $N\mathfrak{h}$ از ایده‌آل $\mathfrak{h}$.

$$N\mathfrak{h} = [\sigma : \sigma\mathfrak{h}]$$

در واقع، باتوجه به گزارهٔ ۴، عضوی مثل $\gamma \in D$ وجود دارد، به‌نحوی‌که داشته‌باشیم: $(\sigma\mathfrak{h}, \gamma) = \sigma$. بنابراین (دستور (۷) را ببینید):

$$\sigma(\sigma\mathfrak{h} \cap (\gamma)) = (\sigma\mathfrak{h}, (\gamma))(\sigma\mathfrak{h} \cap (\gamma)) = \sigma\mathfrak{h}(\gamma)$$

از این‌جا، با ساده کردن به σ به‌دست می‌آید:

$$\sigma\mathfrak{h} \cap (\gamma) = \mathfrak{h}(\gamma)$$

بنابراین (باتوجه به دستور (۶)):

$$[(\gamma) : \mathfrak{h}(\gamma)] = [(\gamma) : (\sigma\mathfrak{h} \cap (\gamma)] =$$
$$= [(\sigma\mathfrak{h}, \gamma) : \sigma\mathfrak{h}] = [\sigma, \sigma\mathfrak{h}]$$

ولی، از تعبیر اندیس به‌عنوان دترمینان، روشن است که

$$[(\gamma) : \mathfrak{h}(\gamma)] = [(1) : \mathfrak{h}] = N\mathfrak{h}$$

بنابراین

$$N\mathfrak{h} = [\sigma : \sigma\mathfrak{h}]$$

گزارهٔ ۳. (ویژگی ضربی نُرم‌ها). برای ایده‌آل‌های دلخواه σ و $\mathfrak{h}$، این برابری برقرار است:

$$N(\sigma\mathfrak{h}) = N\sigma \cdot N\mathfrak{h}$$

اثبات. باتوجه به دستور (۵) که دربارهٔ ایده‌آل‌های $\sigma\mathfrak{h}$، σ و (1) به‌کار ببریم)، داریم:

$$[(1) : \sigma\mathfrak{h}] = [(1) : \sigma] \cdot [\sigma : \sigma\mathfrak{h}]$$

یعنی

$$N(\sigma\mathfrak{h}) = N\sigma \cdot N\mathfrak{h}$$

نتیجه. اگر نُرم $N\mathfrak{p}$ از ایده‌آل $\mathfrak{p}$ عددی اول باشد، آن‌وقت ایده‌آل $\mathfrak{p}$، ایده‌آلی اول است.

اثبات. کافی است یادآوری کنیم، وقتی و تنها وقتی $N\sigma = 1$، که داشته‌باشیم: $\sigma = (1)$.

توجه کنیم: عکس این گزاره درست نیست: به‌سادگی می‌توان مثال‌هایی پیدا کرد (خودتان پیدا کنید)، که برای آن‌ها، $\mathfrak{p}$ ایده‌آلی اول باشد، در حالی‌که نُرم آن عددی اول نباشد.

مساله. ثابت کنید، نُرم ایده‌آل اول، به‌ناچار توانی از یک عدد اول است.

گزارهٔ ۴. برای هر عضو $\alpha \in D^*$ داریم:

$$N(\alpha) = |N\alpha|$$

اثبات. برای سادگی کار، این گزاره را با یک فرض اضافی ثابت می‌کنیم، یعنی همهٔ عددهای $\alpha^{(1)}$، ...، $\alpha^{(n)}$ را مختلف می‌گیریم. ω_1، ...، ω_n را پایهٔ حلقهٔ D، یعنی $\alpha\omega_1$، ...، $\alpha\omega_n$ را پایهٔ ایده‌آل (α) فرض می‌کنیم. سپس، فرض کنید:

$$\begin{aligned} \alpha\omega_1 &= a_{11}\omega_1 + \ldots + a_{1n}\omega_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha\omega_n &= a_{n1}\omega_1 + \ldots + a_{nn}\omega_n \end{aligned} \qquad (۸)$$

در این‌صورت $N(\alpha) = [(1) : (\alpha)]$، برابر است با قدرمطلق دترمینان

$$\begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nn} \end{vmatrix} \qquad (۹)$$

از طرف دیگر، اگر از برابری‌های (۸)، عددهای ω_1، ...، ω_n را حذف کنیم، به این معادله می‌رسیم (با اثبات پیش‌قضیهٔ ۱ مقایسه کنید):

$$\begin{vmatrix} a_{11}-\alpha & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nn}-\alpha \end{vmatrix} = 0 \qquad (۱۰)$$

که عدد $\alpha = \alpha^{(1)}$ در آن صدق می‌کند. اگر نگاشت $\alpha \to \alpha^{(i)}$ را در (۸) به‌کار بریم، بلافاصله قانع می‌شویم که همهٔ عددهای $\alpha^{(i)}$ (برای i از ۱ تا n) در معادلهٔ (۱۰) صدق می‌کنند. از آن‌جاکه معادلهٔ (۱۰) از درجهٔ n است، ریشهٔ دیگری ندارد. بنابراین، حاصل‌ضرب $\alpha^{(1)} \ldots \alpha^{(n)}$، مقدار ثابت این معادله، یعنی دترمینان (۹) است.

نتیجه. اگر $N\alpha$ عددی اول باشد، آن‌وقت ایده‌آل اصلی (α)، ایده‌آلی اول است.

چون، باتوجه به دستور (۱۳) بخش ۶، این برابری را در حلقهٔ D داریم:

$$N\lambda = 1,\ \lambda = 1 - \zeta$$

(و روشن است، همهٔ عددهای $\lambda^{(1)}$، ...، $\lambda^{(l-1)}$ مختلف‌اند)، آن‌وقت در حالت خاص، معلوم می‌شود، در حلقهٔ D_l، ایده‌آل اصلی $(\lambda) = \downarrow$، ایده‌آلی اول است. و اگر ثابت کنیم در حلقهٔ D_l، قضیهٔ کلی ما درست است، آن‌وقت رخنه‌ای که در استدلال بخش ۱۰ داشتیم، پر می‌شود.

همان‌طور که می‌دانیم، برای این منظور، کافی است ثابت کنیم، حلقهٔ D_l، یک حلقهٔ بستهٔ صحیح است.

۱۲

عددهای جبری درست

بارها، با معادله‌های به‌صورت

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \qquad (1)$$

برخورد داشته‌ایم که در آن، a_1، ...، a_n عددهایی گویا و درست‌اند. ریشه‌های چنین معادله‌ای را، عددهای جبری درست نامیده‌اند.

در حالت کلی‌تر، می‌توان عددهای جبری را (که البته لازم نیست درست باشند) به ریشه‌های معادله‌ای به‌صورت

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0 \qquad (2)$$

گفت که در آن، عددهای a_0، a_1، ...، a_n عددهایی درست‌اند.

روشن است، اگر در معادلهٔ (۲)، ضریب‌های a_0، a_1، ...، a_n را عددهای گویای دلخواهی بگیریم، در خانوادهٔ عددهای جبری، تغییری پیش نمی‌آید. به‌این ترتیب، بنابر این تعریف، عددهای جبری، چیزی جز عددهای جبری روی میدان $\mathbf{Q}$ نیستند.

با تجزیهٔ سمت چپ معادلهٔ (۲) به ضرب عامل‌ها و انتخاب عاملی که ریشهٔ آن عدد α است، معلوم می‌شود که هر عدد جبری، ریشهٔ یک چندجمله‌ای با ضریب‌های گویا است که قابل تبدیل به ضرب عامل‌های ساده‌تر نیست. بدون این‌که به کلی بودن مطلب لطمه‌ای وارد شود، می‌توان فرض کرد که ضریب بزرگ‌ترین جملهٔ این چندجمله‌ای برابر واحد است.

α را عددی درست، یعنی ریشهٔ معادلهٔ (۱) می‌گیریم. بنابر پیش‌قضیهٔ گاوس (بخش ۵ را ببینید)، سمت چپ معادلهٔ (۱) را می‌توان (در میدان $\mathbf{Q}$) به ضرب چندجمله‌ای‌هایی با ضریب‌های درست تجزیه کرد، به‌نحوی‌که هریک از این چندجمله‌ای‌ها به‌صورت ضریب چندجمله‌ای‌های ساده‌تری قابل تجزیه نباشند. چون ضریب بزرگ‌ترین جملهٔ این چندجمله‌ای‌ها برابر ± 1 (و حاصل‌ضرب آن‌ها، برابر ۱) است، بنابراین چندجمله‌ای غیرقابل تبدیل

$h(x)$، که ریشهٔ آن عدد جبری درست α و ضریب بزرگ‌ترین درجهٔ آن برابر واحد است، دارای ضریب‌هایی درست است.

اگر دو طرف معادلهٔ (۲) را در a_0^{n-1} ضرب کنیم، می‌توانیم آن را به‌این صورت بنویسیم:

$$(a_0x)^n + a_1(a_0x)^{n-1} + \ldots + a_na_0^{n-1} = 0$$

به‌این ترتیب، با فرض $y = a_0x$، به معادله‌ای به‌صورت (۱) می‌رسیم و این ثابت می‌کند، هر عدد جبری ξ را می‌توان به‌صورت

$$\xi = \frac{\alpha}{a}$$

نشان داد که در آن، α عددِ جبری درست و a عدد گویای درست است.

می‌توان ثابت کرد، مجموع، تفاضل، حاصل‌ضرب و خارج‌قسمت دو عدد جبری، خود یک عدد جبری است؛ به‌زبان دیگر، همهٔ عددهای جبری، تشکیل یک میدان می‌دهند. در این‌جا، اثبات مستقیمی از این حکم را، که البته به مقداری محاسبه نیاز دارد، می‌آوریم.

α و β را دو عدد جبری می‌گیریم. بنابر تعریف، α ریشهٔ معادله‌ای به‌صورت (۲) است. فرض می‌کنیم

$$\alpha_1 = \alpha,\ \alpha_2, \ldots, \alpha_n \qquad (۳)$$

همهٔ ریشه‌های این معادله باشند. به‌همین ترتیب، فرض کنید

$$\beta_1 = \beta, \beta_2, \ldots, \beta_m \qquad (۴)$$

همهٔ ریشه‌های معادلهٔ

$$b_0x^m + b_1x^{m-1} + \ldots + b_m = 0$$

باشند که β در آن صدق کند (در حالت کلی، درجهٔ m را غیر از درجهٔ n می‌گیریم).

اکنون، این چندجمله‌ای را با درجهٔ mn درنظر می‌گیریم:

$$F(x)=\prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i\beta_j)$$

که ضریب‌های آن، چندجمله‌ای‌هایی با ضریب‌های درست از ریشه‌های (۳) و (۴) و، درضمن، متقارن نسبت به این ریشه‌ها هستند، یعنی هرگونه جایگشتی از این ریشه‌ها، تغییری در آن ایجاد نمی‌کند. بنابراین، چندجمله‌ای‌هایی از چندجمله‌ای‌های متقارن مقدماتی‌اند، یعنی باتوجه به دستورهای ویت، چندجمله‌ای‌هایی با ضریب‌های درست‌اند، نسبت به

$$\frac{a_1}{a_0},\cdots,\frac{a_m}{a_0},\frac{b_1}{b_0},\cdots,\frac{b_m}{b_0}$$

و این ثابت می‌کند، همهٔ ضریب‌های چندجمله‌ای F، عددهایی گویا هستند. از این‌جا به این نتیجه می‌رسیم که همهٔ ریشه‌های $\alpha_i\beta_j$ و به‌ویژه ریشهٔ $\alpha\beta=\alpha_1\beta_1$، عددی جبری است.

به‌این ترتیب، گزارهٔ ما در رابطه با حاصل‌ضرب $\alpha\beta$ ثابت شد. برای مجموع، تفاضل و خارج‌قسمت دو عدد جبری هم، به‌همین ترتیب می‌توان عمل کرد.

این اثبات، حقیقت دیگری را هم نشان می‌دهد که برای ما بسیار مهم است؛ به‌ازای $a_0=b_0=1$، همهٔ ضریب‌های چندجمله‌ای F (که ضریب بزرگ‌ترین درجهٔ آن برابر واحد است)، عددهایی جبری و درست‌اند. روشن است، این نتیجه برای مجموع و تفاضل (و نه برای نسبت آن‌ها) درست است. به‌این ترتیب، ثابت می‌شود، مجموع، تفاضل و حاصل‌ضرب دو عدد جبری درست، خود عددهای جبریِ درست‌اند، یعنی مجموعهٔ همهٔ عددهای جبری، یک حلقه را تشکیل می‌دهند.

باوجود این، حساب این حلقه، کمتر جالب است. ازجمله، در این حلقه، عضوهای تجزیه‌ناپذیر (یعنی اول) وجود ندارد. در واقع، هر عدد جبری درست α را می‌توان برای نمونه، با این دستور تجزیه کرد:

$$\alpha = \sqrt{\alpha}\sqrt{\alpha}$$

و به‌سادگی می‌توان روشن کرد که $\sqrt{\alpha}$ هم، یک عدد جبری است. بنابراین، خانوادهٔ عددهای جبری را باید به‌نحوی محدود کرد.

زیر میدان K از میدان عددهای مختلط را، میدان با درجهٔ متناهی گویند، وقتی به‌عنوان فضای خطی روی میدان $\mathbf{Q}$، بُعد متناهی داشته‌باشد (این بعد را درجهٔ میدان K گویند).

به‌سادگی دیده می‌شود، هر عضو از میدان با درجهٔ متناهی (یا محدود)، یک عدد جبری است. در واقع، اگر درجهٔ میدان برابر n باشد، آن‌وقت برای هر عضو ξ از آن، عضوهای ۱، ξ، ...، ξ^n، به‌صورت خطی به هم بستگی داند (زیرا تعداد آن‌ها برابر $n+1$ است)، یعنی داریم:

$$c_0\xi^n + c_1\xi^{n-1} + \ldots + c_n = 0$$

که ضریب‌های آن، عددهایی گویا هستند.

بر این اساس، میدان با درجهٔ محدود را، میدان عددهای جبری هم می‌نامند (algebraic number field)، گرچه این اصطلاح تا اندازه‌ای دارای مفهوم دوگانه است و محدود بودن درجهٔ میدان را نمی‌رساند.

K را میدان دلخواهی از عددهای جبری (با درجهٔ محدود) فرض می‌کنیم. روشن است، زیرمجموعهٔ D از آن، شامل همهٔ عددهای درست میدان K، یک حلقه است که حلقهٔ عددهای درستِ میدان K نامیده می‌شود. حساب همین‌گونه حلقه‌ها است که مضمون نظریهٔ عددهای جبری را تشکیل می‌دهد.

چون هر عضو $\xi \in K$ به‌صورت $\xi = \frac{\alpha}{a}$ است، که در آن، α، عدد

جبری درستی (و بنابراین عضوی از حلقهٔ D) و a عدد گویای درستی (یعنی باز هم عضوی از D) است، بنابراین K کسرهای حلقهٔ D است.

از آن‌جاکه حلقهٔ D، بنابر تعریف، شامل همهٔ عددهای درست میدان K است، ثابت می‌شود که D، حلقهٔ بسته صحیح است.

اکنون به میدان K_l و زیرحلقهٔ آن D_l برمی‌گردیم. میدان K_l، میدانی با درجهٔ محدود است (با درجهٔ $l-1$)، بنابراین می‌توان همهٔ آن‌چه را در بالا گفته‌ایم، دربارهٔ آن به‌کار برد. به‌ویژه D، حلقهٔ عددهای درستِ آن، بستهٔ صحیح است. به‌این ترتیب، برای این‌که ثابت کنیم حلقهٔ D_l هم بستهٔ صحیح است، کافی است روشن کنیم که $D = D_l$.

اثبات رابطهٔ $D_l \subset D$. کافی است ثابت کنیم، هر عضو $\alpha \in D_l$. ریشه‌ای از چندجمله‌ای

$$f(x) = (x - a^{(1)}) \dots (x - a^{(l-1)}) \qquad (۵)$$

با ضریب‌های گویا و درست و ضریب بزرگ‌ترین درجهٔ آن برابر واحد است.

اثباتی دیگر. فرض می‌کنیم $\alpha \in D_l$، یعنی

$$\alpha = a_0 + a_1\zeta + \dots + a_{l-2}\zeta^{l-2}$$

(a_0، a_1، ...، a_{l-2} عددهایی گویا و درست‌اند). این برابری را، پشت‌سرهم در ۱، ζ، ...، ζ^{l-2} ضرب می‌کنیم؛ با استفاده از رابطهٔ $\zeta^{l-1} = -1 - \dots - \zeta^{l-2}$، به این دستگاه برابری‌ها می‌رسیم:

$$\alpha = a_0 + a_1\zeta + \dots + a_{l-2}\zeta^{l-2}$$
$$\alpha\zeta = a_0^{(1)} + a_1^{(1)}\zeta + \dots a_{l-2}^{(1)}\zeta^{l-2}$$
$$\dots\dots\dots\dots\dots\dots$$
$$\alpha\zeta^{l-2} = a_0^{(l-2)} + a_1^{(l-2)}\zeta + \dots + a_{l-2}^{(l-2)}\zeta^{l-2}$$

با ضریب‌های $a_i^{(j)}(i,j=0,1,\ldots,l-2)$ که عددهایی گویا و درست‌اند.

ولی در این‌صورت، باتوجه به پیش‌قضیهٔ ۱ بخش ۱۱، عدد α ریشهٔ معادله‌ای است به‌صورت

$$x^{l-1}+A_1x^{l-2}+\ldots+A_{l-1}=0$$

که در آن A_1، ...، A_{l-1} عددهایی گویا و درست‌اند. بنابراین $\alpha\in D$.

این روش تشکیل معادله‌ای که α در آن صدق کند، تنها محاسبهٔ با عددهای گویا را نیاز دارد.

چندجمله‌ای (۵) برای هر عضو $\alpha\in K_l$ معین است. مقدار ثابت آن، برابر است با نُرم $N\alpha$ از عدد α. ضریب جالب دیگر در این چندجمله‌ای، ضریب x^{l-2} است. اگر آن را با علامت مخالف درنظر بگیریم، اثر (trace) عضو α نامیده می‌شود و برای آن نماد $Tr\alpha$ را انتخاب کرده‌اند. باتوجه به دستور اول ویت داریم:

$$Tr\alpha=\alpha^{(1)}+\ldots+\alpha^{(l-1)}$$

از این‌جا نتیجه می‌شود که، اثر دارای ویژگی خطی است، یعنی برای عددهای دلخواه α و β عضو K_l و هر عدد گویای $a\in\mathbf{Q}$ داریم:

$$Tr(\alpha+\beta)=Tr\alpha+Tr\beta$$
$$Tr(a\alpha)=aTr\alpha$$

با دقت بیشتری چندجمله‌ای (۵) را بررسی می‌کنیم. در پیش‌قضیه‌هایی که در این‌جا می‌آوریم،

$$\alpha=a_0+a_1\zeta+\ldots+a_{l-2}\zeta^{l-2} \qquad (۶)$$

عضو دلخواهی از میدان K_l است.

پیش‌قضیهٔ ۱. اگر چندجمله‌ای $g(x)$ (با ضریب‌های گویا)، دارای این ویژگی باشد که دست‌کم برای یکی از مقدارهای i (از ۱ تا $l-1$) داشته‌باشیم: $g(\alpha^{(i)}) = 0$، آن‌وقت برای همهٔ مقدارهای $i = 1, \ldots, l-1$ داریم: $g(\alpha^{(i)}) = 0$.

اثبات. فرض کنید:

$$a(x) = a_0 + a_1 x + \ldots + a_{l-2} x^{l-2}$$

در این‌صورت $\alpha = a(\zeta)$ و به‌طور کلی $\alpha^{(i)} = a(\zeta^{(i)})$ برای i از ۱ تا $l-1$.

چندجمله‌ای

$$F(x) = g((ax))$$

را با شرط

$$F(\zeta^{(i)}) = g(a(\xi^{(i)})) = g(a^{(i)}) = 0$$

(دست‌کم برای یکی از مقدارهای $i = 1$، ...، $i = l-1$) درنظر می‌گیریم. این در واقع، به‌معنای آن است که چندجمله‌ای $F(x)$ با چندجمله‌ای تجزیه‌ناپذیر

$$\varphi(x) = x^{l-1} + x^{l-2} + \ldots + 1$$

ریشهٔ مشترک دارد. بنابراین، $F(x)$ بر این چندجمله‌ای بخش‌پذیر است و درنتیجه $F(\zeta^{(i)}) = 0$، یعنی $g(a^{(i)}) = 0$ برای هر i از ۱ تا $l-1$.

پیش‌قضیهٔ ۲. عدد درستی مثل q وجود دارد، به‌نحوی‌که

$$f(x) = h(x)^q$$

دارای ریشهٔ عدد جبری α باشد؛ $f(x)$ چندجمله‌ای (۵) و $h(x)$ چندجمله‌ای ساده‌نشدنی روی میدان $\mathbf{Q}$ با ضریب بزرگ‌تر برابر واحد است.

اثبات. چون $f(\alpha) = ۰$، بنابراین $f(x)$ بر $h(x)$ بخش‌پذیر است. فرض کنید $f(x)$ بر $h(x)^q$ بخش‌پذیر، ولی بر $h(x)^{q+۱}$ بخش‌ناپذیر باشد، و فرض کنید

$$f(x) = g(x)h(x)^q$$

اگر $g(x)$ برابر مقدار ثابتی نباشد، آن‌وقت دست‌کم یکی از ریشه‌های $\alpha^{(i)}$ چندجمله‌ای $f(x)$ $(i = ۱, \ldots, l-۱)$، $g(x)$ را برابر صفر می‌کند. ولی در این‌صورت، بنابر پیش‌قضیهٔ ۱،

$$g(\alpha^{(i)}) = ۰, (i = ۱, \ldots, l-۱)$$

و به‌ویژه $g(\alpha) = g(\alpha^{(i)}) = ۰$. به‌این ترتیب، چندجمله‌ای $g(x)$ با چندجمله‌ای ساده‌نشدنی $h(x)$ ریشهٔ مشترک دارد، یعنی بر $h(x)$ بخش‌پذیر است و نتیجه می‌گیریم، چندجمله‌ای $f(x)$ بر $h(x)^{q+۱}$ بخش‌پذیر می‌شود. تناقض حاصل، ثابت می‌کند که $g(x)$ مقداری ثابت است، یعنی باید داشته‌باشیم: $f(x) = h(x)^q$ (زیرا ضرب جمله‌های بزرگ‌تر در $f(x)$ و $h(x)$ برابر واحد است).

پیش‌قضیهٔ ۳. اگر α عدد جبری درستی باشد، آن‌وقت همهٔ ضریب‌های چندجمله‌ای $f(x)$، عددهای گویای درستی هستند.

اثبات. می‌دانیم، چندجمله‌ای $h(x)$ که (روی $\mathbf{Q}$) ساده‌نشدنی باشد، ریشهٔ α را بپذیرد و ضریب بزرگ‌تر آن برابر ۱ باشد، ضریب‌های درستی دارد. بنابراین، چندجمله‌ای $f(x) = h(x)^q$ هم ضریب‌های درستی خواهد داشت.

نتیجه. اثر $Tr\alpha$ از هر عدد جبری درست $\alpha \in K_l$، عدد گویا و درستی است.

توجه به این نکته سودمند است که، این حکم، خصلتی بسیار کلی دارد.

θ را عدد جبری درست و دلخواهی می‌گیریم. فرض کنید، این عدد، ریشه‌ای از یک معادلهٔ ساده‌نشدنی درجهٔ n باشد. در این‌صورت، می‌توان

ثابت کرد (با بخش ۶ مقایسه کنید)، مجموعهٔ K از همهٔ عددهای به‌صورت

$$a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1} \qquad (۷)$$

(a_0، a_1، ...، a_{n-1} عددهای گویای دلخواه‌اند)، میدانی (و البته از درجهٔ n) است. آن را با نماد $\mathbf{Q}(\theta)$ نشان می‌دهند. هرچه در بازهٔ میدان K_l گفته‌ایم، برای هر میدان $\mathbf{Q}(\theta)$ هم درست است (البته، به‌شرطی‌که $l-1$ را به n و ζ را به θ تبدیل کنیم). به‌ویژه، اثر هر عدد جبری درست از $\mathbf{Q}(\theta)$، عددی گویا و درست است.

شبیه حلقهٔ D_l، حلقهٔ $\mathbf{Z}[\theta]$، شامل همهٔ عددهای به‌صورت (۷) با عددهای درست a_0، a_1، ...، a_{n-1} است. اثبات این‌که، همهٔ این عددها، عددهای جبری درست‌اند، یعنی رابطهٔ $\mathbf{Z}[\theta] \subset D$ برقرار است (D، حلقهٔ عددهای درست میدان $K = \mathbf{Q}(\theta)$ است)، باز هم به قوت خود باقی می‌ماند (در هر دو حالت).

این یادآوری، به‌ویژه از این جهت جالب است که، هر میدان با درجهٔ محدود، به‌صورت $\mathbf{Q}(\theta)$ است.

اکنون می‌توانیم به‌عکس مطلب بپردازیم.

اثبات رابطهٔ $D \supset D_l$. باید ثابت کنیم، اگر عضو (۶) از میدان K_l عدد جبری درستی است، آن‌وقت همهٔ ضریب‌های a_0، a_1، ...، a_{l-2} عددهای گویا و درست‌اند.

برای این منظور، در آغاز، اثر $Tr\alpha$ از عدد α را محاسبه می‌کنیم (که باتوجه به نتیجهٔ پیش‌قضیهٔ ۲، عدد گویا و درستی است).

اگر $\alpha = \zeta^k$ $(k = 1, \ldots, l-1)$، آن‌وقت عددهای $\alpha^{(1)}$، ...، $\alpha^{(l-1)}$، بدون توجه به ردیف آن‌ها، بر عددهای $\zeta^{(1)}$، ...، $\zeta^{(l-1)}$ منطبق‌اند (بخش ۶، دستور (۱۰) را ببینید)، یعنی این برابری برقرار است:

$$Tr\zeta^k = -1, k = 1, \ldots, l-1$$

زیرا باتوجه به دستور ویت، مجموع ریشه‌های $\zeta^{(1)} + \ldots + \zeta^{(l-1)}$ از

چندجمله‌ای $x^{l-1}+x^{l-2}+\ldots+1$ برابر است با -1. اگر هم $k=0$، آن‌وقت $\zeta^k=l-1$.

از این‌جا، باتوجه به خطی بودن اثر، نتیجه می‌شود که اثر عدد (۶) با این دستور بیان می‌شود:

$$Tr\alpha=(l-1)a_0-a_1-\ldots-a_{l-2}$$

با روشی مشابه، می‌توان محاسبه کرد که برای هر k (از ۰ تا $l-2$) داریم:

$$Tr(\zeta^{-k}\alpha-\zeta\alpha)=la_k$$

چون $\zeta^{-k}\alpha-\zeta\alpha$، همراه با α، عدد جبری درستی است (متعلق به حلقهٔ D)، ثابت می‌شود که همهٔ عددهای la_k (برای k از ۰ تا $l-2$)، عددهایی گویا و درست‌اند.

بنابراین $l\alpha\in D_l$ و درنتیجه

$$\alpha=b_0+b_1\lambda+\ldots+b_{l-2}\lambda^{l-2},\lambda=1-\zeta \qquad (8)$$

که در آن b_0، b_1، ...، b_{l-2} عددهایی درست‌اند (بخش ۶، دستور (۱۵) را ببینید).

برای کامل کردن اثبات، اکنون باید ثابت کنیم، همهٔ ضریب‌های b_0، b_1، ...، b_{l-2} بر l بخش‌پذیرند. با فرض $b_{-1}=0$، از استقرای ریاضی نسبت به k، از $k=-1$ تا $k=l-2$ استفاده می‌کنیم.

فرض می‌کنیم، برای مقداری از k $(0\le k<l-2)$، همهٔ ضریب‌های b_s $(s<k)$ بر l بخش‌پذیر باشند. در این‌صورت، همهٔ جمله‌ها در (۸)، به‌جز جملهٔ $b_k\lambda^k$، بر λ^{k+1} بخش‌پذیرند (زیرا $l\sim\lambda^{l-1}$؛ بخش ۶ دستور (۱۴) را ببینید). بنابراین، جمله $b_k\lambda^k$ هم بر λ^{k+1} بخش‌پذیر می‌شود، یعنی عدد گویا و درست b_k بر λ بخش‌پذیر است. و این، به‌معنای آن است که b_k بر l بخش‌پذیر است.

توجه کنیم، در این استدلال، در واقع از ویژگی میدان K_l استفاده کردیم. بنابراین، تعجبی ندارد که، شبیه برابری $D_l = D$ در میدان دلخواهی از عددهای جبری $\mathbf{Q}(\theta)$، در حالت کلی نادرست باشد، یعنی میدان‌هایی از $\mathbf{Q}(\theta)$ وجود داشته‌باشد، که در آن، عددهای درست

$$a_۰ + a_۱\theta + \ldots + a_{n-۱}\theta^{n-۱}$$

با ضریب‌های غیردرست $a_۰$، $a_۱$، ...، $a_{n-۱}$ وجود داشته‌باشند.

برای نمونه، میدان $\mathbf{Q}(\sqrt{-۳})$ را درنظر می‌گیریم. از شرطی که در بخش ۵ دربارهٔ میدان $K_۳$ آوردیم، نتیجه می‌شود که میدان $\mathbf{Q}(\sqrt{-۳})$ بر میدان $K_۳$ منطبق است و بنابراین، عددهای درست آن، به‌این صورت‌اند:

$$\frac{a + b\sqrt{-۳}}{۲}$$

که در آن، a و b عددهای گویا و درستی هستند که یا هردو زوج و یا هردو فردند.

باوجود این، بدون دشواری خاصی می‌توان ثابت کرد، برای هر میدان K با درجهٔ محدود n، گروه جمع حلقهٔ D آن از عضوهای درست، شبکه‌ای از مرتبهٔ n است، یعنی چنان عددهای درست $\omega_۱$، ...، ω_n وجود دارند که هر عدد درست $\alpha \in D$، تنها به یک شکل به‌صورت

$$a_۱\omega_۱ + \ldots + a_n\omega_n$$

نمایش داده می‌شود ($a_۱$، ...، a_n عددهایی درست‌اند). به‌همین مناسبت، بهتر است گفته شود که $\omega_۱$، ...، ω_n، پایهٔ اصلی میدان K را تشکیل می‌دهند.

ازجمله، برای $K = \mathbf{Q}(\sqrt{-۳})$، پایهٔ اصلی از عددهای

$$۱, \frac{۱ + \sqrt{-۳}}{۲}$$

تشکیل شده‌است.

این حقیقت که پایهٔ اصلی وجود دارد، به این معنا است که حلقهٔ D، دارای ویژگی الف) از قضیهٔ ۱ بخش ۱۱ است. پیش از این هم یادآوری کردیم که، به‌خودی‌خود، ویژگی ج) را هم دارد. به‌جز این، به‌سادگی دیده می‌شود (که ما هم در واقع، آن را ثابت کردیم) که، دارای ویژگی ب) هم هست. بنابراین حلقهٔ عددهای درستِ یک میدان عددهای جبری، دارای نظریهٔ بخشیاب‌ها است؛ درضمن، گروه متناظر خانواده‌های بخشیاب‌ها، گروهی متناهی است.

و این، بنیادی‌ترینِ نتیجه‌گیری، در تمامی نظریهٔ عددهای جبری است.

۱۳

عددهای اول سامان‌پذیر

به‌این ترتیب، ثابت کردیم، می‌توان تعریف عدد اول سامان‌پذیر را تا حد زیادی ساده کرد. تعریف نهایی را می‌توان به‌این ترتیب ارائه داد. عدد اول l وقتی سامان‌پذیر است که بخشیابی از عدد h، تعداد خانواده‌های ایده‌آل‌های حلقهٔ D_l نباشد.

در رابطه با این تعریف، باید از مسالهٔ مربوط به محاسبهٔ عدد h آغاز کنیم. باید برای این عدد، دستور روشنی پیدا کنیم. ثابت می‌شود، چنین دستوری وجود دارد، ولی اثبات آن، از چارچوب این کتاب بیرون است. به‌همین مناسبت، آن را بدون اثبات می‌آوریم.

جدا از همهٔ آن‌چه گفتیم، باید با دقت تمام، انتخاب ریشهٔ ζ از چندجمله‌ای دایره بُر را (با بخش ۶ مقایسه کنید)، تنظیم کنیم. فرض می‌کنیم:

$$\zeta = \cos\frac{۲\pi}{l} + i\sin\frac{۲\pi}{l}$$

می‌دانیم، خانواده‌های مخالف صفر

$$\{۱\}, \{۲\}, \ldots, \{l-۱\} \qquad (۱)$$

از عددهای گویای درست، نسبت به مدول اول l، گروه نسبت به ضربِ $\mathbf{Z}^*/l$ از مرتبهٔ $l-۱$ را تشکیل می‌دهند (بخش ۲ را ببینید).

پیش‌قضیهٔ ۱. گروه $\mathbf{Z}^*/l$، یک گروه دوری است.

اثبات. m را کوچک‌ترین مضرب مشترک مرتبه‌های همهٔ عضوهای گروه $\mathbf{Z}^*/l$ می‌گیریم. در این‌صورت

$$\{a\}^m = \{۱\} \qquad (۲)$$

که در آن $\{a\}$ عضو دلخواهی از $\mathbf{Z}^*/l$ و m کوچک‌ترین عددی است که این ویژگی را دارد. بنابراین $m \leq l-۱$، زیرا برای هر $\{a\} \in \mathbf{Z}^*/l$ داریم: $\{a\}^{l-۱} = \{۱\}$ (زیرا $l-۱$، مرتبهٔ گروه $\mathbf{Z}^*/l$ است).

اکنون مجموعهٔ $\mathbf{Z}/l$ از همهٔ خانواده‌ها را نسبت به مدول l درنظر می‌گیریم. این مجموعه، یک میدان است که گروه ضربی آن همان گروه $\mathbf{Z}^*/l$ است. برابری (۲) به این معنی است که معادلهٔ $x^m - ۱$ در این میدان، $l - ۱$ ریشهٔ مختلف (۱) را دارد. چون معادله از درجهٔ m است، این وضع تنها وقتی ممکن است که داشته‌باشیم: $m \geq l - ۱$.

به‌این ترتیب $m = l - ۱$. از این‌جا نتیجه می‌شود (با استدلالی مشابه) که در $\mathbf{Z}^*/l$، عضوی با مرتبهٔ $l - ۱$ وجود دارد. و این هم، به‌معنای آن است که $\mathbf{Z}^*/l$ گروهی دوری است.

عددهای g از خانوادهٔ $\{g\}$، که مولدهای گروه $\mathbf{Z}^*/l$ هستند، ریشه‌های اولیه (primitive roots) نسبت به مدول l نامیده می‌شوند. این عددها، با این ویژگی مشخص می‌شوند: کوچک‌ترین m مثبت، که برای آن داشته‌باشیم $g^m \equiv ۱(\mathrm{mod} l)$، برابر است با $l - ۱$.

برای نمونه، به‌ازای $l = ۵$، ریشهٔ اولیه برابر ۲ و به‌ازای $l = ۷$ برابر عدد ۳ است. در واقع

$$۲^۰ \equiv ۱(\mathrm{mod}۵),\ ۲^۱ \equiv ۲(\mathrm{mod}۵),\ ۲^۲ \equiv ۴(\mathrm{mod}۵),\ ۲^۳ \equiv ۳(\mathrm{mod}۵)$$

$$۳^۰ \equiv ۱(\mathrm{mod}۷),\ ۳^۱ \equiv ۳(\mathrm{mod}۷),\ ۳^۲ \equiv ۲(\mathrm{mod}۷),$$

$$۳^۳ \equiv ۶(\mathrm{mod}۷),\ ۳^۵ \equiv ۵(\mathrm{mod}۷)$$

یک بار و برای همیشه، ریشهٔ اولیهٔ g را نسبت به مُدول l، انتخاب و تثبیت می‌کنیم. برای هر $k \geq ۰$، نماد g_k را برای عددی از رشتهٔ ۱، ۲، ...، $l - ۱$ به‌کار می‌بریم که دارای این ویژگی باشد که

$$g^k \equiv g_k(\mathrm{mod} l),\ k = ۰, ۱, \ldots, l - ۲$$

(کم‌ترین ماندهٔ مثبت عدد g^k) چون g، ریشهٔ اولیه است، همهٔ عددهای $g_۰ = ۱$، $g_۱$، ...، $g_{l-۲}$ مختلف‌اند.

سپس، فرض می‌کنیم

$$G(x) = g_0 + g_1 x + \ldots + g_{l-2} x^{l-2},$$
$$\theta = \cos \frac{2\pi}{l-1} + i \sin \frac{2\pi}{l-1}$$

و

$$h_1 = \frac{1}{(2l)^{s-1}} |G(\theta) G(\theta^3) \ldots G(\theta^{l-2})|$$

که در آن $s = \frac{l-1}{2}$.

گزارهٔ ۱. h_1، عدد درست مثبتی است.

برای نمونه، $l = 5$ می‌گیریم. در این‌صورت

$$s = 2,\ \theta = i,\ g = 2$$
$$G(x) = 1 + 2x + 4x^2 + 3x^3$$

و بنابراین

$$G(\theta) = 1 + 2i + 4i^2 + 3i^3 = -3 - i,$$
$$G(\theta^3) = 1 - 2i + 4i^2 - 3i^3 = -3 + i$$

از آن‌جا

$$h_1 = \frac{1}{(2 \times 5)^1} |(-3 - i)(-3 + i)| = \frac{9 + 1}{10} = 1$$

به‌همین ترتیب، اگر $l = 7$، آن‌وقت

$$s = 3,\ \theta = \frac{1 + i\sqrt{3}}{2},\ g = 3$$

و

$$G(x) = ۱ + ۳x + ۲x^۲ + ۶x^۳ + ۴x^۴ + ۵x^۵$$

و به‌سادگی محاسبه می‌شود:

$$|G(\theta)G(\theta^۳)G(\theta^۵)| = ۱۹۶$$

بنابراین

$$h_۱ = \frac{۱۹۶}{(۲ \times ۷)^۲} = ۱$$

مسالهٔ ۱. برای دنبالهٔ عددی دلخواه

$$x_۰, x_۱, \ldots, x_{۲(s-۱)}$$

نماد $H(x_۰, x_۱, \ldots, x_{۲(s-۱)})$ را دربارهٔ دترمینان ماتریس (x_{ij}) درنظر می‌گیریم که در آن: $i, j = ۰, ۱, \ldots, s-۱$ و $x_{ij} = x_{i+j}$. ثابت کنید:

$$h_۱ = \frac{|H(g_s - g_۰, g_{s+۱} - g_۱, \ldots g_{۲s-۲} - g_{۲s-۲})|}{(۲l)^{s-۱}}$$

مسالهٔ ۲. ثابت کنید، به‌ازای $l < ۲۳$ داریم $h_۱ = ۱$ و به‌ازای $l = ۲۳$ به‌دست می‌آید: $h_۱ = ۳$. همچنین ثابت کنید، برای $l = ۳۷$، داریم: $h_۱ = ۳۷$.

می‌توان ثابت کرد (حالت خاصی از قضیهٔ دشوار دیریکله دربارهٔ واحدهای میدان دلخواهی از عددهای جبری)، در حلقهٔ D_l، به تعداد $s-۱$ واحد

$$\varepsilon_۱, \ldots, \varepsilon_{s-۱}$$

وجود دارد (که آن‌ها را واحدهای اصلی می‌نامند)، و هر واحد ε، به‌صورت یک ارزشی، این‌طور نشان داده می‌شود:

$$\varepsilon = (-\zeta)^a \varepsilon_۱^{a_۱} \ldots \varepsilon_{s-۱}^{a_{s-۱}}$$

که در آن a، $a_۱$، ...، $a_{s-۱}$ عددهایی درست‌اند و درضمن $۰ \le a < ۲l$.

به‌عنوان ریشهٔ $\zeta^{(k)}$ $(k = ۱, \dots, l-۱)$ از چندجمله‌ای دایره بُر که با نگاشت $\alpha \to \alpha^{(k)}$ معین می‌شود (بخش ۶ را ببینید)، مثل همیشه، عدد ζ^k را انتخاب می‌کنیم. باتوجه به انتخاب ریشهٔ ζ، برای هر $\alpha \in K_l$، این رابطه‌ها برقرار است:

$$\alpha^{(s+۱)} = \overline{\alpha^{(s)}}, \alpha^{(s+۲)} = \overline{\alpha^{(s-۱)}}, \dots, \alpha^{(l-۱)} = \overline{\alpha^{(۱)}}$$

برای انتخاب $\varepsilon_۱$، ...، $\varepsilon_{s-۱}$ (واحدهای اصلی)، قدرمطلق دترمینان

$$\begin{vmatrix} \ln|\varepsilon_۱^{(۱)}| & \dots & \ln|\varepsilon_۱^{(s-۱)}| \\ \dots & \dots & \dots \\ \ln|\varepsilon_{s-۱}^{(۱)}| & \dots & \ln|\varepsilon_{s-۱}^{(s-۱)}| \end{vmatrix}$$

را با $R_۰$ نشان می‌دهیم. می‌توان ثابت کرد، عدد $R_۰$ به انتخاب واحدهای اصلی بستگی ندارد و تنها باتوجه به میدان K_l معین می‌شود (معمول است که به‌جای $R_۰$، عدد $R = ۲^{s-۱}R_۰$ را درنظر می‌گیرند و آن را «تنظیم کن» (regulator) میدان K_l می‌نامند).

فرض می‌کنیم

$$h_۲ = \frac{۱}{R_۰} \prod_{k=۱}^{s-۱} \left| \sum_{j=۰}^{s-۱} \theta^{۲kj} \ln|۱ - \zeta^{g_j}| \right|$$

گزارهٔ ۲. $h_۲$، عددی درست و مثبت است.

برای نمونه، به‌ازای $l = ۵$، یعنی به‌ازای $s = ۲$، در دستور $h_۲$ تنها یک عامل وجود دارد:

$$\sum_{j=۰}^{۱} \theta^{۲j} \ln|۱ - \zeta^{g_j}| = \ln|۱ - \zeta| - \ln|۱ - \zeta^۲|$$

که پاسخ‌گوی مقدار $k = ۱$ است (به یاد بیاوریم که در این حالت: $\theta = i$، $g_۰ = ۱$ و $g_۱ = ۲$). بنابراین

$$R_۰ h_۲ = |\ln|۱ - \zeta| - \ln|۱ - \zeta^۲|| = |\ln|۱ + \zeta||$$

که در آن عدد $۱ + \zeta$ واحد است. زیرا (بخش ۶ را ببینید):

$$N(۱ + \zeta) = N(۱ - \zeta^۲)N(۱ - \zeta)^{-۱} = ۱$$

چون در این حالت $s - ۱ = ۱$، بنابراین دستگاه واحدهای اصلی، تنها شامل یک واحد $\varepsilon_۱$ است. درنتیجه $R_۰ = |\ln|\varepsilon_۱||$ و

$$۱ + \zeta = (-\zeta)^a \varepsilon_۱^b$$

که در آن a و b، عددهایی درست‌اند. ولی در این صورت $|۱ + \zeta| = |\varepsilon_۱|^b$ و از آن‌جا

$$h_۲ = \left|\frac{\ln|۱ + \zeta|}{\ln|\varepsilon_۱|}\right| = |b|$$

بنابراین، به‌ازای $l = ۵$، عدد $h_۲$ به‌واقع عددی مثبت و درست است.

گزارهٔ ۳. خانواده‌های بخشیاب‌های h از حلقهٔ K_l برابر است با حاصل‌ضرب عددهای

$$h = h_۱ h_۲$$

و این، دستور روشنی برای محاسبهٔ عدد h است. با وجود این، اگر عامل اول یعنی $h_۱$ به خودی خود قابل محاسبه است، دربارهٔ عامل دوم، یعنی $h_۲$، که در آن تنظیم کُنِ $R_۰$ شرکت دارد، چنین ادعایی نمی‌توان کرد. موضوع این است: روشی عملی (یعنی یک اَلگوریتم) وجود ندارد که به‌کمک آن بتوان واحدهای اصلی را، به‌نحوی‌که برای همهٔ حلقه‌های K_l سودمند باشد، محاسبه کرد. اَلگوریتمی نظری وجود دارد؛ ولی برای مقدارهای نه‌چندان بزرگ l هم، منجر به حجم بزرگی محاسبه می‌شود (که تنها به‌کمک رایانه‌ها می‌توان

از عهدهٔ آن‌ها برآمد). به‌همین دلیل، توجه اصلی به قضیهٔ کومر جلب شد که در این‌جا می‌آوریم و، البته، اثباتی بسیار دشوار دارد.

گزارهٔ ۴. عدد h، وقتی و تنها وقتی بر l بخش‌پذیر است که عدد h_1 بر l بخش‌پذیر باشد.

به‌این ترتیب، برای آزمایش دربارهٔ عدد مفروض l و تعیین سامان‌پذیری آن، کافی است عدد h_1 را محاسبه کنیم. ازجمله، باتوجه به مسالهٔ ۲ (که در بالا آوردیم) می‌توان نتیجه گرفت، عدد اول ۳۷ سامان‌پذیر نیست و همهٔ عددهای $l \leq ۲۳$ سامان‌پذیرند.

محاسبهٔ عدد h_1، ولو با ابزارهای خودکار، تا حد زیادی ملال‌آور است (خواننده‌ای که مسالهٔ ۲ را حل کرده‌باشد، در این‌باره با ما هم‌عقیده می‌شود). به‌همین مناسبت، این پرسش پیش می‌آید: آیا بدون محاسبهٔ h_1، نمی‌توان دربارهٔ بخش‌پذیری آن بر l تحقیق کرد؟ معلوم شده‌است که، به این پرسش، می‌توان پاسخ مثبت داد. در واقع، اگر از این حقیقت استفاده کنیم که در دستور مربوط به عدد h_1 مقدارهای $G(\theta^h)$ از چندجمله‌ای $G(x)$، عددهای درست میدان $(l-1)$ دوری K_{l-1} شرکت دارد (میدان K_m، وقتی m عددی اول نباشد، شبیه حلقهٔ K_l معین می‌شود)، می‌توان بی دشواری ثابت کرد، h_1 وقتی و تنها وقتی بر l بخش‌پذیر است (یعنی l عدد اولی سامان‌پذیر نیست) که دست‌کم به‌ازای یکی از مقدارهای k (از $k=1$ تا $k=l-4$)، عدد گویا و درست $G(g^k)$ بر l^2 بخش‌پذیر باشد (درضمن، فرض می‌شود، ریشهٔ اولیه g طوری انتخاب شده‌باشد که هم‌نهشتی $g^{l-1} \equiv 1 (\mathrm{mod} l^2)$ برقرار باشد؛ و این عمل را همیشه، با تغییر g به خانوادهٔ آن $\{g\}$ می‌توان انجام داد). در این‌جا، به اثبات کامل و دقیق این گزاره نمی‌پردازیم و خود را به این محدود می‌کنیم که، از این شرط به‌صورتی راحت‌تر استفاده کنیم.

بنابر تعریف، برای هر j (از $j=0$ تا $j=l-2$)

$$g_j = g^j (\mathrm{mod} l)$$

یعنی عددهای درستی مثل a_j می‌توان پیدا کرد که داشته‌باشیم:

$$g_j \equiv g^j + la_j (\mathrm{mod} l^۲)$$

اگر این هم‌نهشتی را به توان $k+۱$ برسانیم $(k = ۱, ۳, \ldots, l-۴)$، به این هم‌نهشتی می‌رسیم:

$$g_j^{k+۱} \equiv g_j^{j(k+۱)} + (k+۱) g^{jk} l a_j (\mathrm{mod} l^۲)$$

از این‌جا محاسبه می‌شود که

$$g_j^{k+۱} \equiv g^{j(k+۱)} + (k+۱) g^{jk} (g_j - g^j) (\mathrm{mod} l^۲)$$

یعنی

$$g_j^{k+۱} \equiv (k+۱) g_j g^{jk} - k g^{j(k+۱)} (\mathrm{mod} l^۲)$$

بنابراین

$$\sum_{j=۰}^{l-۲} g_j^{k+۱} \equiv (k+۱) \sum_{j=۰}^{l-۲} g_j g^{jk} - k \sum_{j=۰}^{l-۲} g^{j(k+۱)} (\mathrm{mod} l^۲)$$

ولی

$$\sum_{j=۰}^{l-۲} g^{j(k+۱)} = \frac{g^{(l-۱)(k+۱)} - ۱}{g^{k+۱} - ۱} \equiv ۰ (\mathrm{mod} l^۲)$$

زیرا بنابر شرط $g^{l-۱} \equiv ۱ (\mathrm{mod} l^۲)$ و $g^{k+۱} - ۱ \not\equiv ۰ (\mathrm{mod} l)$ (به‌ازای $k+۱ \leq l-۳$). به‌جز این، بنابر تعریف

$$\sum_{j=۰}^{l-۲} g_j g^{jk} = G(g^k)$$

و

$$\sum_{j=۰}^{l-۲} g_j^{k+۱} = \sum_{n=۱}^{l-۱} n^{k+۱}$$

(عددهای g_0، g_1، ...، g_{l-2}، بدون توجه به ردیف آن‌ها، همان عددهای ۱، ۲، ...، $l-1$ هستند). اگر مجموع اخیر را $S_{k+1}(l)$ بنامیم، به این هم‌نهشتی می‌رسیم:

$$S_{k+1}(l) \equiv (k+1)G(g^k) \pmod{l^2}$$

به‌این ترتیب، هم‌نهشتی $G(g^k) \equiv 0 \pmod{l^2}$ هم‌ارز است با هم‌نهشتی $S_{k+1}(l) \equiv 0 \pmod{l^2}$.

بنابراین، عدد l وقتی و تنها وقتی سامان‌ناپذیر است که چنان عددی برای k $(k = 1, 3, \ldots, l-4)$ وجود داشته‌باشد، به‌نحوی‌که $S_{k+1}(l)$ بر l^2 بخش‌پذیر باشد.

به‌زبان دیگر، عدد l، وقتی و تنها وقتی سامان‌پذیر است که برای هر k $(k = 2, 4, \ldots, l-3)$، عدد

$$S_k(l) = 1^k + 2^k + \ldots + (l-1)^k$$

بر l^2 بخش‌پذیر نباشد.

راحت‌تر است، مجموع کلی‌تری را درنظر بگیریم:

$$S_k(m) = 1^k + 2^k + \ldots + (m-1)^k$$

به‌سادگی و با استقرای ریاضی می‌توان ثابت کرد، عددهای $S_k(m)$، مقدارهای چندجمله‌ای $S_k(x)$ از درجهٔ k به‌ازای $x = m$ که ضریب‌های گویایی دارد، ضریب جملهٔ بزرگ‌تر آن برابر $\frac{1}{k+1}$ و جملهٔ ثابت آن برابر صفر است. برای نمونه

$$S_1(x) = \frac{(x-1)x}{2} = \frac{1}{2}x^2 - \frac{1}{2}x,$$

$$S_2(x) = \frac{(x-1)x(2x-1)}{6} = \frac{1}{3}x^3 - \frac{1}{2}x^2 + \frac{1}{6}x,$$

$$S_3(x) = \frac{(x-1)^2x^2}{4} = \frac{1}{4}x^4 - \frac{1}{2}x^3 + \frac{1}{4}x^2$$

فرض کنید:

$$(k+1)S_k(x) = x^{k+1} + \binom{k+1}{1} B_1 x^k + \\ + \binom{k+1}{2} B_2 x^{k-1} + \ldots + \binom{k+1}{k} B_k x$$

ثابت می‌شود، عددهای B_1، B_2، ...، به k بستگی ندارند. آن‌ها را، عددهای برنولی می‌نامند.

جالب است که، عددهای برنولی، ضمن حل یکی از مساله‌های اخترشناسی وارد در ریاضیات شد.

مطلب بر سر این است که دنبالهٔ بی‌پایان عددهای برنولی

$$B_1, B_2, B_3, \ldots$$

ضمن تبدیل برخی تابع‌های ساده به‌صورت رشتهٔ توانی ظاهر می‌شوند؛ ازجمله می‌توان ثابت کرد که:

$$\cot x = \frac{1}{x} - \frac{B_2}{2!}2^2 x + \frac{B_4}{4!}2^4 x^3 - \ldots + \\ + (-1)^k \frac{B_{2k}}{(2k)!}2^{2k} x^{2k-1} + \ldots$$

همین رشته بود که، ضمن بررسی‌های اخترشناسی، در برابر برنولی قرار گرفت.

این‌که در رشتهٔ مربوط به بسط $\cot x$، تنها آن عددهای برنولی ظاهر می‌شوند که اندیسی زوج دارند، تصادفی نیست، زیرا به‌سادگی می‌توان ثابت کرد، همهٔ عددهای برنولی که اندیسی فرد دارند (به‌جز عدد B_1)، برابر صفرند:

اگر $k > 0$، آن‌وقت $B_{2k+1} = 0$

عددهای برنولی با اندیس زوج $(B_{۲k})$، ویژگی‌های جالبی دارند. ازجمله، مقدارهای تابع معروف ریمان (تابع ζ)، وقتی آوندی زوج داشته‌باشد، برحسب عددهای برنولی بیان می‌شوند:

$$\zeta(۲k) = (-۱)^{k-۱}\frac{(۲\pi)^{۲k}}{۲(۲k)!}B_{۲k}, k \geq ۱$$

نخستین عددهای برنولی به‌این صورت‌اند:

$$B_۱ = -\frac{۱}{۲},\ B_۲ = \frac{۱}{۶},\ B_۴ = -\frac{۱}{۳۰},\ B_۶ = \frac{۱}{۴۲},\ B_۸ = -\frac{۱}{۳۰},$$

$$B_{۱۰} = \frac{۵}{۶۶},\ B_{۱۲} = -\frac{۶۹۱}{۲۷۳۰},\ B_{۱۴} = \frac{۷}{۶},\ B_{۱۶} = -\frac{۳۶۱۷}{۵۱۰},$$

$$B_{۱۸} = \frac{۴۳۸۶۷}{۷۹۸},\ B_{۲۰} = -\frac{۱۷۴۶۱۱}{۳۳۰}$$

صورت این کسرها، به‌سرعت بزرگ می‌شود. برای نمونه

$$B_{۳۴} = \frac{۲\ ۵۷۷\ ۸۶۷\ ۸۵۸\ ۳۶۷}{۶}$$

فرض کنید

$$B_k = \frac{P_k}{Q_k}$$

معرف عدد B_k باشد. بدون دشواری خاصی، می‌توان ثابت کرد، به‌ازای $m < l - ۱$، مخرج Q_m از عدد B_m، بر l بخش‌پذیر نیست.

ولی باتوجه به دستور (۳)، برای هر $k \geq ۱$، این برابری را داریم:

$$(k+۱)S_k(l) = \sum_{m=۰}^{k-۱}\binom{k+۱}{m}B_m l^{k+۱-m} + (k+۱)B_k l$$

یعنی

$$(k+۱)S_k(l)Q_k =$$
$$= \left[\left(\sum_{m=۰}^{k-۱}\binom{k+۱}{m}B_m l^{k-۱-m}\right)Q_k\right] l^۲ + (k+۱)P_k l$$

بنابراین، برای $k < l - ۱$، عدد واقع در سمت راست در پرانتزها، عددی درست است.

به هم‌نهشتی نسبت به مُدول $l^۲$ برمی‌گردیم و آن را به $(k + ۱)$ ساده می‌کنیم؛ به‌دست می‌آید:

$$S_k(l)Q_k \equiv P_k l (\mathrm{mod} l^۲)$$

بنابراین هم‌نهشتی $S_k(l) \not\equiv ۰ (\mathrm{mod} l^۲)$، وقتی و تنها وقتی برقرار است که داشته‌باشیم: $P_k \not\equiv ۰ (\mathrm{mod} l)$.

به‌این ترتیب ثابت شد:

قضیهٔ کومر. عدد اول l، وقتی و تنها وقتی سامان‌پذیر است که بخشیابی از صورت عددهای برنولی $B_۲$، $B_۴$، ...، $B_{l-۳}$ نباشد.

نمونه‌هایی می‌آوریم (عددهای برنولی را که پیش از این آوردیم، ببینید):

صورت $P_۲ = ۱$ بر ۵ بخش‌پذیر نیست.

صورت $P_۲ = ۱$ و صورت $P_۴ = -۱$ بر ۷ بخش‌ناپذیرند؛

صورت‌های $P_۲ = ۱$، $P_۴ = -۱$، $P_۶ = ۱$ و $P_۸ = -۱$ بر ۱۱ بخش‌پذیر نیستند.

صورت‌های $P_۲ = ۱$، $P_۴ = -۱$، $P_۶ = ۱$، $P_۸ = -۱$ و $P_{۱۰} = ۵$ بر ۱۳ بخش‌پذیر نیستند.

صورت‌های $P_۲ = ۱$، ...، $P_{۱۰} = ۵$، $P_۶ = -۶۹۱$ و $P_{۱۴} = ۷$ بر ۱۷ بخش‌ناپذیرند.

$P_۲ = ۱$، ...، $P_{۱۲} = ۷$ و $P_{۱۶} = -۳۶۱۷$ بر ۱۹ بخش‌پذیر نیستند.

$P_۲ = ۱$، ...، $P_{۱۶} = -۳۶۱۷$، $P_{۱۸} = ۴۳۸۸۷$ و $P_{۲۰} = -۱۷۴\,۶۱۱$ بر ۲۳ بخش‌پذیر نیستند.

بنابراین، همهٔ این نماها، سامان‌پذیرند. به‌زبان دیگر، برای نماهای ۵، ۷، ۱۱، ۱۳، ۱۷، ۱۹ و ۲۳، قضیهٔ فرما درست است.

به‌این ترتیب، دست‌کم برای این نماها، پاسخ قطعی را به‌دست آوردیم. در این مسیر تا کجا می‌توان پیش رفت؟

محاسبه‌های مشابه، ما را قانع می‌کند، بین صد عدد نخستین، تنها عددهای ۳۷، ۵۹ و ۶۷ سامان‌پذیر نیستند؛ ازجمله برای $l = ۶۷$، برای عدد $h_۱$ داریم:

$$h_۱ = ۸۵۳\,۵۱۳ = ۶۷ \times ۱۲\,۷۳۹$$

ولی، همان‌طور که گفته‌ایم، کومر توانست با استدلال‌های خاص، درستی قضیهٔ فرما را، برای این عددها هم ثابت کند.

درضمن، قضیهٔ بِن‌سِن، که در بخش ۲ از آن یاد کردیم، به‌سادگی از قضیهٔ کومر و برخی ویژگی‌های مقدماتی عددهای برنولی، نتیجه می‌شود.

۱۴

حل قطعی قضیهٔ فرما

دکتر شهریار شهریاری

پیش‌گفتار

کتاب حاضر داستان قضیهٔ آخر فرما را تا سال‌های دهه هفتاد دنبال می‌کند. اهمیت این کتاب در گردآوری جزئیات روش‌های جبری‌ای است که برای حل قضیهٔ آخر فرما اول بار توسط کومر[1]، به کار گرفته شد. برای مطالعهٔ کارهای کومر و ریاضی‌دان‌های بعدی که روش‌های او را تکمیل کردند، به جز کتاب‌های تخصصی منبع‌های کمی وجود دارد. این روش‌ها، خارج از کوشش برای اثبات قضیهٔ آخر فرما، برای بسیاری مساله‌های دیگر هم به کار می‌روند و لذا آشنایی با آن‌ها، برای خواننده علاقه‌مند، سودمند است. کتاب حاضر منبع نمونه‌ای برای این هدف است.

قضیهٔ آخر فرما، بعد از سیصد و پنجاه سال کوشش، در ۱۹۹۵ به وسیلهٔ آندرو وایلز[2] و با استفاده از نتایج بسیاری از ریاضی‌دانان دیگر ثابت شد. این اثبات به واقع یکی از مهم‌ترین موفقیت‌های ریاضیات سدهٔ بیستم است و در آن روش‌های جبری با روش‌های هندسی به نحو زیبا ولی بغرنجی مخلوط شده است.

در این موخرهٔ کوتاه، که برای علاقه‌مندان ریاضی، که تخصصی در هندسه جبری ندارند، نوشته شده است، می‌کوشیم خواننده را با جنبه‌هایی از این اثبات آشنا کنیم. هدف ما تنها توضیح رابطه اثبات قضیه آخر فرما با حدس‌های پایه‌ای در هندسه جبری است و در نتیجه به اصل اثبات وایلز نخواهیم پرداخت. کوشش ما تنها در این است که خواننده ایده‌ای کلی از

1-Kummer 2-Andrew Wiles

این بخش ریاضیات بگیرد. واضح است که فهم دقیق اثبات وایلز کار ساده‌ای نیست و نیاز به سال‌ها مطالعه عمیق دارد.

روش‌های مقدماتی، جبری و هندسی

قضیهٔ آخر فرما می‌گوید، اگر x، y، z، و $n > ۲$ عددهای درست باشند و فرض کنیم $x^n + y^n = z^n$، آن‌گاه دست‌کم یکی از سه عدد x، y و z برابر صفر خواهد بود. چگونه چنین حدسی را ثابت کنیم؟ سه نوع برخورد به چنین مساله‌ای طبیعی است.

روش اول کوشش در استفاده از روش‌های مقدماتی نظریهٔ عددها است. در چنین کوششی از ساختمان‌های جبری، از نظریهٔ عددهای مختلط، و از هندسه جبری استفاده نمی‌کنیم و فقط خاصیت‌های بخش‌پذیری عددهای درست را به کار می‌گیریم. اثبات معمول گنگ بودن عدد $\sqrt{۲}$ از همین نوع است. همان‌طور که در کتاب حاضر شرح داده شده است، خود فرما از همین روش‌ها برای اثبات حالت $n = ۴$ قضیه استفاده کرد. این روش‌های مقدماتی به‌معنای روش‌های ساده‌ای نیستند و به وسیلهٔ آن‌ها می‌توان نتیجه‌های زیادی دربارهٔ قضیه آخر فرما گرفت. اما اگر تنها به این روش‌ها بسنده کنیم فقط می‌توانیم چند حالت خاص قضیهٔ فرما را ثابت کنیم.

روش دوم استفاده از روش‌های جبری است. کتاب حاضر، اهمیت و کاربرد روش‌های جبری را به خوبی توضیح داده است و لذا در این‌جا دوباره به آن‌ها نمی‌پردازیم. به وسیلهٔ این روش‌ها قضیهٔ آخر فرما برای همهٔ عددهای درست n به نحوی که $n < ۴,۰۰۰,۰۰۰$ ثابت شد. با این‌که روش‌های جبری نقش مهمی در اثبات وایلز داشتند، ولی به تنهایی از عهدهٔ حل قضیهٔ آخر فرما برنیامدند.

روش سوم استفاده از هندسهٔ جبری است. چگونه می‌شود از هندسه برای حل مساله‌ای شبیه قضیهٔ آخر فرما استفاده کرد؟ قضیهٔ آخر فرما حکمی دربارهٔ عددهای درست است و دست‌کم در ریاضیات مقدماتی به طور معمول از

هندسه برای این‌گونه مساله‌ها استفاده نمی‌شود.

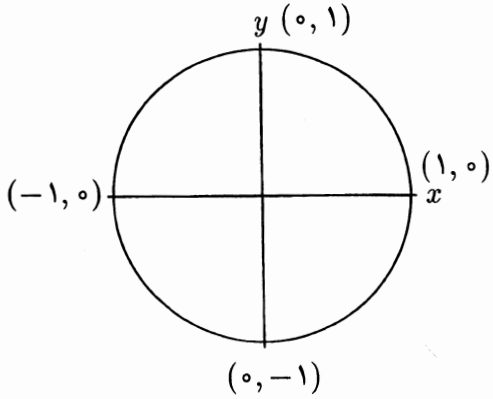
با یک مثال می‌توان امکان به کارگیری استدلال‌های هندسی را نشان داد. فرض کنید، همهٔ عددهای درستی را بخواهیم که در معادلهٔ $X^۲+Y^۲ = Z^۲$ صدق کنند. با تقسیم دو طرف بر $Z^۲$ خواهیم داشت:

$$\left(\frac{X}{Z}\right)^۲ + \left(\frac{Y}{Z}\right)^۲ = ۱$$

اگر فرض کنیم: $x = \frac{X}{Z}$ و $y = \frac{Y}{Z}$، آن وقت مساله تبدیل به یافتن جواب‌های گویای معادلهٔ

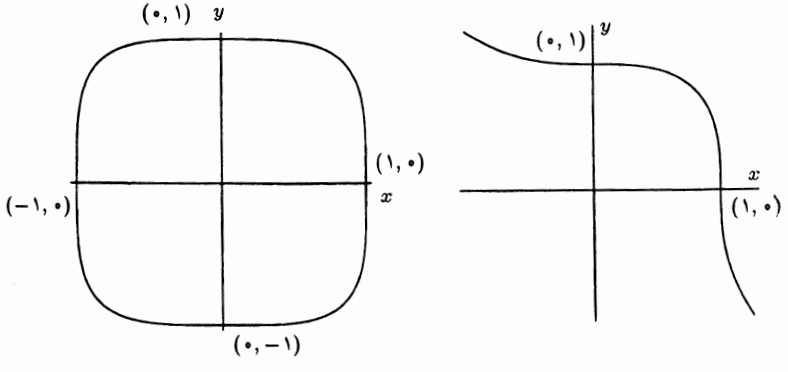
$$x^۲ + y^۲ = ۱$$

می‌شود. هر جواب گویا برای معادلهٔ اخیر جوابی درست برای معادلهٔ اول می‌دهد و برعکس هر جواب درست معادلهٔ اولی (با فرض $Z \neq ۰$) جوابی گویا برای معادلهٔ دوم می‌دهد. $x^۲ + y^۲ = ۱$ معادلهٔ دایره‌ای به مرکز مبداء مختصات و به شعاع یک است. در نتیجه باید به‌دنبال نقطه‌هایی روی دایره باشیم که مختصات آن‌ها عددهایی گویا باشند.



شکل ۱. دایرهٔ $x^۲ + y^۲ = ۱$

به همین ترتیب پیدا کردن جواب‌های درست برای معادله‌هایی همچون $X^۳ + Y^۳ = Z^۳$، $X^۴ + Y^۴ = Z^۴$ و سایر معادله‌های فرما منجر به پیدا کردن نقطه‌های با مختصات گویا بر خمی در صفحه می‌شود.

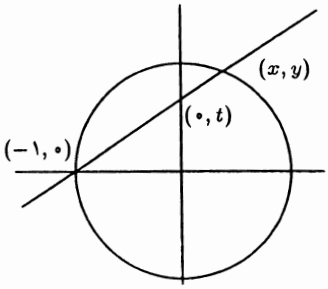


شکل ۲. خم‌های $x^۳ + y^۳ = ۱$ و $x^۴ + y^۴ = ۱$

نکته جالب این است که طبق قضیهٔ آخر فرما، خم اول (دایره) نقطه‌های بسیار با مختصات گویا دارد، ولی روی خم‌های بعدی همهٔ نقطه‌های با مختصات گویا دارای یک مختص صفر هستند.

چگونه نقطه‌های با مختصات گویا را روی یک خم پیدا کنیم؟ دربارهٔ دایره، راه حل ساده است. (x, y) را نقطه‌ای روی دایرهٔ $x^۲ + y^۲ = ۱$ درنظر بگیرید. خط راست بین نقطه $(۰, -۱)$ و نقطه (x, y) را رسم کنید (فرض کرده‌ایم که $(x, y) \neq (۰, -۱)$). محل برخورد این خط با محور yها را $(۰, t)$ بخوانید. با کمی محاسبه، و به سادگی دیده می‌شود که

$$t = \frac{y}{۱ + x} \qquad x = \frac{۱ - t^۲}{۱ + t^۲} \qquad y = \frac{۲t}{۱ + t^۲}$$



شکل ۳. پیدا کردن نقطه‌های با مختصات گویا روی خم $x^۲ + y^۲ = ۱$

نتیجه می‌گیریم، (x, y) نقطه‌ای با مختصات گویا وقتی و تنها وقتی روی دایره به شعاع واحد است که t عددی گویا باشد. لذا اگر $t = \frac{a}{b}$، و a و b عددهای درست، آن‌گاه

$$x = \frac{a^۲ - b^۲}{a^۲ + b^۲}, \quad y = \frac{۲ab}{a^۲ + b^۲}$$

پس برای پیدا کردن نقطه‌ای روی دایره با مختصات گویا، اول دو عدد درست a و b را انتخاب می‌کنیم و بعد با استفاده از دستورهای بالا، مختصات (x, y) را می‌یابیم. به‌جز نقطه $(-۱, ۰)$ همهٔ نقطه‌های روی دایره با مختصات گویا به این ترتیب به‌دست می‌آیند. با اضافه کردن چند استدلال مقدماتی دیگر می‌توان نتیجه گرفت که تمام جواب‌های درست معادلهٔ $X^۲ + Y^۲ = Z^۲$ با این معادله‌ها داده شده‌اند:

$$\begin{cases} X = a^۲ - b^۲ \\ Y = ۲ab \\ Z = a^۲ + b^۲ \end{cases}$$

همان‌طور که دیدیم، استفاده از مفهوم‌های هندسی برای حل معادلهٔ فرما در حالت $n = ۲$ بسیار موفق بود. البته برای این حالت می‌توانستیم از

روش‌های مقدماتی و یا جبری هم استفاده کنیم. برای $n > ۲$ کار البته بس پیچیده‌تر است. بیشترین موفقیت در این زمینه در سال ۱۹۸۶ و به وسیلهٔ فالتینگز[1] به‌دست آمد. او ثابت کرد، خم‌های بسیاری، و از جمله خم‌های $x^n + y^n = ۱$ برای $n > ۲$، تعداد محدودی نقطهٔ گویا دارند. از این‌جا نتیجه شد که برای هر n داده شده، تعداد مثال نقض برای معادلهٔ فرما بی‌نهایت نیست.

اثبات قضیهٔ فرما از راهی غیرمستقیم

روشی که در نهایت برای اثبات قضیهٔ آخر فرما کارا بود هیچ کدام از این روش‌های مستقیم نبود. البته اثبات وایلز بر پایهٔ هندسه جبری است و از روش‌های جبری هم استفاده فراوان می‌کند، ولی این اثبات به‌طور مستقیم به‌جنگ قضیهٔ فرما نمی‌رود. استفادهٔ مستقیم از هندسهٔ جبری به این معنی بود که نقطه‌های روی خم $x^n + y^n = ۱$ و با مختصات گویا را پیدا کنیم. چند سال قبل از کار وایلز، ریاضی‌دانان دیگری استراتژی جدیدی برای حل قضیهٔ آخر فرما تدوین کردند. اندرو وایلز این روش جدید را به نتیجه رساند. گو این‌که در نظر اول و در چشم غیرمتخصص، این روش جدید شاید اندکی عجیب باشد. اندیشهٔ این استراتژی از این قرار است: فرض کنیم مثال نقضی برای قضیهٔ آخر فرما وجود داشته باشد. پس عددهای درست A، B ، و C داریم به نحوی که

$$A + B = C$$

و $A = a^n$، $B = b^n$، و $C = c^n$. عدد C همان $A + B$ است و لذا با دانستن A و B پیدا کردن C کار دشواری نیست. اما دو عدد درست A و B باید عددهای درست بسیار جالبی باشند. این دو عدد درست مثال نقض قضیهٔ آخر فرما هستند و ریاضی‌دانان حدود ۳۵۰ سال به دنبال آن‌ها بوده‌اند. لذا این دو عدد با احتمال زیاد باید دارای خاصیت‌های جالب دیگری هم باشند.

1- Faltings

با این استدلال اگر بخشی از ریاضیات را انتخاب کنیم که عنصرهای مورد مطالعهٔ آن دارای دو پارامتر باشند و اگر به جای این دو پارامتر A و B را قرار دهیم، باید انتظار داشته باشیم، صفر به دست آمده خاصیت‌های جالبی داشته باشد. البته A و B عددهای درست هستند و لذا عنصر موردانتخاب ما باید آگاهی‌های حسابی را در خود نگاه دارد. پس به‌این ترتیب، از عددهای A و B به عنوان پارامترهای یک عنصر ریاضی دیگر استفاده می‌کنیم با این امید که این عنصر جدید با این پارامترهای جالب دارای خاصیت‌های استثنایی باشد. این روش شاید بیشتر به انداختن تیری در تاریکی شبیه باشد، ولی همین روش درنهایت به اثبات قضیهٔ آخر فرما انجامید.

عنصر ریاضی که در این استراتژی به کار گرفته شد، عبارت است از خم بیضوی[1]. در بخش بعد مقدمه‌ای از خاصیت‌های خم‌های بیضوی را می‌آوریم و بعد به ربط آن‌ها با قضیهٔ آخر فرما می‌پردازیم. اثبات وایلز تنها به قضیهٔ آخر فرما نمی‌پردازد، بلکه خاصیت‌های مهمی را برای خم‌های بیضوی ثابت می‌کند. خم‌های بیضوی جای مهمی در هندسهٔ جبری دارند و در نتیجه آگاهی دربارهٔ آن‌ها بسیار به کار می‌آید.

خم‌های بیضوی

به هر خم درجه سه ناتکین[2] خم بیضوی گویند. از آن‌جا که نیاز به کلی‌ترین (و دقیق‌ترین) تعریف‌ها نداریم، تنها خود را منحصر به خم‌هایی می‌کنیم که با معادلهٔ

$$y^2 = x^3 + ax + bx + c \qquad (1)$$

داده شده باشند. معادله‌های درجه سوم دیگر را می‌توان، بدون تغییر خاصیت‌های خم، به چنین معادله‌ای تبدیل کرد. این خم درجه سوم ناتکین

1-Elliptic Curve 2-non-singular cubic curve

است اگر در هر نقطه دارای خط مماس خوش تعریفی[1] باشد و درنتیجه گره[2] و یا تیزک[3] نداشته باشد. برای این‌گونه معادله‌ها تعریف‌های معادل دیگری برای ناتکین بودن داریم. از جمله اگر

$$F(x,y) = y^۲ - x^۳ - ax^۲ - bx - c$$

و اگر دستگاه معادله‌های زیر بی‌جواب باشد:

$$F(x,y) = ۰, \frac{\partial F}{\partial x}(x,y) = ۰, \frac{\partial F}{\partial y}(x,y) = ۰$$

آن‌گاه خم درجه سوم (۱) ناکتین است (و لذا یک خم بیضوی است). با کمی دقت، از این تعریف آخری نتیجه می‌شود که خم درجه سوم (۱) ناتکین است اگر معادلهٔ

$$x^۳ + ax^۲ + bx + c = ۰$$

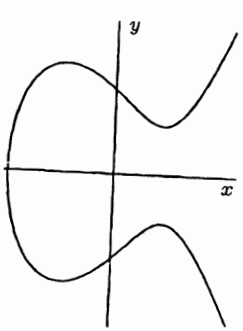
سه جواب متمایز داشته باشد.

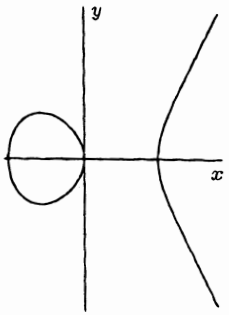
برای مثال، خم $y^۲ = x^۳ - x$ و خم $y^۲ = x^۳ - ۳x + ۳$ (شکل ۴) بیضوی هستند. مبداء مختصات گرهی (نقطه دو گانه) برای خم $y^۲ = x^۳ + x^۲$ و تیزکی (نقطه سه گانه) برای خم $y^۲ = x^۳$ است. لذا این دو خم (شکل ۵) بیضوی نیستند.

در هندسهٔ جبری می‌توان تعریف کوتاه‌تری از خم بیضوی داد. خم بیضوی یک خم تصویری هموار با گونهٔ ۱[4] است. در این نوشته ما خم بیضوی را همان خم درجه سوم ناتکین، که با معادله (۱) داده شده است، تعریف می‌کنیم.

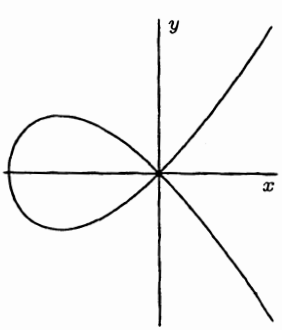
1-well defined tangent 2-node 3-cusp

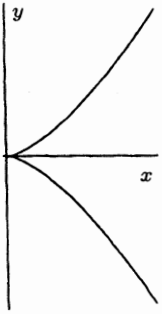
4-smooth projective curve of genus I





شکل ۴. خم‌های بیضوی $y^۲ = x^۳ - x$ و $y^۲ = x^۳ - ۳x + ۳$





شکل ۵. خم‌های $y^۲ = x^۳$ و $y^۲ = x^۳ + x^۲$

خواننده توجه داشته باشد دست‌کم از تعریف خم بیضوی نمی‌توان حدس زد که این عنصر ریاضی ربطی به قضیهٔ آخر فرما دارد. البته معادلهٔ فرما برای $n = ۳$، یعنی $x^۳ + y^۳ = ۱$ خمی بیضوی است (همان‌گونه که اشاره شد، این معادله، به نحوی که از حوصلهٔ این کوتاه خارج است، معادل خمی درجه سوم از نوع معادلهٔ (۱) است). اما معادله‌های درجهٔ بالاتر فرما خم بیضوی تشکیل نمی‌دهند. همان‌گونه که قبلا گفته شده بود، این اثبات از خم‌های بیضوی به نحوی غیره منتظره استفاده می‌کند.

اگر دربارهٔ نام خم‌های بیضوی کنجکاوید و خواهان فهم رابطه خم‌های بیضوی با بیضی هستید به مقاله [۱]، که زبان بسیار ساده نوشته شده است، رجوع کنید. به طور خلاصه، خم‌های بیضوی در محاسبه طول کمان‌های بیضی به کار می‌آیند.

خم بیضوی فری و قضیه آخر فرما

با استفاده از استدلال‌های مقدماتی، می‌توان ثابت کرد، اگر مثال نقضی برای قضیهٔ آخر فرما وجود داشته باشد، آن‌گاه مثال نقضی هم با شرط‌های زیر وجود دارد:

A، B، و C سه عدد درست‌اند، به نحوی که

الف. $A + B = C$،

ب. $ABC \neq 0$،

ج. عدد اول $n \geq 5$ وجود دارد به نحوی که A، B و C توان‌های nام کاملی هستند.

د. A، B و C عامل مشترکی ندارند،

ه. B بر ۳۲ بخش‌پذیر است،

و. $A \equiv 3 \pmod 4$،

ز. $C \equiv 1 \pmod 4$.

گرهاردفری[1] ریاضی‌دان آلمانی در سال ۱۹۸۵ پیشنهاد کرد، اگر A، B و C در این شرط‌ها صدق کنند آن‌گاه می‌توانیم خم بیضوی

$$y^2 = x(x - A)(x + B) \qquad (2)$$

را در نظر بگیریم. از نظر فری این خم می‌بایست خاصیت‌های بسیار جالبی داشته باشد. توجه کنید که، به‌خاطر شرط‌های داده شده، معادلهٔ $x(x - A)(x + B) = 0$ دارای سه ریشهٔ مجزا است و لذا معادلهٔ (۲)

1-Gerhard Frey

خم درجه سوم ناتکین است و درواقع یک خم بیضوی تعریف می‌کند. این خم بیضوی به خم بیضوی فری مشهور است.

چرا خم بیضوی؟

معادلهٔ (۲) تعریف یک خم بیضوی خاص بر مبنای مثال نقضی بر قضیهٔ آخر فرما می‌باشد. ولی به چه دلیل به مطالعهٔ این خم بیضوی بپردازیم؟ دلیل واقعی این است که خم‌های بیضوی دارای خاصیت‌های فراوانی هستند و به همین دلیل حدس‌های بسیاری دربارهٔ رفتار آن‌ها وجود دارد. گرهارد فری به دنبال حل قضیه آخر فرما نبود. او می‌خواست خم بیضوی جالبی پیدا کند تا به کمک آن درستی بعضی از حدس‌های راجع به خم‌های بیضوی را بسنجد.

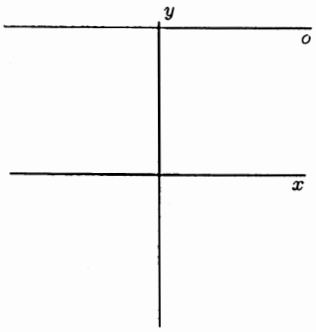
در این بخش بعضی از خاصیت‌های کلیدی خم‌های بیضوی را توضیح می‌دهیم تا بتوانیم به حدس پایه‌ای تانیاما-شیمورا-وایل[1]، که اثبات بخشی از آن توسط وایلز منجر به حل قضیهٔ آخر فرما شد، برسیم.

نکته اساسی دربارهٔ خم‌های بیضوی این است که نقطه‌های با مختصات گویا روی هر خم بیضوی تشکیل یک گروه آبلی می‌دهند! این به‌معنای آن است که می‌توانیم یک نوع جمع را تعریف کنیم، به‌نحوی‌که وقتی دو نقطه با مختص گویا روی یک خم بیضوی را با هم جمع کنیم، حاصل جمع نقطه‌ای با مختص گویا روی همان خم بیضوی شود. درضمن، برای این جمع باید یک عضو خنثا (عضو صفر) داشته‌باشیم، هر نقطه با مختص گویا باید دارای وارون باشد، و جمع ما باید خاصیت شرکت پذیری داشته باشد. این کار ساده‌ای نیست و برای خم‌های غیربیضوی اغلب ممکن نیست. در این‌جا با چند مثال این عمل جمع را نشان می‌دهیم.

برای مقدارهای حقیقی می‌توانیم نمودار خم بیضوی را در صفحهٔ دو بعدی رسم کنیم. برای این‌که بتوانیم عمل جمع را روی نقطه‌های با مختصات گویا تعریف کنیم، در گام نخست، باید یک نقطه به صفحه اضافه کنیم. این نقطه را نقطه در بی‌نهایت می‌نامیم و به‌طور شهودی تصور می‌کنیم که

1-Taniyama-Shimura-Weil Conjecture

این نقطه‌ای است بسیار دور در جهت محور yها. هر خط راست موازی با محور yها این نقطه را قطع می‌کند. در ضمن، همیشه این نقطه را جزو نقطه‌های با مختصات گویا به حساب می‌آوریم. اضافه کردن این نقطه شاید برای خواننده عجیب به نظر برسد، ولی در واقع برای تعریف عمل جمع مورد نظرمان باید خم بیضوی را در صفحهٔ تصویری[1] در نظر بگیریم و این نقطه در بی‌نهایت، و در واقع یکی از نقطه‌های در بی‌نهایت صفحهٔ تصویری است. برای دنبال کردن این بحث نیازی به درک دقیق از صفحه تصویری نیست و خواننده می‌تواند، همان‌طور که در این‌جا آمده، همان صفحه اقلیدسی معمولی به‌اضافه یک نقطه اضافی را در نظر بگیرد. این نقطهٔ در بی‌نهایت را ما با O نشان می‌دهیم.



شکل ۶. نقطهٔ در بی‌نهایت

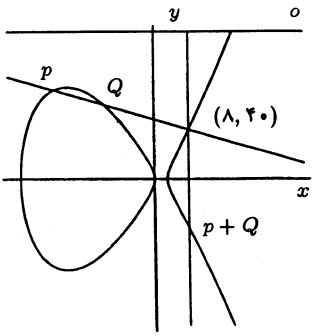
در شکل ۷، خم بیضوی $y^۲ = x(x-۳)(x+۳۲)$ را رسم کرده‌ایم. نقطه‌های $P = (-۲۴, ۷۲)$ و $Q = (-۱۲, ۶۰)$، نقطه‌های با مختصات گویا روی این خم هستند. حال نقطهٔ $P + Q$ کدام است؟ ممکن است فکر کنید که باید مختصات P و Q را با هم جمع کنیم، ولی این کار، نقطه‌ای روی منحنی به‌دست نمی‌دهد. تعریف $P + Q$ کمی بغرنج‌تر و از دو مرحله

1-Projective Plane

تشکیل شده است. اول خط راستی را از P و Q می‌گذرد، رسم می‌کنیم. می‌توان ثابت کرد، این خط خم بیضوی را در نقطهٔ سومی با مختصات گویا قطع می‌کند. در مثال ما این نقطهٔ سوم $(۸, ۴۰)$ است. حال خطی موازی محور yها از این نقطهٔ سوم رسم می‌کنیم (در واقع، این خط نقطهٔ سوم را به نقطهٔ در بی‌نهایت وصل می‌کند). از آن‌جا که نمودار خم بیضوی نسبت به محور xها متقارن است، این خط خم بیضوی را در نقطه چهارمی با مختصات گویا قطع می‌کند. در مثال ما این نقطهٔ چهارم نقطه $(۸, -۴۰)$ است. این نقطه را $P + Q$ می‌نامیم. پس برای خم $y^۲ = x(x - ۳)(x + ۳۲)$ داریم:

$$(-۲۴, ۷۲) + (-۱۲, ۶۰) = (۸, -۴۰)$$

البته می‌توان دستوری برای این جمع به دست آورد، ولی نوشتن این دستور بغرنج کمک زیادی به فهم این عمل جمع خاص نمی‌کند.

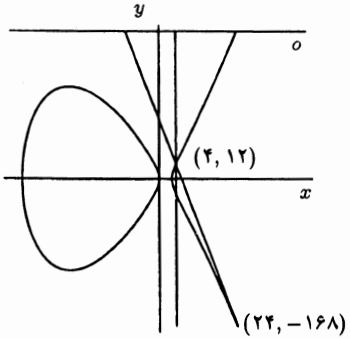


شکل ۷. روی خم $y^۲ = x(x - ۳)(x + ۳۲)$ داریم
$(-۲۴, ۷۲) + (-۱۲, ۶۰) = (۸, -۴۰)$

برای این‌که این عمل جمع را درست بفهمیم به چند مثال دیگر هم نیاز داریم. جمع یک نقطه با خودش چگونه خواهد بود؟ تنها تفاوتی که این حالت

با حالت کلی دارد، این است که به جای خط راست اول که از دو نقطه P و Q می‌گذشت باید خط مماس در نقطهٔ داده شده را رسم کنیم. برای مثال (شکل ۸)، روی خم بیضوی $y^۲ = x(x-۳)(x+۳۲)$، نقطه $(۲۴, -۱۶۸)$ نقطه‌ای با مختصات گویا است. خط مماس در این نقطه خم را در نقطه $(۴, ۱۲)$ قطع می‌کند و یعنی برای این خم بیضوی داریم:

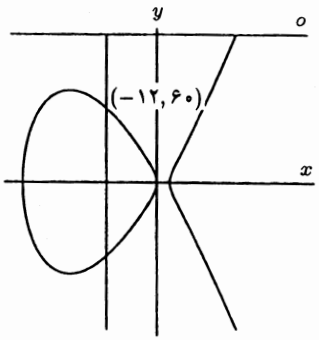
$$(۲۴, -۱۶۸) + (۲۴, -۱۶۸) = (۴, -۱۲)$$



شکل ۸. روی خم $y^۲ = x(x-۳)(x+۳۲)$ داریم
$۲ \times (۲۴, -۱۶۸) = (۴, -۱۲)$

چگونه نقطه‌ای را با نقطهٔ O جمع کنیم؟ خط راست اول عمودی خواهد بود و خط دوم همان خط اول است، در نتیجه به‌سادگی دیده می‌شود که نتیجه جمع هر نقطه با O خود نقطه اولی است. به بیان دیگر خنثا در این عمل جمع است و نقش صفر را بازی می‌کند. برای مثال، در شکل ۹ برای خم بیضوی $y^۲ = x(x-۳)(x+۳۲)$ نشان داده‌ایم که

$$(-۱۲, ۶۰) + O = (-۱۲, ۶۰)$$



شکل ۹. روی خم $y^۲ = x(x-۳)(x+۳۲)$ داریم:
$$(-۱۲, ۶۰) + O = (-۱۲, ۶۰)$$

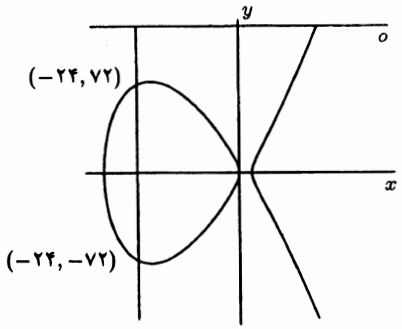
در شکل ۱۰، باز هم برای خم بیضوی $y^۲ = x(x-۳)(x+۳۲)$ نشان داده‌ایم که

$$(-۲۴, ۷۲) + (-۲۴, -۷۲) = O$$

در حالت کلی، اگر (p, q) هم نقطه‌ای با مختصات گویا روی همان خم بیضوی باشد، آن‌گاه $(p, -q)$ هم نقطه‌ای با مختصات گویا روی همان خم است و در ضمن داریم:

$$(p, q) + (p, -q) = O$$

این به‌معنای آن است که برای عمل جمع تعریف شده، هر عضو داری یک وارون است.



شکل ۱۰. روی خم $y^2 = x(x-3)(x+32)$ داریم:
$$(-24, 72) + (-24, -72) = O$$

البته این نکته که نقطه‌های با مختصات گویا و با این عمل جمع تشکیل یک گروه آبلی را می‌دهند، احتیاج به اثبات دارد. امیدواریم مثال‌هایی که آوردیم، خواننده را متقاعد کرده باشد که این، حکمی دور از انتظار نیست.

اگر E یک خم بیضوی باشد، $E(Q)$ نشان‌دهندهٔ گروه آبلی نقطه‌های با مختصات گویای E است.

در این‌جا فرض می‌کنیم خواننده کمی دربارهٔ گروه‌های آبلی می‌داند. البته هدف بلافاصلهٔ ما گفت‌وگو دربارهٔ بعضی خاصیت‌های $E(Q)$ است. این بحث خواننده را متقاعد خواهد کرد که اطلاعات و مساله‌های باز دربارهٔ نقطه‌های با مختصات گویا روی خم‌های بیضوی بسیار است و این بخش ریاضیات شامل نتیجه‌های عمیق و جالبی است. جزئیات بحث کنونی در فهم بقیه این نوشته تاثیر زیادی ندارد لذا می‌توانید از آن بگذرایید.

هر گروه آبلی، و از جمله $E(Q)$، حاصل جمع مستقیم[1] تعدادی زیـــرگـــروه دوری[2] است. بعضی از این زیرگروه‌های دوری متناهی و بقیه نامتناهی هستند. حاصل‌جمع مستقیم این زیرگروه‌های دوری متناهی را زیر

1-direct sum 2-cyclic subgroup

گروه تابدار[1] گروه آبلی می‌خوانیم. زیرگروه تابدار به طور دقیق شامل عضوهای با مرتبهٔ متناهی[2] است. هر گروه دوری نامتناهی با گروه عددهای درست، Z یکریخت[3] است. در نتیجه هر گروه آبلی حاصل جمع مستقیم زیر گروه تابدار و تعدادی زیر گوهی یکریخت با Z است. هر گروه دوری، طبق تعریف، یک مولد[4] دارد، ولی تعداد مولدهای یک گروه آبلی دلخواه می‌تواند بی‌نهایت باشد. موردل[5] ثابت کرد گروه نقطه‌های با مختصات گویا روی یک خم بیضوی را همیشه می‌توان به‌وسیلهٔ تعدادی محدود عضو تولید کرد. این قضیه را وایل[6] به هیات‌های عددی[7] تعمیم داد:

قضیه موردل-وایل، اگر E یک خم بیضوی باشد، آن‌گاه تعداد مولدهای $E(Q)$ متناهی است.

این قضیه از آن‌جا مهم است که، بدون داشتن هیچ گونه اطلاعی از E، می‌توانیم محدودیت‌هایی برای ساختار $E(Q)$ در نظر بگیریم. از آن‌چه دربارهٔ گروه‌های آبلی گفته شد و با استفاده از قضیه موردل-وایل نتیجه می‌گیریم که برای هر خم بیضوی E داریم:

$$E(Q) \cong \underbrace{Z \oplus Z \oplus \ldots \oplus Z}_{r} \oplus T$$

که در آن T و r به ترتیب زیر گروه تابدار و رتبه[8] $E(Q)$ هستند.

آگاهی‌های مربوط به گروه $E(Q)$ به قضیهٔ موردل-وایل ختم نمی‌شود. قضیهٔ عمیق زیر می‌گوید که زیر گروه تابدار این گروه، هر گروهی نمی‌تواند باشد و محدود به تنها ۱۵ گروه بسیار مشخص است.

1-torsion subgroup	2-elements of finite order	3-isomorphic
4-generator	5-Mordell	6-Weil
7-number fields	8-rank	

قضیه می‌زر[1]. اگر E یک خم بیضوی باشد و T زیر گروه تابدار آن، آن‌گاه T یکی از ۱۵ گروه زیر است:

$$\begin{array}{ll} Z/nZ & n = ۱, ۲, \ldots, ۹, ۱۰, ۱۲ \\ Z/۲nZ \oplus Z/۲Z & n = ۱, ۲, ۳, ۴ \end{array}$$

در این‌جا Z/mZ نمانگر گروه دوری از مرتبهٔ m است.

قضیه می‌زر به معجزه می‌ماند. برای نمونه فرض کنید روی یک خم بیضوی نقطه‌ای با مختصات گویا پیدا کردید. این نقطه را P بنامید. بااستفاده از عمل جمع تعریف شده، می‌توانید $۲P = P + P$ را پیدا کنید. $۲P$ هم به ناچار نقطه‌ای روی خم بیضوی و با مختصات گویا خواهد بود. به همین ترتیب، $۳p$، $۴P$ و سایر نقطه‌های او نوع kP، که در آن k مقدار درستی است، نقطه‌های با مختصات گویا روی خم بیضوی هستند. فرض کنید، برای نقطهٔ Pرابطه $۷P = O$ برقرار باشد. این، به معنای آن است که مرتبهٔ نقطهٔ P در گروه $E(Q)$ برابر ۷ است. از قضیهٔ می‌زر نتیجه می‌شود که تنها نقطه‌های با مختصات گویا و با مرتبهٔ متناهی روی خم بیضوی داده شده عبارت‌اند از P، $۲P$، ...، $۷P$. اگر نقطهٔ دیگری با مختصات گویا روی این خم وجود داشته باشد، آن‌گاه مرتبه‌اش نامتناهی است.

تحقیق درباره نقطه‌های بامختصات گویا روی خم‌های بیضوی هم‌چنان ادامه دارد. دو سوال باز، که جوابشان تا این نوشته معلوم نشده، به قرار زیراند:

۱) آیا r، رتبه $E(Q)$، می‌تواند به اندازه دلخواه بزرگ باشد؟

۲) آیا الگوریتمی عملی برای تشخیص صفر بودن r وجود دارد؟

خم‌های بیضوی و هیات‌های متناهی

E را یک خم فرض کنید. در بخش قبل گفتیم که نقطه‌های با مختصات گویا روی E تشکیل یک گروه آبلی می‌دهند، و ما این گروه را با $E(Q)$

1-Mazur

نشان دادیم. به همین ترتیب، و با همان عمل جمع قبلی، نقطه‌های با مختصات حقیقی روی E هم تشکیل یک گروه آبلی را با $E(R)$ نشان می‌دهیم. به‌طور معمول، وقتی خم E را رسم می‌کنیم، نموداری از عضوهای $E(R)$ به دست می‌آوریم. مجموعهٔ عددهای گویا Q، و مجموعهٔ عددهای حقیقی R، نمونه‌هایی از هیات‌ها[1] هستند. در یک هیات دو عمل جمع و ضرب داریم و می‌توانیم عضوهای هیات را با هم جمع و ضرب، از هم کم، و به هم تقسیم کنیم (البته به شرطی که بخشیاب صفر نباشد). مجموعهٔ عددهای مختلط C نمونهٔ دیگری از یک هیات است. به طور کلی، اگر F یک هیات باشد، و E یک خم بیضوی، آن‌گاه $E(F)$ تشکیل یک گروه آبلی می‌دهد. منظور از $E(F)$ چیست؟ عضوهای $E(F)$ دو تایی‌های (a, b) هستند به‌نحوی که aو b عضوهایی از F باشند که در معادلهٔ تعریف کننده E صدق می‌کنند.

با مثالی مطلب را روشن می‌کنیم. P را عددی اول و F_P را هیات متناهی[2] با P عضو می‌گیریم. از جمله $F_۷ = \{۰, ۱, ۲, ۳, ۴, ۵, ۶, \}$؛ و عمل‌های جمع و ضرب به پیمانه[3] ۷ می‌باشند. پس در $F_۷$ داریم $۱ = ۵ + ۳$، $۶ = ۵ \times ۴$، $۴ = -۳$ و $۵ = \frac{۱}{۳}$. خم بیضوی E را که با معادلهٔ

$$E : y^۲ + y = x^۳ - x$$

داده شده است در نظر بگیریم. می‌توان نشان داد که این خم بیضوی ۵ نقطه با مختصات گویا دارد (توجه کنید، شرط کرده‌ایم که نقطه بینهایت O در هر $E(F)$ قرار دارد):

$$E(Q) = \{O, (۰, ۰), (۰, -۱), (۱, ۰), (۱, -۱)\}$$

هرکدام از این نقطه‌ها در معادلهٔ E صدق می‌کنند و درنتیجه اگر آن‌ها را به پیمانهٔ ۷ بگیریم، نقطه‌هایی در $E(F_۷)$ به‌دست خواهیم آورد. توجه کنید

1-field 2-finite field 3-mod

که در $F_۷$ داریم $۶ = -۱$ و درنتیجه

$$E(Q) = \{O, (۰, ۰), (۰, ۶), (۱, ۰), (۱, ۶)\} \subseteq F(F_۷)\}$$

البته، می‌توان به‌طور مستقیم دید که هر کدام از این نقطه‌ها در معادلهٔ E صدق می‌کنند. برای مثال، اگر در معادلهٔ E نقطهٔ $(۰, ۶)$ را بگذاریم، خواهیم داشت:

$$۶^۲ + ۶ = ۰^۳ - ۰^۲$$

که به پیمانه ۷ درست است.

از طرف دیگر $E(F_۷)$ محدود به این ۵ نقطه نیست. از جمله داریم $(۵, ۱) \in E(F_۷)$ زیرا

$$۵^۳ - ۵^۲ = (۱^۲ + ۱)(\text{mod}۷)$$

از این مثال دو نتیجه می‌گیریم:

۱) اگر $E(Q) \neq \{O\}$ آنگاه $E(F_p) \neq \{O\}$، و

۲) تعداد نقطه‌های $E(F_p)$ به‌ناچار محدود است و درنتیجه پیدا کردن $E(F_p)$ ساده است.

گروه $E(F_p)$ به چه کار می‌آید؟ همان‌طور که در ابتدای این مقاله دیدیم، پیدا کردن $E(Q)$ در بسیاری حالت‌ها، در نظریهٔ عددها کاربرد دارد، ولی کاربرد $E(F_p)$ آن‌قدرها واضح نیست. در این بخش هندسهٔ جبری سوال کلیدی این است که آیا با دانستن $E(F_P)$ برای Pهای مختلف، می‌توان آگاهی‌هایی دربارهٔ $E(Q)$ به دست آورد؟ برای مثال، اگر برای یک عدد اول P، داشته باشیم $E(F_p) = \{O\}$ آنگاه نتیجه می‌گیریم $E(Q) = \{O\}$. ولی در حالت‌های دیگر چه نوع نتیجه‌گیری‌هایی می‌توانیم بکنیم؟ این پرسش از آن نظر اهمیت دارد که پیدا کردن $E(F_p)$ کم و بیش ساده است، ولی ارزش دانستن $E(Q)$ بیشتر است. اگر معادله‌های مورد نظر ما درجه یک و یا درجه دو بودند، آنگاه قضیهٔ هاسه‌ـمینکوفسکی[1] جواب مثبت به پرسش

1-Hasse-Minkowski theorem

ما می‌داد. در این‌جا به این قضیه نمی‌پردازیم، چرا که در حالت معادله‌های درجه سوم (و در نتیجه در حالت خم‌های بیضوی) صادق نیست. در حالت خم‌های بیضوی ممکن است، $E(R)$ و $E(F_p)$ برای همه عددهای اول p، شامل نقطه‌ای به غیر از O باشند، در حالی که $E(Q) = \{O\}$.

ولی داستان به همین جا ختم نمی‌شود. رابطهٔ عمیق و معجزه‌گونه‌ای بین $E(F_p)$ و $E(Q)$ وجود دارد که در بخش‌های بعد به آن خواهیم پرداخت. فهم این رابطه برای درک اولیه از اثبات قضیه آخر فرما بسیار مهم است.

تعداد عضوهای $E(F_p)$

خم بیضوی

$$E : y^۲ = x^۳ - ۴x^۲ + ۱۶$$

را در نظر بگیرید. p را عددی اول می‌گیریم و با M_p تعداد عضوهای گروه آبلی $F(F_p)$ را نشان می‌دهیم. از آن‌جا که F_p فقط p عضو دارد، M_p عددی درست و متناهی است. از جمله، برای $p = ۳$ خواننده می‌تواند به راحتی ببیند که

$$E(F_۳) = \{O, (۰, ۱), (۰, ۲), (۱, ۱), (۱, ۲)\}$$

و از آن‌جا $M_۳ = ۵$. یادآوری می‌کنیم، وقتی می‌گوییم $(۱, ۲) \in E(F_۳)$، این به‌معنای آن است که نقطهٔ $(۱, ۲)$ در معادلهٔ E صدق می‌کند. البته همهٔ عمل‌های حساب در هیات $F_۳$ و به پیمانه ۳ انجام می‌شوند:

$$۲^۲ \equiv ۱^۳ - ۴(۱)^۲ + ۱۶ (\mathrm{mod} ۳)$$

از خواننده می‌خواهیم، عضوهای $E(F_p)$ را دست‌کم برای دو عدد اول p پیدا کند. این کار سختی نیست، ولی خواننده را متقاعد خواهد کرد، وقتی p عوض می‌شود عمل‌های جمع، ضرب و غیره به کلی تغییر می‌کنند و درنتیجه

نمی‌توان انتظار داشت که رابطه‌ای بین M_p و $M_{p'}$ برای دو عدد اول متفاوت p و p' وجود داشته باشد. برای نمونه عضوهای $E(F_۳)$ را که در بالا داده شده، با عضوهای $E(F_{۱۳})$ مقایسه کنید:

$$E(F_{۱۳}) = \{O,(۰,۴),(۰,۹),(۱,۰),(۴,۴),(۴,۹),$$
$$(۶,۶),(۶,۷),(۸,۵),(۸,۸)\}$$

مشکل بتوان رابطه‌ای بین $E(F_۳)$ و $E(F_{۱۳})$ و یا بین $M_۳$ و $M_{۱۳}$ تصور کرد. البته $M_{۱۳} = ۱۰$ و این دو برابر $M_۳$ است، ولی منظور ما رابطه‌ای است که بشود آن را از قبل پیش‌بینی کرد.

در جدول زیر مقدارهای M_p، برای عددهای اول فرد تا ۴۷ داده شده است:

P	۳	۵	۷	۱۱	۱۳	۱۷	۱۹	۲۳	۲۹	۳۱	۳۷	۴۱	۴۳	۴۷
M_p	۵	۵	۱۰	۱۱	۱۰	۲۰	۲۰	۲۵	۳۰	۲۵	۳۵	۵۰	۵۰	۴۰

سوال این است، آیا هیچ رابطه‌ای بین این عددها وجود دارد؟ حدس تانیاما-شیورا-وایل به‌نحو زیبایی به این پرسش پاسخ می‌دهد. چیزی که دربارهٔ این پاسخ جالب است، این است که نقطهٔ شروع آن در نظریهٔ تابع‌های مختلط، یعنی در آنالیز، است. این رابطه جبر و آنالیز بسیار عمیق و غیرمنتظره است. برای فهم این حدس خواننده باید کمی حوصله داشته باشد و اجازه بدهد که ما از بحث به ظاهر بی‌ربطی شروع کنیم. در ضمن جای تعجب نیست اگر خواننده نگران ربط کل این بحث به قضیهٔ آخر فرما باشد. جالبی اثبات قضیهٔ آخر فرما در همین است که بخش کلیدی آن در واقع ربطی به قضیهٔ آخر فرما ندارد.

قبل از هر چیز بگوییم، با استدلالی شهودی می‌توان دید که M_p باید مقداری حدود $p + ۱$ داشته باشد. از جدول بالا دیده می‌شود که به‌تقریب برای هیچ‌کدام از مقدارهای p این مقدار تقریبی دقیق نیست، ولی شاید بتوان قبول کرد که M_p و $p + ۱$ تا حدی با هم رشد می‌کنند. برای این‌که رابطهٔ

M_p و $p+1$ را ببینیم به خم‌های ساده‌تر از درجه سوم می‌پردازیم. خط $y=ax+b$ را در نظر بگیرید. تعداد عضوهای F_p برابر p است و هر کدام از این p عضو را می‌توان به جای x گذاشت و به این ترتیب p نقطه روی خط به‌دست می‌آید. نقطهٔ O را هم همیشه به عنوان نقطه‌ای روی خط به‌حساب می‌آوریم. پس در مجموع $p+1$ نقطه روی هر خطی در F_p خواهیم داشت. استدلال‌های مشابهی برای چند نوع خم دیگر هم می‌توان آورد. ازجمله، باز هم برای F_p، خم $y^2=f(x)$ را در نظر بگیرید. برای هر مقدار x باید معادلهٔ $y^2-f(x)$ را حل کنیم. این معادله به طور کلی جواب دارد. که $f(x)$ یک مانده درجه دوم به پیمانه p[1] باشد. درنظریهٔ مقدماتی عددها ثابت می‌شود که درست نصف عددهای $1, 2, \ldots, p-1$ ماندهٔ درجه دوم هستند و اگر a یک ماندهٔ درجه دوم باشد، آن‌گاه معادلهٔ $y^2=a$ دو جواب دارد. معادلهٔ $y^2=0$ هم یک جواب دارد و طبق معمول O را هم یک جواب به حساب می‌آوریم. از این‌جا نتیجه می‌شود که، اگر مقدارهای $f(x)$ به طور تصادفی و یکنواخت بین عددهای $0, 1, \ldots, p-1$ پخش شده باشند، آن‌گاه تعداد نقطه‌های با مختصات در F_p روی خم $y^2=f(x)$ برابر $p+1$ است. پس به این ترتیب، برای فهم دنبالهٔ M_p، باید به تفاوت M_p و $p+1$ توجه کنیم. این تفاوت را جمله خطا[2] می‌نامیم و ان را با a_p نشان می‌دهیم:

$$M_p = p+1-a_p$$

قضیهٔ زیر نشان می‌دهد، این جملهٔ خطا نمی‌تواند از دو برابر $\sqrt{p}$ بیشتر باشد.

قضیه هاسه‌ـوایل[3]. E یک خم بیضوی و p عددی اول است. طبق معمول M_p برابر تعداد عضوهای $E(F_p)$ و $a_p=(p+1)-M_p$. آنگاه

$$|a_p| \le 2\sqrt{p}$$

برای ادامهٔ بحث به مثال ۱۶ + $y^2=x^3-4x^2$ برمی‌گردیم و همان‌طور که وعده داده بودیم از آنالیز تابع‌های مختلط کمک می‌گیریم. بگذارید

1-quadratic residue mod p 2-error term

3-Hasse-Weil theorem

$q = e^{۲\pi iz}$ و تابع

$$\Phi = (q) = q \prod_{n=۱}^{\infty} (۱ - q^n)^۲ (۱ - q^{۱۱n})^۲ \qquad (۳)$$

را در نظر بگیرید. اگر با $\mathcal{H}$ نیم صفحهٔ عددهای مختلط[1] را نشان دهیم، آن‌گاه

$$\Phi : \mathcal{H} \to C$$

تعریف، Φ شامل حاصل‌ضرب بی‌نهایت جملهٔ است. وقتی این عبارت را بسط دهیم، یک سری توانی[2] در q به‌دست می‌آید که در واقع بسطه فوریه[3] تابع Φ است. توجه کنید که اگر به‌فرض $q^۷$ را در این بسط بخواهیم، باید فقط به تعداد محدودی جمله توجه کنیم چرا که هیچ‌کدام از جمله‌های با $n \geq ۷$ نقشی در ضریب $q^۷$ ندارند.

پرسش این است، این تابع چه ربطی به بحث ما دارد؟ بسط فوریه این تابع را پیدا کنید و اگر p عدد اول است آن‌گاه C_p را برابر ضریب q^p در این بسط بگذارید. پیدا کردن c_p برای مقدارهای کوچک p بسیار ساده است (نگارنده آن‌ها را بااستفاده از نرم‌افزار میپل[4] محاسبه کرده است)، و این‌ها در جدول زیر آورده شده‌اند:

P	۳	۵	۷	۱۱	۱۳	۱۷	۱۹	۲۳	۲۹	۳۱	۳۷	۴۱	۴۳	۴۷
C_p	−۱	۱	−۲	۱	۴	−۲	۰	−۱	۰	۷	۳	−۸	−۶	۸

برای دیدن اهمیت این عددها، در جدول زیر هم M_p و هم c_p را آورده‌ایم:

p	۳	۵	۷	۱۱	۱۳	۱۷	۱۹	۲۳	۲۹	۳۱	۳۷	۴۱	۴۳	۴۷
M_p	۵	۵	۱۰	۱۱	۱۰	۲۰	۲۰	۲۵	۳۰	۲۵	۳۵	۵۰	۵۰	۴۰
c_p	−۱	۱	−۲	۱	۴	−۲	۰	−۱	۰	۷	۳	−۸	−۶	۸
$M_p + c_P$	۴	۶	۸	۱۲	۱۴	۱۸	۲۰	۲۴	۳۰	۳۲	۳۸	۴۲	۴۴	۴۸

1-complex upper half plane 2-Power series

3-Fourier series expansion 4-Maple

می‌بینیم که $M_p + c_p = p + ۱$ که یعنی c_p برابر با همان جمله خطا می‌باشد. نتیجه می‌گیریم که $c_p = a_p$. به بیان دیگر، در این مثال خاص توانسته‌ایم، تابعی پیدا کنیم که ضرایب بسط فوریه آن بادقت جمله‌های خطا را می‌دهد و لذا با استفاده از آن می‌توانیم تعداد عضوهای $E(F_p)$ را بادقت پیدا کنیم. البته ممکن است اول a_p را حساب کنیم و بعد با استفاده از آن بسط فوریه را بنویسیم. در این صورت تنها نکتهٔ جالب دربارهٔ تابع Φ این است که Φ به نحو ساده‌ای تجزیه شده است. حدس تانیاما-شیمورا-وایل می‌گوید، برای هر خم بیضوی یک چنین تابعی وجود دارد و به علاوه این تابع از خاصیت‌های بسیار خوب تحلیلی برخوردار است. در واقع، Φ یک تابع معمولی نیست، بلکه یک صورت مدولی[1] است.

هنوز برای فهم حدس تانیاما-شیورا-وایل به تعاریف بیشتری نیاز داریم. از طرفی باید تعریف یک صورت مدولی را بدهیم و از طرف دیگر، و از آن‌جا که این حدس رابطهٔ دقیقی بین خم‌های بیضوی و صورت‌های مدولی را بیان می‌کند، باید چند تعریف دیگر برای خم‌های بیضوی بیاوریم. درواقع، برای این حدس بعضی عددهای اول، عددهای اول «خوبی» هستند. پس حدس تانیاما-شیمورا-وایل به‌تقریب می‌گوید، اگر E یک خم بیضوی باشد، آن‌گاه صورت مدولی Φ وجود دارد به نحوی که ضریب‌های بسط فوریه Φ جمله‌های خطا برای $|E(F_p)|$ را، که در آن p اول «خوبی» است، به‌دست می‌دهند.

عددهای اول خوش تقلیل و هادی یک خم بیضوی

E را یک خم بیضوی و p را عددی اول در نظر بگیرید. اگر ضریب‌های معادله را به پیمانه p تقلیل بدهیم، خم جدیدی به دست می‌آید که ممکن است تکین و یا ناتکین باشد. در صورت ناتکین بودن خم، ممکن است، نقطهٔ دوگانه (گره) و یا نقطه سه‌گانه (تیزک) داشته باشد. پس می‌شود، خم‌های

1-modular form

بیضوی را نسبت به عدد اول p به سه دسته تقسیم کرد:

۱) اگر E به پیمانهٔ p ناتکین باشد، آنگاه p عدد اول خوش تقلیلی[1] برای E است.

۲) اگر به پیمانهٔ p نقطهٔ دوگانه (گره) داشته باشد، آنگاه p عدد اول با تقلیل ضربی[2] برای E نامیده می‌شود.

۳) اگر E به پیمانهٔ p نقطهٔ سه‌گانه (تیزک) داشته باشد، آنگاه p عدد اول با تقلیل جمعی[3] برای E نامیده می‌شود.

عددهای اول با تقلیل ضربی و یا تقلیل جمعی را عددهای اول بدتقلیل[4] می‌نامند. در ضمن اگر E یک خم بیضوی باشد و همهٔ عددهای اول برایش خوش تقلیل و یا با تقلیل ضربی باشند، آنگاه E را نیم‌پایدار[5] می‌خوانند.

البته تعریف‌های بالا خیلی دقیق نیست. در این‌جا، هدف این بوده است، بدون وارد شدن به جزئیات، تصویری کلی از تقسیم‌بندی عددهای اول برای خم بیضوی E به‌دست آوریم. یک دلیل عدم دقت تعریف بالا این است که ممکن است، با یک تغییر متغیر خطی شکل معادلهٔ تعریف کنندهٔ E تغییر کند، در حالی که خاصیت‌های E تغییری نکرده است. برای نمونه $E : y^۲ = x^۳ - ۶۲۵x$ را در نظر بگیرید. این معادله به پیمانهٔ ۵ تبدیل به معادله $y^۲ = x^۳$ می‌شود که نقطهٔ سه‌گانه دارد و تکین است. ولی اگر در معادله E، بگذاریم $x = ۲۵u$ و $y = ۱۲۵v$ آنگاه معادلهٔ $v^۲ = u^۳ - u$ به دست می‌آید که به پیمانهٔ ۵ ناتکین است. تعریفی که با یک تغییر متغیر خطی عوض شود، خیلی نمی‌تواند استفاده داشته باشد. ولی اشکال در عدم

1-Prime of good reduction

2-Prime of multiplicative reduction

3-Prime of additive reduction

4-Primes of bad reduction

5-semistable

دقت تعریف بالا است. درواقع، برای هر خم بیضوی یک معادلهٔ «کمین»[1] وجود دارد که برای آن تعداد عددهای اول بدتقلیل، حداقل مقدار ممکن است. تقسیم‌بندی بالا برای عددهای اول را باید برای معادلهٔ کمین هر خم بیضوی به کار گرفت.

اگر E یک خم بیضوی باشد، آن‌گاه عددی مهم را برایش تعریف می‌کنیم. این عدد را با N نشان می‌دهیم و آن را هادی[2] E می‌خوانیم. در این‌جا تعریف دقیق N را نمی‌آوریم و تنها می‌گوییم که

$$N = \prod_{p \in P} p^{n(p)}$$

که در آن مجموعهٔ P همهٔ عددهای اول است. اگر p عدد اول خوش تقلیل باشد، آن‌گاه $n(p) = 0$ و اگر p عدد اول با تقلیل ضربی باشد، آن‌گاه $n(p) = 1$ است. در حالتی که p عدد اول با تقلیل جمعی باشد $n(p)$ عدد درستی بزرگتر از ۱ است. تنها کمبود این تعریف در این است که $n(p)$ را برای عددهای اول با تقلیل جمعی به دقت تعریف نکرده‌ایم.

توجه کنید که E نیم‌پایدار است، اگر و تنها اگر N بر توان دوم عدد اولی بخش‌پذیر نباشد.

صورت‌های مدولی

صورت‌های مدولی در ریاضیات مدرن جایگاه مهمی دارند و به نظر می‌رسد، به‌وسیلهٔ آن‌ها می‌توان پدیده‌های گوناگونی را توضیح داد. در این‌جا ما تنها نگاهی به این صورت‌ها می‌اندازیم. بعضی جاها به عمد کمی گنگ خواهیم بود و همهٔ جزئیات را نمی‌آوریم، تا، به خاطر ریزه‌کاری‌های پیچیدهٔ این بحث، دنبال کردن خطوط کلی آن غیرممکن نشود.

$\mathcal{H} = \{x + iy | y > 0\}$ نیم بالایی صفحه عددهای مختلط[3] است.

1-minimal Polynomial 2-conductor

3-complex upper half plane

N عددی درست و مثبت است. مجموعهٔ ماتریس‌های زیر را در نظر بگیرید:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in Z, ad - bc = 1, N|c \right\}$$

پس عضوهای $\Gamma_0(N)$ ماتریس‌های دو در دویی هستند که درایه‌های آن‌ها عدد درست، دترمینان آن‌ها برابر ۱، و درایه سمت چپ پایینی آن‌ها بر N بخش‌پذیر است.

$\Gamma_0(N)$ یک گروه است. عمل این گروه ضرب ماتریس‌ها است. نکتهٔ جالب این است که این گروه بر $\mathcal{H}$ عمل[1] می‌کند. این یعنی که هر عضو گروه $\Gamma_0(N)$ جایگشتی[2] از $\mathcal{H}$ به دست می‌دهد. در واقع اگر $\gamma \in \Gamma_0(N)$ و $z \in \mathcal{H}$ آن‌گاه می‌توانیم $\gamma(z)$ را به وسیلهٔ

$$\gamma(z) = \frac{az + b}{cz + d}$$

تعریف کنیم. ساده است که ببینیم، $\gamma(z) \in \mathcal{H}$ و، برای

$$\gamma_1, \gamma_2 \in \Gamma_0(N)$$

داریم $\gamma_1(\gamma_2(z)) = (\gamma_1\gamma_2)(z)$. توجه کنید، در سمت چپ این معادله، جایگشت‌های γ_1 و γ_2 را با هم ترکیب کرده‌ایم، در حالی که در سمت راست معادله، دو عضو گروه $\Gamma_0(N)$ را با هم ضرب کرده‌ایم.

اکنون تابع‌های تمامریخت[3] $f : \mathcal{H} \to C$ را در نظر بگیرید. اگر چنین تابعی، به‌غیر از تمامریخت بودن، چند خاصیت دیگر هم داشته باشد، آن‌گاه f را یک صورت مدولی[4] خوانند. اکنون به شرح خاصیت‌های لازم یک صورت مدولی می‌پردازیم. توجه داشته باشید، هر چه این خاصیت‌های تعریف کننده، محدود کننده‌تر باشند، صورت‌های مدولی ویژگی‌های بیشتری

1-acts 2-permutation

3-holomorphic 4-modular form

خواهند داشت و این به معنای دقت بیشتر حدس تانیاما-شیمورا-وایل خواهد بود.

شرط اول این است که عددهای درست N و k وجود داشته باشند به نحوی که برای $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ داشته باشیم:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

توجه کنید، برای هر N دلخواه ماتریس $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ عضو $\Gamma_0(N)$ است. اگر شرط بالا را دربارهٔ این عضو محاسبه کنیم، می‌بینیم که

$$f(z+1) = f(z)$$

یعنی f باید تابعی با دورهٔ تناوب ۱ باشد. از این‌جا نتیجه می‌شود که چنین تابعی دارای بسط فوریه[1] است و می‌توان آن را به‌صورت زیر نوشت:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n, \quad q = e^{2\pi i z}$$

این بسط فوریه f در صفر است. اگر در این بسط و در بسط f در سایر تیزک‌های f، هیچ توان منفی q نداشته باشیم، آن‌گاه f را صورت مدولی با وزن k و در سطح[2] می‌نامیم. اگر در این بسط‌های f همهٔ توان‌های q مثبت باشند (یعنی توان صفر نداشته باشیم) آن‌گاه f را یک تیزک صورت[3] نامیم.

پس صورت‌های مدولی مورد نظر ما عنصرهای بسیار خاص‌اند و درنتیجه این حدس که ضریب‌های یکی از این صورت‌های مدولی اطلاعات زیادی دربارهٔ خم‌بیضوی موردنظر ما می‌دهد، بسیار جالب و غیره‌منتظره است.

1-Fourier expansion

2-modular form of weight k at level N

3-cusp form

داستان به همین جا ختم نمی‌شود. مجموعهٔ صورت‌های مدولی با وزن k و در سطح N تشکیل یک فضای برداری[1] می‌دهد. بر روی این فضای برداری دنباله‌ای از تبدیل‌های خطی[2] جالب وجود دارند. در این‌جا تعریف این عمل‌گرها را نمی‌آوریم و تنها به اسم آن‌ها اکتفا می‌کنیم. به این عمل‌گرها عمل‌گرهای هکه[3] می‌گویند. اگر یک صورت مدولی ویژه بردار[4] همهٔ عمل‌گرهای هکه باشد، به آن ویژه صورت[5] گویند.

تکرار می‌کنیم، برای بحث ما جزئیات این تعریف‌ها آن‌قدر مهم نیست. تنها لازم است بدانیم، یک ویژه صورت نوع بسیار خاص یک تابع تمامریخت است و لذا پیدا شدن آن در ضمن مطالعه خم‌های بیضوی به معجزه می‌ماند. از آن‌جا که ویژه صورت‌ها خاصیت‌های بسیار دارند، رابطهٔ آن‌ها با خم‌های بیضوی موجب محدودیت‌های زیادی روی این خم‌ها می‌شود. یکی از این محدودیت‌ها می‌گوید که خم بیضوی فری نمی‌تواند وجود داشته باشد و در نتیجه مثال نقضی برای قضیه آخر فرما نمی‌توان یافت! امیدواریم، خواننده قبول کرده باشد که این، روشی به غایت غیرمستقیم برای اثبات قضیهٔ آخر فرما است.

حدس تانیاما_شیمورا_وایل و قضیه آخر فرما

در سال ۱۹۵۵، یک ریاضی‌دان جوان ژاپنی به نام یوتاکا تانیاما[6] با عنوان تعدادی مساله در یک کنفرانس حدس عجیب و شجاعانه‌ای را مطرح کرد. این حدس بعدها به وسیلهٔ گوروشیمورا[7] دقیق‌تر شد. نقش وایل[8] در این حدس کمی نامشخص‌تر است و شاید به شناساندن این حدس به بقیهٔ ریاضی‌دان‌ها محدود باشد. در متن‌های فعلی این حدس با نام‌های حدس تانیاما_شیمورا و حدس تانیاما_شیمورا_وایل شناخته می‌شود.

1-vector space 2-linear operators 3-Hecke operators

4-eigenfunction 5-eigenform 6-Yutaka Taniyama

7-Goro Shimura 8-Weil

اکنون بااستفاده از تعریف‌های بالا می‌توانیم این حدس را با دقت بیشتری بیان کنیم:

حدس تانیاما-شیمورا-وایل. E یک خم بیضوی با ضریب‌های درست و N هادی E است. برای هر عدد اول خوش تقلیل p، بگذارید

$$a_p = p + ۱ - |E(F_p)|$$

آن‌گاه صورت مدولی f وجود دارد به نحوی که

۱) وزن f برابر ۲ است، و

۲) f در سطح N است، و

۳) f ویژهٔ صورتی برای عمل‌گرهای هکه است، و

۴) بسط فوریه f عددهای a_p را می‌دهد.

هنوز ربط این حدس مهم را با قضیهٔ آخر فرما مشخص نکرده‌ایم. پیش از این گفته بودیم، اگر قضیهٔ آخر فرما نادرست باشد، می‌توان به وسیلهٔ مثال نقض آن خم بیضوی‌ای به نام خم بیضوی فری ساخت. فری کوشش کرد، ثابت کند، حدس تانیاما-شیمورا-وایل دربارهٔ خم بیضوی فری اشتباه است. از این نتیجه می‌شد: اگر حدس تانیاما-شیمورا-وایل‌درست باشد آن‌گاه خم بیضوی فری نمی‌تواند وجود داشته باشد، در نتیجه مثال نقضی برای قضیهٔ آخر فرما نمی‌توان یافت. فری نتوانست اثبات درستی از این حکم به‌دست آورد. ریاضی‌دان فرانسوی سر[1] نشان داد، اگر حدس دیگری (که در این‌جا آن را نمی‌آوریم) درست باشد، آن‌گاه می‌توان حکم فری را ثابت کرد. ریاضی‌دان آمریکایی ریبت[2] توانست در سال ۱۹۸۶ خدس سر را ثابت کند.

قضیه فری-سر-ریبت. فرض کنید E خم بیضوی فری است. اگر بتوان طبق پیش‌بینی حدس تانیاما-شیمورا-وایل یک صورت مدولی برای E پیدا کرد آن‌گاه می‌توان این صورت مدولی را به نحوی پیدا کرد که وزن آن ۲ و

1-Jean-Pierre Serre

2-Kenneth Ribet

سطح آن هم ۲ باشد و در ضمن این صورت یک تیزک صورت باشد. چنین صورت‌هایی وجود ندارد!

نتیجه. اگر حدس تانیاما-شیمورا-وایل درست باشد، آن‌گاه قضیهٔ آخر فرما هم درست است.

در این‌جا اضافه کنیم، این راه حل قضیهٔ آخر فرما تنها راه نیست. در اواخر دهه هشتاد در کنار حدس تانیاما-شیمورا-وایل چندین حدس دیگر هم وجود داشت که درستی هر کدام از آن‌ها به اثبات قضیهٔ آخر فرما می‌انجامید. با وجود کوشش بسیاری از ریاضی‌دان‌های مجرب، این حدس‌های دیگر هنوز اثبات نشده‌اند و هنوز بعید نیست که یکی از این‌ها در نهایت راه هموارتری برای اثبات قضیهٔ آخر فرما به‌دست دهد. البته، در هر صورت، اولین اثبات (و در حال حاضر تنها اثبات) قضیهٔ آخر فرما از طریق حدس تانیاما-شیمورا-وایل بوده‌است.

اندرو وایلز حدس تانیاما-شیمورا-وایل را برای خم‌های بیضوی نیم‌پایدار ثابت کرد و از آن‌جا که خم بیضوی فری هر نیم پایدار است، قضیهٔ آخر فرما ثابت شد. البته اثبات اولیه وایلز یک اشکال مهم داشت که بعد به وسیلهٔ وایلز و تیلور[1] تصحیح شد.

قضیه وایلز و تیلور-وایلز. حدس تانیاما-شیمورا-وایل برای خم‌های بیضوی نیم پایدار درست است.

نتیجه. خم فری نیم پایدار است و لذا قضیهٔ آخر فرما درست است!

ما در این‌جا به اثبات وایلز نپرداخته‌ایم. این اثبات مشکل و جالبی است که بیش از ۲۰۰ صفحه را می‌گیرد. هدف ما فقط این بود که خواننده ربط قضیهٔ وایلز با قضیهٔ آخر قرما را دریابد. در اثبات وایلز از نمایش‌های گالوا[2] استفاده بنیانی شده است. پرداختن به جزئیات این نظریه از حوصلهٔ این مقاله کوتاه خارج است.

در پایان بگوییم، کار در این رشتهٔ ریاضی همچنان ادامه دارد. برای مثال،

1-Richard Taylor

2-Galois Representations

در سال ۱۹۹۹، برویل[1]، کنراد[2] و دیاموند[3] و تیلور[4] حدس تانیاما-شیمورا-وایل را برای همه خم‌های بیضوی (و نه فقط خم‌های بیضوی نیم‌پایدار) ثابت کردند.

برای جزئیات بیشتر درباره اثبات قضیهٔ آخر فرما، خواننده می‌تواند به فهرست منابع مراجعه کند. اکثر مقاله‌هایی که در این فهرست آمده، مقاله‌های توصیفی هستند که برای متخصصین این رشته ریاضی نوشته نشده‌اند. نگارنده از این مقاله‌ها برای تهیه نوشته حاضر استفاده بسیار برده است.

1-Christopher Beuil 2-Brian Conrad

3-Fred Diamond 4-Richard Taylor

فهرست منابع

[1] Ezra Brown, Three Fermat Trails to Elliptic Curves, The College Mathe-matics Journal, 31(2000), no. 3, 162-172.

[2] David A.Cox, Introduction to Fermat's Last Theorem, American Mathe matical Monthly, 101 (1994), no. 1, 3-14.

[3] Henri Darmon, A Proof of the Full Shimura-Taniyama-Weil Conjecture is announced, Notices of the American Mathematical Society, December 1999, 1397-1401.

[4] Harold M. Edwards, Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory, Springer-Verlag, New York, 1977.

[5] Fernando Q. Gouvea, A Marvelors Proof, American Mathematical Monthly, 101 (1994), no. 3, 203-222.

[6] Anthony W.knapp, Elliptic Curves, Princeton University Press, Princeton, 1992.

[7] Barry Mazur, Number Theory as gadfly, American Mathematical Monthly 98 (1991), 593-610.

[8] Barry Mazur, on the Passage from local to global in number theory, Bulletin of the American Mathematical Society, 29 (1993), 14-50.

[9] Alf van der poorten, Notes on Fermat's Last Theorem, John Wiley & Sons, New York, 1996.

[10] paulo Ribenboim, 13 Lectures on Fermat's L... Theorem, Springer-Verlag, New York, 1979.

[11] Kenneth A. Ribet, and Brian Hayes, Fermat's Last Theorem, and Modern Arithmetic, American Scientist, 82 (1994), 144-156.

[12] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.

[13] Joseph H. Silverman, and John H.Tatc, Rational Points on Elliptic Curves, Springer-Verlag, New York, 1992.

[14] Richard Taylor, and Andrew Wiles, Ring-theoretic Properties of certain Hecke algebras, Annals of Mathematics (2) 141 (1995), 553-572.

[15] Andrew Wiles, Modular elliptic curves and Fermat's last theorem, Annals of Mathematics (2) 141 (1995), 443-551.

این کتاب در اساس مقدمه‌ای است بر نظریهٔ عددهای جبری. مفهوم اصلی و اندیشهٔ این نظریه در بستگی با قضیهٔ فرما طرح شد. خواننده در این کتاب قانع می‌شود که عددهای جبری به‌تصادف پدید نیامده‌اند، بلکه برای حل مساله‌های مشخص منطقی مورد نیاز بوده‌اند. یکی از هدف‌های کتاب این است که دشواری قضیهٔ فرما را به خواننده نشان دهد و اینکه چرا راه حل‌های مقدماتی برای آن به نتیجه نرسیده است.

خواننده‌ای که بر مقدمه‌های ریاضیات و تا حد دبیرستان آشنا باشد، می‌تواند از این کتاب استفاده کند. *قضیهٔ فرما* برای دانش‌آموزان سال‌های آخر دبیرستان، دانشجویان و همهٔ علاقه‌مندان به ریاضیات، و همچنین برای همهٔ کسانی که می‌خواهند با نظریهٔ عددهای جبری آشنا شوند، می‌تواند سودمند باشد.

۱۲۵۰ تومان
ISBN 964-312-544-0
9789643125448
نشر نی