نشر ریاضی، سال ۴، شمارهٔ ۱ و ۲، مرداد ۱۳۷۰

ایده‌های کومر در مورد آخرین قضیهٔ فرما*

پائولو ریبنبویم*
ترجمهٔ مهدی مجیدی ذوالبنین

هدف من در این سخنرانی، تشریح ایده‌های اساسی کومر دربارهٔ آخرین قضیهٔ فرما و نشان دادن این‌موضوع‌است که برخورد وی با این مسأله تا چه حد طبیعی بوده وچگونـه توانسته است نظریهٔ هیأتهای دایره‌بری[1] را ابداع کند. من در زمینهٔ قضیهٔ اصلی وسایر کارهـای وی بحث خواهم‌کرد و برخی از راههایی را کـه این مفاهیم درمطالعهٔ حساب گشوده‌اند، شرح خواهم داد.

۱. «آخرین قضیهٔ فرما» (که هنوز درحالت‌کلی اثبات نشده است) چنین حکم می‌کند:

(آ. ق. ف.): اگر $n \geqslant ۳$، آنگاه اعداد صحیح و مثبتی چون x و y و z یافت نمی‌شوند که

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

درشروع بحث‌یادآوری می‌کنم که اگر $n = ۲$، آنگاه‌چنین اعدادی وجود دارند. مثلا:

$$۳^۲ + ۴^۲ = ۵^۲$$

یا

$$۵^۲ + ۱۲^۲ = ۱۳^۲$$

در این گفتار، این «سه‌تاییهای فیثاغورسی» را علی‌رغم خواص جالبشان بررسی نخواهم کرد.

برای اثبات آ. ق. ف. درحالت‌کلی، اثبات آن برای $n = ۴$ و هرنمای‌اول $p \geqslant ۳$ کفایت می‌کند. درواقع اگر n مرکب باشد، $n > ۲$، آنگاه یا عامل فرد اولی دارد ویاعاملی‌که برابر ۴ است. اگر قضیه برای $n = m \cdot l$ (با ضابطهٔ $l > ۱$) نادرست باشد یعنی اگر اعـداد صحیح و مثبت x و y و z وجـود داشته باشند کـه $x^n + y^n = z^n$ آنگاه $(x^l)^m + (y^l)^m = (z^l)^m$ و در نتیجه قضیه برای m نیز نادرست خواهد بود که خلاف فرض است.

فرما برای حالت $n = ۴$ اثباتی پیدا کرد. وی در این اثبات معروف، «روش نزول نامتناهی» را به‌کار برد: بااین‌فرض‌که سه‌تایی (x, y, z) از اعداد صحیح مثبت، یك جواب معادلهٔ فرمـا باشد، موفق شد جواب دیگری مانند (x', y', z') پیداکند کـه درآن $z' < z$ و $۰ < z'$. سپس‌از این‌جواب‌جدیدشروع کرد و با تکرار روش، تـوانست جـواب دیـگری مثل (x'', y'', z'') به‌دست‌آوردکـه $۰ < z'' < z' < z$. ازآنجاکه z و z' و z'' و . . . اعدادی‌صحیح و مثبت‌اند، این روند را نمی‌توان به‌دلخواه ادامه داد واین تناقض است. بنابراین معادلهٔ فرمـا نمی‌تواند در اعـداد صحیح و مثبت جواب داشته باشد.

1. cyclotomic fields

اویلر قضیه را در حالت $n = ۳$ اثبات کرد. اثبات دیـگری برای این حالت در میان نوشته‌های گاوس نیز پیدا شده که پس از مرگش به‌چاپ رسید. درواقع گاوس حکم قویتری را اثبات کرده بود. فرض‌کنید $\omega = (-۱ + \sqrt{-۳})/۲$ یك ریشهٔ سوم یك باشد و هیأت همهٔ اعداد به‌شکل $a + b\omega$ $(a, b \in \mathbf{Q})$ را با $\mathbf{Q}(\omega) = \mathbf{Q}(\sqrt{-۳})$ نشان دهیم. (گاهـی این هیأت را هیأت آیزنشتاین می‌نامند) گاوس نشان داد که در حالت $n = ۳$ معادلهٔ فرما در $\mathbf{Q}(\omega)$ دارای جواب غیرصفر نیست.

وقتی‌لژاندر مقالاتی درمورد‌آخرین قضیهٔ فرمانوشت واثبات اویلر را درکتاب نظریهٔ اعـداد خودآورد، توجه ریاضیدانـان فرانسوی به‌آخرین قضیهٔ فرما جلب شد.

درحدود ۱۸۲۵ تا ۱۸۲۸ لژاندر و دیریکله‌مستقل از یکدیگر و تقریباً به‌طور همزمان قضیه را درحـالت $n = ۵$ اثبات کردند. در ۱۸۳۲ دیریکله قضیه‌را برای $n = ۱۴$ نیز اثبات نمودکه‌به‌طور محسوسی ساده‌تر از حـالت $n = ۷$ بـود. اثبات حالت اخیر در ۱۸۳۹ توسط لامه[1] صورت گرفت و در ۱۸۴۰ لبگ این اثبات را ساده‌تر کرد.

در این زمان درپاریس توجه وعلاقه‌خاصی‌نسبت به‌آ.ق.ف. ابرازمی‌شد. علاوه بر ریاضیدانانی‌که‌نام بردیم (ازجمله دیریکله که‌مدتی را در پاریس به‌سر برد) کوشی‌هم مجموعه‌ای از مقالات اساسی در نظـریـهٔ اعـداد منتشر کـرد. وی روی بـه‌اصطلاح چندجمله‌ایهای رادیکالی کار می‌کرد و تجزیهٔ آنها به عوامل اول رامطالعه می‌نمود. به‌زبان امروزی می‌توان گفت‌که تجسسات وی مطالعهٔ حساب هیأتهای دایره‌بری بوده است. لیکن او مـوفق نشد کار مهمی در زمینهٔ مسألهٔ فرما انجام دهد ولی‌کومر مدت کوتاهی بعد چنین کاری انجام داد.

در ۱۸۴۷ لامه یك اثبات کلی‌برای آ. ق. ف. به‌آکادمی‌علوم پاریس ارائـه کرد. جزئیات این اثبات درمجلـهٔ لیوویل، مجلهٔ (ریاضیات محض و کاربردی)، چاپ شد. امـا لیوویل متوجه شد که اثبات درست نیست. زیرا لامه (بدون هیچ توجیهی) فرض کرده بودکه تجزیهٔ چندجمله‌ایهای معینی از ریشه‌های یك به‌حاصلضرب عوامل تحویل‌ناپذیر، یکتاست. این موضوع به‌هیچ وجـه بدیهی نبود و بعداً معلوم شد کـه نادرست است. پس‌از تلاشهای مکرر برای اصلاح اثبات، لامـه دریافت که بایك مشکل اساسی مواجه است که نمی‌تواند آن را برطرف کند.

۲. با بودن چنین زمینه‌ای است کـه کومر کار مهمش را در

1. Lamé

مورد آخرین قضیه فرما آغاز می‌کند. وی درحدود ۱۸۳۷ اولین مقالهٔ‌خود را درمورد آ.ق.ف. به‌ازای‌نمای‌زوج $2n$ به‌زبان لاتینی منتشرکرد و مطلب زیر را اثبات نمود:

اگر $n>1$ فرد باشد و اگر اعداد صحیح و مثبت x و y و z یافت شوند که $(n, xyz)=1$ ب. م. م. و $x^{2n}+y^{2n}=z^{2n}$، آنگاه لزوماً: (پیمانهٔ ۸) $n\equiv 1$.

این نتیجه، تنها یك نتیجهٔ جزئی است. اثبات آن بسیار ساده بود و بعداً اثباتهای متعدد دیگری نیز برای آن پیدا شد.

اگر نما درمعادلهٔ فرما زوج‌باشد، می‌توان روشهای کارگشایی از نظریهٔ صورتهای‌درجه دوم را به‌کار برد. مثلا در دسامبر ۱۹۷۷ ترجانیان[1] نشان داد: اگر p عدد اول فردی باشد، و اگر اعداد صحیح و مثبت x و y و z موجود باشندکه $x^{2p}+y^{2p}=z^{2p}$، آنگاه $2p$ یکی از دو عدد x یا y را می‌شمارد. جالب اینجاست که اثبات ترجانیان کاملا مقدماتی و کلاسیك است ودرآن، فقط از نماد ژاکوبی و خواص تقسیم‌پذیری عبارتهایی به‌صورت $(x^p+y^p)/(x+y)$ استفاده شده است.

از اینجا امکان پیداشدن یك اثبات مقدماتی برای گزارهٔ زیر به‌ازای نمای اولی چون p (که معمولا حالت اول آ. ق. ف. برای نمای p نامیده می‌شود) به‌ذهن القا می‌شود.

اگر x و y و z اعدادصحیح و مثبتی باشند که $x^p+y^p=z^p$، آنگاه p، xyz را می‌شمارد.

برای چنین اثباتی دست‌کم لازم است ازقانون تقابل برای نماد باقیماندهٔ توانی به‌پیمانهٔ p استفاده شود.

۳. اولین مقالهٔ مهم‌کومر دربارهٔ قضیهٔ فرما از۱۸۴۴ درحال شکل‌گیری‌بود و سرانجام‌در ۱۸۴۷ منتشرشد. روش‌او که به‌زودی آن‌را شرح خواهیم داد، منجر به‌استفادهٔ او از هیأتهای دایره‌بُری شد. فرض‌کنید عدد اول p نمای معادلهٔ فرما باشد. وی

$$\zeta_p=\cos(2\pi/p)+i\sin(2\pi/p)$$

یعنی یك ریشه pام اولیهٔ یك و هیأت $\mathbf{Q}(\zeta_p)$ شامل همه اعداد مختلط به‌صورت

$$\alpha=a_0+a_1\zeta_p+a_2\zeta_p^2+\cdots+a_{p-2}\zeta_p^{p-2}$$
$$(a_0, a_1, a_2, \ldots, a_{p-2}\in\mathbf{Q})$$

را درنظر گرفت. اعدادی که در آنها $a_0, a_1, \ldots, a_{p-2}\in\mathbf{Z}$، حلقهٔ $\mathbf{Z}[\zeta_p]$ از اعداد صحیح دایره‌بری (نسبت به p) را تشکیل می‌دهند. دقیقاً مانند اعداد صحیح معمولی، اگر $\alpha, \beta\in\mathbf{Q}(\zeta_p)$ (α و β غیرصفر) آنگاه α شمارندهٔ β است اگر عدد صحیح دایره‌بری γ موجود باشد به‌طوری که $\alpha\gamma=\beta$. دوعدد صحیح دایره‌بری α و β وابسته به‌هم[2]اند هرگاه α شمارندهٔβباشد وβ، α را بشمارد. عدد صحیح دایره‌بری α، اول‌است هرگاه هرشمارندهٔ آن یا به‌خودش وابسته باشد، یا به۱. این نظریهٔ تقسیم‌پذیری، بین اعدادصحیح دایره‌بری‌وابسته به‌هم‌تمایزی قائل‌نمی‌شود. درحالت خاص، اعداد صحیح دایره‌بری وابسته به ۱، همان نقش بی‌اثر ۱ را دارند و یکه[3]های هیأت دایره‌بری $\mathbf{Q}(\zeta_p)$ نامیده می‌شوند.

قضیهٔ اساسی یکتایی تجزیهٔ اعداد صحیح را می‌توان چنین بیان کرد:

الف) هرعدد صحیح دایره‌بری متعلق به $\mathbf{Q}(\zeta_p)$ را می‌توان به‌حاصلضرب تعداد متناهی عدداول دایره‌بری تجزیه کرد.

ب) هردوتجزیه‌که بدین‌شکل باشند درحد یکه‌ها یکی هستند. یعنی اگر $\alpha=\beta_1\beta_2\cdots\beta_s=\gamma_1\gamma_2\cdots\gamma_t$، که درآن β_i و γ_j اعداد اول دایره‌بری هستند، آنگاه $s=t$ و پس از مرتب کردن، γ_i و β_i وابسته‌اند (برای‌هر $i=1, \ldots, s$).

اثبات درستی قسمت الف واقعاً ساده است. اما کومر قبلا درسال ۱۸۴۴ دریافته‌بود که قسمت ب درحالت‌کلی برقرارنیست. وی توانسته بود نادرستی آن‌را برای حالت $p=23$ نشان دهد.

کومر درنامه‌ای‌که‌در ۱۸۴۷ به‌همراه مقاله‌اش برای لیوویل فرستاد، شرح دادکه چگونه برای اصلاح قضیهٔ یکتایی تجزیه، نوع‌جدیدی از اعدادمختلط را درنظرگرفته است. وی این اعداد را «اعداد ایده‌آل» نامید. در مقاله‌ای دیگر، کومر مفهوم اعداد ایده‌آل‌را به‌کمك مفهوم مشابهی درشیمی توضیح‌داد! درآن‌زمان، وجود برخی مواد شیمیایی که دارای رادیکالهای فلوئورند قطعی شده بود اما هنوز خود فلوئور به‌صورت مجزا به‌دست‌نیامده بود. کومر می‌گفت که‌فلوئور مانند اعداد ایده‌آل اوست و رادیکالهای حاوی فلوئورکه در طبیعت یافت می‌شوند، درحکم اعداد مختلط واقعی‌اند.

تعریف‌کومر از ایده‌آلها، برحسب خواص تقسیم‌پذیری بود. این‌دیدگاه بعداً به‌مفهوم شمارنده تبدیل شدکه درنظریهٔ توابع جبری ظاهر می‌شود.

از سوی دیگر، ددکیند درتلاش برای فهمیدن مفهوم کومر، به‌کمك زیرمجموعه‌های خاصی از $\mathbf{Q}(\zeta_p)$ تعبیری از ایده‌آلها به‌دست داد. از دیدگاه ددکیند، یك ایده‌آل زیرمجموعه‌ای مانند I از $\mathbf{Q}(\zeta_p)$ است که‌دارای این ویژگیها باشد: تمت‌عمل جمع بسته باشد و $0\in I$؛ اگر $\alpha\in\mathbf{Z}[\zeta_p]$ و $\beta\in I$ آنگاه $\alpha\beta\in I$؛ عنصری مانند α موجودباشدکه $\alpha\in\mathbf{Z}[\zeta_p]$ و $\alpha\neq 0$ و برای هر $\beta\in I$، $\alpha\beta\in\mathbf{Z}[\zeta_p]$. اگر $I\subset\mathbf{Z}[\zeta_p]$، ایده‌آل را صحیح ودر غیراین صورت آن را کسری می‌نامیم. ضرایب هر $\alpha\in\mathbf{Q}(\zeta_p)$ یك ایده‌آل پدید می‌آورد: $(\alpha)=\{\beta\alpha|\beta\in\mathbf{Z}[\zeta_p]\}$ که آن را ایده‌آل اصلی α می‌نامیم. شرط‌لازم‌وکافی‌برای اینکه $(\alpha)=(\beta)$ آن‌است‌که $\alpha=\beta=0$ یا $\alpha\beta^{-1}$ یکه‌ای از $\mathbf{Z}[\zeta_p]$ باشد.

بنابرتعریف، حاصلضرب ایده‌آلهای I و J ایده‌آلی است متشکل از همهٔ عناصری که از جمع تعداد متناهی عنصر به‌شکل $\alpha\beta$ $(\alpha\in I$ و $\beta\in J)$ به‌دست‌می‌آیند. کومر برای تعیین محدودهٔ ایده‌آلهای‌غیرصفری که ایده‌آل اصلی نیستند (یا به‌اصطلاح کومر «اعداد ایده‌آلی» که «عدد» نیستند) رابطهٔ‌هم ارزی‌زیر راتعریف کرد: $I\sim J$ اگر عنصری مانند α وجود داشته باشد که $\alpha\neq 0$ و $\alpha\in\mathbf{Q}(\zeta_p)$ و $J=(\alpha)I$. رده‌های هم‌ارزی به‌دست آمده، رده‌های ایده‌آلها نامیده می‌شوند. اینکه بگوییم تنها یك ردهٔ هم‌ارزی در $\mathbf{Q}(\zeta_p)$ وجود دارد، بدین‌معنی است‌که هر ایده‌آل $\mathbf{Q}(\zeta_p)$، ایده‌آل اصلی است. کومر نشان داد که از اینجا نتیجه می‌شود قضیهٔ یکتایی تجزیه برای اعضای حلقهٔ متناظر از اعداد صحیح دایره‌بری برقرار است.

از آنجاکه کومر نادرستی این قضیه را برای حالاتی مثل

1. Terjanian 2. associated 3. unit

$p=۲۳$ نشان داده بود، طبیعتاً به‌بررسی اندازهٔ مجموعهٔ رده‌های ایده‌آلها کشانده شد.

در این‌مورد، توانست نتیجه اساسی زیر را ثابت کند: در هر هیأت دایره‌بری $\mathbf{Q}(\zeta_p)$ تعداد رده‌های ایده‌آلها متناهی است. این تعداد را عدد رده‌ای $\mathbf{Q}(\zeta_p)$ می‌نامند و اغلب آن‌را با h_p نمایش می‌دهند.

این ایده‌ها در مجموعهٔ مقالات مهمی که بین سالهای ۱۸۴۷ تا ۱۸۵۱ انتشار یافتند، عرضه شدند. (یکی از این مقالات در ۱۸۵۱ درفرانسه و در مجلهٔ لیوویل چاپ‌شد) این‌مقالات بسیاری از قضایای اساسی نظریهٔ اعداد جبری راکه بعدها پدید آمد برای ردهٔ خاص هیأتهای دایره‌بری دربرداشتند.

۴. اکنون به‌قضیهٔ اصلی کومر می‌پردازم. من شخصاً میل‌دارم این‌قضیه‌را قضیهٔ تاریخی‌کومر بنامم زیرا بر رأس نظریه‌ای قرار گرفته‌که بسیار پیشرفته‌تر از همهٔ دانشها و فنون آن زمان به‌شمار می‌رود و همهٔ اجزای آن را خود کومر ساخته است.

درمورد داستان ادعایی اثبات آ. ق. ف. توسط کومر (قبل‌از ۱۸۴۴) کـه طبق‌آن گویـا کومر درستی قضیهٔ یکتایی تجزیه را مفروض گرفته‌است،صحبت‌نخواهم کرد. این‌ماجراکه توسط هنزل[1] شایع شده، درمقالـه‌ای از ادواردز (۱۹۷۵) مورد بررسی قرار گرفته است؛موضوع این‌مقاله، نامه‌ای است از لیوویل به دیریکله که اخیراً کشف شده است.

بیان‌دقیق‌قضیه اصلی کومر (۱۸۴۷) چنین‌است: آخرین قضیهٔ فرما به‌ازای‌هرنمای اول‌فردی‌که درشرایط زیرصدق کند، درست است (دراینجا این‌شرایط را به‌زبان امروزی بیان می‌کنیم.):

۱) اگر ایـده‌آل I طوری باشدکـه توان pام آن I^p یك ایده‌آل اصلی باشد، آنگاه I خودش یك ایده‌آل اصلی باشد.

۲) اگر ω یکه‌ای از هیأت دایره‌بری $\mathbf{Q}(\zeta_p)$ باشد و اگر یـك عدد صحیح معمولـی $m\in\mathbf{Z}$ موجـود باشد بـه‌قسمی کـه (پیمانهٔ p) $\omega\equiv m$، آنگاه ω توان pام یك یکه باشد.

این فرضیات،رهگشا بودند ومسأله تبدیل‌شد به‌تحقیق دراین مورد که این شرایط به‌ازای چه اعـداد اولی برقرارند. او ابتدا نشان داد که شرط اول معادل شرط زیر است:

۱′) p، عدد رده‌ای هیأت دایره‌بری $\mathbf{Q}(\zeta_p)$ را نشمارد.

سپس بااستفاده از نتایج مطالعات عمیقش در حساب هیأتهای دایـره‌بری توانست نشان دهد کـه شرط دوم ازشرط اول نتیجه می‌شود. این‌شرط‌اکنون به «لم کومر درموردیکه‌ها» مشهور است. اثبات آن بسیار ظریف است و به‌چیزی احتیاج دارد که امروزه روشهای λ-آدیك[2] نامیده می‌شود. (کـه درآن λ یك عـدد اول دایره‌بری از $\mathbf{Q}(\zeta_p)$ است‌که p را می‌شمارد.)

هرعدد اول p که درشرط (۱′) صدق‌کند، یك عدداول‌منتظم[3] نامیده می‌شود. به‌عبارت دیگر کومر ثابت کرد:

اگر p یك‌عدد اول منتظم باشد، آ. ق. ف.به‌ازای آن درست است. در واقع آنچه کـومر ثابت کرد، بیش‌از این بود: اگر p یك‌عدداول‌منتظم باشد، اعداد غیرصفری چون $\alpha,\beta,\gamma\in\mathbf{Q}(\zeta_p)$ وجود ندارندکه $\alpha^p+\beta^p=\gamma^p$. باید گفت کـه اثبات کومر در مورد عدم وجود جواب در $\mathbf{Q}(\zeta_p)$ اشکال داشت. هیلبرت متوجه این‌موضوع شد و اشکال را برطرف کرد.

دراینجا با بررسی اثبات کومرمی‌خواهم نشان‌دهم که استدلال وی تـا چه حد طبیعی بـوده است. فرض کنید x و y و z اعداد غیرصفری‌باشند به‌طوری‌که $x^p=z^p-y^p$. پس‌از تقسیم x و y و z بر بزرگترین مقسوم علیه مشترك آنها می‌توان فرض کردکه این اعـداد نسبت به‌هم اول‌انـد. هدف، رسیدن به‌یك تناقض است. سمت چپ معادلهٔ فوق، یك حاصلضرب است درحالی‌کـه طرف راست آن‌یك تفاضل است. بسیار طبیعی است‌که تفاضل را به‌یك حاصلضرب تبدیل کنیم. این‌کار را می‌توان با استفاده از $\zeta=\zeta_p$، ریشهٔ pام یك، انجام داد:

$$x^p=z^p-y^p=\prod_{j=0}^{p-1}(z-\zeta^j y).$$

چقدر خوب می‌شد اگر عوامـل $(z-\zeta^j y)$ «نسبت بـه‌هم اول» بودند و می‌شد. نتیجه گرفت‌که هرعامل، توان pام یك‌عدد صحیح دایره‌بری است. اما این امر به این شکل‌کلی و خام صادق نیست. پس‌باید ایده‌آلها راکه قضیهٔ‌یکتایی تجزیه برای‌آنها درست است وارد کار کرد.

فرض کنید ایده‌آل I بزرگترین مقسوم‌علیه مشترك ایده‌آلهای اصلی $(z-\zeta^j y)$ بـاشد $(j=0,1,2,\dots,p-1)$. در این صورت

$$(z-\zeta^j y)=J_j' I\quad (j=0,1,\dots,p-1)$$

کـه در آن، ایده‌آلهای J_j' نسبت به‌هم اول‌انـد. از قضیهٔ یکتایی تجزیه برای ایده‌آلها نتیجه می‌شود که هرکدام ازآنها یك توان pام است. بنابراین:

$$(z-\zeta^j y)=J_j^p I\quad (j=0,1,\dots,p-1)$$

اثبات‌کومر این‌طور شروع می‌شود. پس از آن، دوحـالت مـورد بررسی قرار می‌گیرد: حالتی‌که p، xyz را می‌شمارد و حالتی‌که xyz بر p تقسیم‌پذیر نیست. جزئیات اثبات درکتابم آمده است. دراینجا قصد ندارم توضیحات بیشتری بدهم.

۵. هدف‌کومر پس از اثبات قضیهٔ اصلی روشن بود:

۱°) مشخص‌کردن و یا حداقل مطالعهٔ اعداد اول منتظم.

۲°) بررسی‌اینکه تعداد اعداد اول منتظم‌نامتناهی است یا نه.

۳°) تعمیم قضیهٔ اصلی نمـاهـای اول غیرمنتظم[1]. (یا حداقل آنهایی که درشرایط اضافی مناسبی صدق می‌کنند).

بنابراین‌کومر می‌بـایست مقدار عـدد رده‌ای h_p را محاسبه می‌کرد. وی این‌کار را برای pهای‌کوچك قبل‌از ۱۸۵۰ کـرده بود. به‌کمك نتایجی‌که ازطریق دیریکله ازآنها مطلع شده بـود، توانست فرمول صریحی بـرای عدد رده‌ای h_p پیدا کند. وی h_p را به‌صورت حاصلضرب دوعدد صحیح مثبت نوشت:

$$h_p=h_p^-\cdot h_p^+$$

1. Hensel 2. λ-adic 3. regular

1. irregular

که آنها را به‌ترتیب عوامل اول و دوم عدد رده‌ای نامید و بعداً تعبیرحسابی آنها را پیدا کرد. h_p^+ برابراست با عدد رده‌ای هیأت دایره‌بری حقیقی $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$ متشکل از همهٔ اعداد حقیقی $\mathbf{Q}(\zeta_p)$. به‌همین‌دلیل h_p^+ را اغلب عدد رده‌ای حقیقی $\mathbf{Q}(\zeta_p)$ می‌نامند و h_p^- عدد رده‌ای نسبی است. فرمولهای کومر اینها بودند:

$$h_p^- = \frac{1}{(2p)^{\frac{p-3}{2}}} |G(\eta)G(\eta^3)\dots G(\eta^{p-2})|$$

$$h_p^+ = \frac{2^{\frac{p-3}{2}}}{R} \prod_{k=1}^{\frac{p-3}{2}} \left| \sum_{j=0}^{\frac{p-3}{2}} \eta^{2kj} \log|1-\zeta^{gj}| \right|.$$

توضیح برخی از مقادیری که در فرمولهای فوق ظاهر شده‌اند برای کسانی که با اساس نظریهٔ اعداد جبری آشنایی ندارند، دشوار است.

— g نشاندهندهٔ یک ریشهٔ اولیه به‌پیمانهٔ p است.

— برای هر $j \geqslant 0$، $1 \leqslant g_j \leqslant p-1$ و $g_j \equiv g^j \pmod p$ (پیمانهٔ p)

$$G(X) = \sum_{j=0}^{p-2} g_j X^j$$

— η یک ریشهٔ $(p-1)$ام اولیهٔ یک است.

— R ناظم[1] هیأت دایره‌بری است. یعنی $R = 2^{\frac{p-3}{2}} \det(L)$ که L ماتریس زیر است:

$$L = \begin{pmatrix} \log|\varepsilon_1^{(1)}| & \dots & \log|\varepsilon_1^{(r)}| \\ \dots & \dots & \dots \\ \log|\varepsilon_r^{(1)}| & \dots & \log|\varepsilon_r^{(r)}| \end{pmatrix}$$

که در آن:

— r_1 تعداد مزدوجهای هیأت $\mathbf{Q}(\zeta_p)$ که در هیأت اعداد حقیقی قرار دارند، می‌باشد.

— $2r_2$ تعداد مزدوجهایی است که در هیأت اعداد حقیقی نیستند.

— $r = r_1 + r_2 - 1$

— $\{\varepsilon_1, \dots, \varepsilon_r\}$ یک دستگاه اساسی از واحدهای $\mathbf{Q}(\zeta_p)$ است. یعنی:

الف) اگر $1 \varepsilon_1^{e_1} \dots \varepsilon_r^{e_r}$ (که $e_1, \dots, e_r$ اعداد صحیح‌اند) آنگاه: $e_1 = \dots = e_r = 0$.

ب) اگر ε یکهٔ $\mathbf{Q}(\zeta_p)$ باشد، عدد صحیحی چون j با ضابطهٔ $1 \leqslant j \leqslant p-1$ و اعداد صحیح $e_1, \dots, e_r$ وجود دارند به‌قسمی که:

$$\varepsilon = \zeta_p^j \varepsilon_1^{e_1} \dots \varepsilon_r^{e_r}.$$

— اگر $\alpha \in \mathbf{Q}(\zeta_p)$ آنگاه $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(r_1)}$ نشاندهندهٔ مزدوجهای حقیقی α و $\alpha^{(r_1+1)}, \alpha^{(r_1+2)}, \dots, \alpha^{(r_1+2r_2)}$ نشاندهندهٔ مزدوجهای غیرحقیقی آن هستند به‌طوری که $\alpha^{(r_1+r_2+j)}$ مزدوج مختلط $\alpha^{(r_1+j)}$ است (برای $j = 1, \dots, r_2$).

روی‌هم‌رفته، کشف این فرمولها که توضیح آنها مشکل است، بسیار دشوار بود و ملاحظه می‌کنید که برای محاسبات صریح مناسب نیستند. به‌علاوه این بیشتر به معجزه شبیه است که h_p^+ که یک عدد صحیح است (یک عدد رده‌ای است)، حاصلضربی باشد از مجموعهای حاصلضربهای لگاریتمها و عبارات مثلثاتی

$$\eta^{2kj} = \cos\frac{4kj\pi}{p-1} + i\sin\frac{4kj\pi}{p-1}.$$

بنابراین، محاسبات حتی برای مقادیر نسبتاً کوچک p نیز پرزحمت بودند. اما چیزی که برای کومر مهم بود، تعیین مقدار دقیق h_p نبود. بلکه فقط می‌خواست بداند آیا p، h_p را می‌شمارد یا نه. از این لحاظ، کومر حکم غیرمنتظره و عمیق زیر را ثابت کرد:

اگر p شمارندهٔ h_p^+ باشد، آنگاه h_p^- را نیز می‌شمارد.

درنتیجه p شمارندهٔ h_p است اگر و تنها اگر h_p^- را بشمارد. با توجه به اینکه حتی امروزهم بررسی عامل h_p^+ جز با روشهای پیچیده میسر نیست، درمی‌یابیم که نتیجهٔ فوق یک پیشرفت اساسی است.

۶. با درنظر گرفتن تقسیم‌پذیری h_p^- بر p، کومر توانست مسأله را به‌مسألهٔ دیگری که مقدماتیتر است، تبدیل کند. وی معیار زیر را برای منتظم‌بودن اثبات کرد:

p شمارندهٔ h_p^- است اگر و تنها اگر عدد صحیح k با ضابطهٔ $1 \leqslant k \leqslant (p-3)/2$ موجود باشد به‌طوری که $\sum_{j=1}^{p-1} j^{2k}$ بر p^2 تقسیم‌پذیر باشد.

اویلر این مجموعها را مورد مطالعه قرارداده بود و آنها را برحسب اعداد برنولی که اولین‌بار در نظریهٔ احتمال به‌کار رفته بودند، بیان کرده بود. من تعریف آنها را یادآوری می‌کنم. در تقسیم x بر $e^x - 1 = \sum_{n=1}^{\infty} x^n/n!$ می‌توانیم ضرایب را به‌طور متوالی به‌صورت $B_n/n!$ بنویسیم که در آن B_n، nامین عدد برنولی است:

$$\frac{x}{e^x-1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n.$$

مثلا $B_0 = 1$، $B_1 = -1/2$، $B_2 = 1/6$، $B_3 = 0$، . . . . این اعداد را می‌توان به‌صورت بازگشتی از تعریف فوق به‌دست آورد. پس اگر $B_0, \dots, B_{n-1}$ معین باشند، B_n در رابطهٔ زیر صدق می‌کند

$$\binom{n+1}{1} B_n + \binom{n+1}{2} B_{n-1} + \dots + \binom{n+1}{n} B_1 + 1 = 0.$$

از اینجا نتیجه می‌شود که به‌ازای $n \geqslant 1$، $B_{2n+1} = 0$ و هر B_n یک عدد گویاست.

وقتی می‌گوییم عدد اول p، B_{2k} را می‌شمارد، منظورمان

1. regulator

آن‌است که وقتی $B_{۲۴}$ به‌صورت یک کسر تحویل‌ناپذیر نوشته شده باشد، p صورت آن‌را می‌شمارد.

کومر اولین معیار منتظم بودن را به‌حکم زیر تبدیل کرد:

p، h_p^- را می‌شمارد اگر وتنها اگر p یکی‌از اعداد $B_۲$، $B_۴$، $B_۶$، ...، $B_{p-۳}$ را بشمارد.

به‌نظر می‌رسد که این معیار، بسیار عملیتر باشد زیرا ۰حداقل از لحاظ نظری می‌توان اعداد برنولی را به‌صورت بازگشتی به‌دست آورد. درست‌است که این فرمول بازگشتی طول فزاینده‌ای دارد اما فرمولهای بازگشتی دیگری وجود دارندکه فنی‌تر هستند و در عوض طولشان کمتر است و محاسبات را بسیار ساده‌تر می‌کنند. علی‌رغم همهٔ اینها، مشکل واقعی این است که صورت اعداد برنولی باسرعتی عجیب‌بزرگ می‌شود و نوشتن این اعداد را بسیار دشوار می‌سازد. برای‌مثال تصور کنید که صورت $B_{۲۱۰}$ درحدود ۲۵۰ رقم دارد!

۰۷ همهٔ نتایج فوق، هرقدر هم عمیق و با ارزش باشند، به‌ما امکان پیش‌بینی این‌موضوع را نمی‌دهندکه یک‌عدد اول داده‌شده منتظم است یا نه. (مگر اینکه محاسبات ویژه‌ای انجام شود.) درضمن، این‌نتایج هیچ نشانه‌ای از چگونگی توزیع اعداد اول منتظم به‌دست‌نمی‌دهند. دراین‌مورد، بدون‌دادن‌توضیحات طولانی، می‌خواهم یادآوری کنم‌که کومر با دست‌خالی (یعنی بدون هیچ وسیلهٔ مکانیکی یا الکترونیکی) عدد رده‌ای $\mathbf{Q}(\xi_p)$ را برای $p \leqslant ۱۶۳$ محاسبه کرد و دریافت که اولین اعداد اول غیرمنتظم عبارت‌اند از: ۳۷، ۵۹، ۶۷، ۱۰۱، ۱۰۳، ۱۳۱، ۱۴۹ و ۱۵۷.۰

کومر بدون در دست‌داشتن مبنای محکمی حدس زد که باید تقریباً به‌اندازهٔ اعداد اول غیرمنتظم، عدد اول منتظم وجود داشته باشد (به‌مفهومی‌که‌توضیح‌خواهم داد.) یادآوری می‌کنم‌که پنسن[1] در ۱۹۱۵ نشان داد تعداد اعداد اول غیرمنتظم (حتی آنهایی که به‌پیمانهٔ ۴ همنهشت ۳اند) نامتناهی است. ازطرف دیگر هرگز اثبات نشده است‌که تعداد اعداد اول منتظم نامتناهی است. در ۱۹۶۴ زیگل[2] توانست به‌کمک استدلالهایی راهگشا نشان‌دهدکه:

$$\lim_{N\to\infty} \frac{\text{تعداد اعداد اول غیر منتظم } p \leqslant N}{\text{تعداد اعداد اول } p \leqslant N} = ۱ - \frac{۱}{\sqrt{e}}$$

$$= ۰٫۳۹۳...$$

این‌مقدار تا $N = ۱۲۵۰۰۰$ با محاسبات اخیر واگستاف[3] تطبیق می‌کند.

کومر همچنین آ. ق. ف.را برای رده‌هایی از اعداد اول غیرمنتظم که درشرایطی اضافی‌صدق می‌کردند، اثبات کرد. اینها نتایجی بسیار فنی هستندکه کومر نتوانست درآنها از اشتباه پرهیز کند. واندیور[4] این اشتباهها را تذکر داد وقسمتی از آنها را در ۱۹۲۲ و ۱۹۲۶ تصحیح کرد. ولی تلاشهای کومر در مورد حالت‌اول آ. ق. ف.موفقیت‌آمیزتر بود.وی توانست همنهشتیهای خاصی شامل اعداد برنولی پیداکند که جوابهای احتمالی معادلهٔ فرما باید در آنها صدق کنند. مقالهٔ مربوط به‌این‌کشف، نمونه‌ای از آثار بسیار ارزشمند کومر است که در آن روشهای حسابی و متعالی به‌صورت حیرت‌آوری باهم درمی‌آمیزند. وی براساس این همنهشتیها ثابت‌کرد که اگر حالت اول آ. ق. ف برای نمای p برقرار نباشد، آنگاه p، $B_{p-۳}$ و $B_{p-۵}$ را می‌شمارد. ضمناً این موضوع که p، $B_{p-۳}$ را می‌شمارد، قبلا به وسیلهٔ کوشی و جنوچی[1] کشف شده بود.میریمانف[2] نتیجهٔ کومر را بسط داد و ثابت‌کرد که p، $B_{p-۷}$ و $B_{p-۹}$ را نیز می‌شمارد. اخیراً موریشیما[3] ثابت کرده است‌که p باید $B_{p-۱۱}$ و $B_{p-۱۳}$ را نیز بشمارد.

بررسی کاملترین‌جدولها توسط واگستاف‌نشان می‌دهدکه این پدیده بسیار نادر است. در واقع، به‌ندرت اتفاق می‌افتد که p تعداد زیادی از اعداد برنولی (با اندیس حداکثر $p-۳$) را بشمارد و هرگز اعداد برنولی متوالی را نمی‌شمارد. همهٔ اینها به‌ساختار پیچیدهٔ گروه رده‌های ایده‌آلها مربوط است که شاید تا حدودی ازطریق کارهای هکه[4]،شولتس[5]، ایخلر[6] و ریبت[7] روشن شده باشد.

در مورد نتیجه جالب‌توجهی که کراسنر[8] در ۱۹۳۴ به‌دست آورد، چه باید گفت؟ وی مطلب زیر را نشان داد:

فرض‌کنید $n_۰ = (۴۵!)^{۸۸}$. اگر p عدد اولی بزرگتر از $n_۰$ باشد، چنانچه $k(p) = [\sqrt[۳]{\log p}]$ و اگر حالت اول آ. ق. ف. برای نمای p نادرست باشد، آنگاه p، $k(p)$ عدد برنولی‌متوالی $B_{p-۳}$، $B_{p-۵}$، ...، $B_{p-۲k(p)-۱}$ را می‌شمارد. (عدد $n_۰$ اهمیت خاصی‌ندارد وباکمی دقت در اثبات می‌توان آن‌را کوچکتر کرد. با این حال بازهم آنقدر بزرگ خواهد بودکه قضیه کاربرد عملی نخواهد داشت.) این قضیه که کراسنر را در ردهٔ افراد سهیم در مطالعهٔ آ. ق. ف.قرار می‌دهد، بیانگر این موضوع است‌که حالت اول قضیه، موجه است.

در خاتمه منصفانه نیست اگر نگوییم‌که کومر، حتی درنظریهٔ اعداد، دستاوردها وایده‌های تراز اول (وحتی مهمتر) دیگری نیز دارد. این ایده‌ها مربوطاند به‌قانون تقابل برای نماد باقیماندهٔ توانی، که به‌نظریهٔ هیأتهای رده‌ای[9] انجامیده است. به‌طوری‌که فورت‌وانگلر[10] در ۱۹۱۲ و هَسه[11] در ۱۹۲۶ نشان‌دادند، این نظریه را نیز می‌توان درمطالعهٔ آ. ق. ف به‌کار گرفت.

کارهای کومر به‌وسیلهٔ ریاضیدانانی که با آ. ق. ف.سروکار داشتند (و خواهند داشت) دنبال و تکمیل شد (و خواهد شد). اما هنوز نکات بسیاری در این زمینه مانده است که باید آموخت و فهمید، و انتشار مجموعهٔ آثار کومر در ۱۹۷۵ به‌همت وِیل برای ریاضیدانان این امکان را فراهم می‌سازدکه به‌طور جدی ایده‌های غنی وی را بررسی کنند.

من در کتابم کارهای کومر و روشهای مهمتری را که درمطالعه آخرین‌قضیهٔ فرما به‌کار رفته‌اند، تحلیل کرده‌ام. این‌کتاب، دارای یک کتابشناسی مفصل است.

---

1. Jensen 2. Siegel 3. Wagstaff 4. Vandiver

---

1. Genocchi 2. Mirimanoff 3. Morishima
4. Hecke 5. Scholz 6. Eichler
7. Ribet 8. Krasner 9. class field
10. Furtwängler 11. Hasse

مراجع

? FERMAT, P. de. Ad problema XX commentarii in ultimam questionem Arithmeticorum Diophanti. Area trianguli rectanguli in numeris non potest esse quadratus. *Œuvres*, Vol. I,p. 340 (in Latin); Vol. III, p. 271-272 (in French). Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthiers-Villars, Paris, 1891, 1896.

1770 EULER, L. *Vollständige Anleitung zur Algebra*. Royal Acad. of Sciences, St. Petersburg, 1770. See also *Opera Omnia*, Ser. I, Vol. I, 484-489. Teubner, Leipzig-Berlin, 1915.

1823 LEGENDRE,A.M. Sur quelques points d'analyse indéterminée et particulièrement sur le théorème de Fermat. *Mém. de l' Acad. des Sciences, Institut de France, 6* (1823), 1-60.

1828 DIRICHLET, G.L. Mémoire sur l'impossibilité de quelques équations indéterminées du 5^e degré. *J. reine u. angew. Math., 3* (1828), 354-375.

1830 LEGENDRE, A.M. *Théorie des Nombres* (3^e édition), Vol.II. Firmin Didot Frères, Paris, 1830. Reprinted by A. Blanchard, Paris, 1955.

1832 DIRICHLET, G.L. Démonstration du théorème de Fermat pour les 14^e puissances. *J. reine u. angew. Math., 9* (1832), 390-393.

1839 LAMÉ, G. Mémoire sur le dernier théorème de Fermat. *C.R.Acad.Sci. Paris, 9* (1839), 45-46.

1840 LEBESGUE, V.A. Démonstration de l'impossibilité de résoudre l'équation $x^7+y^7+z^7=0$ en nombres entiers. *J. Math. Pures et Appl., 5* (1840), 276-279.

1847 CAUCHY, A. Mémoire sur les racines des équations algébriques à coefficients entiers et sur les polynômes radicaux. *C.R. Acad. Sci. Paris, 24* (1847), 407-416. Reprinted in *Œuvres Complètes*, (1), 10, 231-239. Gauthier-Villars, Paris, 1897.

1847 CAUCHY, A. Mémoire sur diverses propositions relatives à la Théorie des Nombres. *C.R. Acad. Sci. Paris, 24,* (1847), 177-183, Reprinted in *Œuvres Complètes*, (1), 10, 360-366. Gauthier-Villars, Paris, 1897.

1847 LAMÉ, A. Mémoire sur la résolution en nombres complexes de l'équation $A^n+B^n+C^n=0$. *J. Math. Pures et Appl., 12* (1847), 172-184.

1852 GENOCCHI, A. Intorno all'espressioni generali di numeri Bernoulliani. *Annali di scienze mat. e fisiche, compilati da Barnaba Tortolini, 3* (1852), 395-405.

1876 GAUSS, C.F. Zur Theorie der complexen Zahlen: (I) Neue Theorie der Zerlegung der Cuben. *Werke,* Vol. II, p. 389-391. Königl. Ges. d. Wiss. zu Göttingen, 1876.

1893 DEDEKIND, R. Supplement XI to the fourth edition of Dirichlet's *Vorlesungen über Zahlentheorie*. Vieweg, Braunschweig, 1893. Reprinted by Chelsea Publ. Co., New York, 1968.

1905 MIRIMANOFF, D. L'équation indéterminée $x^l+y^l+z^l=0$ et le critérium de Kummer. *J. reine u. angew. Math., 128* (1905), 45-68.

1910 HECKE, E. Über nicht-reguläre Primzahlen und den Fermatschen Satz. *Nachr. Akad. d. Wiss. zu Göttingen* (1910), 420-424.

1912 FURTWÄNGLER, P. Letzter Fermatschen Satz und Eisensteins'ches Reziprozitätsgesetzt. *Sitzungsber. Akad. d. Wiss. Wien, Abt. IIa, 121* (1912), 589-592.

1915 JENSEN, K. L. Om talteoretiske Egenskaber ved de Bernoulliske tal. *Nyt Tidsskrift f. Math., B, 26* (1915), 73-83.

1922 VANDIVER, H. S. On Kummer's memoir of 1857 concerning Fermat's last theorem. *Bull. Amer. Math. Soc., 28* (1922), 400-407.

1926/ 1927/ 1930 HASSE, H. *Bericht über Neuere Untersuchungen und probleme aus der Theorie der algebraischen Zahlkörper*. Jahrsber. d. Deutschen Math. Verein., 35 (1926), 1-55; 36 (1927), 233-311; supplementary volume 6, 204 pages. Reprinted in two volumes. Physica Verlag, Würzburg, 1965.

1926 VANDIVER, H. S. Summary of results and proofs concerning Fermat's last theorem. *Proc. Nat. Acad. Sci., U.S.A., 12* (1926), 106-109.

1932 SCHOLZ, A. Über die Beziehung der Klassenzahlen quadratischer Zahlkörper zueinander. *J. reine u. angew. Math., 166* (1932), 201-203.

1932 MORISHIMA, T. Über die Fermatsche Vermutung, VII. *Proc. Imp. Acad. Japan, 8* (1932), 63-66.

1934 KRASNER, M. Sur le premier cas du théorème de Fermat. *C.R. Acad. Sci. Paris, 199* (1934), 256-258.

1964 SIEGEL, C.L. Zu zwei Bemerkungen kummers. *Nachr. Akad. d. Wiss. zu Göttingen, Math. Phys. Kl., II* (1964), 51-57. Reprinted in *Gesammelte Abhandlungen*, Vol. III, 436-442. Springer-Verlag, New York, 1966.

1965 EICHLER, M. Eine Bemerkung zur Fermatsche Vermutung. *Acta Arithm., II* (1965), 129-131, and 261.

1975 EDWARDS, H.M. The background of Kummer's proof of Fermat's last theorem for regular primes. *Arch. for . History of Exact Sciences, 14* (1975), 219-236.

1976 RIBET, K. A modular construction of unramified p-extensions of $\mathbf{Q}(\mu_p)$. *Invent. Math.,34* (1976),151-162.

1977 TERJANIAN, G. Sur l'équation $x^{2p}+y^{2p}=z^{2p}$. *C.R. Acad. Sci. Paris, 285* (1977), 973-975.

1978 WAGSTAFF, S. The irregular primes to 125000. *Math. Comp., 32* (1978), 583-592.

1979 RIBENBOIM, P. *13 Lectures on Fermat's Last Theorem*. Springer-Verlag. New York, 1979.

و بالاخره، جلد اول از مجموعه مقالات ارنست ادوارد کومر که به ویراستاری آلبرت‌ویل به وسیلهٔ انتشارات اشپرینگر-فرلاگ در ۱۹۷۵ منتشر شد، به مقالاتی در نظریهٔ اعداد اختصاص دارد.

مقالاتی از کومر که مستقیماً با قضیهٔ فرما ارتباط دارند، اینها هستند [شمارهٔ صفحات مربوط به جلد اول مجموعه مقالات است]:

1837(pp.135-141).	1844/1847(pp.165-192),	
1847(pp.203-210).	1847(pp.274-297),	1847(p.298),
1850(pp.299-322).	1850(pp.323-335),	1850(pp.336-344),
1851(pp.363-484).	1857(pp.631-638),	1857(pp.639-672),
1870(pp.919-944).	1874(pp.945-954).	

****

● این مقاله، متن یك سخنرانی است که در «سمینار فلسفه و فیزیك» در اکول نرمال سوپریور پاریس به تاریخ ۵ مارس ۱۹۷۹ انجام شده و ترجمهٔ فارسی آن ازروی منبع زیر صورت گرفته است

P. Ribenboim, "Kummer's ideas on Fermat's last theorem," *L'Enseignement Mathématique,* **29** (1983) 165-177.

★ پائولو ریبنبویم، دانشگاه کوین کانادا