ساختار گروهی خمهای درجهٔ سوم

رحیم زارع نهندی *

مقدمه

نظریهٔ خمهای درجهٔ سوم بالاخص خمهای بیضوی، فصل مشترک شاخه‌های مختلفی از ریاضیات مانند هندسه، نظریهٔ اعداد، توپولوژی، نظریهٔ گروهها، هندسهٔ جبری و هندسهٔ حسابی است. به‌علاوه، مسائل متنوعی در این نظریه وجود دارند که هنوز حل نشده‌اند و نکتهٔ جالب این است که اکثر این مسائل صورت ساده‌ای دارند.

نویسندهٔ مقاله‌ای در این زمینه، بسته به آنکه چه علایقی داشته باشد به خمهای بیضوی بیشتر در ارتباط با آن علایق می‌پردازد. با این توضیح، مقالهٔ حاضر رنگ‌وبوی هندسهٔ جبری خواهد داشت. با این حال سعی شده است که به‌خصوص به جنبه‌های نظریهٔ اعدادی نیز توجه شود. ضمناً تلاش بر این بوده که مقاله تاحدی خودکفا باشد و سیر مطلب از ساده به پیچیده به صورتی باشد که مقاله برای خوانندگان مختلف خسته‌کننده یا غیرقابل فهم نباشد. برهان بعضی از قضایا برای سهولت دسترسی ارائه شده است و می‌توان برهانهای طولانی را به‌طور گذرا مطالعه کرد.

خم E به معادلهٔ $y^2 = x^3 + ax + b = f(x)$ را در صفحه در نظر می‌گیریم به‌قسمی که $f(x)$ ریشهٔ چندگانه نداشته باشد. یک قانون ترکیب طبیعی روی E وجود دارد: برای هر دو نقطهٔ P و Q روی E، خطّ PQ خم را در نقطهٔ یکتای R قطع می‌کند و قانون $P \star Q = R$ یک ساختار طبیعی روی E است. هرچند قانون $\star$ تنها دارای خواص تعویضپذیری و شرکتپذیری است و عضو خنثی ندارد، با مختصر تصرفی در این قانون، E یک گروه آبلی خواهد بود. ساختار اخیر دارای خواص شگفت‌آور هندسی و حسابی است و کاربردهای جالبی دارد. در این مقاله، پس از یادآوری بعضی از تعاریف و مطالب، سعی می‌کنیم با استفاده از خواص هندسی دسته خمهای درجهٔ سوم، به برهان ساختار گروهی خم درجهٔ سوم بپردازیم. البته برهانی دقیقتر با استفاده از تعریف مناسب عدد تقاطع دو خم در یک نقطه و قضیهٔ بزو (Bèzout)و قضیه ماکس نویتر وجود دارد که به پیشنیازهای بیشتری نیازمند است و خوانندهٔ علاقه‌مند می‌تواند به [۳، صفحات ۱۲۴ و ۱۲۵] مراجعه کند. بخشی قابل توجه از مقاله به مباحثی درباره مسائل دیوفانتوسی و نظریهٔ اعداد و ارتباط ساختار گروهی خم درجهٔ سوم با این مسائل، اختصاص یافته است. و بالاخره، ساختار گروهی خم درجهٔ سوم را در رابطه با هندسهٔ جبری به‌اختصار مطالعه می‌کنیم.

یادآوری تعریفها

k را یک هیأت دلخواه می‌گیریم. مجموعهٔ k^n را که با $\mathbf{A}_k^n$ نمایش می‌دهیم، *فضای آفین* n بعدی روی k گوئیم. برای $n = 1, 2$، اصطلاحات *خط آفین* و *صفحهٔ آفین* روی k را بکار می‌بریم که وقتی $k = \mathbf{R}$، همان مفهوم اصطلاحات معمول را دارند. گاهی k را جبری‌بسته فرض می‌کنیم (مانند $k = \mathbf{C}$)، در عین حال، حالات $k = \mathbf{Q}$ و $k = \mathbf{R}$ از اهمیت ویژه‌ای برخوردارند. برای پرهیز از مشکلات تکنیکی همواره مشخصهٔ k مخالف ۲ و ۳ فرض خواهد شد.

زیرمجموعهٔ $V \subset \mathbf{A}_k^n$ یک مجموعهٔ جبری *آفین* گفته می‌شود هرگاه V مجموعهٔ صفرهای مشترک تعدادی چندجمله‌ای n متغیره باشد، یعنی چندجمله‌ایهای $f_1, \cdots, f_r \in k[x_1, \cdots, x_n]$ وجود داشته باشند به‌طوری‌که

$$V = \{P = (a_1, \cdots, a_n) \in \mathbf{A}_k^n | f_i(P) = 0, i = 1, \cdots, r\}$$

مجموعه‌های جبری، مجموعه‌های بستهٔ یک توپولوژی را روی $\mathbf{A}_k^n$ تشکیل می‌دهند که آن را *توپولوژی زاریسکی* گویند.

در صفحهٔ آفین، مجموعهٔ جبری تعریف شده توسط یک معادلهٔ $f(x, y) = 0$ را یک خم *(مسطح) آفین* گوییم. و اگر درجهٔ f برابر d باشد خم را از درجهٔ d گوییم. برای $d = 2$، خمهای درجهٔ دوم آفین و یا مقاطع مخروطی آفین، و برای $d = 3$، خمهای درجهٔ سوم آفین مورد توجه خواهند بود.

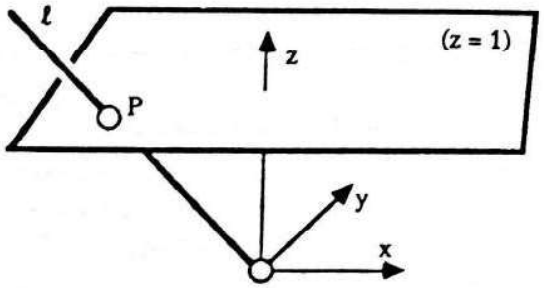
این مفاهیم در فضای آفین nبعدی تا حدی ساده و ملموس‌اند لیکن تکامل قضایای هندسهٔ جبری ایجاب می‌کند که مفاهیم اخیر در فضای تصویری nبعدی نیز تعریف شوند. *فضای تصویری* nبعدی $\mathbf{P}_k^n$ روی k، عبارت است از مجموعهٔ خطوط گذرنده از مبدأ در $\mathbf{A}_k^{n+1}$. به عبارت دیگر

$$\mathbf{P}_k^n = (\mathbf{A}_k^{n+1} \backslash \{o\}) / \sim$$

که $(X_0, \cdots, X_n) \sim (\lambda X_0, \cdots, \lambda X_n)$ به‌طوری‌که $\lambda \in k$، $\lambda \neq 0$.

با این ترتیب مختصات در $\mathbf{P}_k^n$ یکتا نیستند و با تقریب یک ضریب غیرصفر

معین می‌شوند. یک مجموعهٔ جبری تصویری توسط تعدادی چندجمله‌ای همگن تعریف می‌شود و توپولوژی حاصل از آنها را نیز توپولوژی زاریسکی گوییم. بالاخص، خطوط تصویری و خمهای درجهٔ دوم و سوم تصویری در صفحهٔ تصویری مورد نظر خواهند بود. تصور اینکه صفحهٔ تصویری اجتماع صفحهٔ آفین و «خط در بینهایت» است، کمک موثری به تجسم صفحهٔ تصویری می‌کند، به بیان دقیقتر، هر خط غیرافقی گذرنده از مبدأ در $\mathbf{P}_k^3$ صفحهٔ $Z = 1$ را دقیقاً در یک نقطه قطع می‌کند و هر خط افقی گذرنده از مبدأ غیر از محور Xها، خط $\{\frac{Z=0}{Y=1}\}$ را در یک نقطه قطع می‌نماید. لذا تحت این تناظر یک‌به‌یک، می‌توان $\mathbf{P}_k^3$ را اجتماعی از $\mathbf{A}_k^2$ و یک خط تصویری «در بینهایت» دانست که خود این خط تصویری نیز، اجتماعی از $\mathbf{A}_k^1$ و یک نقطهٔ «بینهایت» است.



شکل ۱

از طرف دیگر، صفحهٔ تصویری $\mathbf{P}_k^2$، توسط سه صفحهٔ آفین پوشانده می‌شود. زیرا با فرض $U_1 = \{(X:Y:Z) \in \mathbf{P}_k^2 | X \neq 0\}$ نگاشت $U_1 \to \mathbf{A}_k^2$ که به صورت $(X:Y:Z) \longmapsto (y,z) = (\frac{Y}{X}, \frac{Z}{X})$ تعریف می‌شود یک‌به‌یک و پوشاست. به همین ترتیب هرکدام از زیرمجموعه‌های $U_2 = \{(X:Y:Z) \in \mathbf{P}_k^2 | Y \neq 0\}$ و $U_3 = \{(X:Y:Z) \in \mathbf{P}_k^2 | Z \neq 0\}$ را می‌توان با یک صفحهٔ آفین یکی گرفت. حال داریم

$$\mathbf{P}_k^2 = U_1 \cup U_2 \cup U_3$$

هرگاه $E \subset \mathbf{P}_k^2$ یک خم تصویری باشد، هریک از مجموعه‌های $E \cap U_i$، $i = 1,2,3$ مثل یک خم آفین است که معادلهٔ آن تحت نگاشتهای دوسویی بالا، به‌ترتیب با قراردادن $X = 1$ یا $Y = 1$ و یا $Z = 1$ در معادلهٔ همگن E به‌دست می‌آید.

حال خم درجهٔ سوم $E: Y^2Z = X^3 + aXZ^2 + bZ^3$ را در نظر بگیرید. روی این خم تنها یک نقطه با ضابطهٔ $Z = 0$ وجود دارد که نقطهٔ $(0:1:0)$ است. لذا خم تصویری بالا اجتماع خم آفین $y^2 = x^3 + ax + b$ با نقطهٔ اخیر است. نقطهٔ $(0:1:0)$ با تعبیری که از $\mathbf{P}_k^2$ به‌صورت اجتماع صفحه آفین و خط در بینهایت کردیم، نقطه‌ای روی محور yها «در بینهایت» خواهد بود که این نقطه را با «∞» نمایش می‌دهیم. در قسمتی از این مقاله، به‌جای خم تصویری بالا یا خمهای مشابه، خمهای آفین متناظر همراه با نقطهٔ ∞ و یا نقاط در بینهایت، مد نظر خواهند بود.

دستگاههای خطی از خمها

گاهی لازم است همهٔ خمهای تصویری از درجهٔ $d \geq 1$ را بررسی کنیم. فرض کنیم $(M_0, \cdots, M_N)$ ترتیب مشخصی از مجموعهٔ تکجمله‌ایهای سه‌متغیرهٔ $X^\alpha Y^\beta Z^\gamma$ از درجهٔ d باشد (یعنی $\alpha + \beta + \gamma = d$)، که طبق محاسبه، $N = \binom{d+2}{2} - 1 = d(d+3)/2$. (در دنبالهٔ بحث منظور از N همین عدد خواهد بود). مثلاً اگر ترتیب الفبایی مورد نظر باشد، برای $d = 3$، داریم: $N = 9$ و

$$(M_0, \cdots, M_9) = (X^3, X^2Y, X^2Z, XY^2, XYZ, XZ^2, Y^3, Y^2Z, YZ^2, Z^3)$$

در نظرگرفتن یک خم از درجهٔ d در صفحهٔ تصویری، معادل انتخاب $(a_0, \cdots, a_N) \in k^{N+1}$ است که همهٔ a_iها صفر نیستند و $F = \sum_{i=0}^{N} a_i M_i$، با این توضیح که $(a_0, \cdots, a_N)$ و $(\lambda a_0, \cdots, \lambda a_N)$ به‌ازای $\lambda \in k$ و $\lambda \neq 0$، هردو یک خم را معین می‌کنند، به‌عبارت دیگر هر خم تصویری $F = 0$ از درجهٔ d به نقطهٔ یکتایی از $\mathbf{P}_k^N$ نظیر می‌شود و هر نقطهٔ $\mathbf{P}_k^N$ خم یکتایی را معرفی می‌کند. با این ترتیب می‌توان خم $F = 0$ را با نقطهٔ متناظر آن در $\mathbf{P}_k^N$ یکی گرفت و اصطلاح «*خمی با درجهٔ d از فضای تصویری $\mathbf{P}_k^N$*» به همین معنی خواهد بود.

مثال ۱. $d = 1$؛ هر خط $aX + bY + cZ = 0$ به نقطهٔ $(a,b,c) \in \mathbf{P}_k^2$ متناظر می‌شود، لذا خطوط $\mathbf{P}^2{}_k$ تشکیل یک $\mathbf{P}_k^2$ می‌دهند

مثال ۲. $d = 2$، مقطع مخروطی $aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2 = 0$ به نقطهٔ $(a:b:c:d:e:f) \in \mathbf{P}_k^5$ متناظر می‌شود. به‌عبارت دیگر مقاطع مخروطی تشکیل یک $\mathbf{P}_k^5$ می‌دهند.

مثال ۳. خمهای درجهٔ سوم تشکیل $\mathbf{P}_k^9$ و خمهای درجهٔ چهارم تشکیل $\mathbf{P}_k^{14}$ می‌دهند.

معمولاً شرایطی روی مجموعهٔ خمهای درجهٔ d در نظرگرفته می‌شود و مجموعه خمهای درجهٔ dی که این شرایط را برآورده می‌کنند یک زیرمجموعهٔ $\mathbf{P}_k^N$ را تشکیل می‌دهند. اگر این زیرمجموعه یک زیرفضای خطی $\mathbf{P}_k^N$ باشد (یعنی با معادله‌های خطی داده شده باشد)، آن را یک *دستگاه خطی از خمهای درجهٔ d* گویند.

لم. (الف) اگر $P \in \mathbf{P}_k^2$ یک نقطهٔ ثابت باشد، مجموعهٔ خمهای درجهٔ d که از P می‌گذرند یک ابر صفحهٔ $\mathbf{P}_k^N$ است (به‌خصوص یک دستگاه خطی است.)

(ب) اگر $P_1, \cdots, P_r \in \mathbf{P}_k^2$ نقاط ثابتی باشند، مجموعهٔ خمهای درجهٔ d که از نقاط $P_1, \cdots, P_r$ می‌گذرند یک دستگاه خطی است که بعد آن از $N - r$ کمتر نیست، و در حالت $r = N$ نیز دستگاه خطی ناتهی است.

برهان سادهٔ لم بالا به خواننده واگذار می‌شود.

نتیجه. از هر پنج نقطه لااقل یک مقطع مخروطی و ازهر نه نقطه لااقل یک خم درجهٔ سوم می‌گذرد.

حالات خاصی از قضیهٔ بزو

قضیهٔ بزو حاکی است که اگر $E_1, E_2 \subset \mathbf{P}_k^2$ دو خم با درجه‌های m و n باشند که مؤلفه مشترکی نداشته باشند، تعداد نقاط فصل مشترک آنها از mn بیشتر نیست که اگر k جبری ـ بسته باشد و نقاط مشترک با چندگانگی مناسبی شمرده شوند، این تعداد دقیقاً mn است. به‌عنوان مثال، دو حکم زیر که بعداً مورد استفاده قرار خواهند گرفت، موارد خاصی از قضیهٔ بزو هستند

که بهتر است خواننده سعی کند آنها را مستقیماً ثابت کند.

قضیه. (الف) در صفحهٔ $\mathbf{P}_k^2$ هر خط یک خم درجهٔ سوم را حداکثر در سه نقطه قطع می‌کند مگر آنکه خم درجهٔ سوم اجتماع این خط با یک مقطع مخروطی باشد.

(ب) در صفحهٔ $\mathbf{P}_k^2$ هر مقطع مخروطی یک خم درجهٔ سوم را حداکثر در شش نقطه قطع می‌کند، مگر آنکه خم درجهٔ سوم اجتماع یک مقطع مخروطی با یک خط باشد.

خاصیتی از دسته خمهای درجهٔ سوم

قضیه. فرض کنیم k یک هیأت نامتناهی و D و D' دو خم درجهٔ سوم تصویری (در $\mathbf{P}_k^2$) باشند که همدیگر را دقیقاً در نه نقطه متمایز قطع می‌کنند. هرگاه خم درجهٔ سوم تصویری D'' شامل هشت نقطه ازنه نقطهٔ بالا باشد، شامل نقطهٔ نهم نیز خواهد بود، به‌علاوه

$$D'' = aD + a'D' \qquad a, a' \in k$$

(یعنی معادلهٔ D'' ترکیبی خطی از معادله‌های D و D' است).

برهان. این نه نقطه را با $P_1, \cdots, P_8, P_9$ نمایش می‌دهیم. ابتدا توجه می‌کنیم که هیچ چهار نقطه از نه نقطه فوق نمی‌توانند همخط باشند، زیرا اگر همخط، باشند، طبق قضیهٔ قبل، خط گذرنده از چهار نقطه مشمول D و D' خواهد بود که خلاف فرض است. همچنین هیچ هفت نقطه از نه نقطهٔ مفروض نمی‌توانند روی یک خم درجهٔ دوم واقع شوند زیرا اگر واقع شوند، طبق قضیهٔ قبل، مؤلفه‌ای از خم درجهٔ دوم مشمول D و D' خواهد بود که خلاف فرض است چون در هر دو حالت $D \cap D'$ فقط شامل نه نقطه است.

حال فرض کنید D'' به‌صورت $aD + a'D'$ نباشد. مجموعهٔ خمهای درجهٔ سوم فضای تصویری $\mathbf{P}_k^9$ را تشکیل می‌دهند و فرض اخیر در $\mathbf{P}_k^9$ بدین معنی است که نقاط متناظر با D، D' و D'' همخط نیستند، درنتیجه مجموعهٔ نقاط متناظر با $aD + a'D' + a''D''$ تشکیل یک صفحهٔ تصویری می‌دهند. دو نقطه P' و P'' را در نظر می‌گیریم. طبق لم قبل، مجموعهٔ خمهای درجهٔ سومی که از این دو نقطه می‌گذرند به یک زیرفضای خطی $\mathbf{P}_k^9$ نظیر می‌شوند که بعد آن حداقل ۷ است. این زیرفضا، فضای خطی دوبعدی متناظر با مجموعهٔ $aD + a'D' + a''D''$ها را لااقل در یک نقطه قطع می‌کند (جواب غیرصفر ۹ معادلهٔ همگن خطی از ۱۰ مجهول!). مفهوم این مطلب آن است که از هر دو نقطهٔ P' و P'' در صفحه، لااقل یک خم درجهٔ سوم به شکل $aD + a'D' + a''D''$ می‌گذرد.

حال نشان می‌دهیم هیچ سه نقطه از نه نقطهٔ مفروض همخط نیستند. فرض کنید P_1، P_2 و P_3 روی یک خط L واقع‌اند. چون هیچ چهار نقطه از این نه نقطه همخط نیستند، هیچ‌یک از نقاط $P_4, \cdots, P_9$ روی L نیست. فرض می‌کنیم E خم مخروطی گذرنده از نقاط $P_4, \cdots, P_8$ باشد. نقطهٔ جدید P' را روی L و نقطهٔ دیگر P'' را در صفحه طوری انتخاب می‌کنیم که روی L یا E نباشد. حال ترکیب $aD + a'D' + a''D''$ را که از نقاط P' و P'' می‌گذرد، در نظر می‌گیریم. چون این خم درجهٔ سوم با L حداقل چهار نقطهٔ مشترک دارد، طبق قضیهٔ قبل، L مشمول این خم است یعنی L مؤلفه‌ای از این خم است و مؤلفهٔ دیگر آن طبعاً یک خم درجهٔ دوم مانند E' خواهد بود که شامل نقاط $P_4, \cdots, P_8$ و P'' می‌باشد. حال چون $E' \cap E$ شامل حداقل پنج نقطهٔ $P_4, \cdots, P_8$ است، E و E' مؤلفهٔ مشترک دارند. E و E' نمی‌توانند تنها در یک مؤلفهٔ خطی مشترک باشند چه اگر باشند، تنها سه نقطه از نقاط $P_4, \cdots, P_8$ می‌توانند روی این مؤلفهٔ خطی واقع شوند و دو نقطهٔ دیگر روی مؤلفه‌های خطی دیگر E و E' به‌طور مشترک قرار می‌گیرند و در نتیجه مؤلفه‌های خطی اخیر بر هم منطبق خواهند بود یعنی E و E' بر هم منطبق‌اند و نتیجه اینکه خم درجهٔ سوم $aD + a'D' + a''D''$ برابر $L \cup E'$ است که این موضوع با نحوهٔ انتخاب P'' تناقض دارد.

در این مرحله ثابت می‌کنیم هیچ شش نقطه از نه نقطهٔ مفروض روی هیچ مقطع مخروطی واقع نیست. فرض کنید $P_1, \cdots, P_6$ روی یک مقطع مخروطی E است. خط L را که از P_7 و P_8 می‌گذرد در نظر بگیرید. نقطهٔ P' را روی E و نقطه P'' را خارج از L و E انتخاب کنید؛ خم درجهٔ سوم $aD + a'D' + a''D''$ که از P' و P'' می‌گذرد از هشت نقطهٔ $P_1, \cdots, P_8$ نیز می‌گذرد و با استدلالی مشابه استدلال پاراگراف بالا، L و E مؤلفه‌های $aD + a'D' + a''D''$ هستند و لذا خم $aD' + a'D' + a''D''$ با اجتماع $L \cup E$ مساوی خواهد بود که‌این موضوع با نحوهٔ انتخاب P'' تناقض دارد.

حال برای اتمام اثبات قضیه، فرض کنید L خط گذرنده بر P_1 و P_2 و E مقطع مخروطی گذرنده از $P_3, \cdots, P_7$ باشد. نقاط P' و P'' را روی L طوری انتخاب می‌کنیم که روی E نباشند. خم درجهٔ سوم $aD + a'D' + a''D''$ را که از P' و P'' می‌گذرد در نظر می‌گیریم، این خم از ده نقطهٔ $P_1, \cdots, P_8$، P' و P'' میگذرد و لذا با استدلال مشابه استدلال قبلی مساوی $L \cup E$ خواهد بود که با توجه به‌این نکته که طبق دو پاراگراف بالا P_8 نمی‌تواند روی L یا E واقع باشد، تناقض پیش می‌آید. نتیجه اینکه، $D'' = aD + a'D'$ و بنابراین D'' ازنقطهٔ P_9 نیز می‌گذرد. ■

ساختار گروهی خمهای بیضوی

فرض کنیم خم تصویری E با چندجمله‌ای همگن درجهٔ سوم تحویلناپذیر $F(X, Y, Z) = 0$ داده‌شده به طوری که در هر نقطه E خط مماس یکتایی وجود دارد، به‌عبارت دیگر در هر نقطهٔ خم، لااقل یکی از مشتقّات جزئی $\frac{\partial F}{\partial X}$، $\frac{\partial F}{\partial Y}$، $\frac{\partial F}{\partial Z}$ غیرصفر است. از نظر هندسی شرط اخیر به این معنی است که خم E *هموار* (= *ناتکین*) است. طبق تعریف، چنین خمی را یک خم بیضوی گوییم. نقطهٔ ثابت $O \in E$ را در نظر می‌گیریم.

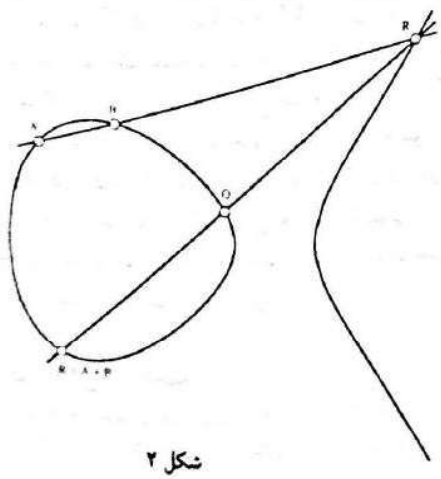
(الف) برای هر نقطهٔ $A \in E$، قرار می‌دهیم:

سومین نقطهٔ تلاقی خم E با خط OA را $\overline{A}$.

(ب) برای هر دو نقطهٔ $A, B \in E$ قرار می‌دهیم:

سومین نقطهٔ تلاقی خم E با خط AB را R.

قانون $+$ را روی نقاط E به شکل $A + B = \overline{R}$ تعریف می‌کنیم.



شکل ۲

این قانون را «*عمل وتر-مماس*» گویند.

توضیح. علت انتخاب نام خم بیضوی برای خمهای بالا این است که از نظر تاریخی، مشابه این چندجمله‌ایها ابتدا در محاسبهٔ محیط بیضی ظاهر شده‌اند (برای ملاحظهٔ توضیح جامعتر، رک.[۱۲، صص ۴۱۲ – ۴۱۵]).

قضیه. خم E با قانون $+$ یک گروه آبلی است که عضو خنثای آن نقطهٔ O است.

برهان. ابتدا باید نشان دهیم قانون $+$ خوشتعریف است و هر نقطه، قرینه دارد. برای دو نقطهٔ $A, B \in E$ دو حالت $A \neq B$ و $A = B$ پیش می‌آید. در حالت اول $L \subset \mathbf{P}^2$ را خط گذرنده از A و B و در حالت دوم L را خط مماس بر E در نقطهٔ A می‌گیریم. در هر حال L به‌صورت یکتا مشخص می‌شود و $F|_L$ یک صورت درجهٔ سوم دومتغیره است که ۲ ریشهٔ آن داده شده است (در $\mathbf{P}^1_k$!). بنابراین بدون استثناء، $F|_L$ به حاصلضرب سه‌عامل خطی تجزیه می‌شود و مختصات نقطهٔ سوم تلاقی L با E در $\mathbf{P}^2_k$ به‌دست می‌آید.

توجه داشته باشید که حالتهای $A = R$، $B = R$ و $A = B = R$ همگی امکانپذیرند. از نظر هندسی $A = B = R$ به این معنی است که A یک نقطهٔ *عطف* E است.

این حکم که O عضو خنثی است، نتیجهٔ واضح همخط بودن سه نقطه O، A و $\bar{A}$ است. برای یافتن قرینهٔ نقطهٔ A، ابتدا فرض کنید $\overline{O}$ نقطهٔ سوم تلاقی خط مماس بر E در نقطهٔ O است. $\bar{O}A$ خم E را در نقطهٔ سومی قطع می‌کند که قرینهٔ A است. روشن است که $A + B = B + A$.

تنها مشکل اصلی قضیه، برهان شرکتپذیری قانون $+$ است که ابتدا آن‌را برای نقاطِ در «وضعیت عمومی» ثابت می‌کنیم. فرض کنیم A و B و C سه نقطهٔ متمایز روی خم E باشند. برای به‌دست آوردن $(A + B) + C = \overline{S}$، چهار خط زیر به‌کار می‌روند (شکل وتر-مماس):

$$L_1 : ABR,\ L_2 : RO\overline{R},\ L_3 : SC\overline{R},\ L_4 : SO\overline{S}$$

و برای پیداکردن $A + (B + C) = \overline{T}$ از چهار خط زیر استفاده می‌شود.

$$M_1 : BCQ,\ M_2 : QO\overline{Q},\ M_3 : A\overline{Q}T,\ M_4 : TO\overline{T}$$

می‌خواهیم ثابت کنیم $\overline{S} = \overline{T}$، که برای این کار اثبات $S = T$ کافی است. فرض کنیم D' و D'' خمهای درجهٔ سوم زیرند.

$$D' = L_1 \cup M_2 \cup L_3 \quad , D'' = M_1 \cup L_2 \cup M_3$$

که طبق ساختار

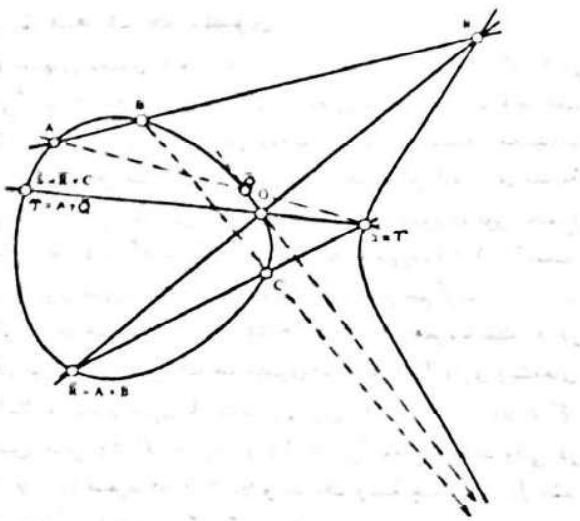
$$E \cap D' = \{A, B, C, O, R, \overline{R}, Q, \overline{Q}, S\}$$

و

$$E \cap D'' = \{A, B, C, O, R, \overline{R}, Q, \overline{Q}, T\}$$

هستند.

حال با این شرایط که نه نقطهٔ $E \cap D'$ همگی متمایز باشند، $D = E$ و D' شرایط قضیه قبل را برآورد می‌کنند، لذا D'' نیز از نقطهٔ S می‌گذرد و این تنها وقتی ممکن است که $S = T$، چون خم درجهٔ سوم D'' که اجتماع سه خط است، نمی‌تواند خم E را در بیش از نه نقطه قطع کند.



شکل ۳

برای تکمیل این برهان، هیأت k را یک زیرهیأت $\mathbf{C}$ فرض می‌کنیم تا بتوانیم از مفهوم پیوستگی معمولی استفاده‌کنیم. مجموعهٔ‌نقاط $(X : Y : Z) \in \mathbf{P}^2_{\mathbf{C}}$ را که $F(X, Y, Z) = 0$، با $E_{\mathbf{C}}$ نمایش می‌دهیم، به‌عبارت دیگر $E_{\mathbf{C}}$ «*مختلط شدهٔ*» خم E است. روشن است اگر خاصیت شرکتپذیری را برای نقاط $E_{\mathbf{C}}$ ثابت کنیم حکم برای نقاط E نیز برقرار است. لذا کافی است $k = \mathbf{C}$ فرض شود.

لم زیر را که برهان آن چندان پیچیده نیست می‌پذیریم.

لم. (الف) $A + B$ تابعی پیوسته از A و B است (نسبت به توپولوژی معمولی القایی از صفحه تصویری مختلط).

(ب) برای هر $A, B, C \in E$، نقاط $A', B', C' \in E$ وجود دارند که به‌قدر دلخواه به A و B و C نزدیک‌اند و نه نقطهٔ A'، B'، C'، O، R، $\overline{R}$، Q، $\overline{Q}$، S که برای به‌دست آوردن $(A' + B') + C'$ به‌کار می‌روند، همگی متمایزند.

با استفاده از (الف)، نگاشت $\varphi : E \times E \to E$ که به‌صورت $(A, B) \longmapsto A + B$ تعریف می‌شود، پیوسته است. لذا نگاشتهای $g = \varphi \circ (id_E \times \varphi) : E \times E \times E \to E$ و $f = \varphi \circ (\varphi \times id_E)$ که $f(A, B, C) = (A + B) + C$ و $g(A, B, C) = A + (B + C)$، پیوسته خواهند بود. مطابق (ب)، مجموعهٔ $U \subset E \times E \times E$ متشکل از سه‌تاییهای (A, B, C) که برای آنها نه نقطهٔ به‌کارگرفته شده متمایزند، یک زیرمجموعهٔ چگال است. حال با توجه به اثبات شرکتپذیری در حالت نقاط متمایز، دو تابع پیوستهٔ f و g روی زیرمجموعهٔ چگال U با هم مساوی‌اند و لذا روی کل $E \times E \times E$ با هم برابرند. یعنی قانون $+$ شرکتپذیر است. ■

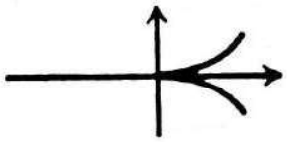
توضیح. در قسمت آخر استدلال بالا از توپولوژی روی $\mathbf{C}$ استفاده شده و درنتیجه برهان، جبری خالص نیست. با این حال در صورتی که هیأت k یک هیأت دلخواه باشد همه استدلالها نسبت به توپولوژی زاریسکی روی E (که در این حالت همان توپولوژی متمم-متناهی است)، اعتبار پیدا می‌کنند، به این معنی که تابع φ نسبت به این توپولوژی نیز پیوسته است و زیرمجموعهٔ $U \subset E \times E \times E$ که برای نقاط آن نه نقطهٔ مورد نظر متمایزند، نسبت به توپولوژی زاریسکی نیز یک زیرمجموعهٔ چگال است. به‌این‌ترتیب، استدلالی کاملاً جبری فراهم می‌شود. ■

صورت متعارف خم بیضوی

معمولاً خمهای بیضوی را به شکل $Y^2Z = X^3 + aXZ^2 + bZ^3$ در نظر می‌گیرند. درواقع می‌توان ثابت کرد که وقتی مشخصهٔ هیأت k مخالف ۲ و ۳ است (که ما نیز چنین فرض کرده‌ایم)، می‌توان در دستگاه مختصات مناسبی، معادلهٔ هر خم بیضوی را به‌صورت اخیر تبدیل کرد (برای مطالعهٔ یک برهان نابدیهی، [۵، ص ۳۱۹] را ببینید). خم تصویری فوق اجتماع خم آفین $y^2 = x^3 + ax + b$ با یک نقطهٔ ∞ به‌صورت $(0,1,0)$ است. صورت اخیر را صورت متعارف یا صورت وایرشتراس خم گویند.

اگر از ابتدا خم $y^2 = x^3 + ax + b = f(x)$ را همراه با نقطهٔ ∞ در نظر بگیریم، این خم وقتی یک خم بیضوی است که $f(x)$ دارای ریشه‌های ساده (مثلاً در بستار جبری k) باشد. زیرا برای $F(x,y) = y^2 - f(x)$، دو مشتق جزئی $\frac{\partial F}{\partial x} = f'(x)$ و $\frac{\partial F}{\partial y} = 2y$ وقتی و فقط وقتی در نقطهٔ (x_0, y_0) صفرند که $y_0 = 0$ و x_0 یک ریشهٔ چندگانه $f(x)$ باشد (مشخصهٔ هیأت k مخالف ۲ و ۳ است).

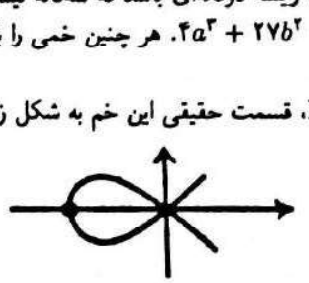
فرض کنیم $f(x)$ دارای ریشهٔ سه‌گانه باشد. باز طبق فرض ما در مورد مشخصهٔ هیأت k، فقط $x = 0$ می‌تواند ریشهٔ سه‌گانهٔ $f(x)$ باشد و در این صورت معادلهٔ خم به شکل $y^2 = x^3$ خواهد بود که آن را خم درجهٔ سوم *تیزه‌ای* گوییم. هرگاه $k \subset \mathbf{R}$، قسمت حقیقی این خم به شکل زیر خواهد بود.



شکل ۴

هرگاه f دارای ریشهٔ دوگانه‌ای باشد که سه‌گانه نیست، در این صورت $a, b \neq 0$ و $4a^3 + 27b^2 = 0$. هر چنین خمی را یک خم درجهٔ سوم گرهی می‌نامیم.

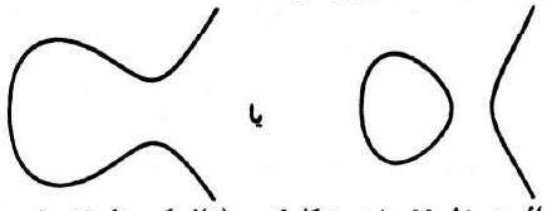
مجدداً اگر $k \subset \mathbf{R}$، قسمت حقیقی این خم به شکل زیر خواهد بود.



شکل ۵

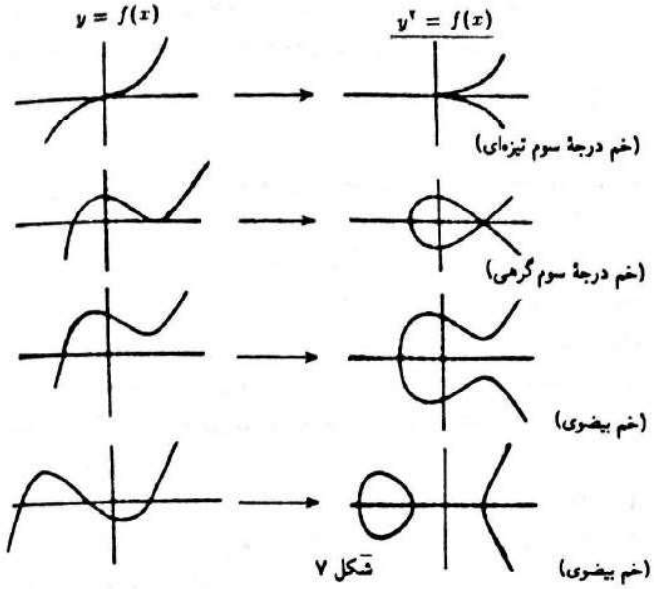
هیچ‌یک از خمهای فوق خم بیضوی نیست چون خم بیضوی ناتکین فرض می‌شود. درواقع روی این دو خم قانون گروهی (پیوسته) وجود ندارد. زیرا به‌طور مجرد، عمل جمع و قرینه‌یابی باید نگاشتهایی پیوسته باشند (نسبت به توپولوژی زاریسکی) و پیوستگی آنها ایجاب می‌کند که خم ناتکین باشد ([۱۲، صص ۴۱۳ به بعد]).

در حالتی که $f(x)$ دارای ریشه‌های ساده باشد، وقتی $k \subset \mathbf{R}$، برحسب آنکه f دارای سه ریشهٔ حقیقی و یا یک ریشهٔ حقیقی باشد، قسمت حقیقی خم $y^2 = f(x)$، اشکال زیر را خواهد داشت:



شکل ۶

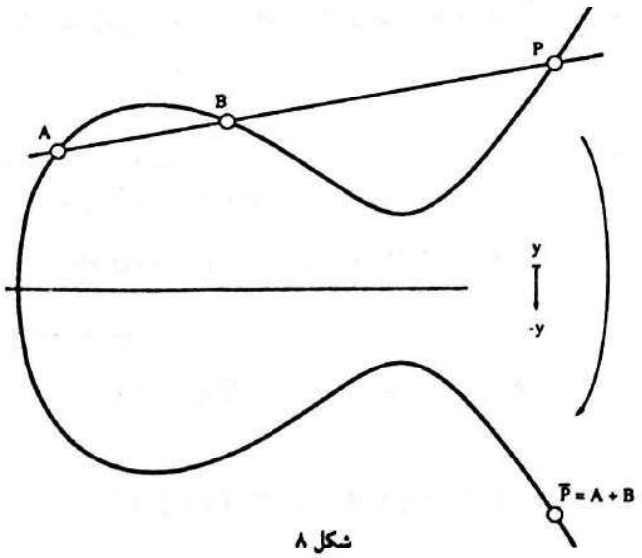
قسمت حقیقی این خمها در چهار حالت بالا را می‌توان با گرفتن «جذر» روی نمودار $y = f(x)$ به‌دست آورد:



شکل ۷

ساختار گروهی ساده‌شدهٔ خم بیضوی

خم بیضوی به‌صورت متعارف $y^2 = x^3 + ax + b$ دارای شکل همگن $Y^2Z = X^3 + aXZ^2 + bZ^3$ است و تنها نقطهٔ آن روی خط بینهایت، نقطهٔ $O = (0:1:0)$ است که امتداد محور yها تلقی می‌شود. خط بینهایت $Z = 0$، در نقطهٔ O با خم بیضوی تماس سه‌گانه دارد. خط تصویری $AX + BY + CZ = 0$ از نقطهٔ O می‌گذرد اگر و تنها اگر $B = 0$. قطعهٔ آفین خط $AX + CZ = 0$ به‌صورت $x = \lambda$ خواهد بود، که خم بیضوی را در دو نقطهٔ $(\lambda, \pm\sqrt{\lambda^3 + a\lambda + b})$ قطع می‌کند. و لذا عمل وتر-مماس به‌صورت سادهٔ «قرینه‌یابی نقطهٔ سوم نسبت به محور xها» درمی‌آید.



شکل ۸

ساختار گروهی خمهای درجهٔ سوم تکین

در هر یک از حالات خم درجهٔ سوم تیزه‌ای و یا خم درجهٔ سوم گرهی، اگر نقطهٔ تکین را کنار بگذاریم روی بقیهٔ نقاط یک ساختار گروهی ساده وجود

دارد که به‌ترتیب از ساختار جمعی و ضربی k نتیجه می‌شود. اگر ساختار وتر-مماس را روی خم $E: y^2 = x^3$ بررسی کنیم، خطوط گذرنده از مبدأ، خم را فقط در یک نقطهٔ دیگر قطع می‌کنند. در حالی که هر خط که دو نقطهٔ غیر از مبدأ را به هم وصل کند، خم را در نقطهٔ سومی قطع می‌کند. لذا $E - \{(0,0)\}$ با قانون وتر-مماس یک گروه آبلی است. لیکن این ساختار، ساختار جدیدی نیست و نگاشت $k \to E - \{(0,0)\}$ که توسط $t \to \left(\frac{1}{t^2}, \frac{1}{t^3}\right)$ تعریف می‌شود یک یکریختی گروههاست (این مطلب را ثابت کنید. توجه کنید که $\infty \mapsto 0$).

در حالت خم گرهی، با تعویض متغیر $x = X' + \sqrt{\frac{-a}{3}}$، معادله خم به صورت $y^2 = X'^3 + aX'$ درمی‌آید که گره آن در مبدأست. معادلهٔ اخیر نیز با تعویض متغیر $X' = \alpha X$ و $Y = \alpha^3 y$ به شکل $E: Y^2 = X^3 + X^2$ درمی‌آید. لذا کافی است قانون گروهی را روی این خم (با برداشتن نقطهٔ $(0,0)$) بررسی کنیم. نگاشت

$$E - \{(0,0)\} \to k^*$$
$$(X,Y) \longmapsto (Y+X)/(Y-X)$$

درسویی است و اگر قانون وتر-مماس را روی $E - \{(0,0)\}$ در نظر بگیریم این نگاشت تبدیل به یکریختی خواهد شد (ثابت کنید!!).

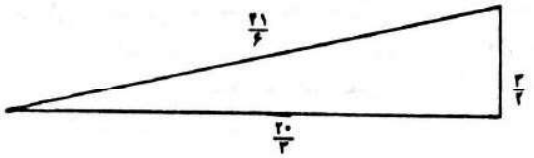
توضیح این نکته مفید است که خم درجهٔ سوم $y = x^3 + ax + b$ نیز به یکی از حالات بالا قابل تبدیل است. زیرا شکل تصویری آن $Z^2Y = X^3 + aXZ^2 + bZ^3$ است که برای $Y = 1$ صورت متعارف خم حاصل به یکی از اشکال بالا خواهد بود. مثلاً خم درجهٔ سوم $y = x^3$ در ∞ تکینگی دارد. به عبارت دیگر، صورت تصویری آن $YZ^2 = X^3$ است که با تغییرنام محورها همان خم درجهٔ سوم تیزه‌ای خواهد بود و لذا قانون گروهی $y = x^3$ (با برداشتن نقطهٔ ∞) نیز قانون جمعی k است.

بنابراین در حالات اخیر، قانون گروهی جدیدی حاصل نمی‌شود. قانون گروهی خم بیضوی، در حالت کلی، با قانون جمعی k و یا با قانون ضربی k^* یکی نیست. مثلاً خم بیضوی $y^2 = x^3 - x$ دارای سه عنصر مرتبهٔ سه است و زیرگروهی یکریخت با $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ دارد، درحالی‌که درگروه جمعی k، معادلهٔ $2x = 0$ دقیقاً یک جواب دارد (مشخصهٔ هیأت مخالف ۲ است) و درگروه ضربی k^* معادلهٔ $x^2 = 1$ حداکثر دو جواب دارد.

اعداد متوافق و مسائل دیوفانتوسی

یکی از مسائل قدیمی در نظریهٔ اعداد، مسألهٔ اعداد متوافق (congruent numbers) است. عدد مثبت و گویای r را یک عدد *متوافق* گوییم هرگاه r مساحت یک مثلث قائم‌الزاویه با اضلاع گویا باشد. به‌ازای هر عدد گویای مثبت r، عدد گویایی مانند s وجود دارد به‌طوری که $s^2 r$ یک عدد صحیح خالی از مجذور است. اگر r عددی متوافق و $X, Y, Z \in Q$ اضلاع مثلث قائم‌الزاویه‌ای با مساحت r باشند، آنگاه مساحت مثلث قائم‌الزاویه به اضلاع sX, sY و sZ برابر $s^2 r$ است. به‌عکس، اگر عدد طبیعی n خالی از مجذور فرض شود، هرگاه n متوافق باشد به‌ازای هر عدد گویای t، عدد $t^2 n$ متوافق است. بنابراین بدون کاستن از کلیت، می‌توان متوافق بودن را فقط در مورد اعداد طبیعی خالی از مجذور بررسی کرد. به زبان نظریهٔ گروهها، هرگاه $\mathbb{Q}^+$ گروه ضربی اعداد گویای مثبت باشد درگروه خارج‌قسمت $\mathbb{Q}^+/(\mathbb{Q}^+)^2$ هر ردهٔ هم‌ارزی دقیقاً یک نماینده به شکل عدد طبیعی خالی از مجذور دارد و متوافق بودن عدد گویای مثبت r خاصیتی است که تنها به ردهٔ هم‌ارزی r در این گروه خارج‌قسمت بستگی دارد. بنابراین مسأله را در مورد اعداد طبیعی خالی از مجذور بررسی می‌کنیم.

توجه کنید که در هر حال، اضلاع مثلث کافی است اعدادی گویا باشند و ممکن است اعداد صحیح نباشند. عدد $n = 6$ کوچکترین عدد طبیعی متوافق است و اضلاع مثلث قائم‌الزاویهٔ به مساحت ۶ اعدادی صحیح‌اند. در عین حال عدد $n = 5$ نیز عددی متوافق است و اضلاع مثلث قائم‌الزاویهٔ با مساحت ۵، برابر $\frac{3}{2}$ و $\frac{20}{3}$ و $\frac{41}{6}$اند. ثابت می‌شود که ۵ کوچکترین عدد طبیعی خالی از مجذور متوافق است.



شکل ۹

می‌دانیم که الگوریتمی وجود دارد که کلیهٔ سه‌تاییهای فیثاغورسی یعنی سه‌تاییهای (X,Y,Z) از اعداد طبیعی با ضابطهٔ $X^2 + Y^2 = Z^2$، را به‌دست می‌دهد. لذا می‌توانیم با محاسبهٔ مساحت مثلث قائم‌الزاویه برای هر سه‌تایی فیثاغورسی، اعداد متوافق را بنویسیم. مشکل بزرگ این روش این است که سه‌تاییهای فیثاغورسی با ترتیب معینی (مثلاً ترتیب معمولی اعداد) ظاهر نمی‌شوند و نمی‌توان گفت چقدر باید صبر کرد تا یک سه‌تایی فیثاغورسی با مساحت n داده شده، ظهور کند. و اگر تا مرحله‌ای، یک سه‌تایی فیثاغورسی با مساحت n ظاهر نشد، معلوم نیست که آیا این عدد متوافق نیست و یا به‌اندازه کافی منتظر نمانده‌ایم.

مسألهٔ پیداکردن اعداد طبیعی متوافق از دیرباز توجه ریاضیدانان را به خود جلب کرده و کارهای متعددی در این زمینه انجام شده است. حتی این مسأله برای یونانیان باستان و نیز در دورهٔ تمدن اسلامی مطرح و مورد بحث بوده است. لیکن اولین‌بار ریاضیدانان مسلمان این مسأله را به‌طور سیستماتیک بررسی کردند. آنها مسأله را به‌صورت دیگری مطرح کردند که چنین است: به‌ازای n داده‌شده، آیا عدد گویای x وجود دارد به‌طوری که $x^2 + n$ و $x^2 - n$ هر دو مجذور اعدادی گویا باشند؟ درواقع به‌آسانی می‌توان ثابت کرد که عدد n متوافق است اگر و تنها اگر به‌ازای n، عدد گویای x با شرایط بالا وجود داشته باشد، زیرا اگر برای عدد طبیعی خالی از مجذور n، اعداد گویای $X < Y < Z$ اضلاع مثلثی قائم‌الزاویه با مساحت n باشند، یعنی n متوافق باشد، به‌ازای عدد گویای $x = \frac{Z}{2}$ اعداد $x^2 + n = \left(\frac{X+Y}{2}\right)^2$ و $x^2 - n = \left(\frac{X-Y}{2}\right)^2$ مجذور اعدادی گویا هستند. به‌عکس، اگر $x^2 + n$ و $x^2 - n$ مجذور اعدادی گویا باشند، اعداد گویای $X = \sqrt{x^2+n} - \sqrt{x^2-n}$ و $Y = \sqrt{x^2+n} + \sqrt{x^2-n}$ و $Z = 2x$ اضلاع مثلثی قائم‌الزاویه با مساحت n هستند.

(در مورد تاریخچه جالب این مسائل، می‌توانید [۱ فصل XVI] و [۴، بخش ۲۷] را مطالعه کنید).

با این حال، اولین آثار مدون در این زمینه منسوب به اویلر و فرماست؛ اویلر برای اولین‌بار ثابت کرد عدد ۷ متوافق است و فرمانشان داد عدد ۱ متوافق نیست، که مطلب اخیر با این حکم که معادلهٔ $X^4 + Y^4 = Z^2$ جواب صحیح نابدیهی ندارد، هم‌ارز است و فرما برای اثبات آن از روش معروف خود (غیرممکن بودن نزول نامتناهی اعداد طبیعی) استفاده کرد.

بالاخره معلوم شد که اعداد ۱، ۲، ۳ و ۴ متوافق نیستند و ۵ و ۶ و ۷ متوافق‌اند. ولی پیداکردن شرایط مناسبی که بتوان توسط آنها معین کرد که آیا عدد طبیعی داده‌شده‌ای متوافق است یا نه، همچنان در پردهٔ ابهام بود. برای

آنکه به پیچیدگی مطلب پی برده شود، آوردن مثال زیر بی‌مناسبت نیست: عدد ۱۵۷ عددی متوافق است و ساده‌ترین اعداد گویا که مثلثی قائم‌الزاویه با مساحت ۱۵۷ می‌سازند در شکل‌مقابل‌مشخص شده‌اند (این اعداد را تساگیر (Zagier) محاسبه کرده است).

در قرن بیستم، تانل، با استفاده از حساب خمهای بیضوی، قضیهٔ معروف خود را که در حد رضایت‌بخشی به مسألهٔ اعداد متوافق پاسخ می‌دهد، ارائه کرد. در اینجا فقط به ذکر صورت قسمتی از این قضیه که در این مقوله مناسب است، اکتفا می‌کنیم.

قضیهٔ تانل. فرض کنید n یک عدد طبیعی خالی از مجذور است: اگر n متوافق باشد آنگاه تعداد سه‌تاییهای صحیح که در تساوی $2x^2+y^2+8z^2=n$ صدق می‌کنند برابر است با دوبرابر تعداد سه‌تاییهایی که در تساوی $2x^2+y^2+32z^2=n$ صدق می‌کنند.

حال به بیان ارتباط اعداد متوافق با خمهای بیضوی می‌پردازیم.

لم. اگر عدد (طبیعی و خالی از مجذور) n متوافق باشد آنگاه روی خم بیضوی $y^2=x^3-n^2x$ نقطه‌ای با مختصات گویا (غیرصفر) وجود دارد.

برهان. طبق فرض داریم $((X\pm Y)/2)^2=\left(\frac{Z}{2}\right)^2\pm n$، که X و Y و Z اضلاع مثلث قائم‌الزاویه‌ای با مساحت n است. با ضرب طرفین دو تساوی بالا در همدیگر، داریم $\left(\frac{X^2-Y^2}{4}\right)^2=\left(\frac{Z}{2}\right)^4-n^2$. با فرض $u=\frac{Z}{2}$، $v=(X^2-Y^2)/4$، خواهیم داشت $u^4-n^2=v^2$، که این تساوی با ضرب طرفین در u^2 به شکل $(uv)^2=u^6-n^2u^2$ درمی‌آید، یعنی نقطهٔ $(x,y)=(u^2,uv)$ با مختصات گویا در معادلهٔ $y^2=x^3-n^2x$ صدق می‌کند.

لیکن آیا می‌توان گفت که اگر روی خم بیضوی $y^2=x^3-n^2x$ نقطه‌ای با مختصات گویای غیرصفر وجود داشته باشد، n عددی متوافق است؟ جواب منفی است. به‌عنوان مثال نقطهٔ گویای $((41/7)^2, 29520/7^3)$ روی خم بیضوی $y^2=x^3-(31)^2x$ واقع است، لیکن ۳۱ عددی متوافق نیست. درواقع، x حاصل از لم بالا مشخصات ویژه‌ای دارد: اول اینکه x مجذور یک عدد گویاست و دوم اینکه مخرج عدد گویای x زوج است، زیرا عدد صحیحی مانند s وجود دارد به‌طوری که sX و sY و sZ اعدادی طبیعی و نسبت به هم اول بوده و اضلاع مثلث قائم‌الزاویه‌ای با مساحت s^2n باشند، لیکن طبق خاصیت سه‌تاییهای صحیح فیثاغورسی که نسبت به هم اول‌اند، sZ عدد فردی است و لذا $x=(Z/2)^2=(sZ/2s)^2$. درواقع دو شرط بالا برای متوافق بودن n، کافی نیز هستند. لذا قضیهٔ زیر را که اثبات آن چندان مشکل نیست، بدون برهان، ذکر می‌کنیم. خوانندهٔ علاقه‌مند می‌تواند برهان قضیه را در [۸ ص ۷، قضیهٔ ۲] مطالعه کند.

قضیه. فرض کنید روی خم بیضوی $y^2=x^3-n^2x$ نقطه‌ای با مختصات گویای (α,β) وجود دارد به‌طوری که α مجذور عددی گویا با مخرج زوج است در این صورت n عددی متوافق است.

$$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$$

$$\frac{6803298487826435051217540}{411340519227716149383203}$$

شکل ۱۰

$$\frac{411340519227716149383203}{21666555693714761309610}$$

پس قضیهٔ اخیر همراه با لم قبلی یک شرط لازم وکافی برای متوافق بودن n برحسب وجود نقطه‌ای گویا به شرح بالا به‌دست می‌دهد.

توضیح. شرط مذکور در لم بالا، با توجه به قانون گروهی روی خم بیضوی، با این شرط معادل است که نقطهٔ گویای $P=(\alpha,\beta)$ روی خم بیضوی $y^2=x^3-n^2x$ بر دو بخشپذیر باشد یعنی نقطهٔ گویای دیگری مانند P' روی این خم بیضوی وجود داشته باشد به‌طوری که $2P'=P'+P'=P$ به عبارت دقیقتر قضیهٔ زیر را داریم.

قضیه. اعداد گویای n، $n-\alpha$ و $n+\alpha$ مجذور اعدادی گویا هستند اگر و تنها اگر نقطه‌ای با مختصات گویا چون $P=(\alpha,\beta)$، روی خم بیضوی $y^2=x^3-n^2x$ موجود باشد و P با قانون جمع خم بیضوی بر دو بخشپذیر باشد.

برهان این قضیه نیز بر اساس محاسبات معمولی وتر-مماس روی خم بیضوی و هندسهٔ تحلیلی است، که خوانندهٔ علاقه‌مند را به مطالعهٔ برهان این قضیه در [۷، ص ۳۷، قضیهٔ ۱.۴] دعوت می‌کنیم.

قضیهٔ موردل

برای خم بیضوی $F(x,y)=0$، که $F(x,y)$ یک چندجمله‌ای است که ضرایبش در k هستند، گروه نقاط خم را با $E(k)$ نمایش می‌دهیم. در حالت خاص، وقتی هیأت L یک توسیع k باشد، $E(k)$ یک زیرگروه $E(L)$ خواهد بود. در نظریهٔ اعداد، $k=\mathbf{Q}$ یا k یک هیأت عددی یعنی، یک توسیع متناهی $\mathbf{Q}$، فرض می‌شود. یکی از مهمترین مسائل در این زمینه، بررسی $E(\mathbf{Q})$ برای یک خم بیضوی با ضرایب گویاست. می‌دانیم این گروه آبلی است. سؤال این است که این گروه در طبقه‌بندی گروههای آبلی در کجا قرار می‌گیرد.

اولین قضیهٔ اساسی در این مورد، قضیهٔ موردل است.

قضیه (موردل، ۱۹۲۱). روی هر خم بیضوی با ضرایب گویا، گروه نقاط با مختصات گویا، مولد متناهی دارد.

معنی قضیهٔ موردل به بیان ساده این است که روی هر خم بیضوی با ضرایب گویا، تعدادی متناهی نقطهٔ گویا وجود دارد که بقیهٔ نقاط گویا را می‌توان با قانون وتر-مماس از این نقاط به‌دست آورد.

برهان این قضیه به مقدماتی نیاز دارد که در این مقاله به آنها دسترسی نداریم. به‌هرحال این قضیه یکی از نتایج جالب‌توجه و عمیق در نظریهٔ اعداد و خمهای بیضوی است.

در سال ۱۹۲۸ آندره‌وِیل ثابت کرد که قضیهٔ موردل برای هر هیأت

عددی، نه فقط $\mathbf{Q}$، برقرار است. طبق قضیهٔ موردل و با استفاده از قضیهٔ اساسی گروههای آبلی با مولد متناهی، برای هر خم بیضوی با ضرایب گویا، گروه $E(\mathbf{Q})$ به شکل زیر خواهد بود:

$$E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus E_t(Q)$$

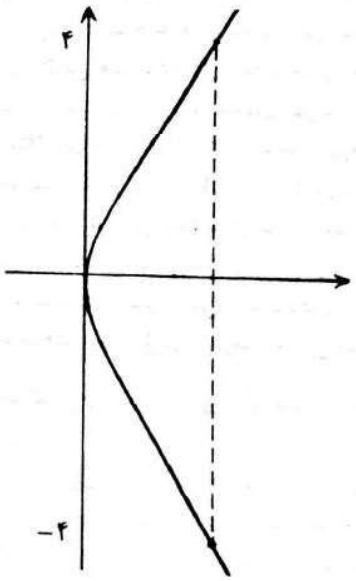
که r عددی طبیعی است و رتبهٔ $E(\mathbf{Q})$ خوانده می‌شود، و $E_t(Q)$ یک گروه متناهی متشکل از همهٔ عناصر $E(\mathbf{Q})$ با مرتبهٔ متناهی است.

در اینجا به ذکر دو مثال از محاسبهٔ $E(\mathbf{Q})$ می‌پردازیم.

مثال ۱. برای خم بیضوی $y^2 = x^3 + 4x$، $E(\mathbf{Q})$ را محاسبه می‌کنیم. نقطهٔ گویای $(2, 4)$ روی این خم واقع است. این نقطه یک عضو مرتبهٔ ۴ از گروه $E(\mathbf{Q})$ است زیرا با روش وتر-مماس داریم (عضو خنثی، نقطهٔ ∞ است):

$$2(2,4) = (0,0)$$
$$3(2,4) = (0,0) + (2,4) = (2,-4)$$
$$4(2,4) = 2(0,0) = \infty$$

یعنی $E(\mathbf{Q})$ شامل یک زیرگروه یکریخت $\mathbf{Z}/4\mathbf{Z}^2$ است. ادّعا می‌کنیم این زیرگروه برابر کل گروه است:



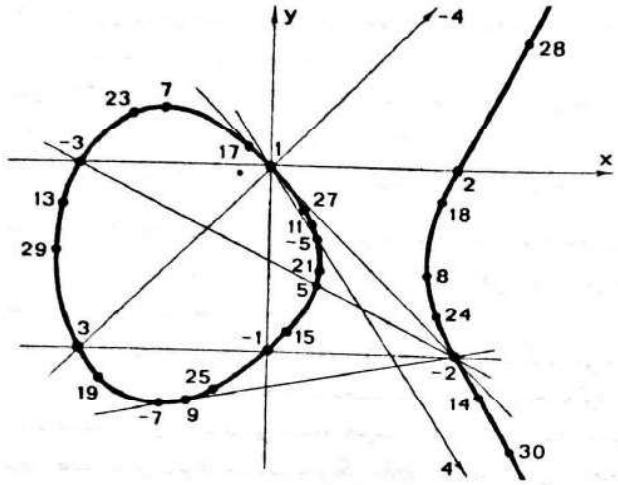
شکل ۱۱

با تعویض متغیر $x = 2(w+v)/(w-v)$ و $y = 4u^2/(w-v)^2$، معادلهٔ بالا به شکل زیر درمی‌آید:

$$w^2 = u^4 + v^4$$

که همان معادلهٔ آشنای فرما برای حالت $n = 4$ است. می‌دانیم تنها جوابهای صحیح این معادله (طبق استدلال خود فرما!) عبارت‌اند از $(0,0,0)$، $(1,0,1)$، $(1,-1,0)$ و $(0,1,1)$، که این جوابها دقیقاً متناظر با چهار نقطهٔ گویای بالا روی خم بیضوی هستند و اگر روی خم بیضوی نقطهٔ گویای دیگری هم بود، این نقطه با جواب صحیح دیگری در $w^2 = u^4 + v^4$ نظیر می‌شد، که چنین نیست. پس $E(Q) \cong \mathbf{Z}/4\mathbf{Z}$.

مثال ۲. برای خم بیضوی $y^2 + y = x^3 - x$، گروه نقاط گویا یک گروه دوری نامتناهی است یعنی $E(Q) \cong \mathbf{Z}$. کلیهٔ نقاط گویای این خم توسط نقطهٔ $(0,0)$ با عمل گروه تولید می‌شوند (عضو خنثی نقطهٔ ∞ است). برای اثبات می‌توانید به [۱۵] مراجعه کنید.



شکل ۱۲

این مطلب را که برای یک خم بیضوی، گروه $E(Q)$ تا چه حد می‌تواند بزرگ باشد، عده‌ای از ریاضیدانان مطالعه کرده‌اند. در سال ۱۹۷۶، میزر (Mazur) قضیهٔ عمیق زیر را که قبلاً آگ (Ogg) آن را حدس زده بود، به اثبات رسانید:

قضیهٔ (میزر). برای هر خم بیضوی E روی $\mathbf{Q}$، گروه $E_t(Q)$ یعنی گروه نقاط با مرتبهٔ متناهی، به یکی از اشکال زیر است:

$$\mathbf{Z}/m\mathbf{Z} \quad , m = 1, 2, 3, \cdots, 10, 12$$

یا

$$\mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \quad , m = 2, 4, 6, 8$$

بالاخص هیچ نقطه‌ای روی $E(\mathbf{Q})$ با مرتبهٔ ۱۱، ۱۳ یا ۱۴ وجود ندارد. در عین حال برای همه حالتهای بالا مثالهایی وجود دارند.

در حالی که در مورد $E_t(Q)$، قضیهٔ بالا (و حتی قضایای دقیقتری که اخیراً ثابت شده‌اند) وجود دارند، اطلاع ریاضیدانان از r یعنی رتبه، خیلی محدودتر است. مثالهایی از خمهای بیضوی حداکثر با رتبهٔ ۱۲ پیدا شده‌اند، ولی آیا برای r یک کران بالا وجود دارد، یعنی آیا عددی وجود دارد که برای همهٔ خمهای بیضوی، رتبهٔ گروه مربوطه از آن عدد کمتر باشد؟ علی‌رغم اینکه خمی بیضوی با رتبهٔ بیش از ۱۲ پیدا شده است، از نظر ریاضیدانان، وجود یک کران بالا برای r غیرمحتمل است. حتی محاسبهٔ r در مثالهای خاص نیز مشکل است. بنابراین در حالت کلی کار با این ناوردای مرموز، بسیار پیچیده است و تحقیقات ریاضیدانان در این زمینه ادامه دارد.

برای اینکه به اهمیت رتبه پی ببریم، ذکر قضیهٔ زیر مناسب است. برهان این قضیه را می‌توان از قضیهٔ میزر و بحثهایی بر دو روی $E(\mathbf{Q})$ نتیجه گرفت. برای مطالعهٔ برهانی دیگر به [۸، ص ۴۶، قضیهٔ ۱۸] مراجعه کنید.

قضیه. عدد طبیعی n یک عدد متوافق است اگر و تنها اگر رتبهٔ $E(\mathbf{Q})$ برای خم بیضوی $y^2 = x^3 - n^2x$ غیرصفر باشد، یعنی $E(\mathbf{Q})$ یک گروه نامتناهی باشد.

می‌دانیم معادلهٔ هر خم بیضوی E روی $\mathbf{Q}$ را می‌توان به‌صورت متعارف $y^2 = x^3 + ax + b$ نوشت. هیچ روش ثمربخشی برای تعیین رتبهٔ $E(\mathbf{Q})$ برحسب a و b وجود ندارد. درواقع هیچ روشی وجود ندارد که بتوان برحسب a و b قضاوت کرد که $E(\mathbf{Q})$ متناهی یا نامتناهی است (یعنی $r = 0$ یا $r > 0$). بررسی این مطالب از مسائل اصلی هندسهٔ دیوفانتوسی است.

حال که از قضیهٔ موردل صحبت شد، بجاست حدس موردل را که در سال ۱۹۸۳ توسط فالتینگز (Faltings) ثابت شد و در اثبات آن قضایای متعددی از ریاضیدانان مختلف بکارگرفته شده است، بیان کنیم. ضمناً این قضیه بیانگر غنای نظریهٔ خمهای بیضوی در ارتباط با نقاط گویاست.

قضیهٔ موردل-فالتینگز. اگر E یک خم تصویری ناتکین با درجهٔ بیش از سه و با ضرایب گویا باشد، تعداد نقاط گویای E متناهی است. (باز هم قضیه برای هر هیأت عددی، نه فقط $\mathbf{Q}$، برقرار است).

توضیح. در ارتباط با نقاط گویا روی یک خم با ضرایب گویا، می‌توان در مورد نقاط صحیح (یعنی نقاط با مختصات صحیح) نیز بحث کرد. با اثبات قضیهٔ موردل-فالتینگز این مسأله اهمیت خود را از دست داده است، لیکن قضیهٔ تناهی زیر که منسوب به زیگل (Siegel) است، هنوز از لحاظ تاریخی اهمیت دارد.

قضیه. تعداد نقاط صحیح یک خم ناتکین تصویری با ضرایب گویا که درجهٔ آن حداقل سه است، متناهی است.

البته اگر خم ناتکین نباشد، قضیه صادق نیست. مثلاً خم درجه سهٔ $y^2 = x^3$ بینهایت نقطهٔ صحیح به شکل (n^2, n^3) دارد.

خمهای بیضوی از دیدگاه هندسهٔ جبری مجرد

استفاده از نظریهٔ «بخشیابها» روش غنی دیگری برای مطالعهٔ خمهای بیضوی است. یک بخشیاب روی خم ناتکین تصویری E عبارت است از یک مجموع صوری $\sum n_iP_i$ که $P_i \in E$ و $n_i \in \mathbf{Z}$ و تنها تعدادی متناهی از n_iها می‌توانند غیرصفر باشند. مجموعهٔ بخشیابها روی E تشکیل یک گروه می‌دهند که همان گروه آبلی آزاد روی نقاط E است و آن را گروه بخشیابهای E گوییم و با $\mathrm{Div}(E)$ نمایش می‌دهیم. برای هر بخشیاب $D = \Sigma n_iP_i$، عدد صحیح $\deg D = \Sigma n_i$ را درجهٔ بخشیاب گویند. اگر $f = \frac{F(X,Y,Z)}{G(X,Y,Z)}$ یک تابع گویا روی E باشد یعنی، F و G دو چندجمله‌ای همگن و همدرجه بوده و G روی E متحد با صفر نباشد، می‌توان F و G را نسبت به هم اول فرض کرد. F و G هرکدام روی تعدادی متناهی از نقاط E صفر می‌شوند (قضیهٔ بزو!) به هر ریشهٔ F یا G چندگانگی آن را منسوب می‌کنیم. اگر $P_1, \ldots, P_r$ ریشه‌های F روی E با چندگانگیهای $n_1, \ldots, n_r$ و $Q_1, \ldots, Q_s$ ریشه‌های G روی E با چندگانگیهای $m_1, \ldots, m_s$ باشند، آنگاه برای تابع گویای f، بخشیاب

$$D = \sum n_iP_i - \sum m_jQ_j$$

نظیر می‌شود که آن‌را یک بخشیاب *اصلی* گوییم. مجموعهٔ بخشیابهای اصلی تشکیل یک زیرگروه $\mathrm{Div}(E)$ را می‌دهند و خارج‌قسمت $\mathrm{Div}(E)$ بر گروه بخشیابهای اصلی راگروه رده‌ای بخشیابها گویند و با $\mathrm{Cl}(X)$ نمایش می‌دهند. $\mathrm{Cl}(X)$ نیز ناوردای مهمی برای خم E است. طبق یک قضیهٔ کلاسیک در هندسهٔ جبری، اگر D یک بخشیاب اصلی باشد، $\deg D = 0$ بنابراین همریختی $D \mapsto \deg D$، $\mathrm{Div}(E) \to \mathbf{Z}$، یک همریختی $\mathrm{Cl}(E) \to \mathbf{Z}$ القا می‌کند. هستهٔ این همریختی راگروه رده‌ای بخشیابهای درجهٔ صفر گویند و با $\mathrm{Cl}^0(E)$ نمایش می‌دهند. اصطلاحاً خمهایی را که قابل پارامتری‌شدن بوسیلهٔ تابعهای گویا از یک متغیر هستند خمهای گویا گوییم. بنابراین تعریف، خمهای درجهٔ دوم گویا هستند و خمهای بیضوی گویا نیستند (اگر برهان این مطلب را ندیده‌اید اثبات ساده‌ای از آن را در [۱۱، ص ۲۸] ببینید). ثابت می‌شود که یک خم گویاست اگر و تنها اگر $\mathrm{Cl}^0(E) = 0$. پس اگر E یک خم بیضوی باشد، $\mathrm{Cl}^0(E) \neq 0$. نکتهٔ جالب این است که برای خم بیضوی E، $\mathrm{Cl}^0(E)$ در تناظر دوسویی با نقاط E است؛ به‌عبارت دقیقتر، اگر نقطهٔ ثابت $P_0 \in C$ را در نظر بگیریم، نگاشت «ردهٔ بخشیاب $P - P_0$» $\mapsto P$ از E در $\mathrm{Cl}^0(E)$ یک نگاشت دوسویی است (ر. ک [۱۲، ص ۱۴۶] یا [۵، ص ۱۳۹]). این نگاشت دوسویی ساختارگروهی $\mathrm{Cl}^0(E)$ را روی خم E انتقال می‌دهد، که همان ساختارگروهی وترـمماس روی خم E است. توجه کنید که در این روش، استفاده از نتایجی از نظریهٔ بخشیابها، ما را از اثبات پیچیدهٔ شرکتپذیری قانون جمع روی E بی‌نیاز می‌کند. البته اهمیت این روش بیشتر در این است که ساختارگروهی خم E را با ساختار مجرد جبری $\mathrm{Cl}^0(E)$ مربوط می‌سازد و روش طبیعی برای تعمیم ساختارگروهی روی چندگوناهای با بعد بیشتر و تعریف گروههای جبری و چندگوناهای آبلی را روشن می‌سازد. ([۱۳، صص ۱۴۸ـ۱۵۵] یا [۱۰] را مطالعه کنید).

مطلب قابل توجه در مورد خمهای بیضوی این است که این خمها تنها خمهای تصویری ناتکین هستند که روی آنها ساختارگروهی (پیوسته) وجود دارد. این مطلب با ساختارگروهی روی خمهای غیربیضوی که قبلاً بیان شد، منافاتی ندارد. مثلاً روی خم آفین $y = x^3$ ساختارگروهی وجود دارد، ولی به‌عنوان یک خم تصویری به شکل $YZ^2 = X^3$ درمی‌آید که در نقطهٔ ∞ دارای تکینگی است. برهان این مطلب در مورد خمهای بیضوی از قضیهٔ معروف ریمان-رخ نتیجه می‌شود. قضیهٔ زیر و چارچوب برهان آن را برای نشان‌دادن ارتباط مفاهیم و به‌عنوان یکی ازکاربردهای قضیهٔ ریمان-رخ بیان می‌کنیم، هرچند مفاهیم مورد نیاز در این برهان، در این مقاله معرفی نشده‌اند.

قضیه. تنها خم تصویری ناتکین که روی آن قانون گروهی (پیوسته) وجود دارد خم بیضوی است.

برهان. اگر خم E دارای ساختارگروهی باشد ثابت می‌شود که بخشیاب متعارف آن k_E برابر صفر است. بنابراین طبق قضیهٔ ریمان-رخ داریم: $\deg k_E = 2g - 2 = 0$، که g گونهٔ خم E است. بنابراین $g = 1$. از طرفی گونهٔ این خمها از دستور $g = (d-1)(d-2)/2$ به‌دست می‌آید که d درجهٔ خم E است. از $g = 1$ نتیجه می‌شود، $d = 3$. ■

سخنی درباره خمهای بیضوی مختلط و کاربرد آنها

خمهای بیضوی از نظر هندسهٔ مختلط نیز قابل مطالعه‌اند. نکتهٔ اصلی در این مورد این است که وقتی یک خم بیضوی E را در صفحهٔ مختلط $\mathbf{C} \times \mathbf{C}$ در نظر می‌گیریم، این خم در فضای حقیقی $\mathbf{C}^2 \cong \mathbf{R}^4$ نمایش یک رویه خواهد بود که چیزی جز یک چنبره نیست. می‌دانیم گونای چنبره برابر یک است. اینکه هر خم ناتکین مختلط از نظر توپولوژیک تنها با ناوردای گونه به‌طور کامل مشخص می‌شود، اهمیت گونه را معلوم می‌سازد. نظریهٔ خمهای بیضوی مؤید این است که گونهٔ یک، تمایز عجیبی با گونهٔ بیش از

یک دارد. خوانندهٔ علاقه‌مند در این زمینه را به مطالعهٔ [۷، صص ۱۷ـ۲۰] و [۱۲، صص ۱۷۸ـ۱۸۰] و [۱۴] دعوت می‌کنیم.

نظریهٔ خمهای بیضوی علاوه بر ارتباط با شاخه‌های مختلف ریاضی، کاربردهای جالبی نیز دارد. برای مثال برای بررسی اینکه عدد صحیح مفروضی اول است یا نه، روشی مبتنی بر نظریهٔ خمهای بیضوی وجود دارد [۶]. اخیراً کاربردهای شگفت‌آوری از خمهای بیضوی در نظریهٔ طرحهای بلوکی و رمزنگاری نیز پیدا شده است [۱۰].

مراجع

1. L. E. Dickson, *History of the Theory of Numbers*, Chelsea (1952).
2. H. Edwards, *Fermat's Last Theorem*, Springer-Verlag (1977).
3. W. Fulton, *Algebraic Curves*, Benjumin/ Cummings (1978).
4. R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag (1981).
5. R. Hartshorne, *Algebraic Geometry*, Springer-Verlag (1977).
6. T. Horwitz, "Elliptic curves", *UMAP, The Journal of Undergraduate Math & its Appl.*, No. 2 (1987).

(این مقاله در جنگ *ریاضی دانشجو*، شمارهٔ مرداد ۶۸، جلد چهارم، به ترجمهٔ حسن حقیقی چاپ شده است.)

7. D. Husemöller, *Elliptic Curves*, Springer-Verlag (1987).
8. N. Koblits, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag (1984).
9. S. Lang, *Abelian Varieties*, Wiley-Interscience, NewYork (1959).
10. N. S. Mendelsohn, R. Padmanabhan, B. Wolk, "Designs embeddable in a planar cubic curve", *Note Mat.* , **7** (1987) 113-148.
11. M. Reid, *Undergraduate Algebraic Geometry*, L. M. S. Student texts **12**, Cambridge Univ. Press (1990).

(این کتاب به‌وسیلهٔ نویسندهٔ مقالهٔ حاضر ترجمه شده است و از طرف مرکز نشر دانشگاهی منتشر خواهد شد.)

12. I. Shafarevich, *Basic Algebraic Geometry*, Springer-Verlag (1977).
13. J. Silverman, The *Arithmetic of Elliptic Curves*, Springer-Verlag (1986).
14. J. T. Tate, "The arithmetic of elliptic curves," Inv. Math., **23** (1974) 179-206.

******

* رحیم زارع نهندی، دانشگاه تهران و مرکز فیزیک نظری و ریاضیات سازمان انرژی اتمی ایران.