فرهنگ و اندیشهٔ ریاضی
شماره ۴۵ (پاییز ۱۳۸۹) صص. ۶۱ تا ۷۳

مسألهٔ اعداد همنهشت و حدسیهٔ BSD دربارهٔ رتبه‌های خم‌های بیضوی

علی سرباز جانفدا ـ سجاد سلامی

چکیده

در این مقاله، مسألهٔ حل نشدهٔ تاریخی اعداد همنهشت مورد مطالعه قرار گرفته و ارتباط تنگاتنگ این مسأله با حدسیه BSD درباره رتبه‌های خم‌های بیضوی تعریف شده روی میدان اعداد گویا مطرح شده است. حدسیهٔ BSD یکی از مسائل یک میلیون دلاری بنیاد ریاضیات کلِی[1] است که توسط بیرچ و سوینرتون ـ دایر[2] در سال ۱۹۶۵ میلادی بیان شده است. با استفاده از قضیهٔ تانِل راه‌حلی برای مسألهٔ اعداد همنهشت بیان شده است که مشروط به درست بودن حدسیهٔ BSD است.

واژه‌های کلیدی: اعداد همنهشت، خم‌های بیضوی، حدسیهٔ BSD.
رده بندی موضوعی (MSC2000): 14G10، 14H52.

۱. مقدمه

در ریاضیات، به‌ویژه در نظریهٔ اعداد، مسائلی وجود دارند که خیلی طبیعی و ساده مطرح می‌شوند ولی یافتن جوابی برای آنها خیلی مشکل بوده و برای اثبات یا رد کردن آنها روش‌های خیلی پیچیده‌ای لازم است. یکی از این مسائل، مسألهٔ اعداد همنهشت، طرح و بیان خیلی ساده‌ای دارد با این حال، بیش از ده قرن است که ذهن خیلی از ریاضی‌دانان را به خود مشغول کرده است. در این مقاله، قصد داریم ارتباط این مسأله را با یکی از حدسیه‌های مهم و پرطرفدار در نظریهٔ اعداد بررسی کنیم. این کار را با استفاده از نظریهٔ خم‌های بیضوی انجام خواهیم داد. در واقع، همین نظریه بود که در اثبات قضیهٔ آخر فرما، توسط وایلز[3] نقش اساسی ایفا کرد. برای اطلاع از روند این اثبات خواننده را به [۲۲] ارجاع می‌دهیم.

1) Clay Mathematical Institute 2) Birch & Swinnerton-Dyer 3) Andrew Wiles

ساختار این مقاله به این صورت است که ابتدا، در بخش ۲، مسألهٔ اعداد همنهشت را به‌طور مختصر از جنبهٔ تاریخی مطرح و برخی از نتایج به‌دست آمده را ذکر می‌کنیم. برای مطالعهٔ بیشتر دربارهٔ تاریخچهٔ این مسأله می‌توانید به [۹] و [۱۷] مراجعه کنید. در بخش ۳، یک الگوریتم ساده برای به‌دست آوردن اعداد همنهشت بیان و معایب آن را بررسی می‌کنیم. در بخش ۴، مختصری از نظریهٔ خم‌های بیضوی را مطرح کرده و حدسیهٔ BSD را دربارهٔ رتبه‌های خم‌های بیضوی ارائه می‌کنیم. برای مطالعهٔ بیشتر دربارهٔ نظریهٔ خم‌های بیضوی و حدسیهٔ BSD می‌توانید مراجع [۳] و [۲۰] را مطالعه کنید. در بخش ۵، ضمن بیان ارتباط بین مسألهٔ اعداد همنهشت با حدسیهٔ BSD، برخی از نتایج مهم به‌دست آمده را ذکر می‌کنیم که قضیهٔ تانل [۲۴] مهم‌ترین آنها است. در دههٔ اخیر، با استفاده از نظریهٔ گراف‌ها برای محاسبهٔ گروه‌های سِلمر خم‌های بیضوی تعریف شده توسط رابطهٔ $y^2 = x^3 - n^2 x$، نتایج جالبی دربارهٔ مسألهٔ اعداد همنهشت به دست آمده است که به‌دلیل طولانی شدن مطلب از آوردن آنها در این مقاله خودداری کرده‌ایم. علاقه‌مندان می‌توانند برای مطالعهٔ بیشتر در این زمینه به [۱۰]، [۱۱] و [۱۲] رجوع کنند.

۲. تاریخچه‌ای مختصر از مسألهٔ اعداد همنهشت

در این بخش قصد داریم تاریخچهٔ مختصری از مسألهٔ اعداد همنهشت بیان کنیم که قدمتی بیش از ده قرن داشته و هنوز هم جذابیت خود را از دست نداده است و جزء مسائل جالب نظریهٔ اعداد به‌شمار می‌آید. کارمان را با تعریف عدد همنهشت آغاز می‌کنیم.

تعریف ۱.۲. عدد طبیعی n را یک عدد همنهشت[1] می‌گوییم هرگاه برابر با مساحت یک مثلث قائم‌الزاویه با اضلاع گویا باشد؛ یعنی اعداد گویای مثبت a، b و c موجود باشند که

$$a^2 + b^2 = c^2, \quad ab = 2n, \quad a < b < c. \tag{۳}$$

به‌عنوان مثال، ۶ عدد همنهشت است چون برابر با مساحت مثلثی قائم‌الزاویه با اضلاع $(3, 4, 5)$ می‌باشد.

تعریف ۲.۲. عدد طبیعی n را خالی از مربع[2] می‌گوییم هرگاه مربع هیچ عددی آن را عاد نکند. به‌طور مثال، ۵ و ۶ خالی از مربع هستند ولی $20 = 2^2.5$ خالی از مربع نیست.

مسأله ۳.۲. کدام یک از اعداد طبیعی n اعداد همنهشت هستند؟

مسألهٔ اعداد همنهشت از دیرباز مورد مطالعهٔ ریاضیدانان قرار گرفته ولی تاکنون به‌طور کامل حل نشده است. قضیهٔ زیر نشان می‌دهد که سابقهٔ مسألهٔ اعداد همنهشت حداقل به زمان دیوفانتوس برمی‌گردد [۵].

---

1) congruent number 2) square-free

قضیه ۴.۲. عدد طبیعی n یک عدد همنهشت است اگر و فقط اگر دستگاه معادلات چهار مجهولی

$$\begin{cases} x^2 + ny^2 = z^2 \\ x^2 - ny^2 = t^2 \end{cases}$$

دارای جواب غیر بدیهی باشد؛ یعنی جوابی با $y > 0$ وجود داشته باشد.

در قرن سیزدهم میلادی، فیبوناتچی در یکی از کتاب‌های خود، بدون ارائهٔ هیچ اثباتی، ادعا کرده بود که عدد ۱ عددی همنهشت نیست. در اوایل قرن شانزدهم میلادی فرما با استفاده از روش نزول نامتناهی[1] این ادعا را ثابت کرد. وی همچنین نشان داد که ۲ و ۳ نیز اعداد همنهشت نیستند [۹]. در سال ۱۲۲۰ میلادی فیبوناتچی نشان داد که عدد ۵ یک عدد همنهشت است. درستی این مطلب را می‌توان با به‌کار بردن قضیهٔ ۴.۲ برای $n = 5$ و با توجه به تساوی‌های زیر نتیجه گرفت:

$$41^2 + 5 \cdot 12^2 = 49^2, \quad 41^2 - 5 \cdot 12^2 = 31^2.$$

چون آن زمان عدد همنهشت به‌مفهوم امروزی جا افتاده نبود، وی مسألهٔ یافتن مجذور کاملی را مطرح کرد که اگر ۵ بدان اضافه یا از آن کاسته شود، عدد حاصل مجذور کامل $(\frac{41}{12})^2$ را بدهد. تقسیم روابط بالا بر 12^2 نشان می‌دهد که این مسأله با همنهشت بودن عدد ۵ معادل است [۹]. بدین ترتیب، ۵ کوچک‌ترین عدد همنهشت است.

بعضی از ریاضی‌دان‌های دورهٔ اسلامی هم از دیرباز به مسألهٔ اعداد همنهشت پرداخته‌اند چنان‌که دیکسون در فصل ۱۶ از [۹] می‌نویسد: «در یک نسخهٔ خطی که پیش از سال ۹۷۲ میلادی به زبان عربی و با عنوان موضوع اساسی مثلث‌های قائم‌الزاویه‌ی گویا، نوشته شده و در کتابخانهٔ ملی پاریس موجود ولی نویسندهٔ آن نامعلوم است، مسألهٔ اعداد همنهشت مطرح و در آن ۳۰ عدد خالی از مربع زیر آمده‌اند که در واقع از لحاظ تاریخی اولین فهرست از اعداد همنهشت به شمار می‌آید:

$$5, 6, 14, 15, 21, 30, 34, 65, 70, 110, 154, 190, 210, 221, 231, 286, 330, 390,$$
$$429, 546, 1155, 1254, 1785, 1995, 2730, 3570, 4290, 5610, 7854, 19374.$$

لم زیر نشان می‌دهد که مسألهٔ اعداد همنهشت را می‌توان از مجموعهٔ اعداد طبیعی به مجموعهٔ اعداد طبیعی خالی از مربع تقلیل داد. بنابراین، در ادامه، n را یک عدد طبیعی خالی از مربع در نظر خواهیم گرفت.

لم ۵.۲. هرگاه عدد طبیعی n به‌صورت $n = t^2 m$ باشد که $t, m \in \mathbb{N}$، آن‌گاه n یک عدد همنهشت است اگر و تنها اگر m یک عدد همنهشت باشد.

---

1) infinite descend

برهان. به‌راحتی می‌توان نشان داد که اعداد گویای مثبت a، b و c در برابری اول رابطهٔ (۱) صدق می‌کنند اگر و تنها اگر به‌ازای هر $u \in \mathbb{Q} \setminus \{0\}$، اعداد a/u، b/u و c/u در برابری اول رابطهٔ (۱) صدق کنند. □

فهرست زیر، تمامی اعداد همنهشت خالی از مربع کمتر از ۱۰۰ را به‌دست می‌دهد [۲۱]:

$$5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 34, 37, 38, 39, 41, 46,$$
$$47, 53, 55, 61, 62, 63, 65, 69, 70, 71, 78, 79, 85, 86, 87, 93, 94, 95.$$

در سال ۱۹۷۲ آلتر[1]، کورتز[2] و کوبوتا[3] حدسیه‌ای را مطرح کردند که تاکنون درستی یا نادرستی آن به اثبات نرسیده است بلکه فقط برای اعداد طبیعی $n \leq 10^8$ توسط گروهی به سرپرستی اِلکیس[4] در دانشگاه هاروارد بررسی شده است.

حدسیه ۶.۲. اگر n یک عدد طبیعی خالی از مربع باشد که (به‌پیمانه ۸) $n \equiv 5, 6, 7$، آنگاه n یک عدد همنهشت است.

لازم به یادآوری است که به‌ازای هر $r \in \{1, 2, 3, 5, 6, 7\}$، تعداد نامتناهی عدد همنهشت n با شرط (به پیمانه ۸) $n \equiv r$ وجود دارند [۶]. همچنین، وجود خانواده‌های پارامتری شده‌ای از اعداد همنهشت ثابت شده است. به‌عنوان مثال، در [۱۹] ثابت شده است که تمامی اعداد طبیعی به شکل زیر اعداد همنهشت هستند:

$$n = \frac{1}{2} m_1 m_2 (m_1 + m_2), \quad \gcd(m_1, m_2) = 1, \quad m_1, m_2 > 1.$$

از طرف دیگر، وجود خانواده‌هایی از اعداد غیرهمنهشت با تعداد دلخواهی از عامل‌های اول نیز ثابت شده است. به‌عنوان مثال، اعداد طبیعی $n = p_1 \cdots p_t$ که در آن (به‌پیمانه ۸) $p_i \equiv 3$ اعداد غیرهمنهشت هستند. علاقه‌مندان می‌توانند برای دیدن خانواده‌های دیگری از اعداد غیرهمنهشت به [۱۱]، [۱۲] و [۱۳] مراجعه کنند.

۳. یک الگوریتم ساده ولی نامناسب

فرض می‌کنیم u و v اعداد صحیح مثبتی باشند که $u < v$ و $u + v$ عددی فرد است. با توجه به تساوی $(v^2 - u^2)^2 + (2uv)^2 = (u^2 + v^2)^2$ نتیجه می‌شود که $v^2 - u^2$ و $2uv$ اضلاع مثلث قائم‌الزاویه‌ای با وتر $u^2 + v^2$ هستند. بنابراین با انتخاب u و vهای متفاوت می‌توان نتیجه گرفت که قسمت خالی از مربع $uv(v^2 - u^2)$، عددی همنهشت است. جدول ۱، برخی از خروجی‌های این الگوریتم را نشان می‌دهد.

---

1) Ronald Alter 2) Thaddeus B. Curtz 3) K. K. Kubota 4) Noam D. Elkies

u	v	$uv(v^۲-u^۲)$	n	(a,b,c)
۱	۲	۲×۳	۶	$(۳,۴,۵)$
۲	۳	$۲\times۳\times۵$	۳۰	$(۵,۱۲,۱۳)$
۱	۴	$۲^۲\times۳\times۵$	۱۵	$(۴,۱۵/۲,۱۷/۲)$
۳	۴	$۲^۲\times۳\times۷$	۲۱	$(۱۲,۷/۲,۲۵/۲)$
۲	۵	$۲\times۳\times۵\times۷$	۲۱۰	$(۲۰,۲۱,۲۹)$
۴	۵	$۲^۲\times۳^۲\times۵$	۵	$(۲۰/۳,۳/۲,۴۱/۶)$
۳	۶	۲×۳^۵	۶	$(۳,۴,۵)$
⋮	⋮	⋮	⋮	⋮
۵	۷	$۲^۳\times۳\times۵\times۷$	۲۱۰	$(۱۲,۳۵,۳۷)$
۳	۸	$۲^۳\times۳\times۵\times۱۱$	۳۳۰	$(۲۴,۵۵/۲,۷۳/۲)$
⋮	⋮	⋮	⋮	⋮

جدول ۱: برخی از خروجی‌های الگوریتم

از خروجی‌های این جدول نتیجه می‌شود که این الگوریتم دارای معایب زیر است:

(۱) به‌ازای ورودی‌های مرتب u و v، خروجی‌های n نامرتب هستند؛

(۲) به‌ازای یک n داده شده، نمی‌توان گفت که n در خروجی ظاهر خواهد شد یا نه و در صورت ظاهر شدن نمی‌توان زمان محاسبهٔ آن را معین کرد؛

(۳) به‌ازای ورودی‌های متفاوت، خروجی‌های یکسانی ظاهر می‌شوند.

همان‌طور که در جدول مشاهده می‌شود، برخی از مثلث‌ها دارای اضلاع صحیح هستند. بنابراین هرگاه مسأله‌ی اعداد همنهشت به یافتن مثلث‌های قائم‌الزاویه‌ای با اضلاع صحیح با مساحت n محدود شود، آنگاه بعد از طی یک الگوریتم با تعداد متناهی مرحله، می‌توان معلوم کرد که آیا عدد n همنهشت است یا نه. ولی هرگاه یافتن مثلث‌های قائم‌الزاویه‌ای با اضلاع گویا و مساحت n مطرح باشد، مسأله با پیچیدگی بیشتری مواجه است. در این حالت، ارتباط نزدیکی بین مسألهٔ اعداد همنهشت و نظریهٔ خم‌های بیضوی برقرار است که در بخش بعدی به آن خواهیم پرداخت.

لازم به ذکر است که اضلاع مثلث‌های ظاهر شده در جدول ۱، همیشه دارای صورت و مخرج کوچک نیستند. به‌عنوان مثال، زاگیر[1] در سال ۱۹۸۲ نشان داد [۱۷] که کوچکترین مثلث قائم‌الزاویه با مساحت ۱۵۷ دارای اضلاع گویایی به‌شکل زیر است:

1) Don Zagier

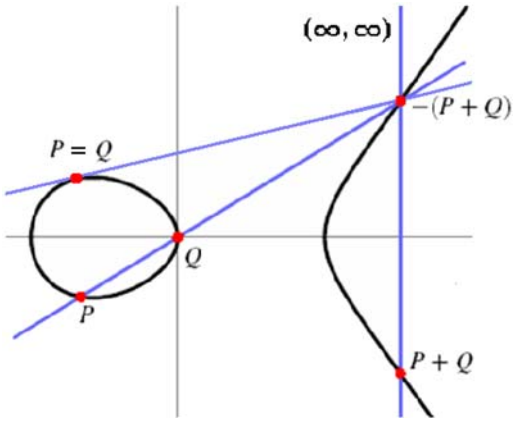
$$a=\frac{۴۱۱۳۴۰۵۱۹۲۲۷۷۱۶۱۴۹۳۸۲۰۳}{۲۱۶۶۶۵۵۵۶۹۳۷۱۴۷۶۱۳۰۹۶۱۰},\quad b=\frac{۶۸۰۳۲۹۸۴۸۷۸۲۶۴۳۵۰۶۱۲۱۷۵۴۰}{۴۱۱۳۴۰۵۱۹۲۲۷۷۱۶۱۴۹۳۸۳۲۰۳},$$
$$c=\frac{۲۲۴۴۰۳۵۱۷۷۰۴۳۳۶۹۶۹۹۲۴۵۵۷۵۱۳۰۹۰۶۷۴۸۶۳۱۶۰۹۴۸۴۷۲۰۴۱}{۸۹۱۲۳۳۲۲۶۸۹۲۸۸۵۹۵۸۸۰۲۵۵۳۵۱۷۸۹۶۷۱۶۳۵۷۰۰۱۶۴۸۰۸۳۰}.$$

۴. مقدمه‌ای بر نظریهٔ خم‌های بیضوی

در این بخش، مختصری از نظریهٔ خم‌های بیضوی را بیان می‌کنیم که یکی از مباحث جدید با کاربردهایی در زمینه‌های رمزنگاری پیشرفته و نظریهٔ اعداد است. به‌جرأت می‌توان گفت که نظریهٔ خم‌های بیضوی نظریه‌ای است که اکثر شاخه‌های ریاضیات در آن نقش‌آفرینی می‌کنند. برای مطالعهٔ بیشتر دربارهٔ نظریهٔ خم‌های بیضوی، می‌توانید مراجع [۱۷]، [۲۰] و [۲۷] را مطالعه کنید. ابتدا تعریف خم بیضوی را بیان می‌کنیم.

تعریف ۱.۴ منظور از یک خم بیضوی[1] روی میدان $\mathbb{Q}$، خم جبری E است که توسط رابطهٔ وایرشتراس تعریف می‌شود (شکل ۱ را ببینید):

$$y^۲=x^۳+ax+b,\quad (a,b\in\mathbb{Z}).$$



شکل ۱: عمل جمع هندسی روی خم بیضوی E

مبین[2] خم بیضوی تعریف شده در بالا، عبارت است از $\Delta=-۱۶(۴a^۳+۲۷b^۲)$، و منظور از

1) elliptic curve 2) discriminant

هموار بودن یک خم بیضوی این است که $\Delta \neq 0$. محل برخورد تمامی خطوط عمودی در صفحه‌ی دکارتی را نقطه در بینهایت نامیده و با $\mathcal{O} = (\infty, \infty)$ نشان می‌دهیم. مطابق با شکل ۱، یک عمل جمع هندسی ـ جبری روی مجموعهٔ

$$E(\mathbb{Q}) = \left\{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid y^2 = x^3 + ax + b : a, b \in \mathbb{Z}\right\} \cup \{\mathcal{O}\}$$

تعریف می‌کنیم. در واقع، برای جمع دو نقطه P و Q روی یک خم بیضوی، ابتدا خط گذرا از P و Q را رسم می‌کنیم. ثابت می‌شود [۲۷] که این خط خم E را در نقطهٔ دیگری قطع می‌کند. در شکل ۱، این نقطه را با $-(P+Q)$ نشان داده‌ایم. حال، مجموع P و Q را برابر با قرینهٔ این نقطه نسبت به محور xها تعریف می‌کنیم. لازم به ذکر است که مختصات نقطهٔ $P+Q$ توسط توابع جبری گویایی از مختصات P و Q قابل بیان است [۲۰]. همچنین، نرم‌افزار PARI/GP [۱۸] یکی از بهترین نرم‌افزارهای به‌روز در نظریهٔ اعداد است که می‌توان با استفاده از آن، بیشتر محاسبات خم‌های بیضوی را انجام داد.

قضیه ۲.۴. **(موردل[1] [۲۰])** به‌ازای هر خم بیضوی E، مجموعهٔ $E(\mathbb{Q})$ با عمل جمع تعریف شده در بالا یک گروه آبلی متناهیاً تولید شده و نقطهٔ $\mathcal{O}$ عنصر همانی آن است. به عبارت دیگر، یک عدد صحیح نامنفی r و یک گروه متناهی $T(E)$ وجود دارد که $E(\mathbb{Q}) \cong T(E) \oplus \mathbb{Z}^r$.

تعریف ۳.۴. عدد صحیح نامنفی r مذکور در قضیهٔ موردل را رتبهٔ (موردل یا هندسی) E نامیده و به‌صورت $r = rank(E)$ نشان می‌دهیم.

تعریف ۴.۴. زیرگروه یکریخت با $T(E)$ از گروه $E(\mathbb{Q})$ را زیرگروه تابی[2] خم بیضوی E خوانده و به‌صورت $E(\mathbb{Q})_{tors}$ نشان می‌دهیم. در واقع زیرگروه تابی، شامل تمامی نقاطی روی E است که نسبت به عمل جمع تعریف شده در بالا دارای مرتبهٔ متناهی هستند.

قضیهٔ زیر یک محدوده برای مرتبهٔ گروه خم‌های بیضوی روی میدان‌های متناهی به‌دست می‌دهد که نقشی اساسی در بیان حدسیه BSD دارد.

قضیه ۵.۴. **(هَس[3] [۲۰])** فرض کنیم p یک عدد اول است و

$$E(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 \equiv x^3 + ax + b \pmod{p}\right\} \cup \{\mathcal{O}\}$$

گروه خم بیضوی E روی میدان $\mathbb{F}_p$ با مبین Δ است به‌طوری که $p \nmid \Delta$. در این صورت

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}.$$

---

1) Louis J. Mordell 2) torsion subgroup 3) Helmut Hasse

تعریف ۶.۴. L– تابع هَس- وِیْل خم بیضوی E به‌صورت زیر تعریف می‌شود:

$$L(E,s)=\prod_{p\nmid\Delta}\left(1-\frac{a_p}{p^s}+\frac{p}{p^{2s}}\right)^{-1}\times\prod_{p\mid\Delta}\ell_p(E,s)^{-1},$$

که $\ell_p(E,s)=1-a_p/p^s$، $a_p=1+p-\#E(\mathbb{F}_p)$ و s متغیری مختلط است.

تعریف ۷.۴. مرتبهٔ تابع $L(E,s)$ در $s=1$ را رتبهٔ تحلیلی E نامیده و آن را به‌صورت $rank_{an}(E)$ نشان می‌دهیم؛ یعنی $rank_{an}(E)=ord_{s=1}(L(E,s))$.

حدسیه ۸.۴ (حدسیه BSD) به ازای هر خم بیضوی E احکام زیر برقرارند:

(۱) **تابع $L(E,s)$ قابل گسترش به یک تابع تحلیلی روی تمام $\mathbb{C}$ است؛**

(۲) $rank(E)=ord_{s=1}L(E,s)$؛ **یعنی رتبهٔ خم بیضوی E برابر با مرتبهٔ تابع مختلط $L(E,s)$ در $s=1$ است.**

این حدسیه یکی از مسائل یک میلیون دلاری بنیاد ریاضیات کلی می‌باشد که توسط بیرچ و سوینرتون ـ دایر در سال ۱۹۶۵ میلادی بیان شده است [۳]. قسمت (۱) حدسیهٔ BSD در سال ۲۰۰۲ به اثبات رسید [۲]. قسمت (۲) فقط برای حالتی که $rank(E)\leq 1$ به‌طور کامل اثبات شده و برای حالتی که $rank(E)\geq 2$، به‌جز موارد خاص، هنوز به‌عنوان یک مسألهٔ باز در نظریهٔ خم‌های بیضوی مطرح است. برای مطالعهٔ بیشتر دربارهٔ این حدسیه و مسائل دیگر مؤسسهٔ کلی به [۴] رجوع کنید.

۵. ارتباط بین خم‌های بیضوی و مسألهٔ اعداد همنهشت

در این بخش، ارتباط بین مسألهٔ اعداد همنهشت و حدسیه BSD را بررسی می‌کنیم. فرض می‌کنیم n یک عدد طبیعی خالی از مربع باشد. مجموعه‌های $\mathcal{A}(n)$ و $\mathcal{B}(n)$ را به‌صورت زیر در نظر می‌گیریم:

$$\mathcal{A}(n)=\left\{(a,b,c)\in\mathbb{Q}^*\times\mathbb{Q}^*\times\mathbb{Q}^*\,|\,0<a<b<c,\ a^2+b^2=c^2,\ ab=2n\right\},$$
$$\mathcal{B}(n)=\left\{(x,y)\in\mathbb{Q}^*\times\mathbb{Q}^*\,|\,y^2=x^3-n^2x,\ y\neq 0\right\}.$$

هرگاه (a,b,c) عضوی از $\mathcal{A}(n)$ باشد، با قرار دادن

$$x=\frac{nb}{c-a},\quad y=\frac{2n^2}{c-a},\tag{۴}$$

نتیجه می‌شود که (x,y) در مجموعهٔ $\mathcal{B}(n)$ قرار دارد. برعکس، هرگاه (x,y) در مجموعهٔ $\mathcal{B}(n)$ قرار داشته باشد، آنگاه با قرار دادن

$$a=\frac{x^2-n^2}{y},\quad b=\frac{2nx}{y},\quad c=\frac{x^2+n^2}{y}, \qquad (5)$$

نتیجه می‌شود که (a,b,c) عضوی از $\mathcal{A}(n)$ است. بنابراین، بحث بالا را می‌توان در قالب قضیهٔ زیر بیان کرد.

قضیه ۱.۵. به ازای هر n، مجموعه‌های $\mathcal{A}(n)$ و $\mathcal{B}(n)$ در تناظر دوسویی قرار دارند.

قضیهٔ زیر نشان می‌دهد که تنها نقاط با مرتبهٔ متناهی روی خم بیضوی E_n، نقاط نابدیهی (x,y) هستند که $y=0$.

قضیه ۲.۵. به‌ازای هر عدد طبیعی n، فرض می‌کنیم خم بیضوی E_n با رابطهٔ وایرشتراس $y^2=x^3-n^2x$ تعریف شده باشد. در این صورت

$$E_n(\mathbb{Q})_{tors}=\{(\infty,\infty),(0,0),(-n,0),(n,0)\}.$$

حال فرض کنیم n یک عدد همنهشت باشد. پس مجموعهٔ $\mathcal{A}(n)$ و در نتیجه $\mathcal{B}(n)$ ناتهی است؛ یعنی نقطهٔ (x,y) روی خم بیضوی E_n با $y\neq 0$ وجود دارد که توسط رابطهٔ (۲) مشخص می‌شود. بنابراین از قضیهٔ ۲.۵ نتیجه می‌شود که $rank(E_n)\neq 0$. برعکس، هرگاه $rank(E_n)\neq 0$، آنگاه (x,y) روی خم بیضوی E_n با مرتبهٔ نامتناهی وجود دارد و از قضیهٔ ۲.۵ نتیجه می‌شود که $y\neq 0$. بنابراین نقطهٔ (x,y) در $\mathcal{B}(n)$ قرار دارد که متناظر با آن می‌توان یک سه‌تایی توسط رابطهٔ (۳) مشخص کرد؛ یعنی عدد n یک عدد همنهشت است. این بحث را می‌توان به‌صورت قضیهٔ زیر خلاصه کرد.

قضیهٔ ۳.۵. عدد طبیعی n یک عدد همنهشت است اگر و تنها اگر $rank(E_n)\neq 0$. در واقع، n یک عدد همنهشت است اگر و تنها اگر مجموعه‌های $\mathcal{A}(n)$ و $\mathcal{B}(n)$ هر دو ناتهی باشد.

با فرض درست بودن حدسیهٔ BSD و در نظر گرفتن قضیهٔ ۳.۵، نتیجه می‌شود که n یک عدد همنهشت است اگر و تنها اگر $L(E_n,1)=0$. یک طرف این عبارت در سال ۱۹۷۷ توسط وایلز[1] و کواتس[2] اثبات شده است [۷]:

قضیه ۴.۵. اگر عدد n یک عدد همنهشت باشد، آنگاه $L(E_n,1)=0$.

در حالت کلی، با فرض $L(E_n,1)=0$ نمی‌توان دربارهٔ همنهشت بودن عدد n چیزی گفت چون هنوز حدسیهٔ BSD در حالت کلی اثبات یا رد نشده است. عکس قضیهٔ بالا در صورتی برقرار است که $ord_{s=1}L(E_n,1)=1$؛ یعنی هرگاه برای یک عدد طبیعی n ثابت شود که $ord_{s=1}L(E_n,1)=1$، آنگاه $rank(E_n)\neq 0$ و در نتیجه n عددی همنهشت خواهد بود. ولی در

1) Andrew Wiles 2) John Coate

حالت $ord_{s=1}L(E_n,1) > 1$ نمی‌توان گفت که حتماً $rank(E_n) \neq 0$ و در نتیجه n عددی همنهشت است.

در این راستا، بهترین نتیجه‌ای که به دست آمده است، قضیهٔ تانل می‌باشد که خلاصهٔ آن را می‌توان به این صورت بیان کرد.

قضیه ۵.۵. (تانل[1] [۲۴]) به‌ازای هر عدد طبیعی n، کمیت‌های زیر را در نظر می‌گیریم:

$$\begin{aligned} f(n) &= \#\{(x,y,z)\in\mathbb{Z}^3 : x^2+2y^2+8z^2=n\},\\ g(n) &= \#\{(x,y,z)\in\mathbb{Z}^3 : x^2+2y^2+32z^2=n\},\\ h(n) &= \#\{(x,y,z)\in\mathbb{Z}^3 : x^2+4y^2+8z^2=n/2\},\\ k(n) &= \#\{(x,y,z)\in\mathbb{Z}^3 : x^2+2y^2+32z^2=n/2\}. \end{aligned}$$

در این صورت،

(۱) اگر n فرد و عدد همنهشت باشد، آنگاه $f(n)=2g(n)$؛

(۲) اگر n زوج و عدد همنهشت باشد، آنگاه $h(n)=2k(n)$.

علاوه بر این، اگر حدسیهٔ BSD برای خم بیضوی E_n برقرار باشد، آنگاه

(۱′) هرگاه n فرد باشد و $f(n)=2g(n)$، آنگاه n عدد همنهشت است؛

(۲′) هرگاه n زوج باشد و $h(n)=2k(n)$، آنگاه n عدد همنهشت است.

مثال ۶.۵. فرض کنیم n یکی از اعداد ۱، ۲، ۳ و ۱۰ باشد. به‌راحتی می‌توان دید که

$$f(1)=g(1)=2,\ f(3)=g(3)=4,$$
$$h(2)=k(2)=2,\ h(10)=k(10)=4.$$

در نتیجه برای $n=1$ یا $n=3$ داریم $f(n)\neq 2g(n)$؛ و برای $n=2$ یا $n=10$ داریم $h(n)\neq 2k(n)$. بنابراین از قضیهٔ تانل نتیجه می‌شود که ۱، ۲، ۳ و ۱۰ عددهای همنهشت نیستند.

$$f(5)=g(5)=0,\ f(7)=g(7)=0.$$

مثال ۷.۵. فرض کنیم n یکی از اعداد ۵ یا ۷ باشد. به‌راحتی می‌توان دید که در نتیجه برای $n=5$ یا $n=7$ داریم $f(n)=2g(n)$. بنابراین از قضیهٔ تانل نتیجه می‌شود که ۵ و ۷ عددهای همنهشت هستند. با در نظر گرفتن قضیهٔ ۳.۵ نتیجه می‌شود که خم‌های بیضوی $E_5 : y^2=x^3-25x$ و $E_7 : y^2=x^3-49x$ دارای رتبهٔ موردل بزرگ‌تر یا مساوی یک هستند. با استفاده از نرم‌افزار MWRANK [۸] نشان داده می‌شود که $rank(E_5)=rank(E_7)=1$.

---

1) Jerrold B. Tunnell

همچنین، با استفاده از نرم‌افزار PARI/GP [۱۸] می‌توان نشان داد که نقطه‌های $P = (-۴, -۶)$ و $Q = (۳۳۶/۲۷, -۹۸۰/۲۷)$، نقطه‌هایی با مرتبهٔ نامتناهی و در نتیجه مولدهایی برای گروه‌های $E_۵(\mathbb{Q})$ و $E_۷(\mathbb{Q})$ هستند. با استفاده از قضیهٔ تانل می‌توان الگوریتمی طراحی کرد که همنهشت نبودن عدد طبیعی n را برای مقادیر نه خیلی بزرگ (مثلاً کوچک‌تر از $۱۰^۹$) مشخص کند. برای مقادیر بزرگ n محاسبهٔ کمیت‌های $f(n)$، $g(n)$، $h(n)$ و $k(n)$ به‌مراتب مشکل‌تر خواهد بود. برعکس، در صورت درست بودن حدسیهٔ BSD، می‌توان از قضیهٔ تانل برای بررسی همنهشت بودن عدد طبیعی n استفاده کرد. بنابراین با درست بودن حدسیه BSD مسألهٔ اعداد همنهشت به‌طور کامل حل خواهد شد که شاید این دلیلی بر اهمیت و جذابیت حدسیهٔ BSD در نظریهٔ اعداد باشد.

مسألهٔ اعداد همنهشت قابل تعمیم به مسألهٔ اعداد θ– همنهشت است. فرض کنیم $۰ < \theta < \pi$، r و s اعداد صحیحی باشند که $(r, s) = ۱$، $r > |s|$، $\alpha_\theta = \sqrt{r^۲ - s^۲}$ و $\cos(\theta) = s/r$. عدد طبیعی n یک عدد θ– همنهشت نامیده می‌شود هرگاه مثلثی با اضلاع گویای a، b و c وجود داشته باشد که زاویهٔ بین اضلاع a و b برابر θ و مساحت آن برابر با $n\alpha_\theta$ است. در حالت خاص، یک عدد همنهشت معمولی چیزی جز یک عدد $\pi/۲$–همنهشت نیست. حالت‌های خاص $\theta = \pi/۳$ و $\theta = ۲\pi/۳$ در [۲۵] مورد مطالعه قرار گرفته است. در [۲۶] مشابه کار تانل، در مورد خم‌های بیضوی اعداد θ–همنهشت انجام شده است. لازم به ذکر است که خم‌های بیضوی مرتبط با اعداد θ–همنهشت به‌صورت $E_{n,\theta} : y^۲ = x(x + (r + s)n)(x - (r - s)n)$ تعریف می‌شوند. به [۱۴]، [۱۵] و [۱۶]، همچنین برای دیدن تعمیم‌های دیگر از مسألهٔ اعداد همنهشت، به [۲۳] مراجعه فرمایید.

مراجع

[1] R. Alter, T. B. Curtz and K. K. Kubota, *Remarks and Results on Congruent Numbers*, Proc. 3rd South Eastern Conf. Combin., Graph Theory and Comput., 1972, Florida Atlantic Univ., Boca Raton, Fla. (1972) 27–35.

[2] C. Breuil, B. Conard, F. Diamond , R. Taylor and A. Wiles, *On the Modularity of Elliptic Curves Over $\mathbb{Q}$ wild 3-adic Exercises,* J. Amer. Math. Soc. 14 (2001), No. 4, 843-939.

[3] B. Birch and H. P. F. Swinnerton, *Notes on Elliptic Curves II*, J. Reine Angew. Math. 218 (1965), 79–108.

[4] Clay Mathematical Institute, Mellinum Prize, www.claymath.org/millenium

[5] J. S. Chahal, *Congruent Numbers and Elliptic Curves*, The American Mathematical Monthly, 113 (2006), No 4, 308–317.

[6] J. S. Chahal, *On an Identity of Desboves*, Proc. Japan Acad. 60 (1984), 105–108.

[7] J. Coates and A. Wiles, *On the Conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 223–251.

[8] cerJ. Cremona, `MWRANK` Program, available at: http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/.

[9] L. E. Dickson, *History of the Theory of Numbers*, Volumn II, Chelsea, New York, 1952.

[10] B. Faulkner and K. James, *A Graphical Approach to Computing Selemer Groups of Congruent Number Curves*, Ramanujan J 14 (2007), 107–129.

[11] K. Feng and Maosheng Xiong, *On Elliptic Curves $y^2 = x^3 - n^2x$ With Rank Zero*, Journal of Numbet Theory 109 (2004) 1–26.

[12] K. Feng, *Non-congruent Numbers, Odd Graphs and the Birch and Swinnerton-Dyer Conjecture*, ACTA ARTIHMETICA LXXV.1 (1996) 71–83.

[13] K. Feng, *New Series of Odd Non-congruent Numbers*, Science in China Series A: Mathematics 49 (2006), No. 11 1642–1654.

[14] M. Fujiwara, *θ-congruent Numbers*, K.Györy, A.Pethö and V.Sós (eds.) de Gruyter (1997), 235–241.

[15] M. Fujiwara, *Some Properties of θ-congruent Numbers*, Natural Science Report, Ochanomizu University, Vol. 52, No. 2 (2001), 1–8.

[16] M. Kan, *θ-congruent Numbers and Elliptic Curves*, ACTA ARTIHMETICA XCIV.2 (200), 153–160.

[17] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, GTM 97, Springer-Verleg, 1993.

[18] PARI/GP, A Computer Algebra System Designed for Fast Computations in Number Theory, Version 2.4.1, Bordeaux, 2008: http://pari.math.u-bordeaux.fr/.

[19] P. Serf, *Congruent Numbers and Elliptic Curves*, Computational Number Theory, A. Petheo, M. Pohst, H. C. William and H. G. Zimmer (eds.) de Gruyter (1991), 227–238.

[20] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verleg, 1983.

[21] N. J. A. Sloane, The on-line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences

[22] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, third edition, A. K. Peters, Ltd. 2002.

[23] J. Top and N. Yui, *Congruent Number Problems and Their Variants*, Algebraic Number Theory, MSRI Publications, Vol. 44 (2008), 613–639.

[24] J. Tunnell, *A Classical Diophantine Problem and Modular Forms of Weight* 3/2, Invent. Math. 72:2 (1993), 323–334.

[25] S. Yoshida, *Some Variants of the Congruent Number Problems, I*, Kyushu J. Math 55:2 (2001), 387–404.

[26] S. Yoshida, *Some Variants of the Congruent Number Problems, II*, Kyushu J. Math 56:1 (2002), 147–165.

[27] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, second edition, CRC, 2008.

علی سرباز جانفدا، a.sjanfada@urmia.ac.ir
سجاد سلامی، salami.sajad@gmail.com
ارومیه، دانشگاه ارومیه، گروه ریاضی