

معادلات دیوفانتی نمایی

پروژه تهیه و ارائه شده است توسط:

I. Klimanova, P. Kozlov, A. Miroshnikov

چکیده

در این پروژه با برخی از معادلات دیوفانتی نمایی و روش های حل بعضی از آنها آشنا می شوید. پروژه از چند بخش تشکیل شده است و قویاً توصیه می شود مسائل را به ترتیب حل کنید.

در بخش ۱ معادلات دیوفانتی نمایی از شکل

$$a^x - b^y = c$$

را بررسی می کنیم.

بخش ۲ به یافتن اعداد صحیح متوالی با مجموعه ای معین از عامل های اول اختصاص دارد. نشان می دهیم که تعداد چنین جفت هایی متناهی است و می توان آن ها را با حل شمار متناهی ای از معادلات پل به طور صریح یافت.

در بخش ۳ حوزه های اقلیدسی معرفی می شوند. برخی از ویژگی های آنها برای حل معادلات دیوفانتی بسیار سودمند است.

در بخش ۴ معادلاتی از نوع لُگ-ناگل را بررسی می کنیم.

۱ درباره معادله $a^x - b^y = c$

این بخش با قضیه زیر آغاز می شود.

قضیه. برای هر سه عدد صحیح مثبت a, b, c با $a, b \geq 2$ ، معادله

$$a^x - b^y = c \quad (*)$$

بیش از دو جواب در اعداد صحیح مثبت ندارد.

اثبات این قضیه دشوار خارج از چارچوب پروژه است. در عوض، برای مقادیر مشخصی از اعداد صحیح مثبت a, b, c با $a, b \geq 2$ ، همه جواب های معادله (*) را جست و جو و شمارش خواهیم کرد.

از این پس فرض می کنیم همه معادلات زیر در اعداد صحیح مثبت x, y حل می شوند.

مسئله 1.1. معادلات زیر را حل کنید:

$$2^x - 3^y = 1, \quad 3^x - 2^y = 1. \quad (\text{الف} \quad \text{ب})$$

گاهی حساب پیمانه ای اطلاعات فراوانی درباره ساختار جواب های معادله (*) می دهد. مسئله بعد نمونه ای از این کاربرد است.

مسئله 1.2. فرض کنید $2^x - 3^y = c$ ، که در آن c, x, y اعداد صحیح مثبت اند. ثابت کنید:

الف) اگر $c \not\equiv 5, 7 \pmod{8}$ ، آنگاه $x \leq 2$ ؛

ب) اگر برای بعضی $3 \leq k$ و $l \geq 1$ داشته باشیم $c = 2^k + 3^l$ ، آنگاه معادله جوابی ندارد.

مسئله 1.3. همه اعداد صحیح مثبت $c \leq 100$ را بیابید که معادله $2^x - 3^y = c$ برای آن ها دو جواب دارد.

اکنون چند حالت خاص از معادله (*) را بررسی می کنیم.

مسئله 1.4. فرض کنید اعداد صحیح مثبت a, b, c دوهو نسبت به هم اول نیستند. ثابت کنید معادله (*) فقط تعداد متناهی جواب دارد.

مسئله 1.5. فرض کنید هر عدد اولی که a را تقسیم می کند، b را نیز تقسیم کند. ثابت کنید معادله (*) حداکثر یک جواب دارد.
از این پس فرض می کنیم a, b, c دویسه دو نسبت به هم اول اند. نخست بر حالت $c = 1$ تمرکز می کنیم.
مسئله 1.6. ثابت کنید برای هر عدد صحیح $b > 1$ ، معادله $2^x - b^y = 1$ هیچ جوابی با $y > 1$ ندارد.
تعریف. مرتبه z به پیمانه M ، با نماد $\text{ord}_z(M)$ ، کوچک ترین عدد صحیح مثبت h است که

$$z^h \equiv 1 \pmod{M},$$

به شرط آن که z و M نسبت به هم اول باشند.
طبق قضیه اولر، برای M ، z نسبت به هم اول، عدد $\text{ord}_z(M)$ به خوبی تعریف شده و مقسوم علیه $\varphi(M)$ است. همچنین به سادگی می توان دید اگر (x, y) جوابی از معادله (*) با $c = 1$ باشد، آنگاه

$$x = \text{ord}_a(b^y).$$

مسئله 1.7. فرض کنید $b = p$ عدد اولی فرد باشد.
الف) ثابت کنید عدد صحیح v وجود دارد به طوری که

$$\text{ord}_a(p^{n+1}) = \begin{cases} \text{ord}_a(p^n), & n < v, \\ p \text{ ord}_a(p^n), & n \geq v. \end{cases}$$

ب) ثابت کنید معادله $a^x - p^y = 1$ بیش از یک جواب ندارد.

مسئله 1.8. ثابت کنید معادله $a^x - b^y = 1$ ، به جز در حالت $a = 3, b = 2$ ، بیش از یک جواب ندارد.
برای $a, b, c > 1$ ، دلخواه، معلوم نیست آیا الگوریتم ابتدایی ای وجود دارد که همه جواب های معادله متناظر (*) را بیابد. باین حال، دو ایده زیر می توانند برای اثبات نبودن جواب هایی با x, y به اندازه کافی بزرگ مفید باشند.
(1) برای هر جواب (x, y) از (*) با $x \geq x_0$ و $y \geq y_0$ ، باقی مانده های x و y به ترتیب به پیمانه های $\text{ord}_a(b^{y_0})$ و $\text{ord}_b(a^{x_0})$ ثابت اند.
(2) اگر عدد اول جادویی P وجود داشته باشد که مجموعه باقی مانده های دنباله های متناظر $\{a_n\}$ و $\{b_m\}$ به پیمانه P جدا از هم باشند، آنگاه برای همه n, m داریم $a_n \neq b_m$.

یافتن چنین عدد اول جادویی ای، حتی اگر وجود داشته باشد، ممکن است دشوار باشد. پیشنهاد می کنیم آن را میان اعداد اول از شکل $dn + 1$ جست و جو کنید، که در آن d برابری از دو عدد $\text{ord}_a(b^{y_0})$ یا $\text{ord}_b(a^{x_0})$ است.
برای نشان دادن این دو ایده، همه جواب های معادله

$$2^x - 11^y = 5$$

را می یابیم.

1. به آسانی جواب $(x, y) = (4, 1)$ را پیدا می کنیم. اکنون ثابت می کنیم جوابی با $x \geq 5$ وجود ندارد.
2. محاسبه می کنیم $\text{ord}_{11}(2^5) = 8$. با حل هم نهشتی $11^y \equiv -5 \pmod{2^5}$ ، به هم نهشتی $y \equiv 5 \pmod{8}$ می رسم.

3. اکنون اعداد اول جادویی از شکل $8n + 1$ را آزمایش می کنیم و از $P = 17$ آغاز می کنیم. بگذارید

$$a_k = 11^{5+8k} + 5, \quad b_m = 2^m.$$

محاسبه نشان می دهد a_k به پیمانه 17 فقط باقی مانده های $-2, -5$ را می گیرد، درحالی که b_m باقی مانده های

$$\pm 1, \pm 2, \pm 4, \pm 8$$

را می گیرد. پس ممکن است $a_k \equiv b_m \equiv -2 \pmod{17}$ باشد و در این مرحله تناقضی به دست نمی آید.

4. سپس می توان توان دیگری از 2 یا 11 را بررسی کرد، یا عدد اول جادویی دیگری برگزید. بررسی می کنیم که $x = 5$ جوابی نمی دهد و همین مراحل را برای توان بعدی، یعنی 2^6 ، تکرار می کنیم.

5. با حل هم نهشتی $(11^y \equiv -5 \pmod{2^6})$ ، به $y \equiv 13 \pmod{16}$ می رسم. اعداد اول از شکل $16n + 1$ را می آزماییم و دوباره $P = 17$ را برمی گزینیم. بگذارید

$$a_k = 11^{13+16k} + 5, \quad b_m = 2^m.$$

داریم

$$a_k \equiv -5 \pmod{17},$$

اما

$$b_m \equiv \pm 1, \pm 2, \pm 4, \pm 8 \pmod{17}.$$

پس $a_k \neq b_m$. بنابراین $P = 17$ یک عدد اول جادویی است و معادله $2^x - 11^y = 5$ هیچ جوابی با $x \geq 6$ ندارد.

در ادامه پیشنهاد می کنیم معادلاتی را حل کنید که ایده های بالا برای آن ها کار می کنند.

مسئله 1.9. معادله $10^x - 7^y = 3$ را حل کنید.

مسئله 1.10. معادله $2^x - 5^y = 3$ را حل کنید.

مسئله 1.11. معادله $3^x - 7^y = 2$ را حل کنید.

مسئله 1.12. الف) دست کم یک عدد صحیح $c > 4$ بیابید که معادله

$$(c+2)^x - 2^y = c$$

پیش از یک جواب داشته باشد.

ب) این معادله را برای c یافته شده حل کنید.

علاوه بر قضیه ای که در آغاز این بخش ذکر شد، معتقدیم حدس زیر درست است.

حدس. تعداد سه تایی های صحیح مثبت (a, b, c) که معادله (*) برای آن ها دقیقاً دو جواب دارد، متناهی است.

هیئت داوران 13 سه تایی از این نوع می شناسد. شما چند سه تایی می توانید پیدا کنید؟

مسئله 1.13. دست کم 8 سه تایی صحیح مثبت (a, b, c) بیابید که معادله (*) برای آن ها دقیقاً دو جواب داشته باشد.

۲ دربارهٔ مسئله‌ای از اشتورمر

متناهی بودن جواب‌های معادلهٔ دیوفانتی (*) را می‌توان چنین بازنویسی کرد. همهٔ توان‌های a و همهٔ توان‌های b را بردارید و آن‌ها را به ترتیب صعودی مرتب کنید. برای $a = 2, b = 3$ داریم

$$2^1, 3^1, 2^2, 2^3, 3^2, 2^4, 3^3, 2^5, 2^6, 3^4, 2^7, \dots$$

فاصلهٔ میان جمله‌های متوالی این دنباله به بی‌نهایت میل می‌کند. به بیان دیگر، برای هر عدد صحیح داده‌شده، از جایی به بعد همهٔ فاصله‌ها از آن عدد بزرگ‌ترند.

گزارهٔ زیر تعمیمی از گزارهٔ قبلی است. مجموعهٔ متناهی Q از اعداد اول را در نظر بگیرید. اعدادی را که همهٔ عامل‌های اولشان در Q قرار دارند به ترتیب صعودی مرتب کنید. برای $Q = \{2, 3, 5\}$ داریم

$$2^1, 3^1, 2^2, 5^1, 2^1 \cdot 3^1, 2^3, 3^2, 2^1 \cdot 5^1, 2^2 \cdot 3^1, 3 \cdot 5, \dots$$

فاصلهٔ میان جمله‌های متوالی این دنباله نیز به بی‌نهایت میل می‌کند.

اثبات این گزارهٔ دشوار بخشی از پروژه نیست. در عوض، کرانی بالا برای تعداد جفت‌های متوالی در این دنباله ثابت خواهیم کرد. این کران فقط به تعداد اعضای Q بستگی دارد.

از این پس فرض می‌کنیم Q از t عدد اول

$$q_1 < q_2 < \dots < q_t$$

تشکیل شده است.

تعریف. اعداد Q -هموار، اعداد صحیحی از مجموعهٔ

$$\{q_1^{e_1} q_2^{e_2} \dots q_t^{e_t} \mid e_i \geq 0\}$$

هستند.

مسئلهٔ 2.1. همهٔ جفت‌های متوالی از اعداد $\{2, 3\}$ -هموار را بیابید؛ یعنی معادلهٔ

$$2^x 3^y - 2^z 3^t = 1$$

را در اعداد صحیح نامنفی x, y, z, t حل کنید.

از این پس D عدد صحیح مثبتی است که مربع کامل نیست. جواب بنیادی، یعنی کوچک‌ترین جواب مثبت، معادلهٔ پل

$$x^2 - Dy^2 = 1$$

را با (x_1, y_1) نشان می‌دهیم. همهٔ جواب‌های مثبت (x_n, y_n) این معادله از رابطهٔ

$$x_n + y_n \sqrt{D} = (x_1 + y_1 \sqrt{D})^n$$

به دست می‌آیند.

مسئلهٔ 2.2. الف) ثابت کنید برای هر عدد صحیح مثبت n ، عدد y_1 مقسوم‌علیه y_n است.

ب) ثابت کنید اگر $n \mid k$ ، آنگاه $y_k \mid y_n$.

گاهی دانستن ساختار عامل‌های اول y_n مفید است. برای نمونه، حل معادلهٔ

$$a^{2k} - b^{2m+1} = 1,$$

که حالت خاصی از (*) است، به حل معادلهٔ پل با $x = a^k, D = b, y = b^m$ کاهش می‌یابد. در شرایط این مثال، مسئلهٔ بعد بررسی وجود جواب را آسان می‌کند.

مسئله 2.3. ثابت کنید معادلهٔ پل حداکثر یک جواب صحیح مثبت (x, y) دارد که هر عامل اول y ، عدد D را نیز تقسیم کند. در سال 1897، این ایده به اشتورمر امکان داد کران بالایی را که وعده داده بودیم ثابت کند.

مسئله 2.4. الف) ثابت کنید تعداد جفت‌های متوالی اعداد Q -هموار از تعداد اعداد Q -هموار از شکل $n^2 - 1$ بیشتر نیست. ب) ثابت کنید بیش از 3^t جفت متوالی از اعداد Q -هموار وجود ندارد.

کران بالایی حاصل با تعداد معادلات پل تعیین می‌شود که باید وجود جواب خاص در آن‌ها بررسی شود. اکنون روش دیگری ارائه می‌کنیم که فقط به حل $2^t - 1$ معادلهٔ پل نیاز دارد. این روش به نکات فنی بیشتری نیازمند است، اما در بسیاری از موارد کران بهتری برای تعداد جفت‌های متوالی اعداد Q -هموار می‌دهد. طبق مسئله 2.2(a)، اعداد

$$U_n := \frac{y_n}{y_1}$$

صحیح‌اند. اکنون مقسوم‌علیه‌های «غیربدیهی» y_n و خواص دنبالهٔ $\{U_n\}$ را بررسی می‌کنیم.

مسئله 2.5. ثابت کنید:

$$\begin{aligned} \text{الف)} \quad x_{2n} &= 2x_n^2 - 1, & \text{ب)} \quad U_{2n} &= 2x_n U_n, \\ \text{ج)} \quad x_{m \pm n} &= x_m x_n \pm D y_m y_n, & \text{د)} \quad U_{m \pm n} &= x_n U_m \pm x_m U_n, \\ \text{ه)} \quad x_n &= \sum_{i \geq 0} \binom{n}{2i} D^i y_1^{2i} x_1^{n-2i}, \\ \text{و)} \quad U_n &= \sum_{i \geq 0} \binom{n}{2i+1} D^i y_1^{2i} x_1^{n-1-2i}, \\ \text{ز)} \quad U_{mn} &= \sum_{i \geq 0} \binom{n}{2i+1} D^i U_m^{2i+1} y_1^{2i} x_m^{n-1-2i}. \end{aligned}$$

تعریف. اگر عدد اول p دست کم یکی از جمله‌های دنبالهٔ $\{U_n\}$ را تقسیم کند، رتبهٔ ظهور p ، با نماد $w(p)$ ، کوچک‌ترین عدد صحیح مثبت j است که $p \mid U_j$.

مسئله 2.6. ثابت کنید $p \mid U_n$ اگر و فقط اگر $n \mid w(p)$. به آسانی می‌توان دید $w(2) = 2$. مسئلهٔ بعد نشان می‌دهد $w(p)$ برای هر عدد اول p وجود دارد.

مسئله 2.7. (قانون ظهور) فرض کنید p عدد اولی فرد باشد. ثابت کنید:

الف) اگر $p \mid D y_1$ ، آنگاه $w(p) = p$ ؛

ب) اگر $p \nmid D y_1$ ، آنگاه

$$w(p) \mid \frac{p-\varepsilon}{2}, \quad \varepsilon = \left(\frac{D}{p}\right) \equiv D^{(p-1)/2} \pmod{p}.$$

مسئله 2.8. فرض کنید $p > 3$ عدد اولی باشد که $p \mid D y_1$. ثابت کنید

$$U_p \equiv p \pmod{p^2}.$$

مسئله 2.9. (قانون تکرار) برای هر عامل اول p از U_n ، هر عدد صحیح مثبت k نسبت به p اول، و هر $\lambda \geq 0$ ، ثابت کنید

$$v_p(U_{knp^\lambda}) = v_p(U_n) + \lambda.$$

برای اختصار می نویسیم

$$\alpha = x_1 + y_1\sqrt{D}, \quad \beta = x_1 - y_1\sqrt{D}.$$

اکنون تعریف می کنیم

$$G_n := \prod_{\substack{h < n \\ (h,n)=1}} (\alpha - \beta e^{2\pi i h/n}).$$

برای نمونه،

$$G_1 = 1, \quad G_2 = \alpha + \beta = 2x_1 = U_2, \quad G_3 = \alpha^2 + \alpha\beta + \beta^2 = U_3.$$

مسئله 2.10. ثابت کنید G_n عددی صحیح است، زیرا چندجمله‌ای متقارنی از α و β است.

مسئله 2.11. ثابت کنید

$$U_n = \prod_{\delta|n} G_\delta.$$

از مسئله قبل نتیجه می شود G_n مقسوم علیه U_n است.

دو نوع عامل اول برای G_n در نظر می گیریم. عامل اولی از G_n که n را نیز تقسیم کند «ذاتی» نامیده می شود؛ سایر عامل های اول G_n را «بیرونی» می نامیم.

مسئله 2.12. فرض کنید p عامل اول ذاتی G_n باشد.

الف) ثابت کنید p بزرگ ترین عامل اول n است.

ب) اگر $n > 3$ ، ثابت کنید $p^2 \nmid G_n$.

مسئله 2.13. فرض کنید $n > 3$ عددی صحیح باشد.

الف) ثابت کنید G_n یک عامل اول بیرونی q دارد.

ب) ثابت کنید $q \geq 2n - 1$.

عدد $M(Q)$ را چنین تعریف می کنیم:

$$M(Q) = \max \left(3, \frac{q_t + 1}{2} \right).$$

مسئله 2.14. فرض کنید $Q \in 2$ ، و Q' مجموعه همه $2^t - 1$ عدد Q -هموار بدون مربع، به جز عدد 2، باشد. اگر S عددی صحیح باشد که هر دو عدد S و $S + 1$ Q -هموار باشند، ثابت کنید

$$S = \frac{x_n - 1}{2},$$

که در آن (x_n, y_n) جوابی از معادله پل

$$x^2 - 2dy^2 = 1$$

است، به طوری که

$$d \in Q', \quad 1 \leq n \leq M(Q).$$

قضیه بعد نتیجه مستقیم مسئله پیشین است.

قضیه. برای هر مجموعه Q از t عدد اول، تعداد جفت های متوالی اعداد Q -هموار حداکثر $(2^t - 1)M(Q)$ است.

مسئله 2.15. همه جفت های متوالی از اعداد $\{2, 3, 5\}$ -هموار را بیابید.