ریاضیات گسسته

نیم‌سال دوم ۱۳۹۹-۱۴۰۰

مدرس: خانم عقبایی

دانشکده علوم ریاضی

پاسخنامه تمرین تحویلی: سری سوم

پرسش ۱

آ) با استفاده از قضیه فرما نشان دهید هر عدد صحیح به شکل $a^2 \pm a + 1$ نمی‌تواند عامل اول به شکل $3k + 2$ داشته باشد.

ب) فرض کنید دنباله‌ی x_n از اعداد صحیح به این صورت تعریف می‌شود که x_0 یک عدد صحیح نامنفی دلخواه بوده و باقی اعضای دنباله به صورت $x_{n+1} = 1 + \prod_{0\leq i\leq n} x_i$ تعریف می‌شود. ثابت کنید بی نهایت عدد اول p وجود دارد که هیچکدام از جملات این دنباله را عاد نمی‌کند.

راه حل.

آ) با برهان خلف فرض می‌کنیم $a^2 \pm a + 1$ عامل اولی به فرم $p = 3k + 2$ داشته باشد. دو حالت زیر را بررسی می‌کنیم:

i) $a^2 \pm a + 1 = a^2 + a + 1$

داریم $p \mid a^2+a+1 \mid (a^2+a+1)(a-1) = a^3-1 \mid (a^3-1)(a^{3^{n-1}}+a^{3^{n-2}}+\cdots+a^3+1) = a^{3n}-1$، پس به ازای هر n طبیعی خواهیم داشت $p \mid a^{3n} - 1$. از طرفی، می‌دانیم $p \nmid a$ چون در غیر این صورت خواهیم داشت $p \mid 1$ که با فرض اول بودن p در تناقض است. پس $\gcd(a,p) = 1$ و طبق قضیهٔ کوچک فرما داریم $p \mid a^{p-1} - 1 = a^{3k+1} - 1$. با قرار دادن $n = k$ در رابطه اول خواهیم داشت $p \mid a^{3k} - 1$. با کم کردن این دو رابطه داریم:

$$p \mid (a^{3k+1} - 1) - (a^{3k} - 1) = a^{3k+1} - a^{3k} = a^{3k}(a - 1)$$

همچنین طبق $\gcd(a,p) = 1$ می‌دانیم $gcd(a^{3k}, p) = 1$. پس داریم

$$p \mid a - 1 \Rightarrow a \equiv 1 (mod\ p) \Rightarrow a^2 \equiv 1 (mod\ p) \Rightarrow a^2 + a + 1 \equiv 3 (mod\ p)$$

اما می‌دانستیم که $a^2 + a + 1$ بر p بخش‌پذیر است. پس داریم:

$$0 \equiv a^2 + a + 1 \equiv 3 (mod\ p) \Rightarrow 0 \equiv 3 (mod\ p) \Rightarrow p = 3$$

که به وضوح تناقض است.

ii) $a^2 \pm a + 1 = a^2 - a + 1$

داریم $a^2 - a + 1 = (a-1)^2 + (a-1) + 1 = b^2 + b + 1$. پس طبق قسمت قبل حکم درست است.

پس در هر دو حالت، این عبارت عامل اولی به فرم $3k + 2$ ندارد و اثبات به پایان می‌رسد.

ب) اعداد اول مجموعهٔ $P = \{p \in \mathbb{P} : p \equiv ۲ \pmod{۳}, p > x_۰ + ۱\}$ را در نظر بگیرید. ادعا می‌کنیم تعداد اعضای این مجموعه نامتناهی است. فرض کنید تعداد اعضای این مجموعه متناهی باشد و $p_۱, p_۲, \ldots, p_m > ۲$ همه‌ی اعداد اول به فرم $۳k + ۲$ باشند. قرار می‌دهیم

$$A = ۳\sum_{i=۱}^{m} p_i + ۲$$

به وضوح $۳ \nmid A$. از طرفی تمام عوامل اول A نمی‌توانند به فرم $۳k + ۱$ باشند. زیرا در آن صورت خواهیم داشت

$$A \equiv (۳k_۱ + ۱) \cdots (۳k_\ell + ۱) \equiv ۱ \pmod{۳}$$

که به وضوح با فرض اولیهٔ ما برای A در تناقض است. پس A شمارندهٔ اولی به فرم $۳k + ۲$ داشته و از آنجا که هیچ یک از اعداد $p_۱, p_۲, \ldots, p_m$ عبارت A را نمی‌شمارند، شمارندهٔ مذکور، عامل اول جدیدی بوده که در بین این اعداد قرار ندارد. پس تعداد اعضای مجموعهٔ P نامتناهی است.

حال، به وضوح برای $p \in P$ با توجه به بزرگ‌تر بودن آن از $x_۰, x_۱$، داریم $p \nmid x_۰, x_۱$. همچنین برای هر $i \geq ۲$، برای عدد x_i می‌توانیم بنویسیم:

$$x_i = \prod_{۰ \leq j \leq i-۱} x_j + ۱ = x_{i-۱} \prod_{۰ \leq j \leq i-۲} x_j + ۱ = x_{i-۱}(x_{i-۱} - ۱) + ۱ = a^۲ - a + ۱$$

بنابراین هر x_i عددی به فرم $a^۲ - a + ۱$ بوده و طبق بخش الف، شمارنده اولی به فرم $۳k + ۲$ و به‌طور دقیق‌تر، از مجموعهٔ P ندارد. پس تمام اعداد این مجموعهٔ نامتناهی در شرط مسئله صدق می‌کنند و حل به پایان می‌رسد.

پرسش ۲

فرض کنید p عددی اول و $a_1, a_2, \dots, a_p$ تصاعدی حسابی باشد که قدر نسبت آن به p بخش پذیر نیست. ثابت کنید عدد i وجود دارد که

$$a_i + a_1 a_2 \dots a_p \equiv 0 \pmod{p^2}$$

راه حل.

ابتدا ثابت می‌کنیم هیچ دو جمله‌ی این دنباله‌ی متناهی به پیمانهٔ p هم‌نهشت نیستند. فرض کنید جملهٔ اول دنباله a_1 و قدر نسبت آن d باشند. برای i, j دلخواه داریم:

$$\begin{aligned}
a_i &\not\equiv a_j && \pmod{p}\\
a_1 + (i-1)d &\not\equiv a_1 + (j-1)d && \pmod{p}\\
(i-1)d &\not\equiv (j-1)d && \pmod{p}\\
p \in \mathbb{P}, p \nmid d \Rightarrow \gcd(d,p) = 1 \Longrightarrow (i-1) &\not\equiv (j-1) && \pmod{p}
\end{aligned}$$

که عبارت آخر به دلیل آن که i, j کوچک‌تر مساوی p و نسبت به آن اول هستند، درست می‌باشد. بنابراین هر یک از این جملات در تقسیم بر p باقی‌مانده‌ای متفاوت از دیگران دارد و در نتیجه، به ازای هر $k \in \{1, 2, \dots, p\}$ عضوی از دنباله مانند a_ℓ پیدا می‌شود که

$$a_\ell \equiv k \pmod{p}$$

طبق نتیجهٔ نهایی، اندیس i وجود دارد که $a_i \equiv 0 \pmod{p}$. در نتیجه خواهیم داشت:

$$\frac{a_1 \cdots a_p}{a_i} \equiv a_1 \cdots a_{i-1} a_{i+1} \cdots a_p \equiv 1 \times 2 \times \cdots \times p-1 \equiv (p-1)! \equiv -1 \pmod{p}$$

که در آن، هم‌نهشتی نهایی توسط قضیهٔ ویلسون نتیجه می‌شود. بنابراین خواهیم داشت:

$$a_i + a_1 \cdots a_p \equiv a_i(1 + a_1 \cdots a_{i-1} a_{i+1} \cdots a_p) \pmod{p^2} \qquad (*)$$

که در آن داریم:

$$1 + a_1 \cdots a_{i-1} a_{i+1} \cdots a_p \equiv 1 + (-1) \equiv 0 \pmod{p}$$

از طرفی، فرض کردیم $a_i \equiv 0 \pmod{p}$. پس هر یک از دو عبارت ضرب شده در هم در عبارت آخر $(*)$، بر p بخش‌پذیر بوده و در نتیجه، کل عبارت بر p^2 بخش‌پذیر می‌باشد.

پرسش ۳

برای هر دو عدد طبیعی n, k ثابت کنید n عدد طبیعی متوالی وجود دارند که تعداد مقسوم علیه های هر یک بر k بخش پذیر باشند.

راه حل.

دستگاه معادلات هم‌نهشتی زیر را برای اعداد اول $p_1, p_2, \dots, p_n$ در نظر بگیرید:

$$\begin{aligned}
x &\equiv p_1^{k-1} - 1 \pmod{p_1^k} \\
x &\equiv p_2^{k-1} - 2 \pmod{p_2^k} \\
x &\equiv p_3^{k-1} - 3 \pmod{p_3^k} \\
&\vdots \\
x &\equiv p_n^{k-1} - n \pmod{p_n^k}
\end{aligned}$$

از آنجا که p_i ها اعدادی اول اند، هر دو تای دلخواه از آن‌ها نسبت به هم اول بوده و برای هر i, j خواهیم داشت $\gcd(p_i^k, p_j^k) = 1$. پس p_i^k ها در شرط قضیهٔ باقی‌مانده چینی صدق کرده و این دستگاه هم‌نهشتی برای x، جواب طبیعی دارد. پس خواهیم داشت:

$$\begin{aligned}
x + 1 &= p_1^k x_1 + p_1^{k-1} = p_1^{k-1}(p_1 x_1 + 1) = p_1^{k-1} x_1' \\
x + 2 &= p_2^k x_2 + p_2^{k-1} = p_2^{k-1}(p_2 x_2 + 1) = p_2^{k-1} x_2' \\
x + 3 &= p_3^k x_3 + p_3^{k-1} = p_3^{k-1}(p_3 x_3 + 1) = p_3^{k-1} x_3' \\
&\vdots \\
x + n &= p_n^k x_n + p_n^{k-1} = p_n^{k-1}(p_n x_n + 1) = p_n^{k-1} x_n'
\end{aligned}$$

که به وضوح در این اعداد، برای i دلخواه، $p_i \nmid x_i'$. بنابراین، این اعداد، n عدد طبیعی متوالی اند که تعداد شمارنده‌های هر یک بر k بخش‌پذیر می‌باشد و حل مسئله به اتمام می‌رسد.

با تشکر از سینا قاسمی‌نژاد