ریاضیات گسسته

پاسخنامه تمرین هفتم – نظریه اعداد

حسام اسدالله زاده

سؤال ۱.

برای اعداد طبیعی n, m, k ثابت کنید اگر $m^n|n^m$ و $n^k|k^n$ آنگاه $m^k|k^m$.

پاسخ .

$$\begin{cases} m^n|n^m \to (m^n)^k|(n^m)^k \\ n^k|k^n \to (n^k)^m|(k^n)^m \end{cases} \longrightarrow (m^n)^k|(k^n)^m \to (m^k)^n|(k^m)^n \to m^k|k^m$$

سؤال ۲.

دنباله $\{a_n\}_{n=1}^{\infty}$ را به صورت $a_n = 10 + n^2$ تعریف می‌کنیم. فرض کنید d بزرگ‌ترین مقسوم‌علیه مشترک دو عضو متوالی این دنباله باشد. بیش‌ترین مقدار ممکن برای d را بیابید.

پاسخ .

می‌دانیم $gcd(a, b) = gcd(b, a - b)$. پس:

$$gcd(a_{n+1}, a_n) = gcd(10 + (n+1)^2, 10 + n^2) = gcd(10 + n^2, 2n + 1)$$

روشن است که عدد $2n + 1$ فرد است. پس توان ۲ در آن صفر است. پس با ضرب کردن سمت دیگر gcd در هر توانی از ۲، حاصل تغییر نمی‌کند. پس:

$$\begin{aligned} gcd(10 + n^2, 2n + 1) &= gcd(40 + 4n^2, 2n + 1) \\ &= gcd((4n^2 - 1) + 41, 2n + 1) \\ &= gcd((2n - 1)(2n + 1) + 41, 2n + 1) \\ &= gcd(41, 2n + 1) \leq 41 \end{aligned}$$

پس $gcd(a_{n+1}, a_n)$ بیش‌تر از ۴۱ نیست. هم‌چنین به ازای $n = 20$، مقدار ۴۱ را می‌گیرد. پس بیش‌ترین مقدار ممکن برای d، ۴۱ است.

سؤال ۳.

برای اعداد طبیعی a, b, c, d داریم $ab = cd$. برای هر عدد طبیعی m تعریف می‌کنیم $T_m = a^m + b^m + c^m + d^m$. ثابت کنید:

الف) T_1 مرکب است.

ب) برای هر m طبیعی، T_m مرکب است.

ج) برای هر عدد طبیعی $n \geq 2$، $n^{T_m} - 1$ مرکب است.

پاسخ.

الف) فرض کنید $(a, c) = x$ و $(b, d) = y$. پس اعداد a_1, b_1, c_1 و d_1 وجود دارند که $a = xa_1$، $c = xc_1$، $b = yb_1$، $d = yd_1$ و $(a_1, c_1) = (b_1, d_1) = 1$. چون $ab = cd$، داریم:

$$(xa_1)(yb_1) = (xc_1)(yd_1) \Rightarrow a_1b_1 = c_1d_1$$

پس $a_1 \mid c_1d_1$. از آن‌جا که $(a_1, c_1) = 1$، پس $a_1 \mid d_1$. از طرف دیگر، چون $d_1 \mid a_1b_1$ و $(b_1, d_1) = 1$، داریم $d_1 \mid a_1$. در نتیجه $a_1 = d_1$. به طور مشابه ثابت می‌شود که $b_1 = c_1$. حال قرار دهید $z = a_1 = d_1$ و $t = c_1 = d_1$. به راحتی می‌توان دید که:

$$T_1 = a + b + c + d = xz + yt + xt + yz = (x + y)(z + t)$$

با توجه به این‌که $x + y > 1$ و $z + t > 1$، پس T_1 عددی مرکب است.

ب) به طور مشابه برای T_m از رابطه زیر می‌توان دید که T_m هم مرکب است:

$$T_m = a^m + b^m + c^m + d^m = x^m z^m + y^m t^m + x^m t^m + y^m z^m = (x^m + y^m)(z^m + t^m)$$

ج) چون T_m مرکب است می‌توان نوشت $T_m = \alpha\beta$ که $\alpha, \beta > 1$. پس:

$$n^{T_m} - 1 = n^{\alpha\beta} - 1 = (n^\alpha - 1)(n^\beta + n^{\beta - 1} + ... + 1)$$

در عبارت فوق، هر دو عامل بزرگ‌تر از یک هستند. پس $n^{T_m} - 1$ عددی مرکب است.

سؤال ۴.

الف) ثابت کنید معادله $15x^2 - 7y^2 = 9$ هیچ جواب صحیحی ندارد.

ب) ثابت کنید برای معادله $x^2 + y^2 + z^2 = 2xyz$ هیچ جواب صحیحی به جز $(0, 0, 0)$ وجود ندارد.

پاسخ.

الف) این مسئله را سعی می کنیم به کمک هم نهشتی و با توجه به یک سری خواص هم نهشتی اعداد مربع کامل بر یک سری اعداد خاص حل کنیم. با نگاه به معادله و کمی تامل می توان فهمید سمت چپ معادله باید به ۳ و ۹ بخش پذیر باشد. $15x^2$ که بر ۳ بخش پذیر است ولی برای بخش پذیر بودن $7y^2$ باید y بر ۳ بخش پذیر باشد یعنی $y = 3y_1$. با این نتیجه گیری یعنی $7y^2 = 63y_1^2$ بر ۹ نیز

بخش پذیر است. در نتیجه برای بخش پذیر بودن سمت چپ معادله بر ۹ باید ترم اول سمت چپ معادله نیز بر ۹ بخش پذیر باشد یعنی داریم $x = ۳x_۱$. حال با توجه به نتیجه گیری های انجام شده برای x, y داریم :

$$y = ۳y_۱, x = ۳x_۱$$

$$\Rightarrow ۱۳۵{x_۱}^۲ - ۶۳{y_۱}^۲ = ۹$$

$$\Rightarrow ۱۵{x_۱}^۲ - ۷{y_۱}^۲ = ۱$$

$$\Rightarrow -۷{y_۱}^۲ \equiv ۱ \mod ۳$$

$$\Rightarrow {y_۱}^۲ \equiv -۱ \equiv ۲ \mod ۳$$

نتیجه به دست آمده غلط است چون برای هر مربع کامل داریم : ${y_۱}^۲ \equiv ۰ \ or \ ۱ \mod ۳$

پس حکم ثابت شد.

ب) فرض کنید جواب صحیح و غیر صفری مثل (x, y, z) وجود داشته باشد. اگر ۲^k بزرگ ترین توانی از ۲ باشد که x, y, z را عاد می کند، آنگاه داریم:

$$x = ۲^k x_۱, y = ۲^k y_۱, z = ۲^k z_۱ \Rightarrow ۲^{۲k}{x_۱}^۲ + ۲^{۲k}{y_۱}^۲ + ۲^{۲k}{z_۱}^۲ = ۲^{۳k+۱}x_۱y_۱z_۱ \Rightarrow {x_۱}^۲ + {y_۱}^۲ + {z_۱}^۲ = ۲^{k+۱}x_۱y_۱z_۱$$

اسم معادله جدید را (۱) می گذاریم. سمت راست (۱) زوج است. پس سمت چپ نیز باید زوج باشد. همچنین به خاطر ۲^k حداقل یکی از ترم های سمت چپ فرد است. با توجه به این شرایط پس دقیقا یکی از ترم های سمت چپ معادله جدید زوج است. فرض کنید آن $y_۱ = ۲y_۲$ باشد. در نتیجه:

$${x_۱}^۲ + {z_۱}^۲ = ۲^{k+۲}x_۱y_۲z_۱ - ۴{y_۲}^۲ \equiv ۰ \mod ۴$$

در حالی که می دانیم باقی مانده مربع هر عدد فرد به ۴ برابر ۱ است و باید داشته باشیم: ${x_۱}^۲ + {z_۱}^۲ \equiv ۲ \mod ۴$

پس چنین جوابی وجود ندارد و حکم اثبات شد.

سؤال ۵.

فرض کنید p عدد اول فرد باشد.

الف) نشان دهید:

$$((\frac{p-۱}{۲})!)^۲ \equiv (-۱)^{\frac{p+۱}{۲}} \mod p$$

ب) اگر $p \equiv ۱ \mod ۴$ باشد، ثابت کنید $(\frac{p-۱}{۲})!$ پاسخی برای معادله $x^۲ \equiv -۱ \mod p$ است.

و اگر $p \equiv ۳ \mod ۴$ باشد، ثابت کنید $(\frac{p-۱}{۲})!$ پاسخی برای معادله $x^۲ \equiv ۱ \mod p$ است.

ج) امتیازی: در نهایت نشان دهید

$$۱^۲ \times ۳^۲ \times ۵^۲ \times \ldots \times (p-۴)^۲ \times (p-۲)^۲ \equiv (-۱)^{\frac{p+۱}{۲}} \mod p$$

پاسخ .

قضیه ویلسون:

$$(p-۱)! \equiv -۱ \mod p$$

الف) داریم:

$$(p-1)! = (1\times(p-1))(2\times(p-2))(3\times(p-3))\dots(\frac{p-1}{2}\times(p-\frac{p-1}{2}))$$

$$Also p-k \equiv -k \mod p \rightarrow (p-1)! \equiv (1\times(-1))(2\times(-2))(3\times(-3))\dots(\frac{p-1}{2}\times(-\frac{p-1}{2})) \mod p$$

$$\Rightarrow (p-1)! \equiv (-1)^{\frac{p-1}{2}}((\frac{p-1}{2})!)^2 \equiv -1 \mod p$$

حال دو طرف معادله بالا را در $(-1)^{\frac{p-1}{2}}$ ضرب می‌کنیم و از آنجایی که p عددی فرد است، $(-1)^{p-1} = 1$ و خواهیم داشت:

$$((\frac{p-1}{2})!)^2 \equiv (-1)^{\frac{p-1}{2}+1} \equiv (-1)^{\frac{p+1}{2}} \mod p$$

ب)

$$p \equiv 1 \mod 4 \rightarrow p = 4k+1 \rightarrow p+1 = 4k+2 \rightarrow (-1)^{\frac{p+1}{2}} = (-1)^{2k+1} = -1$$

$$\xrightarrow{part(a)} ((\frac{p-1}{2})!)^2 \equiv -1 \mod p$$

پس $(\frac{p-1}{2})!$ پاسخی برای $x^2 \equiv -1 \mod p$ است. به طرز مشابه داریم:

$$p \equiv 3 \mod 4 \rightarrow p = 4k+3 \rightarrow p+1 = 4k' \rightarrow (-1)^{\frac{p+1}{2}} = (-1)^{2k'} = 1$$

$$\xrightarrow{part(a)} ((\frac{p-1}{2})!)^2 \equiv 1 \mod p$$

ج) اگر متغیری مانند k روی تمام اعداد فرد بین ۱ و p پیمایش کند، $p-k$ روی اعداد زوج بین ۱ و $p-1$ پیمایش خواهد کرد. پس داریم:

$$(p-1)! = 1\times3\times5\times\dots\times(p-2)\times(p-1)\times(p-3)\times(p-5)\dots(p-(p-2)) \equiv$$

$$\equiv 1\times3\times5\times\dots\times(p-2)\times(-1)\times(-3)\times(-5)\times\dots\times(-(p-2)) = (-1)^{\frac{p-1}{2}}(1\times3\times5\times\dots\times(p-2))^2 \mod p$$

با استفاده از قضیه ویلسون خواهیم داشت:

$$(-1)^{\frac{p-1}{2}}(1\times3\times5\times\dots\times(p-2))^2 \equiv 1 \mod p$$

و مانند بخش قبل در نهایت خواهیم داشت:

$$1^2\times3^2\times5^2\times\dots\times(p-4)^2\times(p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$$

سؤال ۶.

الف) 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 $x_\circ$ یک عدد صحیح نامنفی دلخواه بوده و باقی اعضای دنباله به صورت:

$$x_{n+1} = \prod_{i=1}^{n} x_i + 1$$

تعریف می‌شود. ثابت کنید بی‌نهایت عدد اول p وجود دارد که هیچ‌کدام از جملات این دنباله را عاد نمی‌کند.

پاسخ .

با برهان خلف فرض می‌کنیم $a^۲ \pm a + ۱$ عامل اولی به فرم $p = ۳k + ۲$ دارد. دو حالت زیر را بررسی می‌کنیم:

الف) ۱. $a^۲ \pm a + ۱ = a^۲ + a + ۱$:

$$p \mid a^۲+a+۱ \mid (a^۲+a+۱)(a-۱) = a^۳-۱ \to p \mid (a^۳-۱)(a^{۳n-۱}+a^{۳n-۲}+\ldots+a^۳+۱) = a^{۳n}-۱$$

$$\to \forall n \in \mathbb{N} : p \mid a^{۳n} - ۱$$

از طرفی می‌دانیم $p \nmid a$ چون در غیراین‌صورت خواهیم داشت $p \mid ۱$ که با فرض اول بودن p در تناقض است. پس $\gcd(a,p) = ۱$ و طبق **قضیه کوچک فرما** داریم $p \mid a^{p-۱} - ۱ = a^{۳k+۱} - ۱$. همچنین از رابطه اول می‌دانیم $p \mid a^{۳k} - ۱$. با کم کردن این دو رابطه خواهیم داشت:

$$p \mid a^{۳k+۱} - a^{۳k} = a^{۳k}(a-۱) \;\&\; \gcd(a,p) = ۱ \to \gcd(a^{۳k},p) = ۱$$

$$\to p \mid a - ۱ \Rightarrow a \equiv ۱ \mod p \Rightarrow a^۲ \equiv ۱ \mod p \Rightarrow a^۲ + a + ۱ \equiv ۳ \mod p$$

می‌دانستیم $p \mid a^۲ + a + ۱$ پس داریم:

$$۰ \equiv a^۲ + a + ۱ \equiv ۳ \mod p \Rightarrow ۰ \equiv ۳ \mod p \Rightarrow p = ۳$$

که به وضوح به تناقض رسیدیم پس $a^۲ + a + ۱$ نمی‌تواند عامل اول به فرم $۳k + ۲$ داشته باشد.

۲. $a^۲ \pm a + ۱ = a^۲ - a + ۱$:

$$a^۲ - a + ۱ = (a-۱)^۲ + (a-۱) + ۱ = t^۲ + t + ۱$$

پس طبق قسمت الف حکم برقرار است. پس در هر دو حالت $a^۲ \pm a + ۱$ نمی‌تواند عامل اول به شکل $۳k + ۲$ داشته باشد.

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

$$S = ۳\sum_{i=۱}^{m} p_i + ۲$$

به وضوح $۳ \nmid S$ و از طرفی تمامی عوامل اول S نمی‌توانند به فرم $۳k + ۱$ باشند. زیرا در آن صورت خواهیم داشت:

$$S \equiv (۳k_۱ + ۱)\ldots(۳k_l + ۱) \equiv ۱ \mod ۳$$

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

حال به وضوح برای $p \in P$ با توجه به بزرگ‌تر بودن آن از $x_۰, x_۱$ داریم: $p \nmid x_۰, x_۱$

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

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