به نام خدا

راهنمایی مجموعه تمارین نظریه اعداد جلسه سوم دوره تابستانی ۱۴۰۱

قضایای فرما و اویلر

۱. برای $p = 2$ حکم بدیهیست. برای p فرد داریم: $(p+1)^p = (t - p^{\frac{p+1}{2}})(t + p^{\frac{p+1}{2}}) \iff p^{p+1} + (p+1)^p = t^2$. فرض کنید $m = t - p^{\frac{p+1}{2}}, n = t + p^{\frac{p+1}{2}}$. آنگاه ثابت کنید m, n به فرم $2a^p, 2^{p-1}b^p$ هستند. حل را ادامه داده و با استفاده از قضیه فرما به تناقض برسید.

۲. ابتدا نشان دهید برای هر $n \in \mathbb{N}$، عضوی از $\mathbb{S}$ با $2n - 1$ رقم موجود است که بر 4^n بخش پذیر باشد. حال فرض کنید $m = 2^x k$ که در آن $k \in \mathbb{N}$ عددی فرد است. طبق لم عضو $s \in \mathbb{S}$ موجود است به طوری که بر 2^x بخش پذیر باشد. سعی کنید با اضافه کردن تعدادی رقم به این عدد، اثبات را کامل کنید.

۳. ابتدا دقت کنید $f(n+1) = f(1) + 2^{f(1)} + \cdots + 2^{f(n)}$. سپس حکم را قوی‌تر کرده و با استفاده از استقرای ریاضی نشان دهید برای هر $n \in \mathbb{N}$ مجموعه $\{f(a), \cdots, f(a+3^n)\}$ تشکیل دستگاه کامل مانده‌ها به پیمانه 3^n می‌دهد. برای اثبات گام استقرایی با استفاده از نمایش ارائه شده در ابتدای راه حل، $f(a+3^n)$ را بر حسب $f(a)$ و توان‌هایی از ۲ نمایش دهید.

۴. ابتدا به عنوان یک لم ثابت کنید اگر $p \in \mathbb{P}, p \overset{4}{\equiv} 3$ و همچنین $p \mid a^2 + b^2$ آنگاه $p \mid a, p \mid b$. همچنین دقت کنید $d(n)$ زوج است اگر و فقط اگر n مربع کامل نباشد. با استفاده از این دو، سعی کنید مسئله را در حالت‌های خاص حل کنید و سپس ثابت کنید نامتناهی عدد طبیعی با این شرایط خاص موجود است.

۵. ابتدا دقت کنید کافیست مسئله را در حالت $k = 1$ ثابت کنید. در حالت $k = 1$ سعی کنید با اضافه کردن یک رقم ۱ به همراه تعدادی رقم ۰ به سمت چپ $n - 1$ مسئله را در حالت $\gcd(n-1, 10) = 1$ حل کنید. از این ایده برای تکمیل حل مسئله استفاده کنید.

۶. ابتدا فرض کنید $d = \gcd(a_1, \cdots, a_n)$. آنگاه کافیست مسئله را برای اعداد $a_1' = \frac{a_1}{d}, \cdots, a_n' = \frac{a_n}{d}$ حل کنید. در این حالت ثابت کنید $t \in \mathbb{N}$ موجود است به طوری که $f(t) = {a_1}^t + \cdots + {a_n}^t$ نسبت به همه اعداد $a_1, \cdots, a_n$ اول باشد. حال کافیست مسئله را برای اعداد $a_1' = {a_1}^t, \cdots, a_n' = {a_n}^t$ حل کنیم. در این حالت فرض کنید دنباله شامل متناهی عامل اول است و جمله‌ای از دنباله بیابید که بر هیچ یک از این اعداد اول بخش‌پذیر نباشد و در نتیجه حکم مسئله ثابت می‌شود.

۷. ابتدا به عنوان یک لم ساده ثابت کنید برای $P(x) \in \mathbb{Z}[x]$ و اعداد طبیعی $x, y, m \in \mathbb{N}$ به طوری که $x \overset{m}{\equiv} y$ آنگاه $P(x) \overset{m}{\equiv} P(y)$. سپس فرض کنید دنباله شامل متناهی عامل اول $p_1, p_2, \cdots, p_k$ باشد. با استفاده از این لم و قضیه کوچک فرما ثابت کنید جمله‌ای از دنباله وجود دارد که بر همه این عوامل اول بخش پذیر باشد. یکی از این جمله ها را در نظر گرفته (برای مثال $P(n_0) + 2^{n_0}$) و ثابت کنید نامتناهی جمله دیگر از دنباله مانند $P(n) + 2^n$ وجود دارد به طوری که توان همه عوامل اول $p_1, \cdots, p_k$ در $P(n_0) + 2^{n_0}, P(n) + 2^n$ برابر باشد و با استفاده از این به تناقض برسید.

۸. برای قسمت اول فرض خلف کرده و فرض کنید دنباله دارای متناهی عامل اول $p_1, \cdots, p_k$ است. سپس ثابت کنید نامتناهی جمله از دنباله موجود است به طوری که بر تمام اعداد $p_1, \cdots, p_k$ بخش‌پذیر باشد و توان این عوامل اول در تمام آنها با هم برابر باشند. (جزئیات اثبات را کامل کنید) برای قسمت دوم مسئله فرض کنید $p = 2^{2^{n_0}} + k$ یک عدد اول در دنباله باشد. عدد طبیعی n' را طوری بیابید که $2^{2^{n_0}} + k \mid 2^{2^{n'}} + k$ و اثبات کامل می‌شود.

۹. فرضاً دنباله حسابی $\{ai + b\}_{i=1}^{\infty}$ داده شده باشد. فرض کنید $d = \gcd(a, a+b)$. آنگاه با تکمیل جزئیات، ثابت کنید برای هر عدد طبیعی $n \in \mathbb{N}$ داریم: $(\frac{a+b}{d})^{n\varphi(\frac{a}{d})} \overset{\frac{a}{d}}{\equiv} 1$. برای هر $n \in \mathbb{N}$ تعریف می‌کنیم: $t_n = \dfrac{(\frac{a+b}{d})^{n\varphi(\frac{a}{d})} - 1}{\frac{a}{d}}$. حال دقت کنید از نحوه تعریف بدیهیست که $a(t_n \frac{a+b}{d} + 1) + b = d(\frac{a+b}{d})^{n\varphi(\frac{a}{d})+1}$ و این عبارت عضوی از دنباله حسابی داده شده است. جزئیات اثبات را تکمیل کنید.

۱۰. برای اثبات قسمت اول مجدداً از ایده به کار رفته در راه حل سوال ۸ استفاده می‌کنیم. فرض کنید $q_1, \cdots, q_s$ عوامل اول مشترک a, b باشند. فرض کنید دنباله دارای متناهی عامل اول $p_1, \cdots, p_t$ باشد. جمله دلخواهی از دنباله در نظر بگیرید و فرض کنید توان همه عوامل اول در این جمله از $t \in \mathbb{N}$ کمتر است. سعی کنید نامتناهی جمله از دنباله بیابید به طوری که به پیمانه $\prod {q_i}^t \cdot \prod {p_i}^t$ همنهشت باشند. برای قسمت دوم ابتدا به عنوان یک لم ثابت کنید برای هر $a \in \mathbb{N}$ نامتناهی $p \in \mathbb{P}$ موجود است به طوری که $b \in \mathbb{N}$ موجود باشد که $b^2 \overset{p}{\equiv} a$. سپس ثابت کنید p هایی که در این شرط صادقند و همچنین $p \overset{4}{\equiv} 3$ برای آنها برقرار است، هیچ یک از اعداد به فرم $a^{2n} + b$ را نمی‌توانند عاد کنند. با دستکاری استدلال، مشکل توان‌های فرد را بر طرف کرده و اثبات را کامل کنید.

۱۱. به عنوان یک لم ثابت کنید برای هر $p \in \mathbb{P}$ و $k \in \mathbb{N}$ که $k \neq 1, \gcd(p-1, k) = 1$، اگر برای اعداد طبیعی $x, y \in \mathbb{N}$ داشته باشیم $x^k \overset{p}{\equiv} y^k$ آنگاه نتیجه می‌شود $x \overset{p}{\equiv} y$. از لم مذکور نتیجه می‌شود مجموعه $\{1^3, 2^3, \cdots, p^3\}$ یک دستگاه کامل مانده‌ها به پیمانه p است. با استفاده از این نتیجه اثبات مسئله را کامل کنید.

۱۲. حکم را به استقرای قوی روی مقدار c اثبات کنید. درستی پایه استقرا بدیهیست. فرض کنید حکم برای تمام مقادیر کمتر از c صادق باشد. ابتدا ثابت کنید دنباله $\{a, a^2, a^3, \cdots\}$ از جایی به بعد متناوب است و طول کوچکترین دوره تناوب از c کمتر است. طول این دوره تناوب را r در نظر بگیرید. یک مقدار دلخواه برای x در نظر بگیرید و سعی کنید با ثابت نگاه داشتن a^x به پیمانه c، مقدار x به پیمانه c را آزادانه تغییر دهید. برای پیدا کردن x' جدیدی که در شرایط مذکور صادق باشد، از قضیه باقیمانده چینی تعمیم یافته استفاده کنید.

۱۳. ابتدا ثابت کنید برای هر $k \in \mathbb{N}$، دنباله شامل نامتناهی توان kاُم کامل است. جمله iاُم دنباله را با a_i نمایش می‌دهیم. طبق لم بیان شده در مسئله ۷، برای هر $n \in \mathbb{N}$، جملات $\{a_n, a_{n+1}, \cdots\}$ همگی به پیمانه $a_{n+1} - a_n$ با یکدیگر همنهشتند.حال اگر t توان عامل اول دلخواه p در $a_{n+1} - a_n$ باشد، آنگاه با قرار دادن $k = pt\varphi(p^t)$ نتیجه بگیرید توان این عامل اول در $a_n(a_n - 1)$ از t بیشتر است و در نتیجه $a_{n+1} - a_n \mid a_n(a_n - 1)$. با استفاده از این، درباره درجه P نتیجه‌ای ارائه داده و اثبات را کامل کنید.

۱۴. ابتدا با تغییر حکم مسئله، ثابت کنید کافیست نشان دهیم برای هر $a, m \in \mathbb{N}$، مقدار طبیعی n موجود است به طوری که باقیمانده a^n بر mn کمتر از n باشد. سپس ثابت کنید این معادل است با اینکه باقیمانده a^n بر m, n برابر باشند. حال با استفاده از قضیه اویلر، سعی کنید با استفاده از مقدارگذاری‌هایی مانند $n = k\varphi(m)$ حکم معادل اخیر را ثابت کنید.

۱۵. برای هر $p \in \mathbb{P}$ مجموعه تمام باقیمانده‌هایی که اعضای مجموعه $\{\prod_{p \in \mathbb{S}} p - 1 \mid \mathbb{S} \subset A\}$ به پیمانه یکی از اعداد اولی که در A وجود ندارد را در نظر بگیرید.

۱۶. ابتدا به عنوان یک لم ثابت کنید برای هر عدد طبیعی $n \in \mathbb{N}$ داریم : $\sum_{d|n} \varphi(d) = n$. حال برای ادامه فرض کنید $1 < d_1 < d_2 < \cdots < d_k < n$ مقسوم‌علیه‌های n باشند. آنگاه بدیهیست که $\sigma(n) = 1+d_1+\cdots+d_k+n$. بازه $[1, \sigma(n)]$ را به زیربازه‌هایی به ترتیب به طول‌های $1, d_1, d_2, \cdots, d_k, n$ افراز کنید. ثابت کنید در هر زیربازه با طول d حداکثر $\varphi(d)$ عدد وجود دارد که نسبت به n اول است. با استفاده از لم بالا، اثبات را کامل کنید. سپس ثابت کنید در هر زیربازه به طول d ، دقیقاً $\varphi(n)$ عدد وجود دارد که نسبت به n اول است اگر و فقط اگر n توان کامل یک عدد اول باشد.

۱۷. قرار دهید $x_n = a_n - a_{n-1}$. دنباله $\{x_i\}_{i=1}^{\infty}$ را در نظر بگیرید. آنگاه ثابت کنید $n^{10} - (n-1)^{10} = \sum_{d|n} x_i$. با توجه به مشابهت این تساوی با لم به کار رفته در راه حل مسئله ۱۶، سعی کنید ثابت کنید به ازای هر $i \in \mathbb{N}$، مقدار x_i مضرب صحیحی از $\varphi(i)$ هستند.

۱۸. حکم بسیار قوی‌تری را برای قسمت ج ثابت می‌کنیم. ثابت کنید نامتناهی $x \in \mathbb{N}$ موجود است به طوری که اعداد $x, x+1, \cdots, x+n$ در شرایط مسئله صدق کنند. برای اثبات ابتدا در قالب یک لم ثابت می‌کنیم برای هر $0 \le x < y \le 1$ و هر $z \in \mathbb{N}$ طبیعی، اعداد اول $p_1, \cdots, p_k$ موجودند به طوری که همگی از z بیشتر باشند و همچنین : $x < \frac{\varphi(p_1 \cdots p_k)}{p_1 \cdots p_k} < y$. برای اثبات این لم، ابتدا عدد اول به اندازه کافی بزرگ $A = p_i$ را طوری انتخاب می‌کنیم که $p_i > z$ و همچنین $\frac{p_i - 1}{p_i} > x$. از آنجا که $\prod_{\forall p \in \mathbb{P}} \frac{p-1}{p} = 0$ (این رابطه را می‌توان از قضیه کراندار نبودن $\sum_{\forall p \in \mathbb{P}} \frac{1}{p}$ نتیجه گرفت)، نتیجه می‌شود عدد طبیعی $j > i$ موجود است به طوری که $A = \prod_{k=i}^{j} \frac{p_k - 1}{p_k} > x$. مجدداً می‌توان نتیجه گرفت عدد طبیعی $i' > j$ موجود است به طوری که $A = \frac{p_{i'} - 1}{p_{i'}} \cdot \prod_{k=i}^{j} \frac{p_k - 1}{p_k} > x$ و مجدداً عدد $j' > i'$ موجود است که $A = \prod_{k=i}^{j} \frac{p_k - 1}{p_k} \cdot \prod_{k=i'}^{j'} \frac{p_k - 1}{p_k} > x$. این کار را مکرراً ادامه می‌دهیم و بعد از تعداد متناهی گام، مقدار A از y کمتر خواهد شد. (جزئیات اثبات لم را کامل کنید) اثبات لم طبق این نتیجه به پایان می‌رسد. $\square$

دقت کنید طبق این لم نتیجه می‌شود برای هر $c \in [0, 1]$ مقادیر $x \in \mathbb{N}$ موجودند به طوری که $\frac{\varphi(x)}{x}$ تا حد دلخواه به c نزدیک باشد. حال فرض کنید Q برابر با حاصلضرب $n+1$ عدد اول آغازین باشد. با اعمال لم، اعداد دو به دو نسبت به هم اول $A_0, \cdots, A_n$ به وجود می‌آیند. شرایط لم را طوری تنظیم کنید که داشته باشیم :

$$x_i \frac{\gcd(Q, i)}{\varphi(\gcd(Q, i))} < \frac{\varphi(A_i)}{A_i} < y_i \frac{\gcd(Q, i)}{\varphi(\gcd(Q, i))}$$

که در آن $0 < x_i < y_i < \prod_{\substack{p \in \mathbb{P} \\ p \le n+1}} \frac{p-1}{p}$. بازه ها طبق ترتیب جایگشت تنظیم می‌شوند. حال M طبیعی به اندازه کافی بزرگ را در نظر بگیرید و B را برابر با حاصل‌ضرب تمام اعداد اول مانند p در نظر بگیرید که $n+1 < p < M$ و همچنین p هیچ یک از A_i ها را عاد نکند. طبق قضیه باقیمانده چینی، $x \in \mathbb{N}$ وجود دارد که داشته باشیم :

$$QA_0 \mid x \quad , \quad \forall 1 \le i \le n : A_i \mid x+i \quad , \quad B \mid x-1$$

کوچکترین جواب طبیعی این دستگاه را در نظر بگیرید و ثابت کنید برای M به اندازه کافی بزرگ، این x در شرایط مسئله صدق خواهد کرد.

تمرینات اضافه

۱. ابتدا ثابت کنید دنباله $\{n^k + a^n + c\}_{n=1}^{\infty}$ نامتناهی عامل اول دارد. سپس فرض کنید p یکی از این عوامل اول باشد و بدیهتا n_0 موجود است که $p \mid {n_0}^k + a^{n_0} + c$. بنابراین طبق فرض مسئله $p \mid {n_0}^l + b^{n_0} + d$. نتیجه بگیرید $p \mid (-(a^s + c))^l - (-(b^s + d))^k$ و با توجه به اینکه p به اندازه کافی می‌تواند بزرگ باشد نتیجه بگیرید این دو عبارت برابرند و ادامه اثبات را کامل کنید.

۲. مجموعه دلخواه $P = \{p_1, \cdots, p_k\} \subset \mathbb{P}$ را از اعداد اول انتخاب کنید با این شرط که $p_i - 1$ ها دو به دو نسبت به هم اول باشند. تعریف کنید $N = \left(\prod_{i=1}^{k}(p_i - 1)\right)^{100}$. با استفاده از خواص تابع فی، ثابت کنید برای هر زیرمجموعه $\mathbb{S} \subseteq \mathbb{P}$، داریم : $\varphi(N) = \varphi\left(\frac{N}{\prod_{p\in\mathbb{S}}(p-1)} \prod_{p\in\mathbb{S}} p\right)$

۳. فرض کنید $\mathbb{A}$ مجموعه تمام اعداد طبیعی مثل a باشد به طوری که $2 \le a \le p-2$ و همچنین $a^{p-1} \overset{p^2}{\equiv} 1$. به عنوان لم ثابت کنید برای هر a در این بازه، حداکثر یکی از اعداد $a, p-a$ می‌توانند در $\mathbb{A}$ وجود داشته باشند. همچنین ثابت کنید اگر حاصل‌ضرب دو عضو این مجموعه در این بازه قرار داشته باشد، این حاصل‌ضرب هم عضوی از مجموعه است. با استفاده از لم اول نتیجه می‌شود $|\ \mathbb{A}\ | \le \frac{p-3}{2}$ حال فرض کنید q مطلوب مسئله وجود نداشته باشد. در این صورت تمام اعداد اول این بازه در مجموعه $\mathbb{A}$ هستند، اما طبق لم ۲ این نتیجه می‌دهد که هر عدد مرکب در این بازه هم در مجموعه $\mathbb{A}$ قرار دارد که یک تناقض است. بنابراین وجود q اثبات می‌شود. حال فرض کنید q با خواص مذکور در این بازه یکتا است و با استفاده از لم های اثبات شده به تناقض برسید.