به نام خدا

راهنمایی مجموعه تمارین نظریه اعداد جلسه هفتم دوره تابستانی ۱۴۰۱

مبحث ریشه اولیه

۱. فرض کنید $n = {p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k}$. آنگاه اگر بتوانیم مسئله برای هر $p_i \neq 2$ بتوانیم مقدار $a_1 \cdots a_{\varphi(n)} \pmod{{p_i}^{\alpha_i}}$ را محاسبه کنیم، با استفاده از قضیه باقیمانده چینی مسئله حل خواهد شد. (حالت $p_i = 2$ را جداگانه بررسی کنید) برای حل این حالت نیز، فرض کنبد g_i ریشه اولیه به پیمانه ${p_i}^{\alpha_i}$ باشد. آنگاه داریم :

$$a_1 \cdots a_{\varphi(n)} \overset{{p_i}^{\alpha_i}}{\equiv} \left(\prod_{\substack{\gcd(j, {p_i}^{\alpha_i})=1 \\ 1 \leq j \leq {p_i}^{\alpha_i}}} j \right)^{\frac{n}{{p_i}^{\alpha_i}}} = \left(\prod_{1 \leq j \leq \varphi({p_i}^{\alpha_i})} {g_i}^j \right)^{\frac{n}{{p_i}^{\alpha_i}}} = {g_i}^{\frac{n}{{p_i}^{\alpha_i}} \cdot \left(\frac{\varphi({p_i}^{\alpha_i})(\varphi({p_i}^{\alpha_i})+1)}{2} \right)} \overset{{p_i}^{\alpha_i}}{\equiv} (-1)^{\frac{n}{{p_i}^{\alpha_i}} \cdot (\varphi({p_i}^{\alpha_i})+1)}$$

و با استفاده از این، اثبات مسئله را کامل کنید. به عنوان تمرین سعی کنید همچنین با استدلالی مشابه استدلال به کار رفته در اثبات قضیه ویلسون این مسئله را حل کنید و ثابت کنید اگر N جواب برای معادله $x^2 \overset{n}{\equiv} 1$ موجود باشد، حاصل‌ضرب اعضای دستگاه مخفف مانده‌ها به پیمانه n، به پیمانه n همنهشت با $(-1)^N$ است.

۲. فرض کنید g ریشه اولیه به پیمانه p باشد. همچنین برای تبدیل شرط داده شده در مسئله به یک معادله همنهشتی خطی، فرض کنید $a \overset{p}{\equiv} g^{\alpha}, b \overset{p}{\equiv} g^{\beta}$. در این صورت فرض مسئله معادل با این است که $g^{n\alpha} \overset{p}{\equiv} g^{m\beta} \iff n\alpha \overset{p-1}{\equiv} m\beta$. به طریق حکم مسئله معادل با وجود مقدار طبیعی θ است به نحوی که داشته باشیم : $\alpha \overset{p-1}{\equiv} n\theta$. $\beta, m\theta \overset{p-1}{\equiv}$ حال با توجه به شرط اول بودن m, n ثابت کنید $\gcd(m, p-1) = \gcd(\alpha, p-1), \gcd(n, p-1) = \gcd(\beta, p-1)$. حال فرض کنید $m' = \frac{m}{\gcd(m,p-1)}, n' = \frac{n}{\gcd(n,p-1)}, \alpha' = \frac{\alpha}{\gcd(\alpha,p-1)}, \beta' = \frac{\beta}{\gcd(\beta,p-1)}$ و مسئله را به کمک متغیرهای جدید و وارون ضربی حل کنید.

۳. فرض کنید g یک ریشه اولیه دلخواه به پیمانه p باشد. ابتدا ثابت کنید مجموعه $\{g^n \mid 1 \leq n \leq p, \gcd(n, p) = 1\}$ همان مجموعه ریشه‌های اولیه به پیمانه p است. به عنوان یک لم ساده ثابت کنید برای هر $n \neq 2$ طبیعی، مجموع اعضای دستگاه مخفف مانده‌ها به پیمانه n، بر n بخش‌پذیر است و با استفاده از رابطه زیر اثبات را کامل کنید :

$$\prod_{s \in \mathbb{S}} s \overset{p}{\equiv} g^A \quad , \quad A = \sum_{\substack{\gcd(i,p)=1 \\ 1 \leq i \leq p}} i$$

۴. ابتدا برای تبدیل فرم ضربی مسئله به فرم جمعی، فرض کنید g ریشه اولیه به پیمانه p باشد. در این صورت برای هر $1 \leq i \leq p-1$ قرار دهید $\pi_i \overset{p}{\equiv} g^{t_i}$. دقت کنید در این صورت مجموعه $\{t_1, \cdots, t_{p-1}\}$ نیز جایگشتی از $1, \cdots, p-1$ خواهد بود. در نتیجه حکم مسئله معادل با این است که جایگشت $\{t_1, \cdots, t_{p-1}\}$ از اعضای دستگاه مخفف مانده‌ها به پیمانه p را بیابیم به طوری که مجموعه $\{t_1, t_1 + t_2, t_1 + t_2 + t_3, \cdots\}$ یک دستگاه مخفف مانده‌ها به پیمانه p تشکیل دهند. حال ثابت کنید $t_i = g^i$ در شرایط خواسته شده صادق است و اثبات مسئله را تکمیل کنید.

۵. فرض کنید g یک ریشه اولیه به پیمانه p باشد. چون $\gcd(3, p) = 1$ ، $t \in \mathbb{N}$ موجود است به نحوی که $g^t \overset{p}{\equiv} 1$. از طرفی عدد طبیعی $s = \mathrm{Ord}_p(3)$ موجود است به طوری که $3^s \overset{p}{\equiv} g^{ts} \overset{p}{\equiv} 1$ و از تعریف ریشه اولیه نتیجه می‌شود $2^n \mid ts$. اما از قضایای مرتبه می‌دانیم $s \mid p-1 = 2^n$. پس اگر ثابت کنیم t عددی فرد است اثبات مسئله کامل خواهد شد. ابتدا به عنوان یک لم اثبات کنید معادله $x^2 \overset{p}{\equiv} g^k$ جواب دارد اگر و فقط اگر k زوج باشد. بنابراین کافیست ثابت شود معادله $p \mid x^2 - 3$ جوابی در اعداد صحیح ندارد. فرض خلف کنید که این مقدار موجود باشد. ابتدا دقت کنید $p \overset{4}{\equiv} 1$. طبق یکی لم به کار رفته در راه حل سوال ۱۷ مجموعه تمارین مقدماتی، معادله $p \mid x^2 + 1$ جواب دارد. نتیجه بگیرید معادله $p \mid x^2 + 3$ نیز دارای جواب است. ثابت کنید معادله $p \mid x^2 + 2x + 4$ نیز باید دارای جواب صحیح باشد. حال ثابت کنید $p \overset{3}{\equiv} 2$. طبق لمی از مبحث فرما و اویلر می‌دانستیم اگر $a, b \in \mathbb{N}$ و $q \in \mathbb{P}$ $3k + 2 = q$ داده شده باشند و $q \mid a^2 + ab + b^2$ آنگاه $q \mid a, q \mid b$ و با استفاده از نتایج اخیر به تناقض برسید.

۶. مجدداً مانند سوال قبل فرض کنید g یک ریشه اولیه به پیمانه p باشد. مشابه راه حل سوال قبل، چون $\gcd(2, p) = 1$، مقدار $t \in \mathbb{N}$ موجود است که $g^t \overset{p}{\equiv} 2$. همچنین مقدار طبیعی $s = \mathrm{Ord}_p(2)$ موجود است که $2^s \overset{p}{\equiv} g^{st} \overset{p}{\equiv} 1$. طبق خواص ریشه اولیه می‌دانیم $st \mid 2q = p-1$. حالات $s = 1, s = 2$ را رد کنید. بنابراین $s \mid q$. حال کافیست ثابت کنیم s زوج نیز هست. برای اثبات این نیز مشابه مسئله قبل کافیست اثبات کنیم t فرد است. طبق لم مسئله قبل کافیست ثابت کنیم معادله $x^2 \overset{p}{\equiv} 2$ جوابی در اعداد صحیح ندارد. برای اثبات این حکم کافیست بنویسید :

$$\begin{cases} 1 = (-1)^1 \times (-1) \\ 2 = (-1)^2 \times 2 \\ 3 = (-1)^3 \times (-3) \\ \vdots \\ q = (-1)^q \times (-q) \end{cases} \overset{\times}{\Longrightarrow} q! = (-1)^{1+2+\cdots+q} \times (-1) \cdot 2 \cdots (-q) \overset{p}{\equiv} (-1)^{\frac{q(q+1)}{2}} (p-1)(2) \cdots (q-p) \overset{p}{\equiv} (-1) \cdot 2^q (q!)$$

رابطه همنهشتی آخر از این نتیجه می‌شود که $\{1, 2, \cdots, q\} \overset{p}{\equiv} \{\frac{2}{2}, \frac{p-1}{2}, \cdots, \frac{p-q}{2}\}$ برقرار است! (چرا؟) در نتیجه $2^{\frac{p-1}{2}} \overset{p}{\equiv} -1$ که اثبات را کامل می‌کند.

۷. فرض کنید g یک ریشه اولیه دلخواه به پیمانه p^2 باشد. در وهله اول دقت کنید هر ریشه اولیه به پیمانه p نسبت به p اول است و بنابراین به فرم توانی صحیح از g قابل نمایش است. حال شرط لازم و کافی برای اینکه g^k یک ریشه اولیه برای g^k به پیمانه p ریشه اولیه باشد اما به پیمانه p^2 ریشه اولیه نباشد را به دست آورده و حل مسئله را کامل کنید.

۸. ابتدا دقت کنید تمام اعضای این مجموعه به پیمانه p ریشه اولیه هستند. بنابراین نتیجه بگیرید $p-1 \mid \mathrm{Ord}_{p^2}(g+tp)$. در نتیجه اگر عضو $g+tp$ از این مجموعه ریشه اولیه به پیمانه p^2 نباشد، باید رابطه $\mathrm{Ord}_{p^2}(g+tp)=p-1$ برقرار باشد و بنابراین $(g+tp)^{p-1}\overset{p^2}{\equiv}1$. با بسط دادن این رابطه حل مسئله را کامل کنید.

۹. فرض کنید $a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$. در این صورت مشابه راه حل سوال اول کافیست ثابت کنیم $p_i^{\alpha_i}\mid 1^b+\cdots+p_i^{b\alpha_i}$. (جزئیات این ادعا را تکمیل کنید) حال فرض کنید g_i یک ریشه اولیه به پیمانه $p_i^{\alpha_i}$ باشد. دقت کنید توان‌های g تنها می‌توانند اعضای دستگاه مخفف مانده‌ها به پیمانه $p_i^{\alpha_i}$ را تولید کنند. برای رفع این مشکل، ابتدا با استفاده از ریشه اولیه ثابت کنید برای هر $k\in\mathbb{N}$ داریم : $p_i^k \mid \sum_{\substack{\gcd(j,p_i^k)=1\\ 1\le j\le p_i^k}} j^b$. سپس با استفاده از این رابطه، اثبات مسئله را تکمیل کنید.

۱۰. ابتدا مسئله را مانند راه حل مسائل پیشین به توان‌های اعداد اول تقلیل دهید. سپس ثابت کنید برای توان‌های اعداد اول فرد، با استفاده از ریشه اولیه به پیمانه p^α می‌توان یک ابر ریشه اولیه به پیمانه p^α ساخت. در نهایت کافیست حکم را برای توان‌های ۲ اثبات کنیم. فرض کنید $n=2^k$ که در آن $k\ge 3$. عدد اول فرد دلخواه q را در نظر بگیرید. از خواص مرتبه می‌دانیم $\mathrm{Ord}_{2^k}(q)\mid\varphi(2^k)=2^{k-1}$. همچنین از لم دوخط نتیجه می‌شود $\nu_2(q^{2^t}-1)=\nu_2(q^2-1)+t-1$. همچنین بدیهیست که چون q فرد است، $\nu_2(q^2-1)\ge 3$. برای اینکه تا حد ممکن تعداد باقیمانده‌های تولید شده توسط توان‌های q را زیاد کنیم، سعی می‌کنیم مقدار $\nu_2(q^2-1)$ تا حد ممکن کم باشد (برابر با ۳). برای وقوع حالت تساوی صرفا کافیست قرار دهیم $q=3$. در این صورت می‌توان از روابط عنوان شده نتیجه گرفت $\mathrm{Ord}_{2^k}(3)=2^{k-2}$. حال کافیست برای تکمیل باقیمانده‌ها به پیمانه 2^k یکی از اعدادی که در مجموعه توان‌های 3 قرار ندارد را در نظر بگیریم. فرض کنید $a\in\mathbb{N}$ عددی باشد که در مجموعه $\{3,3^2,\cdots\}$ قرار نداشته باشد. حال ثابت کنید جفت $(a_1,a_2)=(3,a),(m_1,m_2)=(2^{k-2},2)$ در شرایط مسئله صادق است.

۱۱. ابتدا بدیهیست که $p\overset{18}{\equiv}1$. فرض کنید $p=18k+1$ و همچنین فرض کنید g یک ریشه اولیه به پیمانه g باشد. طبق خواص ریشه اولیه داریم : $p\mid g^{9k}+1=(g^{3k}+1)(g^{6k}-g^{3k}+1)$. و در نتیجه به دلیل ریشه اولیه بودنِ g نتیجه می‌شود $p\mid g^{6k}-g^{3k}+1$. حال سعی کنید ثابت کنید جواب داشتن معادله $p\mid n^3-3n+1$ معادل با جواب داشتن معادله $p\mid n^3+n^{-3}+1$ است و با استفاده از رابطه عاد کردن به دست آمده برای g اثبات را کامل کنید. به عنوان تمرین سعی کنید تمام اعداد اولی را بیابید که به ازای آنها مقدار یکتای $n\in\mathbb{Z}$ موجود باشد که $p\mid n^3-3n+1$. به عنوان تمرینی دیگر ثابت کنید تمام عوامل اول اعداد به فرم a^3-3a+1 یا برابر ۳ هستند و یا به فرم $9k\pm1$ می‌باشند.

۱۲. ابتدا فرض کنید g ریشه اولیه به پیمانه q باشد و $x\overset{q}{\equiv}g^\alpha$. آنگاه داریم : $(x+1)^p-x^p\overset{q}{\equiv}(g^\alpha+1)^p-g^{\alpha p}$. حال فرض کنید $g^\alpha+1\overset{q}{\equiv}g^\beta$. در این صورت طبق خواص ریشه اولیه داریم : $q-1\mid p(\alpha-\beta)$. از طرفی بدیهتاً $q-1\nmid\alpha-\beta$. بنابراین نتیجه می‌شود در صورت برقراری رابطه خواسته شده، باید $p\mid q-1$ برقرار باشد. در نتیجه کافیست داشته باشیم : $\frac{q-1}{p}\mid\alpha-\beta$. پس در واقع کافیست ثابت کنید مقدار α موجود است به طوری که مقدار $t\in\mathbb{N}$ موجود باشد که $g^\alpha+1\overset{q}{\equiv}g^{\alpha+t\frac{q-1}{p}}$.

۱۳. فرض کنید p عددی اول باشد به طوری که عدد صحیح m موجود باشد که $p\mid m^b+1$. در این صورت طبق قضیه باقیمانده چینی نامتناهی مقدار طبیعی n موجود است به طوری که $n\overset{p}{\equiv}m, p-1\mid n$. در این صورت این مقدار n در شرایط مسئله صدق خواهد کرد. برای یافتن p به طوری که $m\in\mathbb{Z}$ موجود باشد که $p\mid m^b+1$ از ریشه اولیه به پیمانه p استفاده کنید و شرایط وجود مقدار m را بررسی کنید.

۱۴. شرط همنهشتی را به دو شرط به پیمانه‌های $100,101$ تجزیه کنید. خواهیم داشت : $a+c\overset{100}{\equiv}b+d, 2^a+2^c\overset{101}{\equiv}2^b+2^d$. در نهایت ثابت کنید ۲ یک ریشه اولیه به پیمانه ۱۰۱ است و فرض دوم را به یک رابطه همنهشتی خطی برای a,b,c,d تبدیل کرده و با تکمیل جزئیات، اثبات را کامل کنید.

۱۵. ابتدا با استفاده از ریشه اولیه ثابت کنید هر یک از این مجموعه‌ها یک دستگاه کامل مانده‌ها به پیمانه p هستند اگر و فقط اگر $\gcd(m,p-1)=1$. سپس فرض کنید $1\le j\le p-1$ عددی دلخواه باشد و فرض کنید مجموعه‌های متناظر با $i=x,i=y$ در جایگاه jاُم یکسان باشند. آنگاه داریم : $j^{m^x}\overset{p}{\equiv}j^{m^y}$. از این نتیجه بگیرید $p\mid m^{|x-y|}-1 \iff \mathrm{Ord}_p(m)\mid x-y$. از طرفی از خواص مرتبه می‌دانیم $\mathrm{Ord}_p(m)\mid p-1=2q$. حال اگر $\mathrm{Ord}_p(m)$ برابر با ۱ یا ۲ نباشد، حکم مسئله نتیجه می‌شود. (چرا؟) بنابراین کافیست ثابت کنید $m\in\mathbb{N}$ موجود است به طوری که $p\nmid m^2-1$ و همچنین $\gcd(m,p-1)=1$.

۱۶. با رویکردی مشابه راه حل سوال اول پیش بروید. ابتدا مسئله را به حالتی که n توانی از عددی اول باشد تقلیل دهید. سپس با استفاده از ریشه اولیه مسئله را در حالت $n=p^k$ برای p اول و فرد کنید. دقت کنید اگر $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ آنگاه $\sum_{\substack{\gcd(i,n)=1\\ 1\le i\le n}} i^k \overset{p_i^{\alpha_i}}{\equiv}\frac{\varphi(n)}{\varphi(p_i^{\alpha_i})}\cdot\sum_{\substack{\gcd(i,p_i^{\alpha_i})=1\\ 1\le i\le p_i^{\alpha_i}}} i^k$ و به روش مشابه حل مسئله را کامل کنید.

۱۷. برای اثبات گزاره دوم با گزاره اول، فرض کنید $p\in\mathbb{P}$ عاملی اول از n باشد و همچنین $n=pm$. در این صورت داریم :

$$1^{n-1}+\cdots(n-1)^{n-1}+1\overset{p}{\equiv}1+\sum_{k=0}^{m-1}(pk+1)^{mp-1}+\cdots+(p(k+1)-1)^{mp-1}$$

$$\overset{p}{\equiv}1+\sum_{k=0}^{m-1}1^{m-1}+\cdots+(p-1)^{m-1}\overset{p}{\equiv}1+m\left(1^{m-1}+\cdots+(p-1)^{m-1}\right)$$

حال یک ریشه اولیه از p در نظر گرفته و عبارت آخر را بر حسب توان‌هایی از ریشه اولیه بنویسید و گزاره دوم را نتیجه بگیرید. برای اثبات گزاره اول با استفاده از گزاره دوم، ابتدا ثابت کنید اگر هر عامل اول $p\mid n$ در رابطه $p(p-1)\mid\frac{n}{p}-1$ صدق کند، n خالی از مربع است. سپس کافیست ثابت کنید برای هر عامل اول $p\mid n$ داریم : $p\mid 1+(1^{n-1}+\cdots+(n-1)^{n-1})$. مجدداً فرض کنید $n=mp$ و با استفاده از رابطه به دست آمده در اثبات قسمت اول، گزاره اول را نتیجه گرفته و اثبات را کامل کنید.

۱۸. فرض کنید g یک ریشه اولیه به پیمانه p^2 باشد. حال برای هر $1\le i\le p-1$ تعریف کنید $b_i=g^{a_i}\pmod p$. در این صورت حکم مسئله معادل با این است که اعداد صحیح $b_1,\cdots,b_{p-1}$ موجود باشند به طوری که حاصل‌ضرب هیچ دو جفتی از این اعداد به پیمانه p^2 همنهشت نباشند.

۱۹. فرض کنید g در شرایط مسئله صادق باشد. ابتدا ثابت کنید $\{n^2 \mid 1 \le n \le \frac{p-1}{2}\} \overset{p}{\equiv} \{g^{2n} \mid 1 \le n \le \frac{p-1}{2}\}$. سپس دقت کنید طبق فرض مسئله داریم : $\{n^2 \mid 1 \le n \le \frac{p-1}{2}\} \overset{p}{\equiv} \{g^n - 1 \mid 1 \le n \le \frac{p-1}{2}\}$. بنابراین مجموع اعضای این مجموعه‌ها باید به پیمانه p همنهشت باشند و در نتیجه داریم :

$$\frac{g^{p+1}-1}{g^2-1} = \frac{(g^2)^{\frac{p+1}{2}}-1}{(g^2)-1} = g^2+g^4+\cdots+g^{p-1} \overset{p}{\equiv} (g^1-1)+(g^2-1)\cdots(g^{\frac{p-1}{2}}-1) = \frac{g^{\frac{p+1}{2}}-1}{g-1} - \frac{p-1}{2}$$

با استفاده از نتیجه اخیر و ریشه اولیه بودن g نتیجه بگیرید $p \mid 3g+1$. حال کافیست تمام مقادیر p را بیابید که $-\frac{1}{3}$ به پیمانه p ریشه اولیه باشد و در شرایط داده شده صدق کند.

۲۰. فرض کنید g یک ریشه اولیه دلخواه به پیمانه p باشد و همچنین $4 \overset{p}{\equiv} g^{2k}$. با توجه به اینکه هر ریشه اولیه به پیمانه p به فرم g^t است که در آن $\gcd(t,p-1)=1$ برقرار است، کافیست ثابت کنید مقادیر صحیح $a,b \in \mathbb{Z}_{p-1}$ موجودند به طوری که $b-a=2k$ و همچنین $\gcd(a,p-1)=\gcd(b,p-1)=1$.

۲۱. ابتدا با بررسی‌های اولیه حل را آغاز می‌کنیم. وجود رقم $0 \le d \le 9$ در بسط اعشاری $\frac{1}{4p+1}$ معادل وجود مقدار طبیعی $k \in \mathbb{N}$ است به طوری که $\frac{d}{10} \le \frac{10^k \pmod{4p+1}}{4p+1} < \frac{d+1}{10}$. برای بررسی وجود این $k \in \mathbb{N}$، ابتدا نیاز است درباره اعضای مجموعه $\{10^n \pmod{4p+1} \mid \forall n \in \mathbb{N}\}$ نتایجی به دست آوریم. فرض کنید g یک ریشه اولیه به پیمانه $4p+1 \in \mathbb{P}$ باشد. همچنین فرض کنید $g^t \overset{4p+1}{\equiv} 10$. در نتیجه داریم :

$$10^{\frac{4p}{\gcd(4p,t)}} \overset{4p+1}{\equiv} 1 \implies \mathrm{Ord}_{4p+1}(10) \mid \frac{4p}{\gcd(4p,t)}$$

$$\mathrm{Ord}_{4p+1}(10) \mid \varphi(4p+1)=4p \implies \mathrm{Ord}_{4p+1}(10)=1,2,4,p,2p,4p \quad , \quad p>10^9 \implies \mathrm{Ord}_{4p+1}(10)=p,2p,4p$$

و در نتیجه $4 \mid t$: همواره برقرار است و قوی‌ترین نتیجه قابل حصول چنین است : $\{n^4 \pmod{4p+1} \mid \forall n \in \mathbb{N}\} \subseteq \{10^n \pmod{4p+1} \mid \forall n \in \mathbb{N}\}$.
در نهایت مجموعه $\mathbb{A}=\{1^4,2^4,\cdots,\lfloor\sqrt[4]{4p+1}\rfloor^4\}$ را در نظر بگیرید و اثبات کنید هیچ دو عضوی از این مجموعه به پیمانه $4p+1$ همنهشت نیستند. سپس ثابت کنید برای هر $0 \le d \le 9$ عضوی مثل $k \in \mathbb{A}$ موجود است به طوری که $\frac{d}{10} \le \frac{k^4}{4p+1} < \frac{d+1}{10}$ و اثبات را کامل کنید.

تمرینات اضافه (برای حل تمارین ۲،۳،۴ این بخش به ابزاری به نام کارکتر دیریشله نیازمندیم که منابع مربوطه در اختیار شما قرار داده خواهد شد)

۱. فرض خلف کنید که به ازای هر ریشه اولیه g به پیمانه p، $g+1$ یک ریشه اولیه به پیمانه p نباشد. در این صورت داریم : $g+1 = g\cdot(g^{-1}+1)$. با استفاده از این تساوی نتیجه بگیرید دقیقاً یکی از اعداد $g+1, g^{-1}+1$ نامانده درجه دوم به پیمانه p هستند و نتیجه بگیرید حداقل $\frac{3\varphi(p-1)}{2}$ نامانده درجه دوم به پیمانه p وجود دارد. از این نتیجه به تناقض رسیده و اثبات را کامل کنید.

۲. ابتدا فرض کنید $n, x \in \mathbb{N}$ اعدادی طبیعی و دلخواه باشند. برای تعیین وجود ریشه اولیه بین اعداد $x, \cdots, x+n$ از تابع مشخصه استفاده می‌کنیم :

$$\delta(x) = \frac{\varphi(p-1)}{p-1}\cdot\prod_{d|p-1}\left(1-\frac{\sum_{\text{Ord}(\chi)=d}\chi(x)}{\varphi(d)-1}\right) = \frac{\varphi(p-1)}{p-1}\cdot\sum_{d|p-1}\left(\frac{\mu(d)}{\varphi(d)}\cdot\sum_{\text{Ord}(\chi)=d}\chi(x)\right)$$

می‌دانیم برای هر $a \in \mathbb{N}$ به طوری که $\gcd(a,p)=1$، مقدار $\delta(a)$ برابر صفر است اگر و فقط اگر a ریشه اولیه به پیمانه p باشد و در غیر این صورت، برابر با یک است. حال دقت کنید در بازه $x, x+1, \cdots, x+T$ یک ریشه اولیه موجود است اگر و فقط اگر $\delta(x)+\cdots+\delta(x+T)>0$. از طرفی داریم :

$$\sum_{x=C+1}^{C+T}\delta(x) = \sum_{x=C+1}^{C+T}\left(\frac{\varphi(p-1)}{p-1}\cdot\sum_{d|p-1}\left(\frac{\mu(d)}{\varphi(d)}\cdot\sum_{\text{Ord}(\chi)=d}\chi(x)\right)\right)$$

$$= \sum_{x=C+1}^{C+T}\left(\frac{\varphi(p-1)}{p-1}\cdot\sum_{\substack{d|p-1\\ d\neq 1}}\left(\frac{\mu(d)}{\varphi(d)}\cdot\sum_{\text{Ord}(\chi)=d}\chi(x)\right)\right) + \sum_{x=C+1}^{C+T}\frac{\varphi(p-1)}{p-1}\cdot\left(\frac{\mu(1)}{\varphi(1)}\cdot\chi_0(x)\right)$$

$$= \sum_{x=C+1}^{C+T}\left(\frac{\varphi(p-1)}{p-1}\cdot\sum_{\substack{d|p-1\\ d\neq 1}}\left(\frac{\mu(d)}{\varphi(d)}\cdot\sum_{\text{Ord}(\chi)=d}\chi(x)\right)\right) + T\cdot\frac{\varphi(p-1)}{p-1}$$

$$= \frac{\varphi(p-1)}{p-1}\cdot\sum_{\substack{\text{Ord}(\chi)=d\\ d|p-1\\ d\neq 1}}\left(\frac{\mu(d)}{\varphi(d)}\cdot\sum_{x=C+1}^{C+T}\chi(x)\right) + T\cdot\frac{\varphi(p-1)}{p-1}$$

اما طبق نامساوی پولیا-وینوگرادف می‌دانیم برای هر کارکتر اولیه χ به پیمانه $n \in \mathbb{N}$ داریم :

$\left|\sum_{x=M}^{M+N}\chi(x)\right| < \sqrt{n}\ln(n)$ و در نتیجه :

$$\left|\frac{\varphi(p-1)}{p-1}\cdot\sum_{\substack{\text{Ord}(\chi)=d\\ d|p-1\\ d\neq 1}}\left(\frac{\mu(d)}{\varphi(d)}\cdot\sum_{x=C+1}^{C+T}\chi(x)\right)\right| \leq \frac{\varphi(p-1)}{p-1}\cdot\sum_{\substack{\text{Ord}(\chi)=d\\ d|p-1\\ d\neq 1}}\left(\left|\frac{\mu(d)}{\varphi(d)}\right|\cdot\left|\sum_{x=C+1}^{C+T}\chi(x)\right|\right)$$

$$< \frac{\varphi(p-1)}{p-1}\cdot\sum_{\substack{\text{Ord}(\chi)=d\\ d|p-1\\ d\neq 1}}\left(\left|\frac{\mu(d)}{\varphi(d)}\right|\cdot\sqrt{p}\ln(p)\right) = \frac{\varphi(p-1)}{p-1}\cdot\sqrt{p}\ln(p)\cdot\sum_{\substack{\text{Ord}(\chi)=d\\ d|p-1\\ d\neq 1}}\left|\frac{\mu(d)}{\varphi(d)}\right| = \frac{\varphi(p-1)}{p-1}\cdot\sqrt{p}\ln(p)\cdot\sum_{\substack{d|p-1\\ d\neq 1}}|\mu(d)|$$

$$\Longrightarrow \sum_{x=C+1}^{C+T}\delta(x) > T\cdot\frac{\varphi(p-1)}{p-1} - \frac{\varphi(p-1)\cdot\sqrt{p}\ln(p)}{p-1}\cdot\sum_{\substack{d|p-1\\ d\neq 1}}|\mu(d)| = f(T)$$

همچنین $\sum_{d|p-1}|\mu(d)| = 2^k$ (چرا؟) و با استفاده از اینکه $\forall n\in\mathbb{N} : \varphi(n) \leq n-\sqrt{n}$ و انجام محاسبات ثابت کنید مقدار $f(T)$ برای $T = 2\left\lfloor\frac{p-1}{\phi(p-1)}2^k\sqrt{p}\right\rfloor - 1$ مثبت است.

۳. فرض کنید کوچک‌ترین ریشه اولیه به پیمانه p برابر با $g(p)$ باشد. در این صورت چون اعداد $1, 2, \cdots, g(p)-1$ به پیمانه p ریشه اولیه نیستند، طبق تعریف تابع مشخصه در راه حل سوال اخیر، $\sum_{x=1}^{g(p)-1}\delta(x) = 0$. با روندی مشابه راه حل سوال قبل پیش رفته و در نهایت ثابت کنید $g(p) < 1+\sqrt{p}\ln(p)\sum_{d|p-1}|\mu(d)|$ و اثبات را از اینجا کامل کنید.

۴. ابتدا فرض کنید $\chi(n)$ یک کارکتر دیریشله از مرتبه $p-1$ باشد. تابع مشخصه را این‌گونه تعریف می‌کنیم : $\delta(n) = \prod_{\substack{q|p-1\\ q\in\mathbb{P}}}\left(1-\chi(n)^{\frac{p-1}{q}}\right)$. واضح است که تابع مذکور دارای این خاصیت است که $\delta(n)=0$ اگر و فقط اگر n ریشه اولیه‌ای به پیمانه p باشد و در غیر این صورت $\delta(n)=1$. حال یک تابع مبیّن به این صورت تعریف کنید : $\Delta(n) = \sum_{\substack{d|p-1\\ d|n}}\mu(d)$. این تابع مبیّن دارای این خاصیت است که $\Delta(n)=0$ اگر و فقط اگر $\gcd(n,p-1)>1$ و در غیر این صورت $\Delta(n)=1$. حال با استفاده از رویکردی مشابه راه حل مسئله دوم و با استفاده از نامساوی پولیا-وینوگرادف ثابت کنید $\sum_{i=1}^{p-1}f(i)g(i) \geq \varphi(p-1) - 2^{\omega(p-1)}\sqrt{p}\ln(p)$ برای اعداد اول بزرگ برقرار است. برای اثبات این حکم نیز با روندی کاملاً مشابه نتیجه بگیرید $\sum_{i=1}^{p-1}f(i)g(i) \neq 0$