به نام خدا

راهنمایی مجموعه تمارین نظریه اعداد جلسه هشتم دوره تابستانی ۱۴۰۱

مبحث مانده و نامانده‌های مربعی و قضیه تقابل درجه دوم

۱. ابتدا به عنوان یک لم ساده ثابت کنید برای هر $p > 3$ مجموع مانده‌های درجه دوم به پیمانه p بر p بخش‌پذیر است. سپس دقت کنید اگر مجموعه‌های A, B مجزا از هم باشند، مجموعه B باید همان مجموعه نامانده‌های درجه دوم به پیمانه p باشد و در نتیجه مجموع اعضای B نیز باید بر p بخش‌پذیر باشد.

۲. ابتدا نشان دهید حالت $r \overset{p}{\equiv} 1$ بدیهیست. بنابراین از آنجا که طبق اتحاد چاق و لاغر داریم $r^7 - 1 = (r-1)(r^6 + r^5 + r^4 + r^3 + r^2 + r + 1)$، می‌توانیم فرض کنیم $p \mid r^6 + r^5 + r^4 + r^3 + r^2 + r + 1$. در نتیجه داریم : $(r^3+1)(r^2+1)(r+1) \overset{p}{\equiv} r^3$. در نتیجه از خواص مانده‌های مربعی داریم : $\left(\frac{r^3+1}{p}\right)\left(\frac{r^2+1}{p}\right)\left(\frac{r+1}{p}\right) = \left(\frac{r^3}{p}\right) = \left(\frac{r}{p}\right)$. و بنابراین طبق مفروضات مسئله : $\left(\frac{r^3+1}{p}\right) = \left(\frac{r}{p}\right)$. با استفاده از این نتیجه اثبات را کامل کنید.

۳. مشابه اثبات حالت $n = 1$ عمل می‌کنیم و ثابت می‌کنیم اعداد طبیعی و متمایز $q_1, \cdots, q_{\lfloor \frac{p^{n+1}-1}{2(p+1)} \rfloor + 1} \in \mathbb{Z}_{p^n}$ موجودند به طوری که مربعات آن‌ها به پیمانه p^n دو به دو ناهمنهشت باشند و همچنین هر مانده مربعی به پیمانه p^n همنهشت با حداقل یکی از این اعداد باشد. ابتدا شرط اول را بررسی می‌کنیم : $p^n \mid i^2 - j^2 = (i-j)(i+j)$. حال فرض کنید $i = ap^\alpha, j = bp^\beta$. همچنین فرض کنید بدون کم شدن از کلیت مسئله داشته باشیم $\alpha \geq \beta$. در نتیجه داریم : $p^{n-2\beta} \mid (ap^{\alpha-\beta} - b)(ap^{\alpha-\beta} + b)$. حال دقت کنید اگر $\alpha \neq \beta$ آنگاه سمت راست رابطه نسبت به p اول است. در نتیجه $2\beta \geq n$. در نتیجه تنها یکی از q_iها بر $p^{\lceil \frac{n}{2} \rceil}$ بخش‌پذیر است که متناظر با مانده درجه دوم 0 است. در غیر این صورت $\nu_p(i) = \nu_p(j)$. بنابراین کافیست این شرط را صرفاً در همین حالت خاص بررسی کنیم. حالتی که $p^n \mid (i-j)(i+j)$ و $\nu_p(i) = \nu_p(j) = t$ را بررسی کنید و حداکثر مانده‌های درجه دوم در هر حالت را به دست آورده و حکم را نتیجه بگیرید.

۴. ابتدا فرض کنید $n = {p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k}$. ابتدا از خواص مانده‌های مربعی داریم : $\left(\frac{n}{p}\right) = \prod_{i=1}^{k} \left(\frac{p_i}{p}\right)^{\alpha_i}$. حال تعریف کنید $\mathbb{Q} = \{q_i \mid 2 \nmid \nu_{q_i}(n)\}$. دقت کنید اگر n مربع کامل نباشد، $\mathbb{Q}$ ناتهی است. حال واضح است که $\left(\frac{n}{p}\right) = \prod_{q \in \mathbb{Q}} \left(\frac{n}{q}\right)$. با استفاده از قانون تقابل درجه دوم و قضیه دیریشله اثبات مسئله را کامل کنید.

۵. فرض کنید a کوچکترین نامانده درجه دوم به پیمانه p باشد. طبق قضیه اساسی تقسیم اعداد صحیح $q, r \in \mathbb{Z}$ موجودند به طوری که $0 \leq r < q$ و همچنین $p = qa + r$. واضح است که $r \neq 0$. از طرفی به وضوح داریم : $a(q+1) = qa + a \overset{p}{\equiv} a - r$. از طرف دیگر واضح است $0 < a - r < a$. در نتیجه $a - r$ باید یک مانده درجه دوم به پیمانه p باشد. اما طبق نتایج اخیر $a(q+1) \overset{p}{\equiv} pa - r$ و در نتیجه $a(q+1)$ یک مانده درجه دوم به پیمانه p است. طبق خواص مانده‌های درجه دوم و با توجه به اینکه $\left(\frac{a}{p}\right) = -1$، بدیهیست $q + 1$ باید یک نامانده درجه دوم به پیمانه p باشد ولی طبق تعریف a داریم : $q + 1 \geq a$. با استفاده از یک نامساوی اثبات را کامل کنید.

۶. ابتدا سعی می‌کنیم مسئله را به فرم بهتری تبدیل کنیم. داریم : $p = a^2 - 2ab + b^2 \iff 4p = 4a^2 - 4ab + 4b^2 = (2a-b)^2 + 3b^2$. حال ابتدا ثابت کنید می‌توان بدون کم شدن از کلیت مسئله فرض کرد b فرد است. سپس دقت کنید برای هر b فرد واضح است $\nu_2((2a-b)^2 + 3b^2) = 2$. (چرا؟) حال کافیست جوابی برای رابطه عاد کردن $p \mid (2a-b)^2 + 3b^2$ بیابیم به طوری که $(2a-b)^2 + 3b^2 < 12p$. (چرا این شرط کافیست؟) فرض کنید b^* وارون ضربی b به پیمانه p باشد. با ضرب این عبارت در سمت راست رابطه عاد کردن داریم : $p \mid (2ab^* - bb^*)^2 + 3$. ابتدا ثابت کنید $\left(\frac{-3}{p}\right) = 1$ و نتیجه خواهد شد که $c \in \mathbb{N}$ موجود است به طوری که $p \mid c^2 + 3$. حال کافیست $a, b \in \mathbb{Z}$ را بیابیم به طوری که $2ab^* - bb^* \overset{p}{\equiv} c$ و همچنین $(2a-b)^2 + 3b^2 < 12p$. در این موارد از یک لم بسیار پرکاربرد در زمینه نمایش‌های خاص اعداد طبیعی، مشهور به لم توئه استفاده می‌کنیم. لم توئه بیان می‌دارد که برای هر $a, m \in \mathbb{Z}$ به طوری که $m > 1$ و هر $X, Y \in \mathbb{N}$ به طوری که $X \leq m < XY$، مقادیر $x, y \in \mathbb{Z}$ موجودند به طوری که $ay \overset{m}{\equiv} x$ و همچنین $|x| < X, 0 < y < Y$.ابتدا لم توئه را اثبات کنید و در نهایت برای تکمیل راه حل، دقت کنید $2ab^* - bb^* \overset{p}{\equiv} c \iff 2a - b \overset{p}{\equiv} bc \iff 2a \overset{p}{\equiv} (c+1)b \iff 2a(c+1)^* \overset{p}{\equiv} b$. حال کافیست در صورت لم توئه مقدار $X = Y = \lceil \sqrt{p} \rceil$ را قرار دهید و حل مسئله تکمیل می‌شود.

۷. تعریف کنید $\mathbb{A} = \{a \mid 0 < a \leq \frac{p-1}{2}, \left(\frac{a}{p}\right) = 1\}$ و $\mathbb{B} = \{a \mid \frac{p+1}{2} \leq a < p, \left(\frac{a}{p}\right) = 1\}$. ابتدا ثابت کنید تمام اعضای مجموعه $\mathbb{C} = \{p - a \mid a \in \mathbb{B}\}$ نامانده‌های درجه دوم به پیمانه p هستند. در نتیجه مجموعه‌های $\mathbb{A}, \mathbb{C}$ کاملاً مجزا هستند. از طرفی بدیهیست که مجموعه‌های $\mathbb{A}, \mathbb{B}$ نیز مجزا هستند و اجتماع آنها برابر مجموعه مانده‌های درجه دوم به پیمانه p است که دقیقاً $\frac{p-1}{2}$ عضو ناصفر دارد. بنابراین اجتماع مجموعه‌های $\mathbb{A}, \mathbb{C}$ همان مجموعه $\{1, 2, \cdots, \frac{p-1}{2}\}$ است. از خواص مانده‌های درجه دوم می‌دانیم $\left(\frac{2}{p}\right) = (-1)^{k+1}$. بنابراین مجموعه های $\mathbb{A}' = \{2a \mid a \in \mathbb{A}\}, \mathbb{C}' = \{2a \mid a \in \mathbb{C}\}$ وابسته به زوجیت k، تعدادی مانده و نامانده مربعی به پیمانه p را نمایش می‌دهند. با ادامه استدلال، اثبات را تکمیل کنید.

۸. ابتدا واضح است که کافیست مسئله را برای حالت‌هایی که m توانی از یک عدد اول است حل کنیم و مابقی راه حل با استفاده از قضیه باقیمانده چینی تکمیل خواهد شد. فرض کنید $m = p^\alpha$. ابتدا دقت کنید طبق خواص مانده‌های مربعی $\left(\frac{-1}{p^\alpha}\right) = \left(\frac{a}{p^\alpha}\right)^n = \left(\frac{b}{p^\alpha}\right)^n$. با استفاده از این نتیجه بگیرید مسئله در حالتی که n فرد باشد بدیهیست. در حالتی که n زوج باشد فرض کنید g یک ریشه اولیه به پیمانه p^α باشد و همچنین $g^x \overset{p^\alpha}{\equiv} a, g^y \overset{p^\alpha}{\equiv} b$. در این صورت طبق خواص ریشه اولیه داریم : $nx \overset{\varphi(p^\alpha)}{\equiv} my \overset{\varphi(p^\alpha)}{\equiv} \frac{\varphi(p^\alpha)}{2}$. از طرفی حکم با $2 \mid x + y$ معادل است. حال دقت کنید طبق نتیجه اخیر، $\varphi(p^\alpha) \mid n(x+y)$ و نشان دهید $\nu_2(n) < \nu_2(\varphi(p^\alpha)$.

۹. حالات $p = 2, p = 3$ را جداگانه بررسی کنید. برای $p > 3$، چون $\gcd(3, p) = 1$ برقرار است، می‌توان مقدار $n \in \mathbb{N}$ را یافت به طوری که $3n \overset{p}{\equiv} k$. در نتیجه $\left(\frac{n}{p}\right) = \left(\frac{4n}{p}\right) = \left(\frac{n+k}{p}\right)$. جزئیات اثبات را کامل کنید.

۱۰. ابتدا با ایده‌ای مشابه مسئله شماره ۳ مجموعه تمارین مرتبه، ثابت کنید $\gcd(5^m-1,5^n-1)=5^{\gcd(m,n)}-1=4$. در نتیجه 5^m-1 یک عامل ۲ با توان ۲ دارد و بقیه عوامل آن با توان ۱ ظاهر خواهند شد. (چرا؟) در نتیجه می‌توان نوشت $5^n-1=2(q_1-1)\cdots(q_k-1)\quad,\quad 5^m-1=4q_1\cdots q_k$.
ابتدا ثابت کنید m باید فرد باشد، سپس دقت کنید $5^m\overset{q_i}{\equiv}1 \iff 5^{m+1}\overset{q_i}{\equiv}5, 2\mid m+1 \implies \left(\frac{5}{q_i}\right)=1$. با استفاده از قانون تقابل درجه دوم از این می‌توان نتیجه گرفت $\left(\frac{q_i}{5}\right)=1$. بنابراین تمام عوامل اول 5^m-1 به پیمانه ۵ همنهشت با ۴ هستند. (چرا؟) در نتیجه می‌توان گفت $5^m-1\overset{5}{\equiv}4^{k+1}, 5^n-1\overset{5}{\equiv}2\cdot 3^k$. از رابطه اول نتیجه می‌شود $2\mid k$. فرض کنید $k=2t$ و با استفاده از رابطه دوم به تناقض برسید.

۱۱. ابتدا دقت کنید کافیست ثابت کنید :

$$p\nmid \sum_{1\le x_i\le p-1}\left(1-({x_1}^4+{x_2}^4+{x_3}^4+{x_4}^4)^{p-1}\right)=(p-1)^4-\sum_{1\le x_i\le p-1}\left(\sum_{\substack{t_1+t_2+t_3+t_4=p-1\\0\le t_1,t_2,t_3,t_4\le p-1}}\binom{p-1}{t_1,t_2,t_3,t_4}{x_1}^{4t_1}{x_2}^{4t_2}{x_3}^{4t_3}{x_4}^{4t_4}\right)$$

با استدلالی شمارشی ثابت کنید $\displaystyle\sum_{\substack{\sum t_i=p-1\\0\le t_i\le p-1}}\binom{p-1}{t_1,t_2,t_3,t_4}=\binom{p+2}{3}$ و سعی کنید مقدار $\displaystyle\sum_{1\le x_i\le p-1}{x_1}^{4t_1}{x_2}^{4t_2}{x_3}^{4t_3}{x_4}^{4t_4} \pmod p$ را محاسبه کنید.

۱۲. ابتدا به عنوان یک لم کنید اعداد به فرم 2^n+1 نمی‌توانند عامل اولی به فرم $8k-1$ داشته باشند. در راستای بهبود این نتیجه ثابت کنید در صورت فرد بودن n، این عدد هیچ عامل اولی به فرم $8k+5$ نیز نخواهد داشت. حال فرض کنید $n>2$. در این صورت خواهیم داشت : $2^{3^n}+1=(2+1)(2^2-2+1)\cdots(2^{2\times 3^{n-1}}-2^{3^{n-1}}+1)$.
اما همچنین می‌توان ثابت کرد که برای هر $1\le i<j\le n-1$ داریم : $\gcd(2^{2\times 3^i}-2^{3^i}+1, 2^{2\times 3^j}-2^{3^j}+1)=3$. حال ثابت می‌کنیم هر عدد به فرم $2^{2\times 3^i}-2^{3^i}+1$ عامل اولی به فرم $8k+3$ دارد. (غیر از ۳) طبق نتایج به دست آمده در ابتدای راه حل نتیجه می‌شود $2^{2\times 3^i}-2^{3^i}+1$ تنها یک عامل ۳ دارد و بقیه عوامل اول آن به فرم $8k+1, 8k+3$ هستند. فرض خلف کرده و اثبات حکم را کامل کنید. دقت کنید طبق اتحاد بِنِت می‌دانیم : $f_p=\dfrac{\left(\frac{1+\sqrt5}{2}\right)^p-\left(\frac{1-\sqrt5}{2}\right)}{\sqrt5}$. در نتیجه داریم : $2^pf_p=\dfrac{(1+\sqrt5)^p-(1-\sqrt5)^p}{\sqrt5}$. حال از بسط دوجمله‌ای نیوتن استفاده کرده و اثبات را کامل کنید. $2f_p\overset{p}{\equiv}2^pf_p$.

۱۳. فرض کنید $k=\frac{p-1}{4}$. ابتدا به عنوان یک لم ساده ثابت کنید تعداد مانده‌های مربعی زوج و فرد و تعداد نامانده‌های مربعی زوج و فرد همگی برابر با k هستند. تعریف کنید :

$$\mathbb{A}=\{a^2\mid 1\le a\le \frac{p-1}{2}, 2\mid a\}, \mathbb{B}=\{a^2\mid 1\le a\le\frac{p-1}{2}, 2\nmid a\}$$

$$\mathbb{C}=\{a\mid 1\le a\le p-1, a\not\in\mathbb{A}\cup\mathbb{B}, 2\mid a\}, \mathbb{D}=\{a\mid 1\le a\le p-1, a\not\in \mathbb{A}\cup\mathbb{B}, 2\nmid a\}$$

در این صورت ادعا می‌کنیم مجموعه‌های $\mathbb{B}\cup\mathbb{C}, \mathbb{A}\cup\mathbb{D}$ در تمامی شرایط مسئله صادقند. برای اثبات، دقت کنید مجموعه $\{2a\mid a\in\mathbb{A}\}\cup\{2a\mid a\in\mathbb{B}\}$ مجموعه تمام مانده‌های درجه دوم زوج به پیمانه p در بازه $[0,2p-1]$ هستند. از طرفی می‌دانیم مجوعه $\mathbb{A}\cup\{a+p\mid a\in\mathbb{B}\}$ نیز برابر با همین مجموعه است. در نتیجه داریم :

$$2^{2k}\prod_{a\in\mathbb{A}}a\cdot\prod_{b\in\mathbb{B}}b=\prod_{b\in\mathbb{B}}(p-b)(p+b)=\prod_{b\in\mathbb{B}}(p^2-b^2)\overset{p^3}{\equiv}\left(\prod_{b\in\mathbb{B}}b^2\right)\cdot\left(p^2\sum_{b\in\mathbb{B}}\frac{1}{b^2}-1\right)$$

در پایان نتیجه زیر را ثابت کرده و با روندی مشابه نتایج مشابهی برای مجموعه های $\mathbb{C},\mathbb{D}$ گرفته و اثبات ادعا را کامل کنید.

$$\sum b\in\mathbb{B}\frac{1}{b^2}\overset{p}{\equiv}\sum_{a\in\mathbb{A}}\frac{1}{a^2}\quad,\quad\sum_{b\in\mathbb{B}}\frac{1}{b^2}+\sum_{a\in\mathbb{A}}\frac{1}{a^2}\overset{p}{\equiv}\sum_{b\in\mathbb{B}}b^2+\sum_{a\in\mathbb{A}}a^2\overset{p}{\equiv}0$$

۱۴. ابتدا فرض کنید $z=e^{\frac{2\pi i}{p}\cdot k}$ که در آن $\gcd(k,p)=1$. حال با توجه به خواص مانده‌های مربعی، داریم : $\{\{kn\mid n\in\mathcal{A}\},\{kn\mid n\in\mathcal{B}\}\}=\{\mathcal{A},\mathcal{B}\}$.
در نتیجه می‌توانیم فرض کنیم $z=e^{\frac{2\pi i}{p}}$. حال برای نوشتن α,β به صورت سری‌های توانی، فرض کنید g یک ریشه اولیه به پیمانه p باشد. در این صورت داریم : $\{z^k\mid k\in\mathcal{A}\}=\{z^{g^{2k-1}}\mid 1\le k\le\frac{p-1}{2}\}, \{z^k\mid k\in\mathcal{B}\}=\{z^{g^{2k}}\mid 1\le k\le\frac{p-1}{2}\}$. با استفاده از اتحاد چاق و لاغر مقادیر α,β را محاسبه کنید.

۱۵. برای اثبات قسمت اول، از پیمانه کسری استفاده می‌کنیم :

$$\sum_{a=1}^{p-2}\left(\frac{a(a+1)}{p}\right)=\sum_{a=1}^{p-2}\left(\frac{\frac{a(a+1)}{a^2}}{p}\right)=\sum_{a=1}^{p-2}\left(\frac{\frac{a+1}{a}}{p}\right)=\sum_{a=1}^{p-2}\left(\frac{1+a^{-1}}{p}\right)=\sum_{a=1}^{p-2}\left(\frac{1+a}{p}\right)=\sum_{a=2}^{p-1}\left(\frac{a}{p}\right)=-1$$

برای قسمت دوم ابتدا با استفاده از ریشه اولیه ثابت کنید برای هر $k<p-1$ داریم : $p\mid 0^k+1^k+\cdots+(p-1)^k$. حال به کمک محک اویلر داریم :

$$\sum_{i=0}^{p-1}\left(\frac{i^2+a}{p}\right)=\sum_{i=0}^{p-1}(i^2+a)^{\frac{p-1}{2}}\overset{p}{\equiv}\sum_{i=0}^{p-1}i^{p-1}+pa^{\frac{p-1}{2}}\overset{p}{\equiv}p-1\overset{p}{\equiv}-1$$

در قسمت سوم، فرض کنید $aa^*\overset{p}{\equiv}1$ باشد. با ضرب $\left(\frac{a^*}{p}\right)$ در طرفین، مسئله را به حالت اول تقلیل داده و مشابه روند راه حل قسمت اول، اثبات را کامل کنید.

۱۶. برای هر $n \in \mathbb{N}$ که $\gcd(p,n)=1$، تعریف کنید $f(p,n)=\sum_{d|n}\left(\frac{d}{p}\right)$. به عنوان یک لم پرکاربرد ثابت کنید $\forall n \in \mathbb{N}, \gcd(p,n)=1 : f(p,n) \geq 0$ و حالت تساوی تنها زمانی رخ می‌دهد که $\left(\frac{q}{p}\right)=-1$ و توان q در تجزیه n فرد باشد. حال سعی کنید جمله‌ای با این خاصیت در چندجمله‌ای داده شده بیابید و اثبات را کامل کنید.

۱۷. ابتدا واضح است که $4kxy-1 \overset{4}{\equiv} 3$ و بنابراین $4kxy-1$ دارای عامل اولی به فرم $p=4k+3$ است. طبق قضیه کریسمس فرما، اگر m,n هر دو زوج باشند، چون $p \mid x^m+y^n$، نتیجه می‌شود که $p \mid x, p \mid y$. در صورتی که این ممکن نیست زیرا $\gcd(4kxy-1,x)=\gcd(4kxy-1,y)=1$. حال فرض کنید از بین m,n یکی زوج و دیگری فرد باشد. (فرضاً $2 \mid m, 2 \nmid n$) در این صورت داریم : $\left(\frac{-y}{4kxy-1}\right)=1 \implies 4kxy-1 \mid (x^{\frac{m}{2}})^2+y(y^{\frac{n-1}{2}})^2$. اما اگر y فرد باشد، طبق قانون تقابل درجه دوم داریم : $\left(\frac{-y}{4kxy-1}\right)=\left(\frac{-1}{4kxy-1}\right)\cdot\left(\frac{y}{4kxy-1}\right)=(-1)\cdot(-1)^{\frac{y-1}{2}\cdot\frac{(4kxy-1)-1}{2}}\cdot\left(\frac{-1}{y}\right)=(-1)\cdot(-1)^{\frac{y-1}{2}}\cdot\left(\frac{-1}{y}\right)$. اما عبارت آخر طبق محک اویلر برابر با -1 است که تناقض است. حال فرض کنید $y=2^st$ عددی زوج باشد. $(t \geq 1)$ در این صورت طبق روابط مانده‌های مربعی و نماد لژاندر $\left(\frac{-y}{4kxy-1}\right)=\left(\frac{2}{4kxy-1}\right)^s\cdot\left(\frac{-t}{4kxy-1}\right)$. مشابه حالت قبل، از این رابطه نیز به تناقض برسید. در نهایت فرض کنید m,n هر دو اعدادی فرد باشند. ثابت کنید $\left(\frac{-1}{4kxy-1}\right)=1$ و از این رابطه نیز به تناقض رسیده و اثبات را کامل کنید.

تمرینات اضافه

۱. مجدداً با مشاهدات اولیه حل را آغاز می‌کنیم. با استفاده از قضیه فرما می‌توان نتیجه گرفت : (حالات خاص را بررسی کنید)

$$x^p \overset{p}{\equiv} x, 2^p \overset{2}{\equiv} 2 \implies x+2 \overset{p}{\equiv} x^p+2^p=p^2+y^2 \overset{p}{\equiv} y^2 \implies \left(\frac{x+2}{p}\right)=1$$

از طرف دیگر بدیهیست که x,y غیر هم زوجیتند. حالت فرد بودن y را رد کنید. در حالتی که y مقداری زوج است، ثابت کنید $x \overset{4}{\equiv} 1$. در نتیجه $x+2 \overset{4}{\equiv} 3$. با استفاده از این نتیجه داریم : $\exists q \in \mathbb{P} : q \mid x+2, q \overset{4}{\equiv} 3$. در نتیجه داریم : $q \mid x+2 \mid p^2+y^2$. از قضیه کریسمس فرما نتیجه می‌شود $q \mid p, q \mid y$ که تناقض است.

۲. ابتدا فرض کنید $p \in \mathbb{P}$ عددی اول و دلخواه باشد. طبق شرط اول مسئله، مقدار طبیعی $a \in \mathbb{N}$ موجود است که $g(a)=p$. حال در شرط دوم مسئله قرار می‌دهیم $n=a$. بنابراین $2f(a)^2=a^2+p^2$. با در نظر گرفتن دو طرف این رابطه به پیمانه p داریم : $2f(a)^2 \overset{p}{\equiv} a^2$. در نتیجه اگر $\gcd(f(a),p)=1$، آنگاه می‌توان نتیجه گرفت $\left(\frac{2}{p}\right)=1$. مقدار p را طوری انتخاب کنید که این شرط برقرار نباشد. (طبق خواص مانده‌های مربعی، کافیست مقادیر $p=8k+3$ را در نظر بگیریم) در نتیجه اگر p به فرم $8k+3$ باشد، آنگاه $p \mid a \implies p \mid f(a)$. فرض کنید $f(a)=\alpha p, a=\beta p$. در این صورت طبق شرط سوم مسئله، $\mid (\alpha-\beta)p \mid \leq 2004\sqrt{\beta p}$. از طرفی از شرط دوم مسئله داریم : $2p^2\alpha^2=p^2\beta^2+p^2 \implies 2\alpha^2=\beta^2+1 \implies \left|\left(\sqrt{\frac{\beta^2+1}{2}}-\beta\right)\sqrt{p}\right|=\left(\beta-\sqrt{\frac{\beta^2+1}{2}}\right)\sqrt{p} \leq 2004\sqrt{\beta}$. اما این معادل با این است که $\frac{2004}{\sqrt{p}} \leq \sqrt{\frac{\beta^2+1}{2\beta}}-\sqrt{\beta}$ و نتیجه بگیرید برای p به اندازه کافی بزرگ، $\beta=1$ و اثبات را کامل کنید.

۳. با ضرب دو طرف در $\left(\frac{4a}{p}\right)=\left(\frac{a}{p}\right)$ داریم : $\sum_{i=0}^{p-1}\left(\frac{(2ai+b)^2-(b^2-4ac)}{p}\right)=\sum_{i=0}^{p-1}\left(\frac{4a^2i^2+4abi+4ac}{p}\right)$. حال توجه کنید اعداد به فرم $2ai+b$ تمام دستگاه کامل مانده‌ها به پیمانه p را پوشش می‌دهند و اثبات را با استفاده از مسئله ۱۶ کامل کنید.

به عنوان یک تعمیم قوی، ثابت کنید اگر $f \in \mathbb{Z}[x]$ یک چندجمله‌ای از درجه k باشد و همچنین $f(x)^{\frac{p-1}{2}}=a_0+a_1x+\cdots+a_{\frac{p-1}{2}k}x^{\frac{p-1}{2}k}$ آنگاه :

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right) \overset{p}{\equiv} -\left(a_{p-1}+a_{2(p-1)}+\cdots+a_{\lfloor\frac{k}{2}\rfloor(p-1)}\right)$$

۴. با یک رویکرد شمارشی داریم : $\left|\left\{n \mid \left(\frac{n}{p}\right)=1, \left(\frac{n+1}{p}\right)=-1\right\}\right|=\frac{-1}{4}\sum_{i=0}^{p-1}\left(\frac{i}{p}+1\right)\cdot\left(\frac{i+1}{p}-1\right)$. این مجموع را با اتحادهای ارائه شده به دست آورید.

۵. ابتدا دقت کنید کافیست ثابت کنیم $K(p,a)^2+K(p,b)^2=4p$. (چرا؟) حال به عنوان یک لم ساده ثابت کنید :

$$\frac{p-1}{2}\left(K(p,a)^2+K(p,b)^2\right)=\sum_{n=1}^{p-1}K(p,n)^2=\sum_{n=0}^{p-1}K(p,n)^2=\sum_{n=0}^{p-1}\left(\sum_{0\leq x,y\leq p-1}\left(\frac{xy(x^2+n)(y^2+n)}{p}\right)\right)$$

$$=\sum_{0\leq x,y\leq p-1}\left(\frac{xy}{p}\right)\sum_{n=0}^{p-1}\left(\frac{(n+x^2)(n+y^2)}{p}\right)$$

با استفاده از مسئله قبل، مجموع اخیر را محاسبه کرده و با تکمیل جزئیات اثبات را کامل کنید. حکم را مشابه مسئله قبل به چندجمله‌ای های دیگر تعمیم دهید.