# به نام خدا

## مجموعه تمارین نظریه اعداد جلسه هشتم دوره تابستانی المپیاد ریاضی ۱۴۰۱

### مبحث مانده و نامانده‌های مربعی و قضیه تقابل درجه دوم

۱. فرض کنید $p > 5$ عددی اول و $A = \{b_1, b_2, ..., b_{\frac{p-1}{2}}\}$ مجموعهٔ تمام مانده‌های مربعی به پیمانه‌ی $p$ باشد. ثابت کنید هیچ $a, c$ طبیعی با شرط $(ac, p) = 1$ وجود ندارد به طوری که مجموعه‌های $B = \left\{ab_1 + c, ab_2 + c, \cdots, ab_{\frac{p-1}{2}} + c\right\}$ و $A$ به پیمانهٔ $p$ اشتراک نداشته باشند.

۲. اعداد $p \in \mathbb{P}, r \in \mathbb{N}$ داده شده‌اند، به طوری که $p \mid r^7 - 1$ و $r + 1, r^2 + 1$ به پیمانه $p$ مانده درجه دوم‌اند. ثابت کنید $r^3 + 1$ نیز به پیمانه $p$ مانده درجه دوم است.

۳. برای هر $p \in \mathbb{P}, n \in \mathbb{N}$ ثابت کنید دقیقاً $\lfloor \frac{p^{n+1}-1}{2(p+1)} \rfloor + 1$ مانده‌ی مربعی به پیمانه $p^n$ وجود دارد.

۴. فرض کنید $n \in \mathbb{N}$ داده شده است به طوری که برای هر $p$ به اندازه کافی بزرگ، $\left(\frac{n}{p}\right) = 1$. ثابت کنید $n$ مربع کامل عددی طبیعی‌ست.

۵. برای هر $p \in \mathbb{P}$ اول و فرد ثابت کنید کوچکترین نامانده‌ی درجه دوم مثبت به پیمانه $p$ از $\sqrt{p} + \frac{1}{2}$ کوچکتر است.

۶. فرض کنید $p \in \mathbb{P}$ عددی اول به فرم $3k + 1$ باشد. ثابت کنید $a, b \in \mathbb{Z}$ موجودند به طوری که $p = a^2 - ab + b^2$.

۷. فرض کنید $4k + 3 = p \in \mathbb{P}$ داده شده باشد و $m$ تعداد مانده‌های درجه دوم به پیمانه $p$ است که از $\frac{p}{2}$ کوچکتر باشند. ثابت کنید $2 \cdot 4 \cdots (p-1) \overset{p}{\equiv} (-1)^{m+k}$

۸. فرض کنید $a, b, m, n \in \mathbb{N}$ داده شده باشند به طوری که $a^n \overset{m}{\equiv} -1, b^n \overset{m}{\equiv} -1$. ثابت کنید $c \in \mathbb{N}$ موجود است به طوری که $ab \overset{m}{\equiv} c^2$.

۹. فرض کنید $p \in \mathbb{P}$ داده شده باشد. ثابت کنید برای هر $k \in \mathbb{N}$، مقدار طبیعی $n$ موجود است به طوری که $\left(\frac{n}{p}\right) = \left(\frac{n+k}{p}\right)$.

۱۰. فرض کنید $m, n \in \mathbb{N}$ مفروض باشند به طوری که $\gcd(m, n) = 1$. ثابت کنید $\varphi(5^m - 1) \neq 5^n - 1$.

۱۱. فرض کنید $p \in \mathbb{P}$ عددی اول، بزرگتر از ۱۳ و به فرم $8k + 5$ بوده و همچنین ۳۹ به پیمانه $p$ یک نامانده درجه دوم باشد. ثابت کنید $x_1, x_2, x_3, x_4 \in \mathbb{N}$ موجود است به طوری که $p \mid {x_1}^4 + {x_2}^4 + {x_3}^4 + {x_4}^4 \quad , \quad p \nmid x_1x_2x_3x_4$.

۱۲. برای هر $n \in \mathbb{N}$ ثابت کنید $2^{3^n} + 1$ حداقل $n$ عامل اول به فرم $8k + 3$ دارد.

۱۳. فرض کنید $f_n$ برابر جمله $n$اُم دنباله فیبوناتچی باشد. ثابت کنید اگر $p \in \mathbb{P}$ عددی اول و بزرگتر از ۵ باشد، آنگاه $f_p \overset{p}{\equiv} \left(\frac{p}{5}\right)$.

۱۴. برای هر $8k + 1 = p \in \mathbb{P}$ ثابت کنید دستگاه مخفف مانده‌ها به پیمانه $p$ قابل افراز به دو مجموعه $\mathcal{A}, \mathcal{B}$ با تعداد اعضای برابر است به طوری که $\prod\limits_{a \in \mathcal{A}} a \overset{p^3}{\equiv} \prod\limits_{b \in \mathcal{B}} b$.

۱۵. فرض کنید $p \in \mathbb{P}$ عددی اول و $z \in \mathbb{C}$ یک ریشه $p$اُم اولیه واحد باشد. فرض کنید $\mathcal{A}, \mathcal{B}$ به ترتیب مجموعه‌ی مانده‌ها و نامانده‌های درجه دوم به پیمانه $p$ باشند. همچنین تعریف کنید $\alpha = \sum\limits_{k \in \mathcal{A}} z^k, \beta = \sum\limits_{k \in \mathcal{B}} z^k$. ثابت کنید $\alpha, \beta$ ریشه‌های معادله $x^2 + x + \frac{1 - p \cdot \left(\frac{-1}{p}\right)}{4} = 0$ هستند.

۱۶. اتحاد های زیر را درباره نماد لژاندر اثبات کنید :

(آ) $$\sum_{i=1}^{p-1} \left(\frac{i^2 + i}{p}\right) = -1 \implies p \in \mathbb{P} \quad , p \neq 2$$

(ب) $$\sum_{i=0}^{p-1} \left(\frac{i^2 + a}{p}\right) = -1 \implies \gcd(p, a) = 1 \quad , p \neq 2 \quad , a \in \mathbb{Z} \quad , p \in \mathbb{P}$$

(ج) $$\sum_{i=1}^{p-1} \left(\frac{ai^2 + bi}{p}\right) = -\left(\frac{a}{p}\right) \implies \gcd(a, p) = \gcd(b, p) = 1 \quad , p \neq 2 \quad , p \in \mathbb{P} \quad , a, b \in \mathbb{Z}$$

۱۷. فرض کنید $\Omega(x)$ چندجمله‌ای با ضرایب صحیح باشد به طوری که $\lim\limits_{x \to \infty} \Omega(x) = +\infty$. اگر $\Omega(0) \neq 0$ و $\Omega(3) \overset{4}{\equiv} 3$، ثابت کنید عدد اول فرد $p$ وجود دارد به طوری که $\Omega(p) \neq 0$ و بین مقسوم‌علیه‌های $\Omega(p)$ تعداد یکسانی مانده و نامانده درجه دوم به پیمانه $p$ وجود داشته باشد.

۱۸. فرض کنید $x, y, k, m, n \in \mathbb{N}$ داده شده باشند. ثابت کنید $4kxy - 1 \nmid x^m + y^n$

تمارین اضافه

۱. فرض کنید $4k+1=p\in\mathbb{P}$ داده شده باشد. ثابت کنید معادله $x^p+2^p=p^2+y^2$ در اعداد طبیعی جوابی ندارد.

۲. فرض کنید $f,g:\mathbb{N}\to\mathbb{N}$ توابعی با خواص زیر باشند :

(آ) $g$ روی اعداد طبیعی پوشاست.

(ب) برای هر $n\in\mathbb{N}$ داریم : $2f(n)^2=n^2+g(n)^2$.

(ج) برای هر $n\in\mathbb{N}$ داریم : $\mid f(n)-n\mid\leq 2004\sqrt{n}$.

ثابت کنید نامتناهی $n\in\mathbb{N}$ موجود است به طوری که $f(n)=n$.

۳. (اتحاد بسیار مهم) به عنوان تعمیم سوال ۱۶، فرض کنید $a,b,c\in\mathbb{Z}$ و $p\in\mathbb{P}$ عددی اول باشد به طوری که $p\nmid a$. ثابت کنید :

$$\sum_{i=0}^{p-1}\left(\frac{ai^2+bi+c}{p}\right)=\begin{cases}(p-1)\left(\frac{a}{p}\right) & \text{if}\quad p\mid b^2-4ac\\ -\left(\frac{a}{p}\right) & \text{if}\quad p\nmid b^2-4ac\end{cases}$$

۴. برای هر $p\in\mathbb{P}$ ثابت کنید تعداد زوج‌های متوالی از مجموعه $\{1,\cdots,p-1\}$ به طوری که به ترتیب مانده و نامانده درجه دوم به پیمانه $p$ باشد، برابر است با $\frac{p-(-1)^{\frac{p-1}{2}}}{4}$.

۵. (اختیاری) برای هر $p\in\mathbb{P},a\in\mathbb{Z}$ تعریف کنید $K(p,a)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+a)}{p}\right)$. فرض کنید $4k+1=p\in\mathbb{P}$ و $a,b\in\mathbb{Z}$ داده شده باشند به طوری که $a,b$ به ترتیب مانده و نامانده درجه دوم به پیمانه $p$ باشند. آنگاه ثابت کنید $K(p,a),K(p,b)$ اعدادی زوج هستند به طوری که :

$$K(p,a)^2+K(p,b)^2=4p$$