حل مسایل امتحان میان ترم اول نظریه اعداد

(۴) چون n غیراول است، پس عامل اولی مانند p دارد که $p \le \sqrt{n}$. گیریم $p_1, \dots, p_t$ دیگر عوامل اول n باشند، (در صورت وجود). واضح است که داریم:

$\frac{p}{p-1} \le (\frac{p}{p-1})(\frac{p}{p_1-1}) \cdots (\frac{p}{p_t-1})$ پس $\varphi(n) \le n(1-\frac{1}{p}) \le n(1-\frac{1}{\sqrt{n}}) = n - \sqrt{n}$. ■

(۵) الف. ($\Rightarrow$) فرض کنید x ی باشد که $x^4 \overset{p}{\equiv} -1$ پس $(x^2)^2 \overset{p}{\equiv} -1$ ولذا $p \overset{?}{\equiv} 1$. از طرفی $(x,p)=1$، پس $x^{p-1} \overset{p}{\equiv} 1$ یا $(x^4)^{\frac{p-1}{4}} \overset{p}{\equiv} 1$ یا $(-1)^{\frac{p-1}{4}} \overset{p}{\equiv} 1$. پس $\frac{p-1}{4}$ زوج است ولذا $p \overset{?}{\equiv} 1$. ■

($\Leftarrow$) اگر $p \overset{?}{\equiv} 1$ در اینصورت $4 = (4, p-1) = S$. اما $\frac{p-1}{4}$ زوج است، پس $1 \overset{p}{\equiv} (-1)^{\frac{p-1}{4}}$ ولذا بنابر محک اویلر $-1 \overset{p}{\equiv} x^4$ جواب دارد. ■

ب. فرض کنید این مجموعه متناهی باشد، $p_1, \dots, p_t$ تمام اعداد اول به شکل $8k+1$. قرار دهید: $N = (2p_1 \cdots p_t)^4 + 1$. N عددی فرد و بزرگتر از ۱ می باشد، پس p اول و فرد موجود است که $N \overset{p}{\equiv} 0$ یا $-1 \overset{p}{\equiv} (2p_1 \cdots p_t)^4$ لذا $p \overset{?}{\equiv} 1$ پس $p = p_i$ برای یک $i \le t$. در نتیجه $-1 \overset{p}{\equiv} 0$ که تناقض است. ■

(۶) توجه کنید که $1125 = 3^2 \times 5^3$. الف: حل $x^3 - 3x^2 + 27 \overset{3}{\equiv} 0$. بنابر نتیجه قضیه فرما بدست می آوریم $x \overset{3}{\equiv} 0$.

ب: حل $x^3 - 3x^2 + 27 \overset{3^2}{\equiv} 0$. بنابر قضیه خوانده شده جواب بصورت $x = 0 + 3k$ است که در آن k از رابطه $f'(0)k \overset{3}{\equiv} -\frac{f(0)}{3}$ بدست می آید. پس $-9k \overset{3}{\equiv} 0$ ولذا k دلخواه می تواند باشد. پس $x = 3k$ جواب معادله افراز و جوابهای تمایز عبارتند از: $x \overset{3^2}{\equiv} 0, 3, 6$.

ج: حل $x^3 - 3x^2 + 27 \overset{5}{\equiv} 0$. با بررسی در یک دستگاه کامل مانده ها به هنگ ۵ جوابهای تمایز را بدست می آوریم: $x \overset{5}{\equiv} 1$.

د: حل $x^3 - 3x^2 + 27 \overset{5^2}{\equiv} 0$. $f(x) = x^3 - 3x^2 + 27$. بنابر قضیه خوانده شده جواب بصورت $x = 1 + 5k$ است که در آن k از رابطه $f'(1)k \overset{5}{\equiv} -\frac{f(1)}{5}$ بدست می آید. پس $3k \overset{5}{\equiv} -1$ ولذا $k \overset{5}{\equiv} 2$ یا $k = 5t + 2$. پس $x = 11 + 5^2 t$ جواب معادله افراز و جوابهای تمایز بدست می آیند: $x \overset{5^2}{\equiv} 1$.

ه: حل $x^3 - 3x^2 + 27 \overset{5^3}{\equiv} 0$. بنابر قضیه خوانده شده جواب بصورت $x = 1 + 5^2 k$ است که در آن k از رابطه $f'(1)k \overset{5}{\equiv} -\frac{f(1)}{5^2}$ بدست می آید. پس $-3k \overset{5}{\equiv} -1$ ولذا $K \overset{5}{\equiv} 2$ یا $k = 5t + 2$. پس $x = 51 + 5^3 t$ جواب معادله افراز است ولذا $x \overset{5^4}{\equiv} 51$ جواب این حالت می باشد.

$$x^3 - 3x^2 + 27 \overset{1125}{\equiv} 0 \iff x^3 - 3x^2 + 27 \overset{3^2 \times 5^3}{\equiv} 0$$

$$\iff \begin{cases} x^3 - 3x^2 + 27 \overset{3^2}{\equiv} 0 \\ x^3 - 3x^2 + 27 \overset{5^3}{\equiv} 0 \end{cases} \iff \begin{cases} x \overset{9}{\equiv} 0 \\ x \overset{125}{\equiv} 51 \end{cases} \text{ یا } \begin{cases} x \overset{9}{\equiv} 3 \\ x \overset{125}{\equiv} 51 \end{cases} \text{ یا } \begin{cases} x \overset{9}{\equiv} 6 \\ x \overset{125}{\equiv} 51 \end{cases}$$

برای حل این دستگاه ها از قضیه باقیمانده چینی استفاده می کنیم: $m_1 = 9, m_2 = 125$

داریم: $M = 9 \times 125 = 1125$ ، $M_1 = 125, M_2 = 9$. همچنین $M_1^* = -1$، $M_2^* = 14$ ولذا جوابهای زیر به ترتیب جوابهای ۳ دستگاه بالا می باشند که این جوابها به هنگ $M = 1125$ نهایتاً می باشند:

$$x = (125)(-1)(0) + (9)(14)(51) \overset{1125}{\equiv} 801$$

$$x = (125)(-1)(3) + (9)(14)(51) \overset{1125}{\equiv} 426$$

$$x = (125)(-1)(6) + (9)(14)(51) \overset{1125}{\equiv} 51$$

پس جوابهای تمایز معادله هندسی داده شده $x = 51$، $x = 426$، $x = 801$ می باشد. ■

(۷) چون $\operatorname{ord}_p a = 3$، پس $(a,p)=1$، $a \overset{p}{\not\equiv} 1$، $a^2 \overset{p}{\not\equiv} 1$ و $a^3 \overset{p}{\equiv} 1$. پس $a^3 - 1 \overset{p}{\equiv} 0$ یا $(a-1)(a^2+a+1) \overset{p}{\equiv} 0$. چون $a \overset{p}{\not\equiv} 1$ پس $a^2 + a + 1 \overset{p}{\equiv} 0$ و یا $(a+1)^2 \overset{p}{\equiv} a$ ولذا $(a+1)^6 \overset{p}{\equiv} 1$. پس $(a+1,p)=1$؛ یعنی $\operatorname{ord}_p(a+1)$ معنی دارد و $\operatorname{ord}_p(a+1) \mid 6$. در نتیجه $\operatorname{ord}_p(a+1) = 1$ یا ۲ یا ۳ یا ۶. اگر $\operatorname{ord}_p(a+1) = 1$ آنگاه $a+1 \overset{p}{\equiv} 1$ یا $a \overset{p}{\equiv} 0$ که تناقض است.

اگر $ord_p(a+1)=2$ آنگاه $(a+1)^2 \overset{p}{\equiv} 1$ یا $a \overset{p}{\equiv} 1$ که تناقض است.

اگر $ord_p(a+1)=3$ آنگاه $(a+1)^3 \overset{p}{\equiv} 1$ یا $(a+1)(a+1)^2 \overset{p}{\equiv} 1$

یا $(a+1)a \overset{p}{\equiv} 1$ یا $a^2+a \overset{p}{\equiv} 1$ یا $-1 \overset{p}{\equiv} 1$ که تناقض است.

پس لزوماً $ord_p(a+1)=6$. ■

(۸) ثابت می‌کنیم:

$$ord_p(-g) = \begin{cases} p-1 & : p \overset{4}{\equiv} 1 \\ \frac{p-1}{2} & : p \overset{4}{\equiv} 3 \end{cases}$$

الف: $p \overset{4}{\equiv} 1$.

چون g ریشه اولیه به هنگ p است، پس $(g,p)=1$ و لذا $(-g,p)=1$

در نتیجه $(-g)^{p-1} \overset{p}{\equiv} 1$. حال گیریم $(-g)^t \overset{p}{\equiv} 1$. لذا داریم:

$g^{2t} \overset{p}{\equiv} 1$ ، پس $(-1)^t g^t \overset{p}{\equiv} 1$ ، لذا $ord_p g \mid 2t$

یا $p-1 \mid 2t$ یا $\frac{p-1}{2} \mid t$. چون $p \overset{4}{\equiv} 1$، پس

$\frac{p-1}{2}$ زوج است و لذا t نیز زوج خواهد بود، یعنی $(-1)^t = 1$

پس $g^t \overset{p}{\equiv} 1$ و لذا $t \geq p-1$. پس $ord_p(-g) = p-1$.

ب: $p \overset{4}{\equiv} 3$.

چون g ریشه اولیه به هنگ p است، پس $ord_p g = p-1$. یعنی

$g^{p-1} \overset{p}{\equiv} 1$ یا $0 \overset{p}{\equiv} 1-(g^{\frac{p-1}{2}})^2$ یا $0 \overset{p}{\equiv} (g^{\frac{p-1}{2}}+1)(g^{\frac{p-1}{2}}-1)$

اما $g^{\frac{p-1}{2}} - 1 \overset{p}{\neq} 0$ پس $g^{\frac{p-1}{2}} \overset{p}{\equiv} -1$. چون $p \overset{4}{\equiv} 3$

پس $\frac{p-1}{2}$ فرد است و لذا داریم: $(-g)^{\frac{p-1}{2}} \overset{p}{\equiv} 1$.

حال گیریم $(-g)^t \overset{p}{\equiv} 1$، لذا $g^{2t} \overset{p}{\equiv} 1$ پس $ord_p g \mid 2t$

یا $p-1 \mid 2t$ یا $\frac{p-1}{2} \mid t$ پس $t \geq \frac{p-1}{2}$.

لذا $ord_p(-g) = \frac{p-1}{2}$.

حال واضح است که $-g$ یک ریشه اولیه به هنگ p است اگر و فقط

اگر $ord_p(-g) = p-1$ اگر و فقط اگر $p \overset{4}{\equiv} 1$. ■