دانشگاه صنعتی شریف
دانشکده علوم ریاضی

حل مسائل امتحان میان ترم اول نظریه اعداد

۲۲-۲۱۵

۵. $f(x)=x^4+2x+36$ ، $f'(x)=4x^3+2$

I) حل معادلهٔ $f(x)\overset{5}{\equiv}0$

اگر x جواب باشد، سپس $x^4\overset{5}{\equiv}1$ ، پس $f(x)\overset{5}{\equiv}1$ ولذا

$1+2x+36\overset{5}{\equiv}0 \Rightarrow 2x\overset{5}{\equiv}3 \Rightarrow x\overset{5}{\equiv}4$

پس $x=4$ تنها جواب این قسمت است.

II) حل معادلهٔ $f(x)\overset{5^2}{\equiv}0$

جواب بصورت $x=4+5k$ است که در آن k از رابطهٔ $f'(4)k\overset{5}{\equiv}-\frac{f(4)}{5}$ بدست می‌آید.

$$25\wedge k\overset{5}{\equiv}-60 \Rightarrow 3k\overset{5}{\equiv}0 \Rightarrow k\overset{5}{\equiv}0 \Rightarrow k=5t$$

پس $x=4+5^2t$ یا $x\overset{5^2}{\equiv}4$.

یعنی $x=4$ تنها جواب این قسمت است.

III) حل معادلهٔ $f(x)\overset{5^3}{\equiv}0$

جواب بصورت $x=4+5^2k$ است که در آن k از رابطهٔ $f'(4)k\overset{5}{\equiv}-\frac{f(4)}{5^2}$ بدست می‌آید.

$$25\wedge k\overset{5}{\equiv}-12 \Rightarrow 8k\overset{5}{\equiv}3 \Rightarrow k\overset{5}{\equiv}1 \Rightarrow k=1+5t$$

پس $x=29+5^3t$ یا $x\overset{5^3}{\equiv}29$.

یعنی $x=29$ تنها جواب این قسمت است.

IV) حل معادلهٔ $f(x)\overset{7}{\equiv}0$

با بررسی در دستگاه کامل مانده‌ها به هنگ ۷: $\{0,\pm1,\pm2,\pm3\}$

جوابهای این قسمت $x\overset{7}{\equiv}-1$ ، $x\overset{7}{\equiv}2$ بدست می‌آیند.

V) حل معادلهٔ $f(x)\overset{175}{\equiv}0$

$$f(x)\overset{175}{\equiv}0 \Rightarrow \begin{cases} f(x)\overset{5^3}{\equiv}0 \\ f(x)\overset{7}{\equiv}0 \end{cases} \Rightarrow \begin{cases} x\overset{5^3}{\equiv}29 \\ x\overset{7}{\equiv}2 \text{ یا } x\overset{7}{\equiv}-1 \end{cases}$$

$$(A):\begin{cases} x\overset{125}{\equiv}29 \\ x\overset{7}{\equiv}-1 \end{cases} \qquad (B):\begin{cases} x\overset{125}{\equiv}29 \\ x\overset{7}{\equiv}2 \end{cases}$$

$M=125\times7=875$

$M_1=7$ $\qquad M_2=125$

$M_1^*=18$ $\qquad M_2^*=-1$

جواب A: $x=18\times7\times29+125(-1)(-1)=4779\overset{875}{\equiv}279$

جواب B: $x=18\times7\times29+125(-1)(2)=3406\overset{875}{\equiv}779$

پس $x=279$ ، $x=779$ جوابهای معادلهٔ داده شده است. □

۶. مسأله را به استقرای روی n ثابت می‌کنیم. برای $n=4$ داریم: $p_4<p_1p_2p_3$ یا $5+6+2>7$ که برقرار است. فرض کنید حکم برای n درست باشد، طبق اصل برتراند بین عدد اول q موجود است که $p_n<q<2p_n$؛ پس $p_{n+1}<2p_n=p_n+p_n<p_1+\cdots+p_{n-1}+p_n$ یا بنابر فرض استقرا که حکم به ازای $n+1$ است. پس مسأله بنابر قضیه استقرای ریاضی برای $n\geq4$ برقرار است. □

۷. فرض کنید تعداد این اعداد متناهی باشد. آنها را فهرست کنید: $p_1, p_2, \ldots, p_t$. بگیرید $N=(2p_1\cdots p_t)^2+1$ که عدد فرد و بزرگتر از یک است، پس یک عامل اول فرد مانند p دارد پس $N\overset{p}{\equiv}0$ یا $(2p_1\cdots p_t)^2\overset{p}{\equiv}-1$؛ پس بنابر قضیه فرموده شده p به شکل $4k+1$ است؛ پس $p=p_i$ برای یک $1\leq i\leq t$. در نتیجه $1\overset{p_i}{\equiv}(2p_1\cdots p_t)^2$ یا $1\overset{p_i}{\equiv}-1$ که تناقض است. پس تعداد این اعداد نامتناهی است. □

دانشگاه صنعتی شریف
دانشکده علوم ریاضی

۸. $a^n \overset{a^n-1}{\equiv} 1$ برای $K<n$ ؛ باتوجه به اینکه $a^{K-1} < a^n-1$ پس $a^{K-1} \overset{a^n-1}{\not\equiv} 0$ یا $a^K \overset{a^n-1}{\not\equiv} 1$.
پس $\underset{a^n-1}{ord}\, a = n$ و بنابر قضیه خوانده شده $n \mid \varphi(a^n-1)$.
□

۹. g ریشه اولیه به هنگ p^2 است ؛ پس $\underset{p^2}{ord}\, g = \varphi(p^2) = p(p-1)$
$(g,p^2)=1 \Rightarrow (g,p)=1 \Rightarrow g^{p-1} \overset{p}{\equiv} 1$
حال فرض کنید $g^K \overset{p}{\equiv} 1$ پس $g^K = 1+tp$ در نتیجه
$g^{Kp} \overset{p^2}{\equiv} 1$ پس ؛ $g^{Kp} = (1+tp)^p = 1+t'p^2$
ولذا $Kp \geq p(p-1)$ یا $K \geq p-1$ ؛ در نتیجه
$\underset{p}{ord}\, g = p-1 = \varphi(p)$ ؛ یعنی g ریشه اولیه به هنگ p است.
□

۱۰. فرض کنید $a \overset{p}{\not\equiv} 0$ در اینصورت $(a,p)=1$ ولذا a^* وجود دارد که $aa^* \overset{p}{\equiv} 1$. پس $a^{*2}a^2 + a^{*2}b^2 \overset{p}{\equiv} 0$ یا $(a^*b)^2 \overset{p}{\equiv} -1$ ولذا بنابر قضیه خوانده شده p به شکل $4k+1$ است که تناقض است. پس $a \overset{p}{\equiv} 0$ و در نتیجه $b \overset{p}{\equiv} 0$.
□