PROBLEM I Find the solution of $6x^3+27x^2+17x+20\equiv 0 \pmod{30}$.

SOLUTION. Easily $30=2\times 3\times 5$, so we consider three equations:

$$\begin{cases} 6x^3+27x^2+17x+20\equiv 0 \mod 2 \\ 6x^3+27x^2+17x+20\equiv 0 \mod 3 \\ 6x^3+27x^2+17x+20\equiv 0 \mod 5 \end{cases}$$

The first equation is always true, because $6x^3+27x^2+17x+20\equiv x^2+x\equiv 0 \mod 2$. The second equation is equivalent to $2x+2\equiv 0 \mod 3$. Solve it and get $x\equiv 2 \mod 3$. The last equation is equivalent to $x^3+2x^2+2x=x(x^2+2x+2)\equiv 0 \mod 5$. Easy to get that $x\equiv 0,1,2 \mod 5$. So finally we get that $x\equiv 2,20,26 \mod 30$. $\square$

PROBLEM II Find the solution of $31x^4+57x^3+96x+191\equiv 0 \pmod{225}$.

SOLUTION. Easy to get that $225=3^2\times 5^2$. So the equation is equivalent to

$$\begin{cases} 4x^4+3x^3+6x+2\equiv 0 \mod 9 \\ 6x^4+7x^3-4x-9\equiv 0 \mod 25 \end{cases}$$

First we consider $4x^4+3x^3+6x+2\equiv 0 \mod 3$. Easy to get $x\equiv 1,2 \mod 3$. If $x\equiv 1 \mod 3$, assume $x\equiv 1+3k \mod 9$, then $(4+3+6+2)+16\times 3k+9\times 3k+6\times 3k\equiv 0 \mod 9$, then $2+k\equiv 0 \mod 3$, so $x\equiv 4 \mod 9$. If $x\equiv 2 \mod 3$, then for the same reason we get $(4\times 2^4+3\times 2^3+6\times 2+2)+(-16+9+6)\times 3k\equiv 0 \mod 9$, thus $x\equiv 5 \mod 9$. So $x\equiv 4,5 \mod 9$.

Second we consider $6x^4+7x^3-4x-9\equiv 0 \mod 5$. Obviously $x\not\equiv 0 \mod 5$, so $x^4\equiv 1 \mod 5$. So $2x^3+x-3\equiv 0 \mod 5$, i.e., $(x-1)(2x^2+2x+3)\equiv 0 \mod 5$. Then $x\equiv 1 \mod 5$ or $2x^2+2x+3\equiv 0 \mod 5$. Noting $2x^2+2x+3\equiv (x-2)(2x+6) \mod 5$, so we finally get $x\equiv 1,2 \mod 5$. Use the same method as above, we can get that $x\equiv 1,22 \mod 25$

Finally, we consider

$$\begin{cases} x\equiv 4,5 \mod 9 \\ x\equiv 1,22 \mod 25 \end{cases}$$

We obtain that $x\equiv 22,122,76,176 \mod 225$. $\square$

PROBLEM III Prove: $\forall m\in\mathbb{N}^+, \exists x,y\in\mathbb{Z}, 5x^2+11y^2\equiv 1 \pmod{m}$.

SOLUTION. Let $s=3^{16}\times\prod_{p\in\mathbb{P},5<p\leq m}p^{16}$, then easily $s\equiv 1 \mod 32$. Let $t=5$, and let

$$\begin{cases} a=11s^2-22st-5t^2 \\ b=-11s^2-10st+5t^2 \\ c=20t^2+44s^2 \end{cases}$$

Then easy to check that $5a^2+11b^2=c^2$. Easily $a\equiv 11-110-125\equiv 0 \mod 32$. Then since $32 \mid b+a=-32st$ we get $32\mid b$. Then $32^2 \mid 5a^2+11b^2=c^2$, thus $32\mid c$. Let $a_1=\frac{a}{32}, b_1=\frac{b}{32}, c_1=\frac{c}{32}$, then $5a_1^2+11b_1^2=c_1^2$. Now we will prove that $\gcd(c_1,m)=1$. If not, assume $p\in\mathbb{P}$ and $p\mid \gcd(c_1,m)$. If $p>5\vee p=3$, then since $p\mid m$ we get $p\le m$, so $p\mid s$. Since $p\mid c=20t^2+44s^2$, we get $p\mid t$, then $p=5$, contradiction! If $p=5$, then $p\mid 20t^2$, then $p\mid 44s^2$, but $5\nmid s$, contradiction! If $p=2$, then $2\mid\frac{c}{32}$, then $16\mid 5t^2+11s^2$. But easily $5t^2+11s^2\equiv 125+11\equiv 8 \mod p$, contradiction! So we get $\gcd(c_1,m)=1$. So $\exists d, c_1d\equiv 1 \mod m$. Let $x=a_1d, y=b_1d$, then $5x^2+11y^2=c^2d^2\equiv 1 \mod m$. □

PROBLEM IV If $n\mid p-1, n>1, \gcd(a,p)=1$, prove :

1. $x^n\equiv a \pmod p$ has solution $\iff a^{\frac{p-1}{n}}\equiv 1 \pmod p$.
2. If $x^n\equiv a \pmod p$ has solution, then it has n solutions.

SOLUTION . 1. "$\implies$":Since $\gcd(a,p)=1$ easily $\gcd(x,p)=1$. So $a^{\frac{p-1}{n}}\equiv x^{p-1}\equiv 1 \mod p$. "$\impliedby$": Easy to know that there is at most $\frac{p-1}{n}$ different a satisfy $\exists x, x^n\equiv a \mod p$. For every a, there is at most n different x satisfy $x^n\equiv a \mod p$. And for every x satisfy $\gcd(x,p)=1$, there is a unique a satisfy $x^n\equiv a \mod p$. So $\sum_{x,a\in\mathbb{Z}/p\mathbb{Z},x^n\equiv a,x\neq 0} 1 = \sum_{a\in\mathbb{Z}/p\mathbb{Z},a^{\frac{p-1}{n}}\equiv 1}\sum_{x\in\mathbb{Z}/p\mathbb{Z},x^n\equiv a} 1\le p-1$. But $\sum_{x,a\in\mathbb{Z}/p\mathbb{Z},x^n\equiv a,x\neq 0}1=\sum_{x\in\mathbb{Z}/p\mathbb{Z},x\neq 0}1=p-1$ So we get $\forall a: a^{\frac{p-1}{n}}\equiv 1 \mod p$, there is n different x satisfy $x^n\equiv a \mod p$.

2. Have been proved above.

□

PROBLEM V $n\in\mathbb{N}^+$, $\gcd(a,m)=1$, $x^n\equiv a \pmod m$ has a solution $x\equiv x_0 \pmod m$. Prove all the solution of $x^n\equiv a \pmod m$ have the form of $x\equiv yx_0 \pmod m$, where y is the solution of $y^n\equiv 1 \pmod m$.

SOLUTION . Easy to know $x\equiv yx_0 \mod m$ is solution of $x^n\equiv a \mod m$. Now only need to check every solution has this form. Assume $x^n\equiv a \mod m$. Easily $\gcd(x,m)=\gcd(x_0,m)=1$. Then $\exists b, bx_0\equiv 1 \mod m$. Then $x^nb^n\equiv x_0^nb^n\equiv 1 \mod m$. Let $y=xb$, then $y^n\equiv 1 \mod m$. Then $yx_0\equiv xbx_0\equiv x \mod m$. □