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

SOLUTION. By observation, we know that $x \equiv 2 \pmod{30}$ is one of the solution of $6x^3 + 27x^2 + 17x + 20 \equiv 0 \pmod{30}$. Besides, $30 = 2 \times 3 \times 5$, we consider all the solution of

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

Since $x \equiv 0 \pmod{2}, x \equiv 1 \pmod{2}$ are all the solution of $6x^3 + 27x^2 + 17x + 20 \equiv 0 \pmod{2}$, $x \equiv 2 \pmod{3}$ is all the solution of $6x^3 + 27x^2 + 17x + 20 \equiv 0 \pmod{3}$, $x \equiv 0 \pmod{5}, x \equiv 1 \pmod{5}, x \equiv 2 \pmod{5}$ are the solution of $6x^3 + 27x^2 + 17x + 20 \equiv 0 \pmod{5}$, and the solution of $6x^3 + 27x^2 + 17x + 20 \equiv 20 \pmod{5}$ are at most 3, then $x \equiv 0 \pmod{5}, x \equiv 1 \pmod{5}, x \equiv 2 \pmod{5}$ are all the solution of $6x^3+27x^2+17x+20 \equiv 0 \pmod{5}$. By Chinese Remainder Theorem, we get to know that $x \equiv \sum_{i=1}^{3} M_i' M_i a_i \pmod{30}$ are all the solution of $6x^3 + 27x^2 + 17x + 20 \equiv 0 \pmod{30}$, where $M_1 = 15, M_2 = 10, M_3 = 6, M_1' = 1, M_2' = 1, M_3 = 1, a_1 \in \{0, 1\}, a_2 = 2, a_3 \in \{0, 1, 2\}$. Therefore, $x \equiv 20 \pmod{30}, x \equiv 26 \pmod{30}, x \equiv 2 \pmod{30}, x \equiv 5 \pmod{30}, x \equiv 17 \pmod{30}, x \equiv 11 \pmod{30}$ are all the solution of $6x^3 + 27x^2 + 17x + 20 \equiv 0 \pmod{30}$. $\square$

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

SOLUTION. Since $225 = 3^2 \times 5^2$, firstly we consider $\equiv 0 \pmod{15}$.

$$\begin{cases} 31x^4 + 57x^3 + 96x + 191 & \equiv 0 \pmod{3^2} \\ 31x^4 + 57x^3 + 96x + 191 & \equiv 0 \pmod{5^2} \end{cases}$$

To find the solution of $31x^4+57x^3+96x+191 \equiv 0 \pmod{3^2}$, we consider $31x^4+57x^3+96x+191 \equiv 0 \pmod{3}$. By observation, we get to know the solution of $31x^4 + 57x^3 + 96x + 191 \equiv 0 \pmod{3}$ are $x \equiv 1, 2 \pmod{3}$. Since $f'(x) = 124x^3 + 171x^2 + 96$, $3 \nmid f'(1) = 391, 3 \nmid f'(2) = 1772$, then suppose $f(1+3k) \equiv 0 \pmod{3^2} f(2+3t) \equiv 0 \pmod{3^2}$, so $f(1) + 3kf'(1) \equiv 0 \pmod{3^2}$, $f(2) + 3kf'(2) \equiv 0 \pmod{3^2}$, then $125 + 391k \equiv 0 \mod 3, 1335 + 5316t \equiv 0 \mod 9$, then $k \equiv 1 \pmod{3}, t \equiv 1 \pmod{3}$, then $x \equiv 4, 5 \mod 9$ are the solution of $31x^4 + 57x^3 + 96x + 191 \equiv 0 \pmod{9}$.

To find the solution of $31x^4 + 57x^3 + 96x + 191 \equiv 0 \pmod{5^2}$, we consider $31x^4 + 57x^3 + 96x + 191 \equiv 0 \pmod{5}$. By observation, we get to know the solution of $31x^4 + 57x^3 + 96x + 191 \equiv 0 \pmod{3}$ are $x \equiv 1, 2 \pmod{5}$. Since $f'(x) = 124x^3 + 171x^2 + 96$, $5 \nmid f'(1) = 391, 5 \nmid f'(2) = 1772$, then suppose $f(1 + 5k) \equiv 0 \pmod{5^2} f(2 + 5t) \equiv 0 \pmod{5^2}$, so $f(1) + 5kf'(1) \equiv 0 \pmod{5^2}$, $f(2) + 5kf'(2) \equiv 0 \pmod{5^2}$, then $75 + 391k \equiv 0 \mod 5, 267 + 391t \equiv 0 \mod 5$, then $k \equiv 0 \pmod{5}, t \equiv 3 \pmod{5}$, then $x \equiv 0, 17 \mod 25$ are the solution of $31x^4+57x^3+96x+191 \equiv 0 \pmod{25}$.

By Chinese Remainder Theorem, we get to know that $x \equiv \sum_{i=1}^{2} M_i' M_i a_i \pmod{225}$, where $M_1 = 25, M_2 = 9, M_1' = 4, M_2' = 14, a_1 \in \{4, 5\}, a_2 \in \{0, 17\}$, then $x \equiv 76, 67, 50, 167 \pmod{225}$. $\square$

PROBLEM III Prove: $5x^2 + 11y^2 \equiv 1 \pmod{m}$ has solution for all $m \in \mathbb{N}$.

SOLUTION. First of all, we consider all of the intergal solution of $5x^2 + 11y^2 = z^2$. After calculating, we get $x = 11s^2 - 22st - 5t^2, y = -11s^2 - 10st + 5t^2, c = 20t^2 + 44s^2, s, t \in \mathbb{Z}$. Let $t = 5, s = 3^{16} \prod_{p \in \mathbb{P}, 5 < p \leq m} p^{16}$, then $x \equiv 11 - 110 - 125 = -224 \equiv 0 \mod 32$, $y \equiv -11 - 50 + 125 = 64 \equiv 0 \mod 32$, then $32^2 \mod z$. Let $x_1 = \frac{x}{32}, y_1 = \frac{y}{32}, z_1 = \frac{z}{32}$. If $\gcd(m, z_1) \neq 1$, then $\exists p \in \mathbb{P}$, $p \mid \gcd(m, z_1)$. If $p > 5$ or $p = 3$, then $p \leq m$, then $p \mid s$. Since $p \mid z_1 \mid z$, then $p \mid t$, then $p = 5$. Contradiction! If $p = 2$, then $2 \mid \frac{z}{32}$, then $16 \mid 5t^2 + 11s^2$. But $5t^2 + 11s^2 \equiv 125 + 11 \equiv 8 \mod 16$, Contradiction. If $p = 5$, then $5 \mid \frac{z}{32}$, then $5 \mid z$. Since $5 \mid 20t^2$, then $5 \mid 44s^2$, then $5 \mid s^2$. But obviously, $5 \mid s$. Contradiction! Thus $\gcd(m, z_1) = 1$. So $\exists w$ such that $wz_1 \equiv 1 \mod m$, then $5(wx_1)^2 + 11(wy_1)^2 = w^2z^2 \equiv 1 \mod m$. □

PROBLEM IV If $n \mid p - 1, n > 1, (a, p) = 1$, 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 solution.

SOLUTION.
1. " $\Longrightarrow$ ":Since $\gcd(a, p) = 1$, then $\gcd(x, p) = 1$. Then $a^{\frac{p-1}{n}} \equiv x^{p-1} \equiv 1 \mod p$.
2. " $\Longleftarrow$ ":

□

PROBLEM V $n \in \mathbb{N}^+$, $\gcd(a, m) = 1$, $x^n \equiv a \pmod{m}$ has one 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.
1. First, we prove that $x \equiv yx_0 \pmod{m}$ is the solution of $x^n \equiv a \pmod{m}$. Since $x_0^n \equiv a \pmod{m}$, then $(yx_0)^n = y^n x_0^n \equiv x_0^n \equiv a \pmod{m}$.
2. Second, we prove that the solution of $x^n \equiv a \pmod{m}$ have the form of $x \equiv yx_0 \pmod{m}$. Assume x is the solution of $x^n \equiv a \pmod{m}$, then $\gcd(x, m) = \gcd(x_0, m) = 1$, then $\exists b$ such that $bx_0 \equiv 1 \pmod{m}$. So $(bx_0)^n \equiv 1 \pmod{m}$. Then $b^n \equiv a^{-1} \pmod{m}$, then $(xb)^n \equiv 1 \pmod{m}$. Then $x \equiv xbx_0 \equiv (xb)x_0 \pmod{m}$. So let $y = xb$.

□