PROBLEM I Find all the solutions to $1215x \equiv 560(\mod 2755)$.

SOLUTION. To find all the solution of $1215x \equiv 560(\mod 2755)$ is equal to find all the solution of $1215x - 2755m = 560$. Since $\gcd(1215, 2755, 560) = 5$, then it is equal to prove that $243x - 551m = 112$. Since $x = \frac{112+551m}{243} = \frac{112+65m}{243} + 2m \in \mathbb{Z}$, then $x_1 = \frac{112+65m}{243} \in \mathbb{Z}$, then $m = \frac{243x_1-112}{65} = 3x_1 - 1 + \frac{48x_1-47}{65} \in \mathbb{Z}$, then $m_1 = \frac{48x_1-47}{65} \in \mathbb{Z}$, then $x_1 = m_1 + 1 + \frac{17m_1-1}{48}$, then $x_2 = \frac{17m_1-1}{48} \in \mathbb{Z}$, then $m_1 = 2x_2 + \frac{14x_2+1}{17}$, then $m_2 = \frac{14x_2-1}{17} \in \mathbb{Z}$, then $14x_2 - 17m_2 = 1$, then $x_2 = \frac{17m_2-1}{14} = m_2 + \frac{3m_2-1}{14} \in \mathbb{Z}$, then $x_3 = \frac{3m_2-1}{14} \in \mathbb{Z}$, then $m_2 = \frac{14x_3+1}{3} = \frac{2x_3+1}{3} + 4x_3 \in \mathbb{Z}$, then $m_3 = \frac{2x_3+1}{3} \in \mathbb{Z}$. Consider equation $3m_3 - 2x_3 = 1$. obviously, $x_3 = 1, m_3 = 1$ is a special solution of $3m_3 - 2x_3 = 1$. So $m_2 = 5, x_2 = 6, m_1 = 17, x_1 = 24, m = 88, x = 200$. Then the solution of $243x - 551m = 112$ have the form of $x = 200 + 551t, m = 88 + 243t, t \in \mathbb{Z}$, then the solution of $1215x - 2755m = 560$ have the form of $x = 1000 + 2755t, m = 440 + 1215t, t \in \mathbb{Z}$. Thus, the solution of $1215x \equiv 560(\mod 2755)$ have the form $x = 1000 + 2755t, t \in \mathbb{Z}$. $\square$

PROBLEM II Find all the solution of $x + 4y - 29 \equiv 0(\mod 143), 2x - 9y + 84 \equiv 0(\mod 143)$.

SOLUTION. Since additive of remainder, then the solution of $x+4y-29 \equiv 0(\mod 143), 2x-9y+84 \equiv 0(\mod 143)$, it is equal to find the solution of $17y \equiv 142(\mod 143), 17x + 75 \equiv 0(\mod 143)$. So by the same method in Problem I, we can get $x = 4+143t_1, y = 42+143t_2, t_1, t_2 \in \mathbb{Z}$ satisfy the equation $17 \equiv 142(\mod 143), 17x + 75 \equiv 0(\mod 143)$. That is the solution of $x + 4y - 29 \equiv 0(\mod 143), 2x - 9y + 84 \equiv 0(\mod 143)$. $\square$

PROBLEM III $a, b, m \in \mathbb{Z}$, $\gcd(a, m) = 1$, then the solution of $ax \equiv b(\mod m)$ have the form of $x \equiv ba^{\phi(m)-1}(\mod m)$.

SOLUTION. Obviously, the solution of $x \equiv ba^{\phi(m)-1}(\mod m)$ satisfy $ax \equiv ba^{\phi(m)} \equiv b(\mod m)$ by Fermet Theorem.

Next, we will prove the solution of $ax \equiv b(\mod m)$ have the form of $x \equiv y(\mod m)$ when $\gcd(a, m) = 1$, where $y \in \mathbb{N}$. To find all the solution of $ax \equiv b(\mod m)$, it is equal to find all the x satisfy $ax - mk = b, k \in \mathbb{Z}$. First we can consider $ax - mk = 1$. Since $\gcd(a, m) = 1 \mid b$, then the solution of $ax - mk = 1$ must exist. Assume $x = x_0, k = k_0$ is the special solution of $ax - mk = 1$. Then $x = x_0 b, k = k_0 b$ is the special solution of $ax - mk = b$. Thus, the solution of $ax - mk = b$ must have the form $x = bx_0 + mt, k = k_0 + mt, t \in \mathbb{Z}$. $\square$

PROBLEM IV Find x satisfy

$$\begin{cases} x & \equiv 1 \mod 2 \\ x & \equiv 2 \mod 5 \\ x & \equiv 3 \mod 7 \\ x & \equiv 4 \mod 9 \end{cases} \tag{1}$$

SOLUTION. Let $m_1 = 2, m_2 = 5, m_3 = 7, m_4 = 9, b_1 = 1, b_2 = 2, b_3 = 3, b_4 = 4$, then $m = \prod_{i=1}^{4} m_i, M_i = \frac{m}{m_i}, i = 1, \cdots, 4$, then $M_i' M_i \equiv 1 \mod m_i, i = 1, \cdots, 4$. So we can get $M_1' \equiv 1$

mod 2, $M_2' \equiv 1 \mod 5$, $M_3' \equiv 4 \equiv 7$, $M_4' \equiv 4 \mod 9$. Then the solution of Equation (1) is $x \equiv \prod_{i=1}^{4} M_i' M_i b_i \equiv m$, $x \equiv 315 \times 1 \times 1 + 126 \times 1 \times 2 + 450 \times 3 \times 4 + 70 \times 4 \times 4 \equiv 7087 \equiv 157 \mod 630$. □

PROBLEM V $b_i, m_i \in \mathbb{N}, i = 1, \cdots, k$, satisfy $\gcd(m_i, m_j) \mid b_i - b_j, i \neq j$. $m_i' = \prod_{p\in\mathbb{P},\forall j<i,V_p(m_j)<V_p(m_i),\forall j\in\mathbb{N}^+,V_p(m_j)\leq$ where $\mathbb{P} \subset \mathbb{N}$ is the set of all prime, $V_p(m) = \sup\{t : p^t \mid m\}$. Prove:

$$\begin{cases} x & \equiv b_1 \mod m_1 \\ & \cdots \\ x & \equiv b_k \mod m_k \end{cases} \tag{2}$$

and

$$\begin{cases} x & \equiv b_1 \mod m_1' \\ & \cdots \\ x & \equiv b_k \mod m_k' \end{cases} \tag{3}$$

have same solutions.

SOLUTION. By the definition of m_i', we get $m_i' \mid m$, $\gcd(m_i', m_j') = 1, i \neq j$. Then Equation (**??**) must have solution, so do Equation (**??**). And the solution of Equation (**??**) must be the solution of Equation (**??**). So we only need to prove the solution of Equation (**??**) is the solution of Equation (**??**). That means we only need to prove $\forall i = 1, \cdots, k$, $x \equiv b_i \mod m_i'$ must satisfy $x \equiv b_i \mod m_i$. That is $m \mid x - b_i$, so it is to prove $p^{V_p(m_i)} \mid x - b_i, \forall p \in \mathbb{P}$. Let $j = \min\{t : V_p(m_t) = \max\{V_p(m_s) : s = 1, \cdots, k\}\}$, then $x \equiv b_j \mod p^{V_p(m_j)}$. Obviously, $p^{V_p(m_j)} \mid m_j', m_j' \mid m_j$, then $x \equiv b_j \mod m_j'$. Then $x \equiv b_j \mod m_j$. And $\gcd(m_i, m_j) \mid b_i - b_j$, then $b_i \equiv b_j \mod \gcd(m_i, m_j)$. Then $x \equiv b_i \mod \gcd(m_i, m_j)$, then $x \equiv b_i \mod m_i$. □

Theorem 1. $f(x) \in \mathbb{Z}[x], p$ is prime, if $f(x_1) \equiv 0 \mod p$ and $p \nmid f(x_1)'$, then $\forall \alpha \in \mathbb{N}^+$, $x \equiv x_\alpha \mod p^\alpha$ is one of the solution of $f(x) \equiv 0 \mod p^\alpha$, where $x_\alpha \equiv x_1 \mod p$.

证明. 1. When $\alpha = 1$, then by $x \equiv x_1 \mod p$, we $f(x) \equiv f(x_1) \mod p$.

2. When $a = \alpha - 1$, we have $x_a \equiv x_1 \mod p$ is one of the solution of $f(x) \equiv 0 \mod p^a$. Next we will prove $x_\alpha \equiv x_1 \mod p$ is one of the solution of $f(x) \equiv 0 \mod p^\alpha$.

□