

**PROBLEM I** Solve this equation:  $1215x \equiv 560 \pmod{2755}$ .

**SOLUTION**. Easily  $1215x \equiv 560 \pmod{2755} \iff 243x \equiv 112 \pmod{551}$ . Obviously  $x = 200$  is a solution, and  $\gcd(243, 551) = 1$ , so all the solutions are  $x = 200 + 551t, t \in \mathbb{Z}$ .  $\square$

**PROBLEM II** Find the solution of 
$$\begin{cases} x + 4y - 29 \equiv 0 \pmod{143} \\ 2x - 9y + 84 \equiv 0 \pmod{143} \end{cases}$$

**SOLUTION**. Double the first equation then minus the second, we get  $17y - 142 \equiv 0 \pmod{143}$ . Then  $y \equiv 42 \pmod{143}$ . Substitute it in the first equation, we get  $x \equiv 4 \pmod{143}$ .  $\square$

**PROBLEM III**

1. Assume  $m \in \mathbb{N}^+, \gcd(a, m) = 1$ , prove that  $x \equiv ba^{\phi(m)-1} \pmod{m}$  is the solution of  $ax \equiv b \pmod{m}$ .
2. Assume  $p$  is prime and  $0 < a < p$ . Prove that  $x = b(-1)^{a-1} \frac{\binom{p}{a}}{p} \pmod{p}$  is solution of  $ax \equiv b \pmod{p}$ .

**SOLUTION**. 1. First to check  $aba^{\phi(m)-1} \equiv b \pmod{m}$ . Since  $\gcd(a, m) = 1$ , easily  $a^{\phi(m)} \equiv 1 \pmod{m}$ , so it's obvious. Second to check  $ax \equiv b \pmod{m} \implies x \equiv ba^{\phi(m)-1} \pmod{m}$ . Multiply  $a^{\phi(m)-1}$ , easily  $x \equiv a^{\phi(m)}x \equiv ba^{\phi(m)-1} \pmod{m}$ .

2. We multiply  $a!$  to the equation, we get  $a!x \equiv b(-1)^{a-1} \prod_{k=1}^{a-1} (-k) \equiv b(a-1)! \pmod{p}$ . Since  $0 < a < p$ , we get  $\gcd((a-1)!, p) = 1$ , so  $ax \equiv b \pmod{p}$ .  $\square$

**PROBLEM IV** Solve the equation:

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

**SOLUTION**. Let  $m_1 = 2, m_2 = 5, m_3 = 7, m_4 = 9$ , and  $M_1 = 315, M_2 = 126, M_3 = 90, M_4 = 70$ . Then  $M'_1 = 1, M'_2 = 1, M'_3 = -1, M'_4 = 4$ . So  $x \equiv 1 \times 315 \times 1 + 1 \times 126 \times 2 - 1 \times 90 \times 3 + 4 \times 70 \times 4 \equiv 1417 \equiv 157 \pmod{630}$ .  $\square$

I think this question should be as follows, but may be I make a mistake. **PROBLEM V**

1. Assume  $m_1, \dots, m_k \in \mathbb{N}^+, b_1, \dots, b_k \in \mathbb{Z}$ , and  $\forall i, j, \gcd(m_i, m_j) \mid b_i - b_j$ . Let  $m'_i := \prod_{p \in \mathbb{P}, \forall j < i, v_p(m_j) < v_p(m_i) \wedge \forall j, v_p(m_j) \leq v_p(m_i)} p^{v_p(m_i)}$ , where  $\mathbb{P}$  is the set of primes, and  $v_p(x)$  is the biggest integer  $t$  such that  $p^t \mid x$ . Then following two equation has same solution:

$$x \equiv b_i \pmod{m_i}, \forall i \tag{1}$$

$$x \equiv b_i \pmod{m'_i}, \forall i \tag{2}$$

2. find the solution of

$$\begin{cases} x \equiv 0 \pmod{5} \\ x \equiv 10 \pmod{715} \\ x \equiv 140 \pmod{247} \\ x \equiv 245 \pmod{391} \\ x \equiv 109 \pmod{187} \end{cases}$$

*SOLUTION.* 1. Easily solution of Equation (1) must be solution of Equation (2), now we will prove the reverse. Assume  $x \equiv b_i \pmod{m'_i}, \forall i$ . Now we will prove  $x \equiv b_i \pmod{m_i}$ . Only need to prove  $\forall p \in \mathbb{P}, x \equiv b_i \pmod{p^{v_p(m_i)}}$ . Assume  $j = \min\{t : v_p(m_t) = \max_r v_p(m_r)\}$ , then by the definition of  $m'_i$ , we know that  $p^{v_p(m_j)} \mid m'_j$ . And easily  $p^{v_p(m_i)} \mid p^{v_p(m_j)}$ , so we get  $x \equiv b_j \pmod{p^{v_p(m_i)}}$ . More over, easily to know  $p^{v_p(m_i)} \mid \gcd(m_i, m_j)$ , so  $b_j \equiv b_i \pmod{p^{v_p(m_i)}}$ . So finally we get the result.

It is easy to prove that  $\forall i \neq j, \gcd(m'_i, m'_j) = 1$ , so we can solve the second equation.

2. From above we get the given equation is equivalent to

$$\begin{cases} x \equiv 0 \pmod{5} \\ x \equiv 10 \pmod{143} \\ x \equiv 7 \pmod{19} \\ x \equiv 245 \pmod{391} \\ x \equiv 0 \pmod{1} \end{cases}$$

Assume  $x = 5y$ , then we get  $\begin{cases} y \equiv 2 \pmod{143} \\ y \equiv 9 \pmod{19} \\ y \equiv 49 \pmod{391} \end{cases}$ . Solve this equation, we get  $y \equiv 2004$

$\pmod{1062347}$ . So finally we get  $x \equiv 10020 \pmod{5311735}$ .

□