The Chinese Remainder Theorem

Lesson 28 · Module 2 — Number Theory & Cryptography · Discrete Mathematics · daily-maths.uk/discrete

Practice problems

1. Find the smallest positive integer x such that $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, and $x \equiv 3 \pmod{5}$.
2. Solve the system $x \equiv 3 \pmod{7}$ and $x \equiv 4 \pmod{11}$.
3. Determine if the system $x \equiv 2 \pmod{6}$ and $x \equiv 5 \pmod{9}$ has a solution. If so, find it; if not, explain why.

Solutions

1. Find the smallest positive integer x such that $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, and $x \equiv 3 \pmod 5$.

   - Calculate $N = 3 \cdot 4 \cdot 5 = 60$.
   - For $n_1 = 3$, $M_1 = 20$. $20 \equiv 2 \pmod 3$, so $y_1 = 2^{-1} \equiv 2 \pmod 3$. Term 1: $1 \cdot 20 \cdot 2 = 40$.
   - For $n_2 = 4$, $M_2 = 15$. $15 \equiv 3 \pmod 4$, so $y_2 = 3^{-1} \equiv 3 \pmod 4$. Term 2: $2 \cdot 15 \cdot 3 = 90$.
   - For $n_3 = 5$, $M_3 = 12$. $12 \equiv 2 \pmod 5$, so $y_3 = 2^{-1} \equiv 3 \pmod 5$. Term 3: $3 \cdot 12 \cdot 3 = 108$.
   - Sum: $x = 40 + 90 + 108 = 238$.
   - Reduce modulo 60: $238 = 3 \cdot 60 + 58$.

   Answer: 58

2. Solve the system $x \equiv 3 \pmod 7$ and $x \equiv 4 \pmod{11}$.

   - Calculate $N = 7 \cdot 11 = 77$.
   - For $n_1 = 7$, $M_1 = 11$. $11 \equiv 4 \pmod 7$. The inverse of $4 \pmod 7$ is 2 because $4 \cdot 2 = 8 \equiv 1 \pmod 7$. Term 1: $3 \cdot 11 \cdot 2 = 66$.
   - For $n_2 = 11$, $M_2 = 7$. $7 \equiv 7 \pmod{11}$. The inverse of $7 \pmod{11}$ is 8 because $7 \cdot 8 = 56 \equiv 1 \pmod{11}$. Term 2: $4 \cdot 7 \cdot 8 = 224$.
   - Sum: $x = 66 + 224 = 290$.
   - Reduce modulo 77: $290 = 3 \cdot 77 + 59$.

   Answer: 59

3. Determine if the system $x \equiv 2 \pmod 6$ and $x \equiv 5 \pmod 9$ has a solution. If so, find it; if not, explain why.

   - Check the coprimality of the moduli: $\gcd(6, 9) = 3$.
   - For a solution to exist, the remainders must be congruent modulo the GCD: $2 \equiv 5 \pmod 3$.
   - Check: $2 \pmod 3 = 2$ and $5 \pmod 3 = 2$. Since $2 \equiv 2 \pmod 3$, a solution exists.
   - List values for $x \equiv 5 \pmod 9$: $5, 14, 23, 32, \ldots$
   - Check against $x \equiv 2 \pmod 6$: $5 \equiv 5 \pmod 6$, $14 \equiv 2 \pmod 6$.
   - The smallest positive solution is 14.

   Answer: 14
