Modular arithmetic II — inverses and linear congruences

Lesson 27 · Module 2 — Number Theory & Cryptography · Discrete Mathematics · daily-maths.uk/discrete

Practice problems

1. Find the modular multiplicative inverse of 9 modulo 20.
2. Solve the linear congruence $11x \equiv 5 \pmod{26}$.
3. Determine if $6x \equiv 3 \pmod{9}$ has a solution. If so, find one.

Solutions

1. Find the modular multiplicative inverse of 9 modulo 20.

   - Check $\gcd(9, 20)$. Since $20 = 2^2 \cdot 5$ and $9 = 3^2$, $\gcd(9, 20) = 1$. The inverse exists.
   - Use Euclidean Algorithm: $20 = 2(9) + 2$, then $9 = 4(2) + 1$.
   - Back-substitute: $1 = 9 - 4(2) = 9 - 4(20 - 2(9)) = 9 - 4(20) + 8(9) = 9(9) - 4(20)$.
   - Modulo 20, this gives $9(9) \equiv 1 \pmod{20}$.

   Answer: 9

2. Solve the linear congruence $11x \equiv 5 \pmod{26}$.

   - Find the inverse of 11 modulo 26. $\gcd(11, 26) = 1$.
   - Euclidean Algorithm: $26 = 2(11) + 4$, $11 = 2(4) + 3$, $4 = 1(3) + 1$.
   - Back-substitute: $1 = 4 - 1(3) = 4 - 1(11 - 2(4)) = 3(4) - 1(11) = 3(26 - 2(11)) - 1(11) = 3(26) - 7(11)$.
   - The inverse is -7, which is $26 - 7 = 19$.
   - Multiply both sides by 19: $x \equiv 19 \cdot 5 \pmod{26}$.
   - Compute $95 \pmod{26}$: $95 = 3 \cdot 26 + 17$.

   Answer: 17

3. Determine if $6x \equiv 3 \pmod{9}$ has a solution. If so, find one.

   - Check $\gcd(6, 9) = 3$.
   - Since $\gcd(6, 9) = 3$ and 3 divides the constant 3, solutions exist.
   - The inverse method fails because $\gcd(6, 9) \neq 1$.
   - Test small values: if $x = 2$, $6(2) = 12$. $12 \pmod{9} = 3$.
   - Thus, $x = 2$ is a solution.

   Answer: x = 2 (or x = 5, 8)
