Module 2 review + self-test

Lesson 34 · Module 2 — Number Theory & Cryptography · Discrete Mathematics · daily-maths.uk/discrete

---

Practice problems

1. Find the modular inverse of 15 modulo 28.
2. Compute $2^{100} \pmod{11}$ using Fermat's Little Theorem.
3. In an RSA system, if $p = 3, q = 11$, and $e = 3$, find the private key d.

Solutions

1. Find the modular inverse of 15 modulo 28.

   - Use the Euclidean algorithm: $28 = 1 \cdot 15 + 13$, then $15 = 1 \cdot 13 + 2$, then $13 = 6 \cdot 2 + 1$.
   - Work backwards: $1 = 13 - 6 \cdot 2$.
   - Substitute $2 = 15 - 13$: $1 = 13 - 6(15 - 13) = 7 \cdot 13 - 6 \cdot 15$.
   - Substitute $13 = 28 - 15$: $1 = 7(28 - 15) - 6 \cdot 15 = 7 \cdot 28 - 13 \cdot 15$.
   - The inverse is -13, which is $28 - 13 = 15$ modulo 28.

   Answer: 15

2. Compute $2^{100} \pmod{11}$ using Fermat's Little Theorem.

   - Since 11 is prime and 2 is not a multiple of 11, $2^{10} \equiv 1 \pmod{11}$.
   - Rewrite the exponent: $100 = 10 \cdot 10 + 0$.
   - Then $2^{100} = (2^{10})^{10} \cdot 2^0 \equiv 1^{10} \cdot 1 \pmod{11}$.
   - The result is 1.

   Answer: 1

3. In an RSA system, if $p = 3, q = 11$, and $e = 3$, find the private key d.

   - Calculate $n = 3 \cdot 11 = 33$.
   - Calculate $\phi(n) = (3 - 1)(11 - 1) = 2 \cdot 10 = 20$.
   - Solve $3d \equiv 1 \pmod{20}$.
   - We look for a multiple of 20 plus 1 that is divisible by 3. 21 is divisible by 3.
   - Since $3 \cdot 7 = 21$, $d = 7$.

   Answer: 7
