Fast Modular Exponentiation

Lesson 31 · Module 2 — Number Theory & Cryptography · Discrete Mathematics · daily-maths.uk/discrete

---

Practice problems

1. Compute $3^{21} \pmod{17}$ using the method of repeated squaring.
2. Compute $2^{50} \pmod{11}$.
3. Compute $5^{103} \pmod{13}$.

Solutions

1. Compute $3^{21} \pmod{17}$ using the method of repeated squaring.

   - Convert exponent to binary: $21 = 16 + 4 + 1$.
   - Compute squares: $3^1 \equiv 3$, $3^2 \equiv 9$, $3^4 \equiv 81 \equiv 13 \equiv -4 \pmod{17}$, $3^8 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$, $3^{16} \equiv (-1)^2 \equiv 1 \pmod{17}$.
   - Multiply components: $3^{21} = 3^{16} \cdot 3^4 \cdot 3^1 \equiv 1 \cdot 13 \cdot 3 = 39$.
   - Reduce modulo 17: $39 = 2 \cdot 17 + 5$.

   Answer: 5

2. Compute $2^{50} \pmod{11}$.

   - Convert exponent to binary: $50 = 32 + 16 + 2$.
   - Compute squares: $2^1 \equiv 2$, $2^2 \equiv 4$, $2^4 \equiv 16 \equiv 5 \pmod{11}$, $2^8 \equiv 25 \equiv 3 \pmod{11}$, $2^{16} \equiv 9 \equiv -2 \pmod{11}$, $2^{32} \equiv 4 \pmod{11}$.
   - Multiply components: $2^{50} = 2^{32} \cdot 2^{16} \cdot 2^2 \equiv 4 \cdot 9 \cdot 4 = 144$.
   - Reduce modulo 11: $144 = 13 \cdot 11 + 1$.

   Answer: 1

3. Compute $5^{103} \pmod{13}$.

   - First, use Euler's Theorem to reduce the exponent: $\phi(13) = 12$. $103 \pmod{12} = 7$.
   - Now compute $5^7 \pmod{13}$. Binary: $7 = 4 + 2 + 1$.
   - Compute squares: $5^1 \equiv 5$, $5^2 \equiv 25 \equiv 12 \equiv -1 \pmod{13}$, $5^4 \equiv (-1)^2 \equiv 1 \pmod{13}$.
   - Multiply components: $5^7 = 5^4 \cdot 5^2 \cdot 5^1 \equiv 1 \cdot 12 \cdot 5 = 60$.
   - Reduce modulo 13: $60 = 4 \cdot 13 + 8$.

   Answer: 8
