# Fermat's Little Theorem — proved two ways

Lesson 29 · Module 2 — Number Theory & Cryptography · Discrete Mathematics · daily-maths.uk/discrete

---

## Practice problems

1. Find the remainder of $3^{121}$ when divided by 11.
2. Find the remainder of $2^{50}$ when divided by 17.
3. Find the modular inverse of 3 modulo 13 using Fermat's Little Theorem.

## Solutions

1. Find the remainder of $3^{121}$ when divided by 11.

    - Check conditions: 11 is prime and 11 does not divide 3.
    - By Fermat's Little Theorem, $3^{10} \equiv 1 \pmod{11}$.
    - Divide the exponent 121 by 10: $121 = 10 \times 12 + 1$.
    - Rewrite the expression: $3^{121} = (3^{10})^{12} \cdot 3^1$.
    - Substitute the congruence: $1^{12} \cdot 3 \equiv 3 \pmod{11}$.

    **Answer:** 3

2. Find the remainder of $2^{50}$ when divided by 17.

    - Check conditions: 17 is prime and 17 does not divide 2.
    - By Fermat's Little Theorem, $2^{16} \equiv 1 \pmod{17}$.
    - Divide the exponent 50 by 16: $50 = 16 \times 3 + 2$.
    - Rewrite the expression: $2^{50} = (2^{16})^3 \cdot 2^2$.
    - Substitute the congruence: $1^3 \cdot 4 \equiv 4 \pmod{17}$.

    **Answer:** 4

3. Find the modular inverse of 3 modulo 13 using Fermat's Little Theorem.

    - We seek $x$ such that $3x \equiv 1 \pmod{13}$.
    - By Fermat's Little Theorem, $3^{12} \equiv 1 \pmod{13}$.
    - Rewrite as $3 \cdot 3^{11} \equiv 1 \pmod{13}$.
    - Thus, the inverse is $3^{11} \pmod{13}$.
    - Compute $3^3 = 27 \equiv 1 \pmod{13}$.
    - Then $3^{11} = (3^3)^3 \cdot 3^2 \equiv 1^3 \cdot 9 \equiv 9 \pmod{13}$.

    **Answer:** 9

---