

Fermat's little theorem

INCORRECT!

$$5^{100} \equiv 2^1 \equiv 2 \pmod{3} \quad (\text{not allowed})$$

$5 \cdot 5 \cdot 5 \dots 5$
100 times

correct: $5^{100} \equiv (-1)^{100} \equiv 1 \pmod{3}$

THM Let p be a prime.

$$a^{p-1} \equiv 1 \pmod{p}$$

a^0

provided that $a \not\equiv 0 \pmod{p}$

EG $5^{100} \equiv 2^{100} \equiv 2^0 \equiv 1 \pmod{3}$

$100 \equiv 0 \pmod{2}$

EG $3^{1003} \pmod{101}$ (prime!)

$\equiv 3^3 = 27$

$1003 \equiv 3 \pmod{100}$

$1003 = 10 \cdot 100 + 3$

$3^{1003} = 3^{10 \cdot 100} \cdot 3^3$

Little Fermat: $3^{100} \equiv 1 \pmod{101}$

$3^3 \equiv 3^3$

Proof

$$a, 2a, 3a, \dots, (p-1)a$$

non zero residues mod p times a
invertible

$$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)$$

$$a^{p-1} \equiv 1 \pmod{p}$$