Fermat's little theorem

INCORRECT!

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

$5^{100} = \underbrace{5 \cdot 5 \cdot 5 \cdots 5}_{100 \text{ times}}$

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

THM Let p be a prime.

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

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

a^0

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

$100 \equiv 0 \pmod 2$

EG $3^{1003} \pmod{101}$

101 prime!

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

$1003 \equiv 3 \pmod{100}$

$1003 = 10 \cdot 100 + 3$

$3^{1003} = 3^{10 \cdot 100} \cdot 3^3 = (3^{100})^{10} \cdot 3^3 \equiv 3^3$

$\equiv 1$, $\equiv 1$

$\equiv 3^3 = 27$

Proof

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

non zero residues mod p times a

a invertible

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

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