Fermat's Last Thm
$a^n + b^n = c^n$
do not have solutions in integers when $n > 2$.

$a^2 + b^2 = c^2$
3, 4, 5

Fermat's Little Theorem

If p is a prime, given an integer a, s.t. $\gcd(a,p) = 1$,

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

Euler's Thm

If p & q are diffnt primes, an integer a s.t $\gcd(a, pq) = 1$

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

$$d \equiv e^{-1} \pmod{(p-1)(q-1)}$$

↓ RSA

$$D(E(m)) = (m^e)^d \equiv m^{e \cdot e^{-1}}$$
$$\equiv m^{1 + k(p-1)(q-1)} \pmod{n}$$
$$\equiv m \cdot m^{k(p-1)(p-1)}$$
$$\equiv m \cdot 1 \pmod{n}$$
$$\equiv m \pmod{n}$$