MATH 242 — 17 April 2026

GOAL: Find BIG primes
say: 50-digits

[Fermat's Last Theorem
$a^n + b^n = c^n$
has no integer solutions for $n > 2$]

Fermat's Little Theorem

If p is prime and a is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

a^{p-1} is 1 more than a multiple of p.

Computer: 1 billion operations/sec: 10^9

"big" prime: 50 digits: 10^{50}

$$\frac{10^{50}}{10^9} = 10^{41}$$

Fermat's Little Theorem Primality Test

TRUE: probably prime $a^{n-1} \equiv 1 \pmod{n}$

FALSE: definitely composite $a^{n-1} \not\equiv 1 \pmod{n}$

EXAMPLE: Want to find $3^{32} \pmod 7$

$3^2 = 9$

$3^4 = (3^2)^2 = 81$

$3^8 = (3^4)^2 = 6561$

$3^{16} = (3^8)^2 = 43,046,721$

$3^{32} = (3^{16})^2 = 1,853,020,188,851,841$

mod 7: 2

$3^2 = 9 \equiv 2 \pmod 7$

$3^4 \equiv 2^2 = 4 \pmod 7$

$3^8 \equiv 4^2 \equiv 16 \equiv 2 \pmod 7$

$3^{16} \equiv 2^2 = 4 \pmod 7$

$3^{32} \equiv 4^2 \equiv 16 \equiv 2 \pmod 7$

Modular Exponentiation