MATH 242 — 7 November 2025

How can we find BIG primes?

Fermat's Little Theorem

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

↖ 1 more than a multiple of p

> Fermat's Last Theorem
> $a^n + b^n = c^n$ has no integer solutions if $n > 2$.

Example: $p = 7$

$a = 1$: $1^{7-1} = 1^6 = 1 \equiv 1 \pmod 7$

$a = 2$: $2^{7-1} = 2^6 = 64 \equiv 1 \pmod 7$

$a = 3$: $3^{7-1} = 3^6 = 729 = 728 + 1 \equiv 1 \pmod 7$

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

$3^2 = 9$

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

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

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

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

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

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

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

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

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

Recall: density of primes near x is about $\frac{1}{\ln(x)}$.

So if you're considering 50-digit numbers,

the density of primes is about $\frac{1}{\ln(10^{50})} \approx 0.008$

That is, only about 8 of every thousand 50-digit numbers are prime.