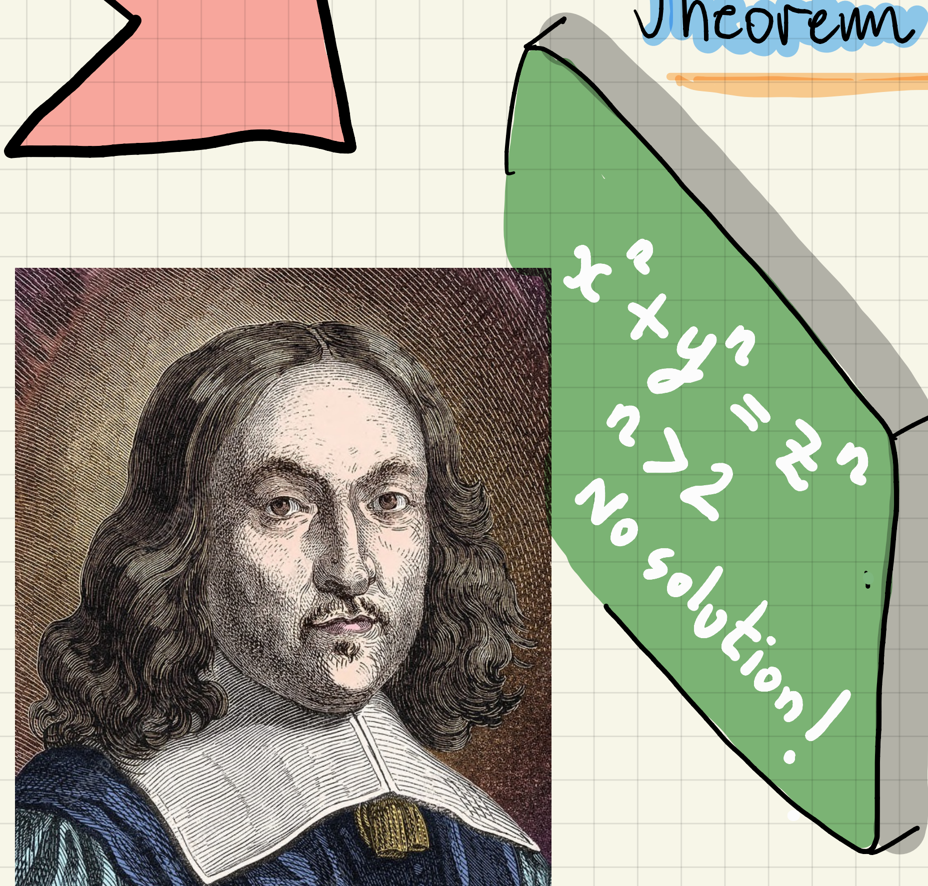
Fermat's little theorem

few years...

Fermat's big Theorem



lecture 23

Testing for primes:

Fermat's little theorem.

If p is prime and $p \nmid a$, then

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

proof: $\gcd(a,p)=1$, so $a\times 1,\ a\times 2,\ a\times 3, \ldots, a\times(p-1)$

are all distinct modulo p

$n=8$

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array}$$

$\times 3$

$a=3.$

$$\begin{array}{cccccccc} 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 \end{array}$$

$$\gcd(3,8)=1 \Rightarrow 3x \not\equiv 3y \pmod 8$$

$3x$ are all different $\Rightarrow$ Permutation.

So $(a\times 1)\times(a\times 2)\times\cdots\times(a\times(p-1)) \equiv 1\times 2\times\cdots\times(p-1) \mod p$

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p$$

$p \nmid (p-1)!$ [otherwise p must divide one of the factors $\{1, 2, \ldots, p-1\}$]

so $(p-1)!$ has an inverse mod p

$$a^{p-1}\underbrace{(p-1)!\,(p-1)!^{-1}}_{\equiv 1} \equiv (p-1)!\,(p-1)!^{-1} \equiv 1 \mod p$$

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

Example: $p = 13$ is prime.

let $a = 8$.

$13 \nmid 8$ $\quad$ $\gcd(8, 13) = 1$

$$8^{13-1} \equiv 1 \pmod{13}$$

$$8^{12} \equiv 1 \pmod{13}$$

In fact, we can strengthen the theorem:

$$\boxed{n \text{ prime} \underset{\text{iff}}{\iff} \forall \underset{\in \mathbb{N}}{a} < n.\ a^{n-1} \equiv 1 \pmod{n}}$$

$\Rightarrow$: n prime. $a < n \Rightarrow n \nmid a$. Therefore $a^{n-1} \equiv 1 \pmod{n}$

$\Leftarrow$: Consider the contrapositive

$$n \text{ composite} \Rightarrow \exists\, a < n.\ a^{n-1} \not\equiv 1 \pmod{n}$$

n composite $\Rightarrow$ $n = a \cdot b$ for some $1 < a < n$

$$a^{n-1} \equiv 1 \pmod{n} \Rightarrow a^{n-1} - 1 \equiv 0 \pmod{n} \Rightarrow n \mid a^{n-1} - 1$$

$$\Rightarrow a \mid a^{n-1} - 1$$

But $a \mid a^{n-1}$, so $a \mid a^{n-1} - (a^{n-1} - 1) \Rightarrow a \mid 1$, contradiction.

Fermat's Test. (Don't test all $a<n$, just few random ones)

repeat 100 times

pick a random $a \in \{1, \dots, n-1\}$

if $a^{n-1} \not\equiv 1 \pmod{n}$

then return NO (composite) (100% sure)

return YES (prime) ← (not sure)

This could have a false positive (saying n is prime while it's not).

Assume $\exists$ a such that

- $\gcd(a, n) = 1$
- $a^{n-1} \not\equiv 1 \pmod{n}$

Some numbers don't satisfy this!

(but very rare)

$$b^{n-1} \equiv 1 \pmod{n} \Rightarrow (ab)^{n-1} \equiv a^{n-1} b^{n-1} \equiv a^{n-1} \not\equiv 1 \pmod{n}$$

$$\gcd(a, n) = 1 \Rightarrow ab \not\equiv ac \text{ when } b \not\equiv c.$$

So for every b that passes the test, $ab \bmod n$ fails the test. There are at least as many failures as successes. So prob. error is $\leq \frac{1}{2}$.

Repeat 100 times $\Rightarrow$ Prob. of error $\leq \frac{1}{2^{100}} \approx 0$

Two problems:

1) a^{n-1} is too big

2) a^{n-1} requires n multiplications.

To solve 1) Compute everything modulo n.

Example: $n = 30$ $a = 2$

$$2^{30-1} = 2^{29} \quad (a^{n-1})$$

$$\underbrace{1 \to 2 \to 4 \to 8 \to 16 \to 32 \equiv 2 \to 4 \to 8 \to \dots}_{29 \text{ times}}$$

To solve 2) use <u>repeated squaring</u>.

$$2^{29} \xleftarrow{\times 2} 2^{28} \xleftarrow{\wedge 2} 2^{14} \xleftarrow{2\wedge} 2^{7} \xleftarrow{\times 2} 2^{6} \xleftarrow{2\wedge} 2^{3} \xleftarrow{\times 2} 2^{2} \xleftarrow{\wedge 2} 2^{1} \xleftarrow{\times 2} 1$$

<u>Combine the two solutions:</u>

$$1 \xrightarrow{\times 2} 2 \xrightarrow{\wedge 2} 4 \xrightarrow{\times 2} 8 \xrightarrow{\wedge 2} 64 \equiv$$

$$4 \xrightarrow{\times 2} 8 \xrightarrow{\wedge 2} 64 \equiv$$

$$4 \xrightarrow{\wedge 2} 16 \xrightarrow{\times 2} 32 \equiv$$

$$2$$

$$2^{30-1} \equiv 2 \pmod{30}$$ [30 is not prime]