Consider the following program in pseudocode where $x = \{...\}$ assigns x a value from the set, and $(x, y) = (..., ...)$ simultaneously assigns x and y their values:

```
(x,y,z)=({1,...,n},{1,...,n},{1,...,n})
while x>0 and y>0 and z>0
  control={1,2,3}
  if control==1 then
    (x,y,z)=(x+1,y-1,z-1)
  else
  if control==2 then
    (x,y,z)=(x-1,y+1,z-1)
  else
    (z,y,z)=(x-1,y-1,z+1)
```

$x+y+z$ decreases by 1 each iteration.

It is typical to prove that a program terminates by finding a quantity that is always decreasing. In the above program, obviously $x + y + z$ decreases by 1 after every iteration. Therefore, one of x, y, or z will eventually reach zero and the program will terminate. However, it is not always possible to find a decreasing quantity, like in the following program:

```
(x,y,z)=({1,...,n},{1,...,n},{1,...,n})
while x>0 and y>0 and z>0
  control={1,2}
  if control==1 then
    x={x,...,n}
    y={y,...,n}
    z=z-1
  else
    y={y,...,n}
    x=x-1
```

In each iteration
either z decreases,
or z remains the same
but x decreases.

Look at (z, x)

let z_i, x_i be values of z and x in iteration i

$$(z_i, x_i) \prec (z_j, x_j) \iff z_i < z_j \lor (z_i = z_j \land x_i < x_j)$$

Iteration i v.s Iteration $(i+1)$

$$(z_{i+1}, x_{i+1}) \prec (z_i, x_i)$$

because either $z_{i+1} < z_i$ or

$z_{i+1} = z_i \land x_{i+1} < x_i$

Finite set of possible tuples, every partial order relation on a finite set has a "minimum", we can't decrease (z, x) indefinitely. Program must stop.

Fermat Theorem

$$p \text{ prime} \wedge p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$$

- $p \nmid a \implies \gcd(a,p) = 1$
- Consider set $\{1, 2, 3, \ldots, p-1\}$

$\times a \pmod{p}$ --- permute ----- (because $\gcd(a,p)=1$)

[idea: $\gcd(a,p)=1$]

$$a \cdot (2a) \cdot (3a) \cdot (4a) \cdots [(p-1)a] \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) = (p-1)!$$

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

[Idea: p prime]

$$p \mid a^{p-1}(p-1)! - (p-1)! \implies p \mid (p-1)!\,[a^{p-1} - 1]$$

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

(because p can't divide $1, 2, 3, \ldots, p-1$)

if p divides a product it must divide one factor

Strengthen:

$$p \text{ prime} \iff \forall a < p,\ a^{p-1} \equiv 1 \pmod{p}$$

<u>Idea:</u> To check if a number n is prime, make sure $a^{n-1} \equiv 1 \pmod{n}$ for all $a < n$.

Not better than checking $\{1, \dots, p-1\}$ for divisors!

But it turns out, it has good random behavior:

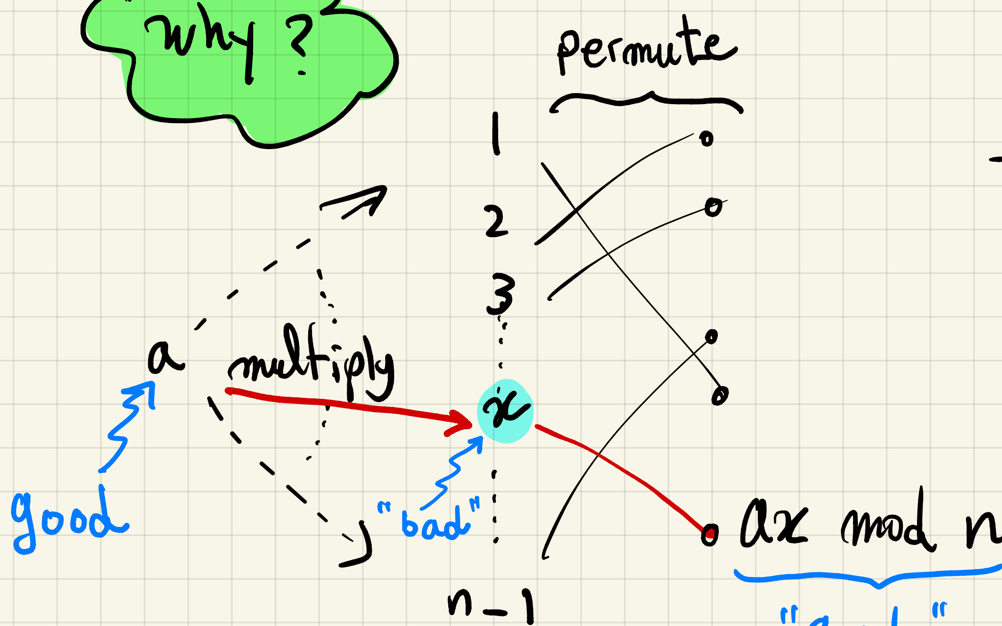
repeat 100 times
- pick random $a < n$
- if $a^{n-1} \not\equiv 1 \pmod{n}$
  return false (n is composite)

return true.

<u>Problem:</u> n might be composite and we still return true because we did not pick the "good" a : $a^{n-1} \not\equiv 1 \bmod n$

For most composites, the probability of picking a "bad" a is $\leq \frac{1}{2}$. Therefore, the prob. of making wrong decision $\leq \left(\frac{1}{2}\right)^{100}$

why?



n is composite

there must be an $a^{n-1} \not\equiv 1 \pmod{n}$

Assume also $\gcd(a,n)=1$

This is true for almost all composites

$$x^{n-1} \equiv 1 \pmod{n}$$

$$(ax)^{n-1} \equiv a^{n-1}x^{n-1} \equiv a^{n-1}\cdot 1 \equiv a^{n-1} \not\equiv 1 \pmod{n}$$

If x is "bad" then $ax \bmod n$ is "good". For every "bad" there is at least one "good".

Problems

- a^{n-1} requires $(n-1)$ multiplication
- a^{n-1} is HUGE !

Repeated Squaring:

$$a^b = \begin{cases} 1 & b = 0 \\ a \cdot a^{b-1} & b \text{ odd} \\ \left[a^{b/2}\right]^2 & b \text{ even} \quad \text{[save mult.]} \end{cases}$$

Combine this with computing everything modulo n on the fly.

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

Need to find $a^{n-1} = 2^{29}$

29 28 14 7 6 3 2 1 $\boxed{0}$ Base case

$\times$ $\wedge^2$ $\wedge^2$ $\times$ $\wedge^2$ $\times$ $\wedge^2$ $\times$

64 8 4 2 1

64 8 4

32 16 4

2

$\# \text{mult} \approx 2 \cdot \log_2 b$

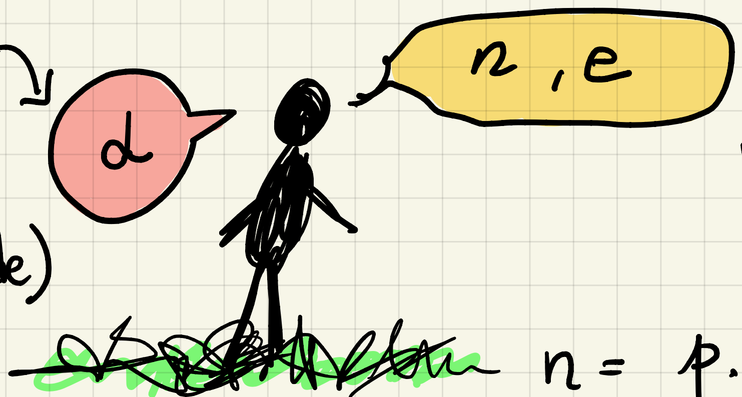
Cryptography

Assume every message is an integer $x < n$.

To send x to person A, send $x^e \bmod n$

where e and n are advertized by A

private key
(see next slide)



public key

$n = p \cdot q$ where p, q are large primes

Fact 1: It's hard to factor n into primes, so it's hard to discover p and q

Fact 2: Given $y = x^e \bmod n$, it's hard to figure out x.

Person A also has : $\gcd(e, (p-1)(q-1)) = 1$

so there exists d such that

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

d can be easily found by A (how?) but not by others.

claim : $y^d \bmod n = x$

$$y^d \equiv (x^e)^d \equiv x^{ed} \equiv x^{(p-1)(q-1)+1} \equiv x.(x^{q-1})^{p-1}$$

- $p \mid x \Rightarrow y^d \equiv x \equiv 0 \pmod{p}$
- $p \nmid x \Rightarrow p \nmid x^{q-1} \Rightarrow (x^{q-1})^{p-1} \equiv 1 \pmod{p}$ [Fermat]

$$\Rightarrow y^d \equiv x \pmod{p}$$

$$y^d \equiv x \pmod{p} \implies p \mid y^d - x$$
$$y^d \equiv x \pmod{q} \implies q \mid y^d - x$$

$$\overline{}$$

$$pq \mid y^d - x \quad (p, q \text{ primes})$$

Therefore $\quad y^d \equiv x \pmod{pq}$

$$y^d \equiv x \pmod{n} \qquad :)$$