Fermat's little theorem: For prime p, for all a where $a \not\equiv 0 \bmod p$ (i.e., a & p are relatively prime)

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

Proof: Fix prime p & a where $a \not\equiv 0 \bmod p$.

Let $S = \{1, \dots, p-1\}$.

Define $S' := aS \bmod p = \{a \bmod p, 2a \bmod p, \dots, (p-1)a \bmod p\}$

Claim: $S = S'$

Proof: For $i \neq j$ where $1 \leq i, j \leq p-1$,

Suppose $ai \equiv aj \bmod p$

Since p is prime & $\gcd(a,p)=1$ then $a^{-1} \bmod p$ exists.

thus, $i \equiv j \bmod p$ which is a contradiction.

— Therefore, we know S' has $p-1$ distinct elements.

Moreover, if $ai \equiv 0 \bmod p$ then $i \equiv 0 \bmod p$.

Thus, S' has $p-1$ distinct elements in $\{1, \dots, p-1\}$. ∎

Since $S = S'$, then $\prod_{i \in S} i \equiv \prod_{j \in S'} j \bmod p$

$$(1)(2)\cdots(p-1) \equiv (a)(1)(a)(2)\cdots(a)(p-1) \bmod p$$

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

Note, $(p-1)!^{-1} \bmod p$ exists, $\quad 1 \equiv a^{p-1} \bmod p$. ∎

Since $\gcd(i,p)=1$ for all $1 \leq i \leq p-1$, Euler's theorem — generalization of Fermat's little theorem

For any N, any a where $\gcd(a, N) = 1$ (i.e., a & N are rel. prime)

$$a^{\phi(N)} \equiv 1 \bmod N$$

where $\phi(N) = |\{b : b \in \{1, \ldots, N\}, \gcd(b, N) = 1\}|$

= # of numbers b/w 1 & N that are relatively prime to N

Note, for prime p, $\phi(p) = p - 1$

for primes p & q, $\phi(pq) = (p-1)(q-1)$

Hence, for $N = pq$, $a^{(p-1)(q-1)} \equiv 1 \bmod N$

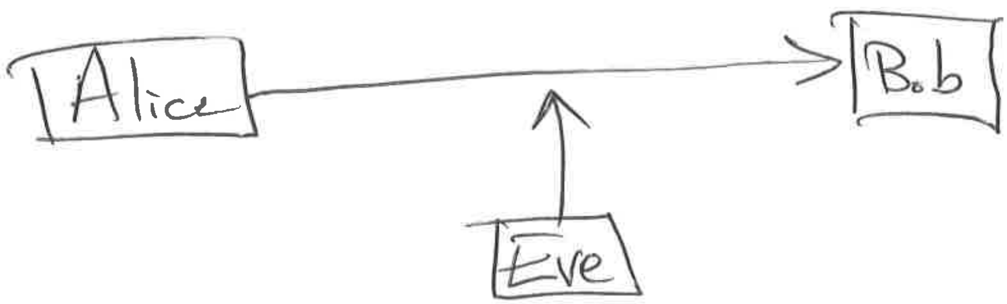
Moreover, consider d & e where $de \equiv 1 \bmod (p-1)(q-1)$

& thus $de = 1 + k(p-1)(q-1)$ for some integer k.

Then, $a^{de} \equiv (a)\left(a^{(p-1)(q-1)}\right)^k \equiv a \bmod N.$

This follows from Euler's theorem when $\gcd(a, N) = 1$, and for a where $\gcd(a, N) > 1$ then this statement still holds by Chinese Remainder Theorem. (but we won't use this N if $\gcd(a, N) > 1$ so doesn't matter).

Public-key cryptography:



1. Bob publishes a public key:

   a. Bob chooses 2 n-bit random primes p & q.
   Here, n is HUGE (e.g., $n \simeq 2048$)
   Bob chooses 2 random n-bit numbers & then checks if they are prime. HOW?

   b. Bob finds e which is relatively prime to $(p-1)(q-1)$
   (i.e., $\gcd(e,(p-1)(q-1))=1$)
   Typically by trying $e=3,5,7,11,\ldots$

   c. Let $N=pq$

   d. Bob publishes his public key (N,e).

   e. He computes his private key:
   $$d \equiv e^{-1} \bmod (p-1)(q-1)$$
   Using extended Euclid algorithm

2. Alice wants to send a message m to Bob:

a. She looks up his public key (N, e)

b. Computes $y \equiv m^e \bmod N$

(Using fast modular exponentiation alg. = repeated squaring)

c. She sends y

3. Bob wants to decrypt y:

a. He computes:

$$y^d \bmod N$$

Note, $y^d \equiv m^{ed} \equiv m \bmod N$,

since $de \equiv 1 \bmod (p-1)(q-1)$.

Generating random primes:

First fact: primes are dense.

<u>Prime number theorem:</u> For integer $x \geq 55$,

$$\pi(x) > \frac{x}{\log x + 2}$$

where $\pi(x) = \#$ of primes b/w 1 & x.

Choose a random n-bit number x.

$$Pr(x \text{ is prime}) \geq \frac{2^n / (\log(2^n)+2)}{2^n} = \frac{1}{n+2}$$

So with prob. $\approx \frac{1}{n}$ then x is prime.
if it is prime then it is a random n-bit prime #.
if it is not, then repeat, & in expectation we do $O(n)$ trials
& with high prob. we do $O(n \log n)$ trials.

How to check if x is prime?

Fermat's test:

if x is prime, then for all $a \in \{1, \dots, x-1\}$,

$$a^{x-1} \equiv 1 \bmod x.$$

What about composite x?

Say $a \in \{1, \dots, x-1\}$ is a Fermat witness if:

$$a^{x-1} \not\equiv 1 \bmod x$$

Since such an a proves that x is composite.

Note, for a where $\gcd(a,x) > 1$ then $a^{x-1} \not\equiv 1 \bmod x$

Since $a^{x-1} \bmod x$ is a multiple of $\gcd(a,x)$.

Thus, composite x has ≥ 2 Fermat witness.

Say a is a nontrivial Fermat witness if:

$$\gcd(a,x) = 1 \;\&\; a^{x-1} \not\equiv 1 \bmod x.$$

Carmichael numbers are composite x with no nontrivial Fermat witnesses, equivalently $a^x \equiv a \bmod x$ for all a

– they are rare, smallest are 561, 1105, 1729, …, but are an infinite number.

Lemma: Choose a u.a.r. from $\{1, \ldots, x-1\}$. If x is composite & not Carmichael, then

$$\Pr(a \text{ is a Fermat witness for } x) \geq 1/2.$$

Proof: Since x is composite & not Carmichael, it has ≥ 1 nontrivial Fermat witness, denote it as y. Thus, $\gcd(x,y)=1$

$$\& \ y^{x-1} \not\equiv 1 \bmod x$$

Let $B = \{b \in \{1, \ldots, x-1\} : b^{x-1} \equiv 1 \bmod x\}$ be the "bad" set

& $G = \{g \in \{1, \ldots, x-1\} : g^{x-1} \not\equiv 1 \bmod x\}$ be the "good" set.

We want to show that: $|G| \geq |B|$

& to do that we'll show an injective map $f: B \to G$.

For $b \in B$, $f(b) = (by) \bmod x$

Note, $(by)^{x-1} \equiv b^{x-1} y^{x-1} \equiv y^{x-1} \not\equiv 1 \mod x$

since $b^{x-1} \equiv 1 \mod x$

Thus, $f(b) \in G$.

And f is injective: for $b, b' \in B$ where $b \neq b'$,

Suppose $by \equiv b'y \mod x$

Since $\gcd(y, x) = 1$ then $y^{-1} \bmod x$ exists

So $b \equiv b' \mod x$

$\Rightarrow\Leftarrow$

∎

Primality testing algorithm (ignoring Carmichael #'s)

For n-bit x:

1. Choose $a_1, \dots, a_\ell$ u.a.r. from $\{1, \dots, x-1\}$
2. For $i = 1 \to \ell$:

   compute $a_i^{x-1} \bmod x$

3. a. If for all i, $a_i^{x-1} \equiv 1 \bmod x$

   then output "x is prime"

   b. If $\exists i$ where $a_i^{x-1} \not\equiv 1 \bmod x$

   then output x is composite.

For prime x, alg. always outputs x is prime.

For composite x which is not Carmichael,

Prob. alg. outputs x is prime is $\leq 2^{-\ell}$!

How to deal with Carmichael numbers?

For x, N if $x^2 \equiv 1 \bmod N$ then

x is a square root of $1 \bmod N$.

Note, $x \equiv 1 \bmod N$ & $x \equiv -1 \bmod N$

are always square roots of $1 \bmod N$.

any other one is a <u>nontrivial</u> square root of $1 \bmod N$.

<u>Claim:</u> For prime p no nontrivial square roots of $1 \bmod p$.

<u>Proof:</u> Let $N = p$.

Consider x where $x^2 \equiv 1 \bmod N$

thus, $x^2 = 1 + kN$ for some integer k.

$\cancel{x^2 - 1 \equiv 0 \bmod}$

$x^2 - 1 = kN$

$(x-1)(x+1) = kN$

This statement is only true for prime N

Since N divides RHS, it also divides LHS

Hence, N divides $x-1$ or $x+1$ & thus $x - 1 \equiv 0 \bmod N$ or $x+1 \equiv 0 \bmod N$ & $x \equiv 1 \bmod N$ or $x \equiv -1 \bmod N$. ∎

To prove x is composite it suffices to find a nontrivial square root of 1 mod N.

For composite $N \Rightarrow N$ is odd so $N-1$ is even.

hence, $N-1 = 2^t u$ where u is odd for some $t \geq 1$.

(take out as many factors of 2 as possible)

Fermat's test checked if $a^{x-1} \stackrel{?}{\equiv} 1 \mod x$ for random $a \in \{1, \dots, x-1\}$.

Let's do the same test by repeated squaring:

Compute:
$$a^{u} \mod x$$
$$a^{2u} \mod x$$
$$a^{2^2 u} \mod x$$
$$\vdots$$
$$a^{2^t u} \mod x \equiv a^{x-1} \mod x.$$

This is known as the Miller-Rabin the algorithm.

If $a^{x-1} \not\equiv 1 \bmod x$ then we know x is composite by Fermat's little theorem.

Suppose $a^{x-1} \equiv 1 \bmod x$.

go back to the first point where

$$a^{2^i u} \equiv 1 \bmod N$$

we know $a^{2^{i-1} u} \bmod N$ is a square root of $1 \bmod x$.

Is it non-trivial, i.e. is it $\not\equiv -1$?

If $a^{2^{i-1} u} \not\equiv -1 \bmod x$ then we proved x is composite.

For every composite x,

$\geq \frac{3}{4}$ of $a \in \{1, \ldots, x-1\}$

Provide a nontrivial square root of $1 \bmod x$ in this manner.

Example: $N = 561$.

$N-1 = 560 = 2^4 \times 35$

Choose $a \in \{1, \ldots, 560\}$, let's try $a = 8$.

Note, $\gcd(8, 561) = 1$.

$$8^{35} \equiv 461 \mod 561$$

$$8^{2 \cdot 35} \equiv 463 \mod 561$$

$$8^{2^2 \cdot 35} \equiv 67 \mod 561$$

$$8^{2^3 \cdot 35} \equiv 1 \mod 561$$

$$8^{2^4 \cdot 35} \equiv 1 \mod 561$$

Hence, 67 is a nontrivial square root

So that shows that 561 is composite.

Proof idea for Miller-Rabin test: (with prob. of success $\geq 1/2$ instead of $\geq 3/4$)

Let $\mathbb{Z}_x^* = \{a : 1 < a < x, \gcd(a,x) = 1\}$

Let $S_r = \{a \in \mathbb{Z}_x^* : a^r = \pm 1 \bmod n\}$

Lemma: if $\exists a \in \mathbb{Z}_x^*$ where $a^r \equiv -1 \bmod x$ then S_r is a proper subgroup of $\mathbb{Z}_x^*$ & hence $|S_r| \leq \frac{1}{2}|\mathbb{Z}_x^*|$

Proof idea: use this a to show that $\exists b \in \mathbb{Z}_x^*$ where $b \notin S_r$ & thus it's a proper subgroup. To do this we use the Chinese remainder theorem.