Finding Primes

$\pi(N) \sim \frac{N}{\log N}$.

$\#$ of primes $< N$

for integers of size $\sim N$, probability of $\frac{1}{\log N}$ of being prime.

finding primes reduces to primality testing.

Primality Testing.

Fermat's Little Theorem: Let p prime. Let a be coprime to p.

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

Fermat Primality Test

Let $n > 1$ be a number to test.

Choose $1 < a < n$. (Could test $\gcd(a, n)$.)

Compute $a^{n-1} \pmod{n}$.

If $a^{n-1} \not\equiv 1$ then n is not prime.

If $a^{n-1} \equiv 1$ then n is "probably prime".

Ex. ① $n = 1007$

Choose $a = 2$

Compute $2^{1006} \pmod{1007}$

$\equiv 271$

$\Rightarrow$ not prime

② $n = 1009$

Choose $a = 2$

Compute $2^{1008} \pmod{1009}$

$\equiv 1$

$\Rightarrow$ probably prime

Try $a = 3$

$3^{1008} \pmod{1009}$

$\equiv 1$

$\Rightarrow$ very probably prime.

③ $n = 561$

Choose $a = 2$

Compute $2^{560} \pmod{561}$

$\equiv 1$

$\Rightarrow$ probably prime

ACK! $3 \mid 561$.

$3^{560} \not\equiv 1$ (since 3 not inv.)

Notes: ① For more confidence, try more a's.

② Stronger versions, e.g. Miller-Rabin, Solovay-Strassen.

How many "fakers" (false positives).

For context, $x < 10^{10}$

3 455 052 511 primes

14 884 pseudoprimes to base $a=2$
(pass Fermat test w/ $a=2$).

3 291 strong pseudoprimes to base $a=2$
(pass Miller-Rabin w/ $a=2$)

0 strong pseudoprimes to base 2, 3, 5, 7 simultaneously.

A Carmichael number is an integer n s.t. for all $0<a<n$, if $\gcd(a,n)=1$ then $a^{n-1} \equiv 1 \pmod{n}$ but n is composite.

We know a lower bd for # of Carmichael #s up to X of $X^{1/3}$.

In practice we use "probably prime" (probabilistic) tests without any issue in cryptographic ranges.

Square roots & factoring

Sps $x^2 \equiv y^2 \pmod n$ but $x \not\equiv \pm y \pmod n$

Then $(x+y)(x-y) \equiv x^2 - y^2 \equiv 0 \pmod n$

$\not\equiv 0 \quad \not\equiv 0$

So $x+y$ and $x-y$ each contain proper factors of n (not 1 or n) but not n itself.

So $\gcd(x+y, n)$ and $\gcd(x-y, n)$ should be proper factors of n.

(finding interesting square roots mod n) $\Longrightarrow$ (factoring n)

Ex. $n = 29927$.

If we notice $544^2 \equiv 3^2 \pmod{n}$.

$\gcd(n, 544-3) = 541$

$\gcd(n, 544+3) = 547$

In fact, $n = 541 \cdot 547$.

Fermat factoring: If $n = x^2 - y^2$ then $n = (x+y)(x-y)$.

try $n + 1^2 \stackrel{?}{=} \square$

$n + 2^2 \stackrel{?}{=} \square$

$n + 3^2 \stackrel{?}{=} \square$ (544^2 in example) $\longrightarrow$ go to example.

This method detects $n = pq$ where p, q are very close in size

Moral: don't choose p, q similar in RSA.

Quadratic Sieve (to factor n)

Factor base of small primes: $2, 3, 5, \cdots, p_k < B$.

Obtain relations:

take $k \sim \sqrt{n}$

try to factor (in factor base):

$k^2 - n$

$(k+1)^2 - n$

$(k+2)^2 - n$

etc.

Ex. $n = 2201$

$47^2 - n = 2^3$

$49^2 - n = 2^3 \cdot 5^2$ $\Rightarrow$ $(47 \cdot 49)^2 \equiv 2^3 \cdot 2^3 \cdot 5^2$

$\equiv 2^6 \cdot 5^2 \pmod{n}$

$(3, 0)$

$+ (3, 2)$

$(6, 2)$ mod $\varphi(n)$