Composite tests and primality tests

Composite test: Answer "composite" has 100% certainty

Answer "prime" → probably prime

1. Fermat test (based on Fermat's little thm)

1. How to efficiently test if a number n is prime?

Attempt: check for all $m \leq \sqrt{n}$ if $m \mid n$

Takes $\sqrt{n} = 2^{1/2 \log n}$ (exponential running time!)

factorization methods from last sections. But those depend on certain parameter settings (recall definition of "s" in the (p−1) test). Also factoring is costly.

Easy test: Fermat test

1. Choose $1 < a < n$ randomly
2. Compute $d = \gcd(a, n)$.
3. If $d > 1$ → "composite"
4. Else Compute $b = a^{n-1} \bmod n$
5. If $b \neq 1$ → "composite"
6. Else "probably prime"

Cost exponentiation up to the power $(n-1)$

If n is a prime numbe then the answe is correct

If n is composite then the answer is wrong with probability

$$\frac{\# L_n}{\varphi(n)}$$

where $L_n = \{ a \in (\mathbb{Z}/n\mathbb{Z})^* \; ; \; a^{n-1} = 1 \}$

is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$.

Lagrange $\rightarrow$ $\# L_n \mid \underbrace{\#((\mathbb{Z}/n\mathbb{Z})^*)}_{= \varphi(n)}$ Eules tolient fct.

There are numbers n such that $L_n = (\mathbb{Z}/n\mathbb{Z})^\times$. They will produce "probably prime" as output of the Fermat test although they are composite.

Numbers which fool the Fermat test because they have $a^{n-1} \equiv 1 \bmod n$ $\forall\ a \in (\mathbb{Z}/n\mathbb{Z})^\times$ are called Charmichael numbers.

Smallest Charmichael number: $n = 561 = 3 \cdot 11 \cdot 17$

There are infinitely many such numbers.

Refine Fermat test!

Have to do better! Reduce failure prob!

Miller - Rabin test

Idea: In $\mathbb{F}_p^*$ there are only two solutions to $x^2 = 1$, namely 1 and $-1 \equiv p-1$.

If n has two factors, p_1 and p_2, then there are 4 solutions, namely

$$x \equiv \pm 1 \mod p_1$$

$$x \equiv \pm 1 \mod p_2$$

By the CRT there is a unique solution modulo $n = p_1 \cdot p_2$ for each of them

Miller Rabin has a lower chance to fail.

If $n = p_1 \cdots p_s$ then there are 2^s solutions to $x^2 = 1 \mod n$.

-1 shows up with prob $\frac{1}{2^s}$.

If $n = p_1 \cdot p_2$ then -1 shows up with $\frac{1}{4}$.

$$n-1 = 2^r \cdot l$$

Lemma

If n is prime and $\gcd(a, n) = 1$.

Then either $a^r \equiv 1 \mod n$

or $\exists\ 0 \le i < r$ such that

$$a^{2^i \cdot l} = -1 \mod n.$$

Proof Assume $a^r \neq 1$. And $a^{2^r \cdot l} = a^{n-1} \equiv 1 \pmod n$

Let $0 \le j < r$ be minimal such that $a^{2^j l} = 1$.

Our assumption says $j > 0$.

So $\left(a^{2^{j-1} l}\right)^2 = 1 \mod n$.

Since n is prime

$$a^{2^{j-1} l} = \pm 1$$

and because of the minimality of j it follows that $a^{2^{j-1} l} = -1$.

Algo Let $n-1 = 2^r \cdot l$, where l is odd.

Pick $1 < a < n$ randomly.

If $a^l \equiv \pm 1 \mod n \rightarrow$ "probably prime" (break)

Else Put $b = (a^l)_n$

For $i = 1$ to $r-1$ do

$b \leftarrow b^2 \mod n$ ← compute powers of b by repeated squaring

If $b = -1 \rightarrow$ "probably prime"

Else if $b = +1 \rightarrow$ "composite"

Output "composite"

After k tests with k independent random choices of a, the chance of a composite number showing up as "provably prime" is $\frac{1}{4^k}$.

AKS test: polynomial primality test deterministic

Can also use elliptic curves

ECPP (elliptic curve primality proving

$\rightarrow \mathbb{F}_p^* \rightarrow E(\mathbb{F}_p)$