Recap

# Primality Test

Content:

- How do we find prime number? in particular, a large prime number (prime number with 1024 bits, i.e., one with roughly 300 digits.
- To answer this, we first need to know how to test if an integer $n$ is prime.

## Brute Force

Try all integer less than or equal to $\sqrt{n}$ and check if the integer divides $n$.
Homework: Why checking less than or equal to $\sqrt{n}$ is sufficient?
Running Time: Exponential in the size of $n$ (the input).

## Fermat Primality Test

The Fermat primality test is a probabilistic test to determine whether a number is a "probable prime."

**Fermat Little Theorem**
If $p$ is a prime, then for any integer $a$ coprime to $p$,
$a^{p-1} \equiv 1 \bmod p$.

**Definition of witness**
An integer $a$ is a *witness* for $n$ if
$a^{n-1} \not\equiv 1 \bmod n$ ~~($\not\equiv$ means not congruent)~~

If one finds a witness to $n$, then $n$ must be a composite number.

Algorithm : aim to find a witness, then we can conclude $n$ is non-prime

Pick a random $a$, test if $a$ is a witness.

If $a$ is not a witness, we will try another value of $a$.

We skip $1, n-1$ because $1^{n-1} \equiv 1 \bmod n$ for all $n$ and

$(n-1)^{n-1} \equiv (-1)^{n-1} \equiv 1 \bmod n$ when $n$ is odd

**Algorithm**

Inputs: *n*: a value to test for primality, *n*>3; *k*: a parameter that determines the number of times to test for primality

Output: *composite* if *n* is composite, otherwise "*probably prime*"

Repeat k times:

Pick a randomly in the range [2, n − 2]

Test if $a^{n-1} \neq 1 \bmod n$, then return *composite.*

If *composite* is never returned, returned *probable prime.*

**Running Time**

$O(k \log^c(n))$ (The constant $c$ depends on the algorithm for modular exponentiation).

**Correctness**

Given a composite integer $n$, how likely is it we can find a witness?

If number of witness is large, then it is likely that we can find a witness after some $k$ repetitions.

However, it turns out that there exists a composite integer $n$ where it has NO witness!

Such an integer is called Carmichael number.

There are infinitely many of them.

Hencer, Fermat little test fail to recognize (infinitely many) Carmichael number as composite numbers.

## Theorem

If $p$ is an odd prime, then for all $a \in [1, \dots, p-1]$

(1) $a^{p-1} \equiv 1 \mod p$ (Fermat's little)

(2) the only square root of $1$ is $1$ and $-1$.

---

## proof (2)

Suppose $x \in \mathbb{Z}_p^*$ such that

$$x^2 = 1 \mod p$$

Then $x^2 - 1 = 0 \mod p$

$$(x-1)(x+1) = 0 \mod p$$

$p$ is prime. So, $p \mid x-1$ or $p \mid x+1$

This implies $x = 1$ or $x = p-1 \equiv -1 \mod p$

## Theorem

If $p$ is an odd prime, write $p-1 = 2^e q$ where $q$ is odd, then for $a \in [1, \dots p-1]$

Then one of the following two condition is true.

(a) $a^q \equiv 1 \mod p$

(b) $a^{2^i q} \equiv -1 \mod p$ for at least one $i$

$0 \le i < e$

---

Proof:

$$a^q \xrightarrow{\text{square}} a^{2q} \xrightarrow{\text{square}} a^{2^2 q} \xrightarrow{\text{square}} a^{2^3 q}, \dots, a^{2^e q} = 1$$

Because $p$ is prime, $a^{p-1} \equiv 1 \mod p$ by fermat's little

$$a^{2^e q} \equiv 1 \mod p$$

Since every subsequent element is square of previous element.
The list ends with a one.
There exists $b = a^{2^i q}$ in the list such that

$$b \not\equiv 1 \mod p \quad \text{but} \quad b^2 \equiv 1 \mod p$$

The only square root of $1$ in $\mathbb{Z}_p^*$ is $1$ and $-1$.

$b$ has to be equal $-1$.

## Algorithm

Aim to find a Miller-Rabin Witness:

Let $a$ be an integer from $[1, n-1]$.

We say $a$ is a Miller-Rabin Witness of $n$ if $n-1 = 2^e q$ where $q$ is odd

(a) $a^q \not\equiv 1 \mod n$

(b) $a^{2^i q} \not\equiv -1 \mod n$ for all $0 \leq i < e$

If a Miller-Rabin witness is found, then we conclude $n$ is not a prime.

# Algorithm

**Algorithm**
Inputs: *n*: a value to test for primality, *n*>3; *k*: a parameter that determines the number of times to test for primality
Output: *composite* if *n* is composite, otherwise "strong *probably prime*"

$n-1 = 2^e q$
$q$ is odd

repeat $k$ times:

pick $a$ number between $[2, n-2]$
Test if $a^q \not\equiv 1 \bmod n$ and $a^{2^i q} \not\equiv -1 \bmod n$ for $0 \le i < e$.
If yes, return "composite".

If composite is not return, return "strong probable prime"

# Complexity

Polynomial $O(k \log^3 n)$

# Accuracy

The error made by the primality test is measured by the probability that a composite number is declared probable prime.

**Proposition 3.18.** *Let $n$ be an odd composite number. Then at least 75% of the numbers $a$ between 1 and $n-1$ are Miller–Rabin witnesses for $n$.*

If $n$ is odd composite number, the probability that Miller-Rabin test return that it is a strong probable prime is at most $\left(\frac{1}{4}\right)^k$.

To generate a prime number, we use Miller-Rabin algorithm

---

Pick an integer $n$ of 1024 bit. ($2^{1023} < n < 2^{1024}$)

Run Miller-Rabin test on $n$ and some values of $t$

If the algorithm return $n$ is strong probable prime, then $n$ will be our prime number.

If not, repeat.

---

Will this algorithm terminate?

What is the expected number of trials?

How many prime numbers of 1024-bit?

# Distribution of Primes

**Definition.** For any number $X$, let

$$\pi(X) = (\#\text{ of primes } p \text{ satisfying } 2 \le p \le X).$$

**Theorem 3.21** (The Prime Number Theorem)**.**

$$\lim_{X\to\infty} \frac{\pi(X)}{X/\ln(X)} = 1.$$

Informally, when $X$ is large, $\pi(X) \simeq \dfrac{X}{\ln(X)}$

$$
\begin{aligned}
\#\text{ of 1024 bit primes} &= \#\text{ of primes in } (2^{1023}, 2^{1024}) \\
&= \pi(2^{1024}) - \pi(2^{1023}) \\
&= \frac{2^{1024}}{\ln(2^{1024})} - \frac{2^{1023}}{\ln(2^{1023})} \\
&\simeq 2^{1014}
\end{aligned}
$$

Expected number of a random 1024-bit number that we need to test until we successfully pick a prime number.

---

Informally, the prime number theorem tells us that a random chosen number N has probability $p = 1/\ln(N)$ of being prime.

If you pick a number in $[\frac{1}{2}N, \frac{3}{2}N]$, the probability that it is a prime number is $\frac{1}{\ln(N)}$

---

By Geometric distribution, the expected number of random 1024-bit numbers that we need to test until we pick a prime number is

$$\frac{1}{p} = \ln(N) = \ln(2^{1024}) \simeq 700.$$

---

In principal, we don't just pick a random number. Choose number that is not even, not divisible by 3, 5, 7, 11.