Primality

AA-GEI FIB, UPC

Spring 2025-2026

The Prime Number Theorem

Gauss, 1793 conjectured the result:

Theorem

Let $n \in \mathbb{Z}^+$ and let $\pi(n)$ be the number of primes $\leq n$, then

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

Corollary (To Prime Number Theorem)

Let p_n be the n-th. prime number, then the value of $p_n \sim n \ln n$

Fermat's Little Theorem and Luca's characterization

Theorem (Fermat's little Th.,XVII)

For any n prime and for all $a \in \mathbb{Z}_n^+$, $a^{n-1} \equiv 1 \mod n$.

Theorem (Eduard Lucas Primality-1876)

Let $a, n \in \mathbb{Z}^+$, then n is prime iff:

1. $a^{n-1} \equiv 1 \mod n$, *and*
2. *for all prime divisors q of $n-1$, we have $a^{(n-1)/q} \not\equiv 1 \mod n$.*

Primality problems

Primality problems

- **Primality problem**: given $n \in \mathbb{Z}^+$ with N-bits, is n prime?
  The Primality problem belongs to P
- Given an integer n, can we generate in polynomial time the n-th prime number?
- Given an integer N, can we generate in polynomial time a N-bit prime number?

The Primality problem: a naive algorithm

Naive algorithm:

Is $n \in \mathbb{N}$ prime?
for $a = 2, 3, \ldots, \sqrt{n}$ **do**
  if $a \mid n$ **then**
    return "composite", and STOP
return prime and STOP

Notice: for large n ($n = 2^{2024}$) the input is $N = \lg n$ i.e. $n = 2^N$
May need to check $O(\sqrt{n})$ integers for divisors of n, each check with a cost $O(N^2)$
$T(N) = O(2^{N/2} N^2)$ Too slow!

Test of pseudo-primality

n is a base a pseudo-prime if $a^{n-1} \equiv 1 \mod n$.

Test of pseudo-primality

n is a base a pseudo-prime if $a^{n-1} \equiv 1 \mod n$.

PseudoPrime(n)
$a =$ random $(1, n-1)$
if $a^{n-1} \equiv 1 \mod n$ **then**
  return pseudo-prime
else
  return not-prime

Cost: $O(N^3)$.

Test of pseudo-primality

n is a base a pseudo-prime if n is composite and $a^{n-1} \equiv 1 \mod n$.

PseudoPrime(n)
$a :=$ random $(1, n-1)$
if $a^{n-1} \equiv 1 \mod n$ **then**
  return pseudo-prime
else
  return not-prime

If the algorithm says not-prime, it is correct. It can err only if n is base 2 pseudo prime. Can we bound the error?

Carmichel numbers

- Recall Fermat's theorem: If n is prime, for $a \in \mathbb{Z}_n^+$, $a^{n-1} \equiv 1 \mod n$
- BUT $\exists n \in \mathbb{Z}$ s.t., for $a \in \mathbb{Z}_n^+$, $a^{n-1} \equiv 1 \mod n$ with n NOT a prime: Carmichael number.

Carmichel numbers

- Recall Fermat's theorem: If n is prime, for $a \in \mathbb{Z}_n^+$, $a^{n-1} \equiv 1 \mod n$
- BUT $\exists n \in \mathbb{Z}$ s.t., for $a \in \mathbb{Z}_n^+$, $a^{n-1} \equiv 1 \mod n$ with n NOT a prime: Carmichael number.
- Carmichael numbers are very rare (255 with value $< 10^8$) 561, 1105, $1729, \cdots$. For example $561 = 3 \cdot 11 \cdot 17$.

Carmichel numbers

- Recall Fermat's theorem: If n is prime, for $a \in \mathbb{Z}_n^+$, $a^{n-1} \equiv 1 \mod n$
- BUT $\exists n \in \mathbb{Z}$ s.t., for $a \in \mathbb{Z}_n^+$, $a^{n-1} \equiv 1 \mod n$ with n NOT a prime: Carmichael number.
- Carmichael numbers are very rare (255 with value $< 10^8$) 561, 1105, 1729, $\cdots$. For example $561 = 3 \cdot 11 \cdot 17$.
- A numerical conjecture is that the number of Carmichael numbers less than n is $\leq n^{2/7}$. (OEIS)

Lowering the error probability

- If we assume the non existence of Carmichael numbers: if n is prime, **PseudoPrime** always gives the correct answer, but if n is composite it errs in telling so with probability $\leq 1/2$.

Lowering the error probability

- If we assume the non existence of Carmichael numbers: if n is prime, **PseudoPrime** always gives the correct answer, but if n is composite it errs in telling so with probability $\leq 1/2$.
- **PseudoPrime** has one-side error, therefore *amplifying* k times the algorithm, the probability of error goes down to $\leq 1/2^k$.

Taking into account the Carmichael numbers

- $x \in \mathbb{Z}$ is a non-trivial root of 1 mod n, if it satisfies $x^2 \equiv 1 \mod n$, but $x \neq \pm 1 \mod n$.
- Example 6 is a non-trivial root of $1 \mod 35$: as $6^2 \equiv 1 \mod 35$ but $6 \neq \pm 1 \mod 35$.

Taking into account the Carmichael numbers

Theorem

If $p > 2$ is prime and $n = p^k$, for $k \geq 1$, the equation $x^2 \equiv 1 \mod n$ has only two solutions $x = 1$ and $x = -1$.

Corollary

If there exists a non-trivial square root of 1 $\bmod n$, then n is composite.

Miller-Rabin: Randomized Algorithm

G. Miller (1976), M. Rabin (1980)

- If equation $x^2 \equiv 1 \mod n$ has exactly solutions $x = \pm 1$ that implies n is prime.
- If there is another solution different than ± 1, then n can not be prime.
- To see if n is prime:
  Randomly choose an integer $a < n$, if $a^2 \equiv 1 \mod n$, then a is a non-trivial root of $1 \mod n$, so n is not prime. Such an n is denoted a witness to the compositeness of n.
  Otherwise, n may be or may be not a prime.

Miller-Rabin: Randomized Algorithm

- generate a random value $a \in \mathbb{Z}_n^+$,
- check if $a^{n-1} \equiv 1 \mod n$,
- in doing so look if an integer x s.t. x is a non-trivial square root of 1 mod n can be found.
- Repeat to decrease the probability of error.

Witness to the compositeness of n

Given an odd integer $n > 2$, and $a \in \mathbb{Z}_n^+$, we say that a is a witness to the compositeness of n, if either:

- $a^{n-1} \not\equiv 1 \mod n$
- $\exists m \in \mathbb{Z}_n^+$ s.t. $x = a^m$ is a non-trivial square root of $1 \quad \mod n$

We define a function Witness (a, n) to test if $a^{n-1} \not\equiv 1 \mod n$ or if we can find a non-trivial root of 1 mod n.

Witness (a, n)

Witness(a, n)
compute t and u s.t. $n - 1 = 2^t u$
$x_0 = a^u \mod n$
for $i = 1$ to t **do**
  $x_i = x_{i-1}^2 \mod n$
  if $x_i = 1 \wedge x_{i-1} \neq 1 \wedge x_{i-1} \neq n - 1$ **then**
    return true $\{x_i$ is a non-trivial root of $1\}$
if $x_t \neq 1$ **then**
  return true {Fermat's fails}
return false $\{a$ is not a witness$\}$

Example: Wish to to test if $a = 7$ is a witness to $n = 561$

$$N - 1 = 560 = \underbrace{100011}_{u}\underbrace{0000}_{2^t} \Rightarrow u = 35, t = 4$$

$x_0 = 7^{35} \mod 561 = 241$
$x_1 = 241^2 \mod 561 = 298$
$x_2 = 298^2 \mod 561 = 166$
$x_3 = 166^2 \mod 561 = 67$
$x_4 = 67^2 \mod 561 = 1$
Non-trivial root of $1 \mod 561$.

The cost of **witness**(a, n) is $O(N^3)$.

Miller-Rabin primality test.

Polynomial time randomized algorithm to decide if a given $n \in \mathbb{Z}$ is prime. The input to the algorithm would be n and the number s of $a \in \mathbb{Z}$ that we will test for witness.

Miller-Rabin(n, s)
for $i = 1$ to s **do**
  $a = \text{random } (1, n-1)$
  if **witness** $(a, n) = \text{true}$ **then**
    return non-prime {Definitely}
return prime. {Almost surely}

The complexity of the algorithm is $O(sN^3)$.

Correctness

Theorem

If n is an odd composite number, the number of witnesses to the compositeness of n is $\geq \frac{n-1}{2}$.

Correctness

Theorem

If n is an odd composite number, the number of witnesses to the compositeness of n is $\geq \frac{n-1}{2}$.

Theorem

For any odd integer $n > 2$ and $s \in \mathbb{Z}^+$ the probability that Miller-Rabin(n, s) errs is $\leq 2^{-s}$.

Correctness

Theorem

If n is an odd composite number, the number of witnesses to the compositeness of n is $\geq \frac{n-1}{2}$.

Theorem

For any odd integer $n > 2$ and $s \in \mathbb{Z}^+$ the probability that Miller-Rabin(n, s) errs is $\leq 2^{-s}$.

Proof.

- If n is composite, Miller-Rabin errs if it misses to discover a witness in the s iterations.
- If n is composite, each execution of the algorithm has probability $\geq 1/2$ of discovering a witness a.
- The probability it misses in all iterations is $< 1/2^{-s}$.

□

Procedure to Generate a large Prime Integer n

1. Choose a random odd N-bit number n,
2. Run Miller-Rabin on n, if passes, output n,
3. else repeat the process at most s times.

With probability $O(1/N)$, n will be prime $\Rightarrow$ n will pass Miller-Rabin.

Using Bayes, the probability that n is prime given that Miller-Rabin has returned prime is $\frac{1}{1+2^{-s}(\ln n-1)}$

Which is below $1/2$ until s exceeds $\log(\ln n - 1)$.

In practice, $s = 50$ suffices for most of the practical applications.