Primality Testing

Aaditya Bilakanti
abilak@gmail.com

Euler Circle

July 7, 2024

Table of Contents

Introduction

Definition and Uses

Primality Testing, as the name suggests, determines if a number n is prime. This is useful in cryptography, which uses large prime numbers.

A Simple Test

A simple test to determine if n is prime:

- Test all numbers $\leq \sqrt{n}$
- If any of these numbers divide n, n is composite
- Otherwise, n is prime
- Optimizations
  - Only test numbers of the form $6k \pm 1$
- Time complexity of $\mathcal{O}(\sqrt{n})$

Probabilistic Tests

Fermat Primality Test

Theorem 2.1 (Fermat's Little Theorem)

Let a, p be positive integers, where p is prime. The following congruence holds:

$$a^p \equiv a \pmod{p}. \tag{2.1}$$

If a and p are relatively prime, then 2.1 can be simplified to:

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2.2}$$

- Fermat Primality Test evaluates $a^{n-1} \equiv 1 \pmod{n}$ for all integers n.
- Higher accuracy with k iterations
- Time complexity of $\tilde{\mathcal{O}}(k \log^2(n))$

Fermat Primality Test

- Fermat Primality Test fails because of Carmichael Numbers
  - Numbers satisfying $a^{n-1} \equiv 1 \pmod{n}$ for all a coprime to n
- Infinitely many of them

Theorem 2.2 (Korselt's Criterion)

A number n is a Carmichael number if $p-1 \mid n-1$ for all prime divisors $p \mid n$, n is odd, and n is squarefree.

561 is the first Carmichael number.

$$47^{560} \equiv 1 \pmod{561}$$
$$59^{560} \equiv 1 \pmod{561}$$
$$28^{560} \equiv 1 \pmod{561}$$

Solovay–Strassen Test

Definition 2.3

We define the Legendre Symbol $\left(\frac{a}{p}\right)$, where p is an odd prime number and $a \in \mathbb{Z}$, as following:

1. $\left(\frac{a}{p}\right) = 1$ if a is a quadratic residue modulo p and $a \not\equiv 0 \pmod{p}$
2. $\left(\frac{a}{p}\right) =$ -1 if a is a non-quadratic residue modulo p
3. $\left(\frac{a}{p}\right) = 0$ if $a \equiv 0 \pmod{p}$.

Definition 2.4

We define the Jacobi Symbol $\left(\frac{a}{n}\right)$, where $a \in \mathbb{Z}$, n is an odd positive integer and is factorized as $p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$, as following: $\left(\frac{a}{p_1}\right)^{a_1} \cdot \left(\frac{a}{p_2}\right)^{a_2} \ldots \left(\frac{a}{p_k}\right)^{a_k}$, where each of the terms are Legendre Symbols.

Solovay–Strassen Test

Theorem 2.5 (Euler's Criterion)

Let $a \in \mathbb{N}$ and p be an odd prime such that $\gcd(a, p) = 1$. *Then,*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}. \tag{2.3}$$

- Solovay–Strassen test generalizes to $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$
- Any n can be a pseudoprime to at most $\frac{1}{2}$ of the bases
- Running k iterations gives a higher accuracy
- Time complexity is $\mathcal{O}(k \log^3(n))$

Example

Let's say we want to see if 15 is prime, and we choose the base 7. We have:

$$7^7 \equiv \left(\frac{7}{15}\right) \pmod{15}$$
$$7^7 \equiv -1 \pmod{15}$$
$$13 \not\equiv -1 \pmod{15}$$

Therefore, 15 is not prime.

Miller–Rabin Test

Let n be an odd integer. Factor $n-1=2^s d$ (where d is odd), and pick a positive integer a relatively prime to n. n is a strong probable prime if:

$$a^d \equiv 1 \pmod{n}$$

or

$$a^{2^r d} \equiv -1 \pmod{n}, \text{ for some } 0 \leq r < s.$$

EXAMPLE

We try to see if 53 is prime. We find that $53-1=2^2 \cdot 13$, so $s=2$ and $d=13$. We pick a as 19. We now perform the test. We find that $19^{13} \not\equiv 1 \pmod{53}$. However, we do find in the second equation that when $r=1$, then $19^{2 \cdot 13} \equiv -1 \pmod{53}$, thus showing that 53 is prime.

Proof

We now show that if n is a prime p, then it passes the Miller–Rabin test. Let's say we factor $p-1$ as $2^s d$ where d is odd. We then pick an x such that $\gcd(x,p)=1$.

Let us have the polynomial $x^{p-1}-1$. By FLT, we know $x^{p-1}-1 \equiv 0 \pmod{p}$. We can repeatedly factor with difference of squares to give us:

$$(x^d-1)(x^d+1)(x^{2d}+1)(x^{4d}+1)\dots(x^{2^{s-1}d}+1) \equiv 0 \pmod{p}.$$

Note that since p is prime, one of the factors is 0 modulo p. Thus, either $x^d \equiv 1 \pmod{p}$ or $x^{2^r d} \equiv -1 \pmod{p}$, for some $0 \le r < s$. We thus shown that any prime p passes the test.

Properties

- Any n can be a pseudoprime to at most $\frac{1}{4}$ of the bases
- Run k iterations of the test
- Time complexity of $\mathcal{O}(k \log^3(n))$
  - FFT-based multiplication gives $\mathcal{O}(k \log^2(n))$

Deterministic Tests

AKS Primality Test

The AKS Primality Test was the first deterministic, unconditional, and general primality test. The test is based off of a corollary of FLT:

Corollary 3.1

Given an $n \geq 2$, and an $a \in \mathbb{N}$ relatively prime to n, n is prime if and only if:

$$(X + a)^n \equiv X^n + a \pmod{n},$$

is true within the polynomial ring $\mathbb{Z}/n\mathbb{Z}[X]$. Here, X is the indeterminate generating the polynomial ring.

The test can be made more efficient by taking it modulo $X^r - 1$ and p. In other words, there exists polynomials $f(x)$ and $g(x)$ such that:

$$(X + a)^n - (X^n + a) = (X^r - 1)g(x) + n \cdot f(x). \tag{3.1}$$

This reduces the amount of computation needed in Corollary 3.1.

AKS Primality Test

Definition 3.2 (AKS Algorithm)

The AKS Primality Test is as follows:

1. Check if n is a perfect power. If n is, then output that n is composite.
2. Find the smallest r such that $\mathrm{ord}_r(n) > \log_2^2(n)$.
3. For all $2 \leq a \leq \min\{r, n-1\}$, check that $a \nmid n$. Otherwise, n is composite.
4. If $n \leq r$, then n is prime.
5. For $a = 1$ to $\left\lfloor \sqrt{\phi(r)\log_2(n)} \right\rfloor$ perform Equation 3.1 (defined on the previous slide). If n does not satisfy one of the equations, then n is composite.
6. If the test has reached here, output that n is prime.

AKS Primality Test

The time complexity of the AKS Algorithm is $\tilde{\mathcal{O}}((\log(n))^{12})$. However, this could be cut down to $\tilde{\mathcal{O}}((\log(n))^{6})$ if the Sophie Germain Prime Density Conjecture is true. The conjecture is as follows:

Conjecture 3.3 (Sophie Germain Prime Density Conjecture)

The number of primes $q \leq m$ such that $2q+1$ is also a prime is asymptotically $\frac{2C_2}{\ln^2(m)}$, where C_2 is the twin prime constant(approximately 0.66*).*

Thanks for Listening!

Thanks for Listening! Any questions?