AKS Primality Testing

Aman K. Foujdar
Ashoka University

Manindra Agrawal, Neeraj Kayal, and Nitin Saxena

Introduction

Primality testing, a fundamental aspect of number theory and cryptography, determines whether a given number is prime. The AKS algorithm is a polynomial-time deterministic algorithm for primality testing. Unlike probabilistic tests, the foundations of the AKS algorithm is set on congruence in polynomials. Thus, it guarantees a definitive answer, ensuring the accuracy required for high-stakes applications in cryptography.

Main Theorem

The AKS algorithm is based on the following theorem:

Theorem 1. ***(Theorem of Agrawal, Kayal, and Saxena).*** *Let $r \in \mathrm{cp}(n)$ be a prime number with $\mathrm{ord}_r(n) > 4(\log n)^2$. Also set $Q := X^r - 1$. If n is not a power of p, then there are at most r polynomials of the form $P = X + a$, with $a \in \{0, \dots, p-1\}$, that satisfy*

$$(P(X))^n \equiv P(X^n) \pmod{p, Q}. \tag{1}$$

Here, the set $\mathrm{cp}(n)$ denotes the collection of all integers from 1 to $n-1$ that are coprime to n.

The AKS Algorithm

Input: integer $n > 1$.

1. If ($n = a^b$ for $a \in \mathbb{N}$ and $b > 1$), output COMPOSITE.
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \le r$, output COMPOSITE.
4. If $n \le r$, output PRIME.[1]
5. For $a = 1$ to $\left\lfloor \sqrt{\varphi(r)} \log n \right\rfloor$ do
   if $((X + a)^n \not\equiv X^n + a \pmod{X^r - 1, n})$, output COMPOSITE;
6. Output PRIME;

Foundation = Fermat

Fermat's Little Theorem states that if p is a prime number and a is an integer not divisible by p, then

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

Theorem 2. ***(Fermat for polynomials).*** *Let p be a prime number. Then*

$$(P(X))^p \equiv P(X^p) \pmod{p} \tag{2}$$

for all polynomials P with integer coefficients.

Let l denote the number of elements $a \in \mathbb{N}_0$ with $a \le p - 1$ for which the polynomial $X + a$ belongs to $\mathcal{P}$. We define H as an irreducible factor of Q modulo p, A as the number of elements of $\mathcal{P}$ that are pairwise distinct modulo p and H, and t as the number of polynomials of the form $X^{n^i \cdot p^j}$, where $i, j \ge 0$, that are pairwise distinct modulo p and H.

$$X^r - 1 = (X - 1) \cdot (X^{r-1} + X^{r-2} + \cdots + X + 1).$$

Here, the polynomial

$$K_r := X^{r-1} + X^{r-2} + \cdots + X + 1 \tag{3}$$

is called the ***r-th cyclotomic polynomial***.

Theorem 3. *If $t > 4(\log n)^2$ and $l \ge t - 1$, then n is a power of p.*

Theorem 4. *Let r and p be prime numbers with $r \ne p$, and let H be an irreducible factor (modulo p) of the r-th cyclotomic polynomial K_r. Also, let $n \in \mathbb{N}$ be any multiple of p such that $\gcd(n, r) = 1$. Then $\mathrm{ord}_r(n) \le t \le r$.*

Proof(Theorem of Agrawal, Kayal, and Saxena). Let n and p be as before, where p is a prime number and n is a multiple of p. Also, let r be a prime number that is coprime to n and satisfies $\mathrm{ord}_r(n) > 4(\log n)^2$. Since r is coprime to n, we have $r \ne p$.
From theorem 3, we know that

$$4(\log n)^2 < t \le r,$$

where t is the number of distinct polynomials X^m modulo p and H.
Now, let l denote the number of integers $a \in \{0, \dots, p-1\}$ for which $X + a$ satisfies the condition in the AKS equation. Suppose that $l \ge r$. Then, we have $l \ge t \ge t - 1$. By theorem 2, n must be a power of p. This proves our main theorem.

□

Asymptotic Time Complexity and Improvements

The asymptotic time complexity of the AKS algorithm is $O \sim (\log^{21/2} n)$. Over time, several improvements have been proposed, including an algorithm by Lenstra and Pomerance, which offers a better running time by using a different polynomial for testing congruences. However, despite these improvements, no deterministic primality test has yet surpassed the efficiency of the Miller-Rabin test for practical use, leaving much room for further developments in the field.