Various Primality Tests

Soham Samanta

July-August 2024

Abstract

Primality testing is an important topic in cryptography and various other fields of mathematics. It is necessary to use primality testing for cryptography encrypting methods such as RSA[1] and Diffie-Hellman[2]. In this paper, we discuss and prove the Fermat Primality Test and Lucas-Lehmer Test[3,4]. We also find counter-examples and improvements for the Fermat Primality Test. In addition, we find the Time Complexity of running these primality tests using different multiplication/exponentiation algorithms, such as the Schöhage-Strassen algorithm[5] and the binary exponentiation algorithm.

1 Introduction

Primality testing is a very important topic in cryptography. For example, in the RSA cryptosystem it is necessary to choose large prime numbers p and q, but how can we check if p and q are primes quickly? There are various primality tests with different complexities that have different usages depending on the size of p and q.

The most basic primality test is trial division. It is easy to prove that if there is a composite number, say n, then n must have a factor from the range 2 to $\sqrt{n}$. This immediately gives an algorithm to check whether n is prime or not: Iterate through all i from 2 to $\sqrt{n}$, if for any i we have that n is a multiple of i, then n is composite, otherwise n is prime.

In 1640, French mathematician Pierre de Fermat proved Fermat's little theorem which is the basis of the Fermat Primality Test. It states the following:

Theorem 1.1. *For a prime p, if $\gcd(a, p) = 1$, $a^{p-1} \equiv 1 \pmod{p}$.*

In 1878, French mathematician Édouard Lucas proposed the Lucas-Lehmer test, and in 1930 Derrick Lehmer proved the test. Nowadays, there are many other primality tests such as the AKS test and the Miller-Rabin test. In this paper, we focus on the Fermat Primality Test and the Lucas-Lehmer Test.

2 Fermat Primality Test

This test is one of the most simple tests that works for all primes, but it is quite easy to find counter-examples.

The Fermat Primality Test is the following:

Theorem 2.1. *Consider an integer n. Choose an integer a such that* $\gcd(a, n) = 1$. *If n is prime then* $a^{n-1} \equiv 1 \pmod{n}$.

Proof. This is exactly Fermat's Little Theorem. But note, that if n is composite, it could be possible that $a^{n-1} \equiv 1 \pmod{n}$. □

2.1 Counter Examples and Improvements

Note that there are many different counter-examples to this primality test.

For example, if we consider when $a = 2$ and $n = 341$, we have that $2^{340} \equiv 1 \pmod{341}$. Here we say that 341 is a Base 2 Fermat pseudoprime. A more general example are the Carmichael numbers. One can notice that for all a such that $\gcd(a, n) = 1$, we have that n is a Base a Fermat pseudoprime.

Cipolla[6] showed that there are an infinite number of Base a Fermat pseudoprimes. Kim and Pomerance[7] showed that for a random odd number $n \leq k$ the probability that n is a b Fermat pseudoprime, where b is a random number $1 < b < n - 1$ is less than $2.77 \cdot 10^{-8}$ for $k = 10^{100}$.

An improvement to the general Fermat Primality Test is to run it multiple times, to reduce the number of counter-examples. But, no matter how many tests you will run, Carmichael numbers will always pass the test. Let $C(x)$ be the number of Carmicheal numbers less than x. Erdős[8] previously showed the following:

$$C(x) < xe^{\frac{-k_2 \log(x) \log(\log(x))}{\log(\log(x))}}$$

Here, k_2 is some constant.

It has been previously calculated that $C(10^{21}) < 3 \cdot 10^8$, so the probability of choosing a Charmiceal number is less than 10^{-12}.

2.2 Time Complexity

Theorem 2.2. *If we apply binary exponentiation and fast multiplication our final complexity is* $O(\log^2(n) \cdot \log(\log(n)))$

Proof. Using binary exponentiation, we need to square a number at most $\log(n)$ times, so using FFT, we get a complexity of $O(\log(n) \cdot \log(n) \cdot \log(\log(n)))$, as desired. □

3 Lucas-Lehmer Test

Let p be a prime number. Let $M_p = 2^p - 1$.

Definition 1. *We call M_p a Merssene number.*

We define a sequence s_i for $i \geq 1$. We let $s_1 = 4$ and for $i \geq 2$, $s_i = s_{i-1}^2 - 2$. The Lucas-Lehmer Test states the following:

Theorem 3.1. *M_p is prime if and only if s_{p-1} is a multiple of M_p, which is equivalent to $s_{p-1} \equiv 0 \pmod{M_p}$.*

We prove the correctness of the Lucas-Lehmer Test by proving Theorems 3.4 and 3.5. Let $\omega = 2 + \sqrt{3}$, $\bar{\omega} = 2 - \sqrt{3}$.

Lemma 3.2. $s_m = \omega^{2^{m-1}} + \bar{\omega}^{2^{m-1}}$.

Proof. We prove this with induction.

Base Case: $m = 1$, we get $\omega + \bar{\omega} = 4$, which is true. Inductive Hypothesis: Assume $s_m = \omega^{2^{m-1}} + \bar{\omega}^{2^{m-1}}$. We show this is true for $m + 1$. Inductive Step: Notice, we have $s_{m+1} = \omega^{2^m} + \bar{\omega}^{2^m} + 2(\omega\bar{\omega})^{2^{m-1}} - 2 = \omega^{2^m} + \bar{\omega}^{2^m}$. □

Lemma 3.3. *If G is a finite group, then the order of any element is at most the order of the group.*

Proof. This is trivial by Lagrange's theorem which states the order of any element in the group is a divisor of the order of the group. □

We start by proving the following theorem:

Theorem 3.4. *If $s_{p-1} \equiv 0 \pmod{M_p}$, we have that M_p is a prime number.*

Proof. Assume $s_{p-1} \equiv 0 \pmod{M_p}$. Let $\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} = kM_p$ for some integer k.

Notice we have that $\omega\bar{\omega} = 1$, so if we multiply both sides by $\omega^{2^{p-2}}$, we get the following:

$$\omega^{2^{p-1}} + 1 = kM_p\omega^{2^{p-2}}$$

Now, for sake of contradiction, we assume that M_p is composite. Let q be the smallest prime factor of M_p. It is obvious that $q > 2$ because $M_p \equiv 1 \pmod{2}$.

Let G be the set of all elements $a + b\sqrt{3}$, where $0 \leq a, b < q$ and $a, b \in \mathbb{Z}$. Multiplication is trivial, we multiply $(a + b\sqrt{3})(c + d\sqrt{3})$ and take the integer part and the $\sqrt{3}$ part, and reduce both of them modulo q. It is easy to see that this makes G a closed set. Notice, we must have that ω and $\bar{\omega}$ are both elements of G.

Let H be the set of elements that has an multiplicative inverse in G.It is easy to

see that H is group. Notice that $|H| \leq q^2 - 1$ because we know that 0 doesn't have an inverse and there are q^2 elements in G.

Now, since we have that $q \mid M_p$, we have that $kM_p\omega^{2^{p-2}}$ is 0, when considered an element in G. Notice from the equation $\omega^{2^{p-1}} + 1 = kM_p\omega^{2^{p-2}}$, we get $\omega^{2^{p-1}} = -1$ and $\omega^{2^p} = 1$.

We have that ω is also an element of H with order 2^p, this means that $2^p \leq q^2 - 1$. Since q is the smallest prime factor of M_p, we have that $q^2 \leq M_p$, so we need that $2^p < M_p = 2^p - 1$, which is an obvious contradiction. □

We now prove another theorem.

Theorem 3.5. *If M_p is prime then we have that $s_{p-1} \equiv 0 \pmod{M_p}$.*

Proof. Assume M_p is a prime number. Let G be the set of all elements $a + b\sqrt{3}$, where $0 \leq a, b < M_p$ and $a, b \in \mathbb{Z}$.

Now, since M_p is a prime number, we have that for all k such that $0 < k < M_p$, $\binom{M_p}{k}$ is a multiple of M_p. Thus, we get $(1 + \sqrt{3})^{M_p} \equiv 1 + (\sqrt{3})^{M_p} \pmod{M_p}$.

Now, by the quadratic reciprocity law, we have that $\left(\frac{M_p}{3}\right)\left(\frac{3}{M_p}\right) = (-1)^{\frac{M_p-1}{2}}$. Since $M_p \equiv 3 \pmod 4$, we must have that M_p is a quadratic residue modulo 3 and 3 is not a quadratic residue modulo M_p or vice versa. But, notice that $M_p \equiv 1 \pmod 3$, so we need that $3^{\frac{M_p-1}{2}} \equiv -1 \pmod p$, so $(\sqrt{3})^{M_p} \equiv -\sqrt{3} \pmod{M_p}$.

Thus, we have $(1 + \sqrt{3})^{M_p} \equiv 1 - \sqrt{3} \pmod{M_p}$. Multiplying both sides by $1 + \sqrt{3}$, we get that $(1 + \sqrt{3})^{M_p} \equiv -2 \pmod{M_p}$, so we get $(2\omega)^{\frac{M_p+1}{2}} \equiv -2 \pmod{M_p}$.

Notice, we have that $M_p \equiv -1 \pmod 8$, so we have that 2 is a quadratic residue $\pmod{M_p}$, so we simplify the left-hand side to get the equation:

$$2\omega^{\frac{M_p+1}{2}} \equiv -2 \pmod{M_p}$$

Notice that the inverse of 2 modulo M_p is $\frac{M_p+1}{2}$, so we can multiply both sides by this to get $\omega^{\frac{M_p+1}{2}} \equiv -1 \pmod{M_p}$.

We can rewrite this as

$$\omega^{2^{p-1}} \equiv \omega^{2^{p-2}}\omega^{2^{p-2}} \equiv -1 \pmod{M_p}$$

Multiplying both sides by $\bar{\omega}^{2^{p-2}}$, we get that $\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}$, which implies that $s_{p-1} \equiv 0 \pmod{M_p}$, as desired. □

Now we prove the Lucas-Lehmer test.

Theorem 3.6. *M_p is prime if and only if s_{p-1} is a multiple of M_p, which is equivalent to $s_{p-1} \equiv 0 \pmod{M_p}$.*

Proof. Combining Theorem 3.4 and Theorem 3.5, we get that M_p is prime if and only if $s_{p-1} \equiv 0 \pmod{M_p}$, as desired. □

3.1 Time Complexity

We also prove the complexity of the Lucas-Lehmer test with basic multiplication and with the Schönhage–Strassen algorithm.

Theorem 3.7. *The complexity with basic multiplication is just $O(p^3)$. The complexity with the Schönhage-Strassen algorithm which applies FFT is $O(p^2 \cdot \log(p) \cdot \log(\log(p)))$*

Proof. Notice that the recurrence formula for s_p, needs squaring. When using basic multiplication, we can do this in $O(p^2)$ time, which would result in a total complexity of $O(p^3)$ because we apply this p times. But, the Schönhage-Strassen algorithm can multiply two numbers in $O(p \cdot \log(p) \cdot \log\log(p))$, which would result in a complexity of $O(p^2 \cdot \log(p) \cdot \log\log(p))$. □

References

[1] Ronald R. Rivest, Adi Shamir, Leonard Adleman (1978) *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*

[2] Whitfield Diffie, Martin E. Hellman (1976) *New Directions in Cryptography*

[3] Micheal I. Rosen (1988) *A proof of the Lucas-Lehmer Test*

[4] James B. Bruce (1993) *A Really Trivial Proof of the Lucas-Lehmer Test*

[5] Arnold Schönhage, Volker Strassen (1971) *Fast multiplication of large numbers*

[6] Michele Cipolla (1904) *On the composite numbers P, which verify Fermat's congruence*

[7] Su H. Kim, Carl Pomerance (1989) *The Probability that a Random Probable Prime is Composite*

[8] Paul Erdős (1956) *On psuedoprimes and Carmicheal numbers*