PRIMALITY TESTING

AADITYA BILAKANTI

Abstract. This paper covers and analyzes various different primality tests, including some "lesser known ones". We also investigate the distribution of primes whose first Euler–Jacobi Pseudoprime is not a Carmichael number.

Contents

1. Introduction

A prime number is a number that only divides 1 and itself, first defined by Euclid. He also proved that there are an infinite amount of primes. Another Greek mathematician, Eratosthene, created a method in order to find prime numbers called the Sieve of Eratosthenes. The algorithm first involved listing all the numbers from 2 through an integer n, giving us

Date: July 13, 2024.

the list $2, 3, 4, \ldots, n$. We then take the smallest number in the list and "cross out" all of its multiples (starting at 2 in this case): $2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, \ldots, n$. We now repeat this for 3, and so on. The numbers left at the end of this process are primes. However, this method is extremely inefficient for large primes. Another method to determine the primality of n is to check if n is divisible by any of the numbers from 2 through $n-1$. However, this also gets quite inefficient for large n (the time complexity is $\mathcal{O}(n)$), so a small optimization can be made, which is that we only have to test the numbers $\leq \sqrt{n}$. We prove this below:

Theorem 1.1. *If a number n is not divisible by any of the positive numbers $\leq \sqrt{n}$, then n is prime.*

Proof. Suppose that n divides a positive integer q such that $2 \leq q \leq \sqrt{n}$. This would mean that n is composite. If n did not divide any such integer, this would mean that n is prime, since this implies that there are no factors $\geq \sqrt{n}$ that divide n. Note that $\frac{n}{q} \geq \sqrt{n}$, since $\frac{n}{q} \geq \frac{n}{\sqrt{n}} = \sqrt{n}$. Therefore, it is redundant to check numbers $> \sqrt{n}$ if we already know that no numbers $\leq \sqrt{n}$ divide n. ■

We can slightly optimize this further by noticing that a prime must be of the form $6k \pm 1$, so therefore, we only have to test numbers of the form $6k \pm 1$ that are $\leq \sqrt{n}$. We now define certain types of algorithms that we reference throughout the paper:

Unconditional: An algorithm is unconditional if it does not use any unproven theorems or conjectures. The opposite of this is a conditional test, meaning that it does depend on certain unproven conjectures.

General: A general algorithm works for any number n, and does not rely on specific qualities of the number.

Deterministic: An algorithm is deterministic if it gives the same result every time it is run. In the context of Primality Testing, it would also mean that the algorithm always identifies whether a number is a prime or a composite correctly.

Probabilistic: An algorithm is probabilistic if it does not give the same result every time. Rather, it gives an answer with some chance that it is correct. Probabilistic tests often require multiple iterations to give an answer with reasonable confidence.

2. Preliminaries

We first define some useful symbols that will be needed later on in the paper:

Definition 2.1. We define $\left(\frac{a}{p}\right)$ as the **Legendre Symbol**, where p is an odd prime number and $a \in \mathbb{Z}$ as follows:

(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 2.2. Let n be an odd positive integer that can be factorized as $p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ \ldots \ \cdot p_k^{b_k}$ ($p_1, p_2, p_3 \ldots p_k$ are prime numbers), and let $a \in \mathbb{Z}$. We define the Jacobi Symbol, $\left(\frac{a}{n}\right)$, as follows:

$$\left(\frac{a}{p_1}\right)^{b_1} \cdot \left(\frac{a}{p_2}\right)^{b_2} \cdot \left(\frac{a}{p_3}\right)^{b_3} \cdot \ \ldots \ \cdot \left(\frac{a}{p_k}\right)^{b_k},$$

where $\left(\frac{a}{p}\right)$ is the Legendre Symbol.

We now will give the following lemmas about the Jacobi Symbol, which be will be particularly useful to us when going over the Solovay–Strassen test. The proofs for these are omitted, as they mainly rely on the properties of Jacobi Symbols. See [Bur10] for these proofs.

Lemma 2.3. *If $a \equiv b \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$, where a, b, and n are integers.*

Lemma 2.4. *Let a and n be integers. If either the top or the bottom argument of the Jacobi Symbol $\left(\frac{a}{n}\right)$ is fixed, then the Jacobi Symbol is completely multiplicative for the remaining argument.*

Lemma 2.5. *Let a and n be integers. If $\gcd(a, n) = h$, where $h \neq 1$ then $\left(\frac{a}{n}\right) = 0$. Otherwise, $\left(\frac{a}{n}\right) = \pm 1$.*

Theorem 2.6 (Law of Quadratic Reciprocity)**.** *If a and b are odd positive relatively prime integers, then:*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = -1^{\frac{a-1}{2} \cdot \frac{b-1}{2}},$$

where $\left(\frac{a}{b}\right)$ and $\left(\frac{b}{a}\right)$ are Jacobi Symbols. If n or $m \equiv 1 \pmod{4}$, then $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = 1$. If $n \equiv m \equiv 3 \pmod{4}$, then $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = -1$.

Lemma 2.7 (1st supplement of the Law of Quadratic Reciprocity)**.** *Let n be an odd positive integer. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$, where $\left(\frac{-1}{n}\right)$ is the Jacobi Symbol. If $n \equiv 1 \pmod{4}$, then$\left(\frac{-1}{n}\right) = 1$. Otherwise, if $n \equiv -1 \pmod{4}$, then $\left(\frac{-1}{n}\right) = -1$.*

Lemma 2.8 (2nd supplement of the Law of Quadratic Reciprocity)**.** *Let n be an odd positive integer. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$, where $\left(\frac{-1}{n}\right)$ is the Jacobi Symbol. If $n \equiv \pm 1 \pmod{8}$, then $\left(\frac{-1}{n}\right) = 1$. Otherwise, if $n \equiv \pm 3 \pmod{8}$, then $\left(\frac{-1}{n}\right) = -1$.*

Definition 2.9. We define the notation $\mathrm{ord}_a(b)$ to be the multiplicative order of b modulo a. The multiplicative order of b modulo a is the smallest number d such that $b^d \equiv 1 \pmod{a}$. Note that a and b must be relatively prime.

We now prove a useful theorem about orders:

Theorem 2.10. *Let a and b be positive integers that are relatively prime, and let n be an integer such that $a^n \equiv 1 \pmod{b}$. Then $d \mid n$, where $d = \mathrm{ord}_b(a)$.*

Proof. Let $n = qd + r$, where q is a positive integer and $0 \leq r < d$. We therefore see that $a^n \equiv 1 \pmod{n}$ can be represented as $a^{qd+r} \equiv 1 \pmod{n}$. We know that $a^{qd} \equiv 1 \pmod{n}$, so we have $a^r \equiv 1 \pmod{n}$. However, since we defined that $r < d$, we do not have a positive r that satisfies this (since d is the smallest number such that $a^d \equiv 1 \pmod{n}$). Therefore, $r = 0$, and therefore, $n = qd$. This means that $d \mid n$. ■

Definition 2.11. We define $\phi(n)$ to be Euler's Totient function (or the phi function), where $n = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ \ldots \ \cdot p_k^{b_k}$ ($p_1, p_2, p_3 \ldots p_k$ are prime numbers), as follows: $n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \ldots (1 - \frac{1}{p_k})$. Euler's Totient function calculates the amount of numbers between 1 and n that are relatively prime to n. We prove the formula later, along with Euler's Totient Theorem.

Definition 2.12. Define the recurrence polynomial $f(x) = x^2 - ax + b$, where a and b are integers such that $\Delta = a^2 - 4b$ is not a perfect square. We now create two sequences using these values:

$$U_j = U_j(a, b) \equiv \frac{x^j - (a - x)^j}{x - (a - x} \pmod{f(x)}$$
$$V_j = V_j(a, b) \equiv x^j + (a - x)^j \pmod{f(x)},$$

where we define $g(x) \pmod{f(x)}$ as the remainder when $g(x)$ is divided by $f(x)$. We can also recursively define the sequences U_j and V_j as follows:

$$U_j = a \cdot U_{j-1} - b \cdot U_{j-2}$$
$$V_j = a \cdot V_{j-1} - b \cdot V_{j-2}.$$

A third definition can also be created by letting p and q be the roots of $f(x)$ as follows:

$$U_j = \frac{p^n - q^n}{p - q}$$
$$V_j = p^n + q^n.$$

Using these definitions, we can easily see that $U_0 = 0$ and $U_1 = 1$. For more information on Lucas Sequences, see [CP05].

2.1. **Fundamental Theorems.**

We now will give and prove some useful theorems that will be important later on. We first prove Fermat's Little Theorem (FLT), which states:

Theorem 2.13 (Fermat's Little Theorem)**.** *If p is a prime number, then $a^p \equiv a \pmod{p}$. Equivalently, if $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. We prove FLT by induction, with the base case being $a = 1$. This is of course satisfies the congruence, and so we now assume that $k^p \equiv k \pmod{p}$, for some integer k. We now show that this implies that $(k + 1)^p \equiv k + 1 \pmod{p}$. We do this by adding $pk^{p-1} + \binom{p}{2}k^{p-2} + \binom{p}{3}k^{p-3} + \ldots + 1$ to both sides of the congruence $k^p \equiv k \pmod{p}$, which gives us: $k^p + pk^{p-1} + \binom{p}{2}k^{p-2} + \binom{p}{3}k^{p-3} + \ldots + 1 \equiv k + pk^{p-1} + \binom{p}{2}k^{p-2} + \binom{p}{3}k^{p-3} + \ldots + 1 \pmod{p}$.

However, the left hand side can be factored by the Binomial Theorem, giving us: $(k+1)^p \equiv k + pk^{p-1} + \binom{p}{2}k^{p-2} + \binom{p}{3}k^{p-3} + \ldots + 1 \pmod{p}$. However, since all the middle terms on the left hand side of the congruence are divisible by p, they become 0 (mod p). This means that we can simplify the congruence to $(k+1)^p \equiv k+1 \pmod{p}$, which means we have shown that $k^p \equiv k \pmod{p}$ implies that $(k+1)^p \equiv k+1 \pmod{p}$. Thus, we have proved this "version" of FLT by induction. In order to obtain the other form of FLT stated in the theorem, notice that we can divide both sides of the congruence by a if and only if $\gcd(a,p) = 1$, which gives us: $a^{p-1} \equiv 1 \pmod{p}$. Therefore, we have proved FLT. ■

Theorem 2.14. *If $n = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ \ldots \ \cdot p_k^{b_k}$ ($p_1, p_2, p_3 \ldots p_k$ are prime numbers. Let $\phi(n)$ be the amount of numbers relatively prime to n between 1 and n. Then $\phi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})(1-\frac{1}{p_3})\ldots(1-\frac{1}{p_k})$.*

Proof. We first show that $\phi(p)$, where p is a prime number, is equal to $p-1$. This is true because a prime must be relatively prime to all numbers less than it, by its definition. We now use this to show that $\phi(p^k)$, where k is an integer is equal to $p^{k-1}(p-1)$. This is true because we notice that the only way for a number not to be relatively prime to p^k is if the number is of the form cp, where $c \geq 1$, and $cp \leq p^k$. We know that there are p^{k-1} numbers of the form cp as we defined as above, since c can be any integer between 1 and p^{k-1}. This means that there are a total of p^{k-1} numbers that are not relatively prime to p^k that are $\leq p^k$. Since we know that there are a total of p^k numbers, this means that the amount of numbers relatively prime to p^k is $p^k - p^{k-1}$, which can be factored as $p^{k-1}(p-1)$, or $p^k(1-\frac{1}{p})$. We now prove that $\phi(n)$ is a multiplicative function, meaning that $\phi(ab) = \phi(a)\phi(b)$ when $\gcd(a,b) = 1$. Suppose we have the set of all positive numbers less than ab that are relatively prime to ab called A, along with the same sets for a and b individually, which we shall call Sets C and D respectively. We now define a function that takes every element $a_1 \in C$ and $b_1 \in D$ and adds a new element $d < ab$ such that $d \equiv a_1 \pmod{a}$ and $d \equiv b_1 \pmod{b}$. We call this set B. We now prove the following lemma, which will be helpful to finding a relationship between sets A and B:

Lemma 2.15. *If x, a, b, c, and d are all positive integers where $\gcd(c,a) = 1$, $\gcd(d,b) = 1$ and $\gcd(a,b) = 1$, then the solution to the congruence reduced (mod ab):*

$$x \equiv c \pmod{a}$$
$$x \equiv d \pmod{b}$$

is relatively prime to ab.

Proof. We can solve this congruence by converting each of the congruences into linear equations and substituting. This gives us that the solution to the congruence is $x \equiv aa^{-1}d - aa^{-1}c + c \pmod{ab}$. We prove that $\gcd(aa^{-1}d - aa^{-1}c + c, ab) = 1$. We prove this by contradiction. Suppose that there exists some number $\gcd(aa^{-1}d - aa^{-1}c + c, ab) = h$. We first examine if $h \mid a$, meaning that $h \nmid b$ (since a and b are relatively prime). We also know that $h \mid aa^{-1}d - aa^{-1}c + c$. This means that $h \mid c$, since all the terms must be divisible by h in

order for the whole expression to be divisible by h. However, this is a contradiction, since we defined that $\gcd(a, c) = 1$. If $h \mid b$, we instead use the solution $x \equiv bb^{-1}c - bb^{-1}d + d \pmod{ab}$, and using the same method, we find a contradiction. However, we could also have $h \mid ab$, with $h \nmid a$ and $h \nmid b$. Informally, this means that h shares some factors with a and b, but not all its factors for either. Again, we know that $h \mid aa^{-1}d - aa^{-1}c + c$. In order for this to be true $h \mid c$. However, since h shares some factors with a, this means that $\gcd(a, c) \neq 1$, which is a contradiction to what we defined in the lemma. Therefore, $\gcd(aa^{-1}d - aa^{-1}c + c, ab) = 1$, meaning we have proved the lemma. ■

By Lemma 2.15, we know that this function creates numbers that are relatively prime to ab, meaning that all elements of B are elements of A, or $B \subseteq A$. We now need to show that $A \subseteq B$. This means that we must show that there exists some numbers c, d that satisfy $\gcd(a, c) = 1$ and $\gcd(c, d) = 1$, such that:

$$x \equiv c \pmod{a}$$
$$x \equiv d \pmod{b},$$

where $x \in A$. This is simply just the converse of the Chinese Remainder theorem, which is true. Therefore, we have that $A \subseteq B$. Therefore, we have that $A = B$, meaning that $\#(A) = \#(B)$. We also know that $\#(B) = \phi(a)\phi(b)$, and $\#(A) = \phi(ab)$. Therefore, $\phi(ab) = \phi(a)\phi(b)$. Therefore, we have shown that Euler's Totient function is multiplicative. Therefore, $\phi(n)$ for a number n that can be factorized as $p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ldots \cdot p_k^{b_k}$, is equal to $\phi(p_1^{b_1})\phi(p_2^{b_2})\phi(p_3^{b_3}) \ldots \phi(p_k^{b_k})$. We can expand each of those theorem using the formula we derived previously, giving us: $\phi(n) = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ldots \cdot p_k^{b_k}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \ldots (1 - \frac{1}{p_k})$. However, $p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ldots \cdot p_k^{b_k}$ can be replaced with n (this is just its factorization), giving us the final formula:

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \ldots (1 - \frac{1}{p_k}).$$

Therefore, the theorem has been proven. ■

Theorem 2.16 (Euler's Totient Theorem)**.** *Define $\phi(n)$ as we have previously. Suppose we have two positive integers a, n such that $\gcd(a, n) = 1$. Then the following congruence holds:*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. Let A denote the set of all numbers that are relatively prime to n as follows: $\{k_1, k_2, k_3, k_4, k_5, \ldots, k_{\phi(n)}\}$. We now create a new set B that multiplies each element by a, giving us: $\{ak_1, ak_2, ak_3, ak_4, ak_5, \ldots, ak_{\phi(n)}\}$. We now show that $\phi(n)$ is always even for any $n > 2$ (if $n \leq 2$ then the theorem holds trivially). We see that in the formula, each term is of the form $\frac{p_i - 1}{p_i}$ (where p_i is one of the prime factors of n). We know that the numerator is always even for any odd p_i, and is only odd for $p_i = 2$. However, $\phi(2) = 1$, so it does not contribute anything to the product. The terms in the denominator "cancel" out with n, leaving us with an even product, meaning that $\phi(n)$ is even. This means that $\#(A)$ is

even. We now use the fact that A is simply the multiplicative group of $\mathbb{Z}/n\mathbb{Z}$, meaning that every element has a multiplicative inverse. Since we know that there are an even number of elements, we know that we can pair up the numbers with their inverses, meaning that the product of the integers (mod n) is just 1. This means that if we were to multiply all the elements in B (mod n), we would get: $a^{\phi(n)}$ (mod n). We now show that all elements of B (mod n) are congruent to the elements of A (mod n). This is true because of all values of B are relatively prime and unique to n as well, so therefore, it must contain the same elements as A. Or in other words, each element of B is congruent to one element of A. This means that we have that $a^{\phi(n)} \equiv k_1 \cdot k_2 \cdot k_3 \cdot \ldots k_{\phi(n)} \pmod{n}$, or $a^{\phi(n)} \equiv 1 \pmod{n}$. Therefore, we have proved the theorem. ■

2.2. **Theorems from Sequences.** We now will prove theorems related to Lucas sequences, that will be needed later on.

Theorem 2.17. *Let a, b, Δ, U_j, and V_j be defined as above. If p is a prime such that $\gcd(p, 2b\Delta) = 1$, then*

$$U_{p-\left(\frac{\Delta}{p}\right)} \equiv 0 \pmod{p},$$

where $\left(\frac{a}{p}\right)$ is the Legendre Symbol.

Proof. We approach this proof by finding an explicit formula for U_j, in terms of a and b. We do this by first assuming that $U_j = c^j$, for some $c \in \mathbb{R}$. We can plug this into the recurrence relation that we defined for U_j previously, giving us $c^j = a \cdot c^{j-1} - b \cdot c^{j-2}$. Dividing by c^{j-2} on both sides of the equation gives us the quadratic $x^2 - ax + b = 0$. The roots to this quadratic are $c_1 = \frac{a+\sqrt{\Delta}}{2}$ and $c_2 = \frac{a-\sqrt{\Delta}}{2}$, where we use Δ as the discriminant of the quadratic, as defined previously. Therefore, our explicit formula satisfies the form $U_j = \lambda_1 c_1^j + \lambda_2 c_2^j$, where $\lambda_1, \lambda_2 \in \mathbb{R}$. We now find the value of λ_1 and λ_2 by using the values of U_0 and U_1 (found previously) to form a system of equations:

$$\lambda_1 + \lambda_2 = 0$$
$$\lambda_1 \frac{a+\sqrt{\Delta}}{2} + \lambda_2 \frac{a-\sqrt{\Delta}}{2} = 1.$$

Solving this system of equations gives us the solutions $\lambda_1 = \frac{1}{\sqrt{\Delta}}$ and $\lambda_2 = -\frac{1}{\sqrt{\Delta}}$. This means that the explicit formula for U_j is $U_j = \frac{(a+\sqrt{\Delta})^j - (a-\sqrt{\Delta})^j}{2^j\sqrt{\Delta}}$, which results from plugging the values of λ_1 and λ_2 back into the equation $U_j = \lambda_1 c_1^j + \lambda_2 c_2^j$.

We now do casework based on the value of $\left(\frac{\Delta}{p}\right)$.

Case 1 $\left(\frac{\Delta}{p}\right) = 1$**:** This means that we are trying to prove that $U_{p-1} \equiv 0 \pmod{p}$. We can plug $p-1$ into the explicit formula for U_j which gives us $U_{p-1} = \frac{(a+\sqrt{\Delta})^{p-1} + (a-\sqrt{\Delta})^{p-1}}{2^{p-1}\sqrt{\Delta}}$.

Expanding this gives us:

$$U_{p-1} = \frac{2(\binom{p-1}{1}a^{p-2}\sqrt{\Delta} + \binom{p-1}{3}a^{p-4}(\sqrt{\Delta})^3 + \ldots + \binom{p-1}{p-2}a(\sqrt{\Delta})^{p-2})}{2^{p-1}\sqrt{\Delta}}$$

$$U_{p-1} = \frac{\binom{p-1}{1}a^{p-2} + \binom{p-1}{3}a^{p-4}(\sqrt{\Delta})^2 + \ldots + \binom{p-1}{p-2}a(\sqrt{\Delta})^{p-3}}{2^{p-2}}$$

$$2^{p-2} \cdot U_{p-1} = \binom{p-1}{1}a^{p-2} + \binom{p-1}{3}a^{p-4}\Delta + \ldots + \binom{p-1}{p-2}a(\Delta)^{\frac{p-3}{2}}.$$

We now take this equation modulo p, which gives us $U_{p-1} \cdot 2^{-1} \equiv \binom{p-1}{1}a^{p-2} + \binom{p-1}{3}a^{p-4}\Delta + \ldots + \binom{p-1}{p-2}a(\Delta)^{\frac{p-3}{2}} \pmod{p}$. We have 2^{-1} on the left hand side of the congruence because we simplified 2^{p-2} with Theorem 2.13. We now prove the following lemma which will allow us to simplify the right hand side:

Lemma 2.18. $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$, *for some prime number* p *and some integer* k.

Proof. We begin by expanding and reducing $\binom{p-1}{k}$ modulo p, which gives us:

$$\begin{aligned}\frac{(p-1)(p-2)\ldots(p-k)}{k!} &\equiv \frac{(-1)(-2)\ldots(-k)}{k!} \pmod{p} \\ &\equiv (-1)^k \cdot k! \cdot (k!)^{-1} \pmod{p} \\ &\equiv (-1)^k \pmod{p}.\end{aligned}$$

Thus, the lemma has been proved. ∎

Using Lemma 2.18, we can simplify the congruence to

$$U_{p-1} \equiv -2(a^{p-2} + a^{p-4}\Delta + \ldots + a(\Delta)^{\frac{p-3}{2}}) \text{ (mod } p).$$

We now apply the finite geometric series formula to the right side, which gives us $U_{p-1} \equiv -2(\frac{a^{p-2}((\frac{\Delta}{a^2})^{\frac{p-1}{2}}-1)}{\frac{\Delta}{a^2}-1}) \pmod{p}$. We now do casework on the $\gcd(a,p)$. If $\gcd(a,p) = p$, this case is trivial, since the numerator becomes a multiple of p, meaning that the whole expression becomes $0 \pmod{p}$. If the $\gcd(a,p) = 1$, we approach this case by first simplifying the numerator using Theorem 2.13:

$$U_{p-1} \equiv \frac{-2a^{p-2}(\Delta^{\frac{p-1}{2}} \cdot (a^{p-1})^{-1} - 1)}{\frac{\Delta}{a^2} - 1} \pmod{p}$$

$$U_{p-1} \equiv \frac{-2a^{p-2}(\Delta^{\frac{p-1}{2}} - 1)}{\frac{\Delta}{a^2} - 1} \pmod{p}.$$

We now apply Euler's Criterion (proven later on in the Solovay-Strassen Primality Test), which states: $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \pmod{p}$, where $\left(\frac{a}{p}\right)$ is the Legendre Symbol, and

p is a prime number. This means that $\Delta^{\frac{p-1}{2}} \equiv \left(\frac{\Delta}{p}\right) \pmod{p}$. However, since we defined that $\left(\frac{\Delta}{p}\right) = 1$ for this case, this means that $\Delta^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. This means that we can simplify the congruence to:

$$U_{p-1} \equiv \frac{-2a^{p-2}(1-1)}{\frac{\Delta}{a^2} - 1} \pmod{p}$$
$$U_{p-1} \equiv 0 \pmod{p}$$

Therefore, this case has been proved.

Case 2 $\left(\frac{\Delta}{p}\right) = -1$**:** This means that we are trying to prove that $U_{p+1} \equiv 0 \pmod{p}$. This means that we can substitute $p+1$ into our explicit formula to obtain the equation $U_{p+1} = \frac{(a+\sqrt{\Delta})^{p+1} - (a-\sqrt{\Delta})^{p+1}}{2^{p+1}\Delta}$. Expanding this gives us:

$$U_{p+1} = \frac{\binom{p+1}{1}a^p + \binom{p+1}{3}a^{p-1}\Delta + \ldots + \binom{p+1}{p}a\Delta^{\frac{p-1}{2}}}{2^p}$$
$$U_{p+1} \cdot 2^p = \binom{p+1}{1}a^p + \binom{p+1}{3}a^{p-1}\Delta + \ldots + \binom{p+1}{p}a\Delta^{\frac{p-1}{2}}.$$

We now take this expression modulo p, which gives us $U_{p+1} \equiv 2^{-1}(a^p + a\Delta^{\frac{p-1}{2}}) \pmod{p}$. We were able to remove the middle terms because they are all $0 \pmod{p}$, however, the only exception to this rule is when $p = 3$. Therefore, we will have to separately prove this case. We first assume that $p \neq 3$. We can apply Theorem 2.13 and Euler's Criterion (similar to the previous case) to simplify the congruence to $U_{p+1} \equiv 2^{-1}(a - a) \equiv 0 \pmod{p}$.

However, we must now deal with the case where $p = 3$. This means that we are trying to prove that $U_4 \equiv 0 \pmod{3}$. Using the recurrence relations defined previously, we find that $U_4 = a^3 - 2ab$. This means that we have $a^3 - 2ab \pmod{3}$. We now do casework based on the $\gcd(a, p)$. The case where $\gcd(a, p) = p$ is trivial, since this means that the whole expression is $0 \pmod{p}$. If $\gcd(a, p) = 1$, we now do more casework on $\Delta \pmod{3}$.

Case 1 $\Delta \equiv 0 \pmod{3}$**:** This case is trivial since this contradicts the fact that $\gcd(2b\Delta, 3) = 1$ (stated in the theorem itself). Therefore, $\Delta \not\equiv 0 \pmod{3}$.

Case 2 $\Delta \equiv 1 \pmod{3}$**:** This case means that $a^2 - 4b \equiv 1 \pmod{3}$. Since we stated that $\gcd(a, p) = 1$, this allows us to use Theorem 2.13, giving us:

$$1 - 4b \equiv 1 \pmod{3}$$
$$b \equiv 0 \pmod{3}$$

However, this again contradicts the statement $\gcd(2b\Delta, 3) = 1$, so therefore, $\Delta \not\equiv 1 \pmod{3}$.

Case 3 $\Delta \equiv 2 \pmod 3$**:** This statement implies $a^2 - 4b \equiv 2(mod 3)$. Simplifying, we find that $b \equiv 2 \pmod 3$. There are no contradictions from this, so this means that $\Delta \equiv 2 \pmod 3$ is valid. We now use $b \equiv 2 \pmod 3$ in the congruence $a^3 - 2ab \pmod 3$ (what we are trying to prove), which gives us:

$$a - 2ab \equiv a - 4a \equiv 0 \pmod 3$$

Thus, we have shown that $p = 3$ also satisfies the Theorem.

We have proved all the cases, and therefore, the Theorem. ■

2.3. **Results from Group Theory.** We first define Cyclic Groups and give some important qualities about them:

Definition 2.19 (Cyclic Groups)**.** A cyclic group is a group generated by a single element. More specifically, it is a group of invertible elements, and contains an element g such that repeatedly performing the group operation on g will obtain every other element of the group. We list some properties of cyclic groups below:

(1) Every cyclic group is abelian (the group operation is commutative).
(2) All subgroups of a cyclic group are also cyclic.
    - One can form a subgroup generated by all the integer powers of a specific element, denoted by $\langle g \rangle$, where g is in the group.
(3) The multiplicative group modulo n is cyclic if and only if $n = 1, 2, 4, p^k, 2p^k$, where p is an odd prime and $k \in \mathbb{N}$.
(4) If $d \mid n$, where n is the order of the group, then there exists some subgroup that has order d.

We now prove Lagrange's Theorem, which will be very useful in our proofs.

Theorem 2.20 (Lagrange's Theorem)**.** *Let G be a finite group. If H is a subgroup of G, then $|H| \mid |G|$.*

Proof. We divide the problem into three cases.

Case 1 $|H| = 1$**:** This means that H is just the trivial group. Of course, $1 \mid |G|$.

Case 2 $|H| = |G|$**:** This means that $H = G$, and obviously, $|G| \mid |G|$.

Case 3 $|H| \neq 1, |H| \neq |G|$**:** Since H is a subgroup of G, it must contain the identity element, which we shall call e. Let us then take an element in G but not in H called g_1, and create a new set:

$$g_1 H = \{g_1 * h \ \forall h \in H\}.$$

Note that the above set is known as a left coset. We now prove the following lemma:

Lemma 2.21. *$g_1 H$ does not share any elements with H.*

Proof. We prove this by contradiction. Suppose we have: $g_1 \cdot h_i = h_j$, where $h_i, h_j \in H$. Multiplying by the inverse of h_i gives us: $g_1 \cdot e = g_1 = h_j \cdot (h_j)^{-1}$. However, note that $h_j \cdot (h_j)^{-1}$ is an element of H, meaning that g_1 is an element of H. However,

this contradicts the fact that we defined that g_1 was not an element of H. Therefore, there cannot be any overlapping elements between g_1H and H. ■

Let us now take another element g_2 that is not in H and g_1H. We can apply the same argument in Lemma 2.21 to show that g_2H do not share any elements. However, we still must show that g_1H and g_2H do not have any overlapping elements.

Lemma 2.22. *g_1H and g_2H do not share any overlapping elements.*

Proof. We again prove this by contradiction. Let $h_i, h_j \in H$. Then we have:

$$\begin{aligned} g_2 \cdot h_j &= g_1 \cdot h_i \\ g_2 \cdot h_j \cdot (h_j)^{-1} &= g_1 \cdot h_i \cdot (h_j)^{-1} \\ g_2 &= g_1 \cdot h_i \cdot (h_j)^{-1}. \end{aligned}$$

However, since $h_j \cdot (h_i)^{-1} \in H$, this means that $g_2 \in g_1H$. However, this is a contradiction to how we defined g_2. Hence, we have proved the lemma. ■

We now continue until there is no element left that is not in a coset or H. We now split G into non-overlapping left cosets. However, we must now prove that all these cosets are the same size. Suppose the coset $g_n \cdot H$ has a duplicate element. Let $h_i, h_j \in H$. We therefore have the following equation:

$$\begin{aligned} g_n \cdot h_i &= g_n \cdot h_j \\ g_n \cdot (g_n)^{-1} \cdot h_i &= g_n \cdot h_j \cdot (g_n)^{-1} \\ h_i &= h_j. \end{aligned}$$

However, the final equation is a contradiction. Therefore, each coset is the same size, which is $|H| = d$. Since we have now managed to split G into non-overlapping cosets, suppose we say we have split G into k non-overlapping cosets. We thus have that $d \cdot k = |G|$, meaning that $d = |H| \mid |G|$. Therefore, we have proved this case.

We have proved all three cases and therefore Lagrange's Theorem. ■

3. Probabilistic Tests

3.1. **Fermat Primality Test.**

We define the Fermat Primality Test using FLT:

Definition 3.1 (Fermat Primality Test)**.** The Fermat Primality Test checks if a number n satisfies $a^{n-1} \equiv 1 \pmod{n}$, for some integer a relatively prime to n. Of course if n is prime, then this is just Fermat's Little Theorem, which is true. If n does not satisfy the congruence, then n is definitely composite. However, if n passes the test, the converse is not necessarily true, and n is called a probable prime (since some composite numbers can pass the test). If n is composite and passes the test, it is called a Fermat pseudoprime to base a.

To lower the chance of a false result being outputted, we can choose k different values of a and therefore run k iterations of the test. If one of these tests fails for n, then n is composite.

Using fast algorithms for modular exponentiation and multiplication, the time complexity of the test is $O(k \log^2(n) \log\log n)$, where k is the number of iterations being performed, and n is the number itself.

However, while the test seems to be relatively accurate and fast, one of the main problems with the test is that there exist numbers such that they are a Fermat pseudoprime to all bases a relatively prime to the number itself. These numbers are known as Carmichael numbers. We show that 561 (the first Carmichael number) satisfies our current definition of a Carmichael Number:

Proposition 3.2. *561 is a Carmichael number.*

Proof. We must show that 561 satisfies $a^{560} \equiv 1 \pmod{561}$ for all integers a relatively prime to 561. We can split the congruence into three equations modulo each of the prime factors of 561 by the Chinese Remainder Theorem. This gives us:

$$a^{560} \pmod 3$$
$$a^{560} \pmod{11}$$
$$a^{560} \pmod{17}$$

We can apply Theorem 2.13 to each congruence, giving us:

$$a^2 \equiv 1 \pmod 3$$
$$a^{10} \equiv 1 \pmod{11}$$
$$a^{16} \equiv 1 \pmod{17}.$$

Since $80 = \text{LCM}(2, 10, 16)$, we know that a^{80} is congruent to 1 modulo all factors of 561 (a solution to the congruence). However, by CRT, the system of modular congruences:

$$x \equiv 1 \pmod 3$$
$$x \equiv 1 \pmod{11}$$
$$x \equiv 1 \pmod{17},$$

has only one solution modulo 561. However, since a^{80} and 1 are both solutions, this must mean that $a^{80} \equiv 1 \pmod{561}$. Since $80 \mid 560$, we have that $a^{560} \equiv 1 \pmod{561}$, for all a relatively prime to n. ■

Robert D. Carmichael proved that every Carmichael number is odd, square-free, and has at least 3 prime factors. Furthermore, in 1899, Korselt's criterion was created, which stated that a positive integer n is a Carmichael number if n is odd, n is squarefree, and $p - 1 \mid n - 1$ for all prime divisors p of n. For a proof, see [Con16]. Additionally, Alford, Granville, Pomerance, et al. proved in 1992 that there were infinitely many Carmichael numbers, a claim that had gone long unproven [AGP94].

The infinitude and existence of the Carmichael numbers makes the Fermat Primality test not very reliable (especially when applied to cryptography), and thus, the next two tests it.

Specifically, they have bounds for the maximum number of bases that allows a composite number to pass the test.

3.2. **Solovay–Strassen Test.** The Solovay–Strassen test relies on Euler's Criterion, which is as follows:

Theorem 3.3. *$x^2 \equiv a \pmod{p}$ has a solution if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, for a prime p and an integer a not divisible by p.*

Proof. Recall that from Theorem 2.13, if z is relatively prime to p, then $z^{p-1} \equiv 1 \pmod{p}$. Therefore, since the only square roots of 1 are 1 and -1, we have that $z^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. This means that we have to show that if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, then a is a quadratic residue, and if $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, then a is a quadratic non-residue.

Case 1 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$**:** Since p is prime, we know that there exists some integer g such that its order modulo p is $p-1$ (the primitive root modulo p). Therefore, we have $g^{p-1} \equiv 1 \pmod{p}$. Since g is the primitive root modulo p, there exists some number m such that $g^m \equiv a \pmod{p}$. Replacing this with a in $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ gives us $(g^{\frac{p-1}{2}})^m \equiv 1 \pmod{p}$. We know that $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, as if $g^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, this would contradict the fact that the order of g modulo p is $p-1$. Therefore, we know that m is even (since -1 must be raised to an even power to become 1). Therefore, we know that since $g^m \equiv a \pmod{p}$, and that m is even, a can be represented as $(g^{\frac{m}{2}})^2 \equiv a \pmod{p}$. Therefore, if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then a is a quadratic residue modulo p.

Case 2 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$**:** Notice that the equation $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ has at most $\frac{p-1}{2}$ roots. However, we have just showed that all quadratic residues satisfy this equation, and there are exactly $\frac{p-1}{2}$ modulo p. Therefore, the only other option for quadratic non-residues is for them to satisfy $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Therefore, we have proved Euler's Criterion. ■

Euler's criterion can be concisely summarized as $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$, where $\left(\frac{a}{p}\right)$ is Legendre's Symbol. We can now define the Solovay–Strassen test:

Definition 3.4 (Solovay–Strassen Primality Test)**.** The Solovay–Strassen test considers the congruence $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$, where n is any odd, positive integer and $\left(\frac{a}{n}\right)$ is the Jacobi symbol. Note that n must be odd because we defined the Jacobi Symbol for only odd integers. If n is prime, as we showed previously, this congruence holds for all a. If n is composite and fails the test, then a is called an Euler witness for the "compositeness" of n. However, if n passes the test and is composite, then a is called an Euler liar and n is known as an Euler pseudoprime (or Euler–Jacobi pseudoprime).

Just as we ran k iterations of the Fermat Primality Test to improve its accuracy, we can use the same technique to improve the Solovay–Strassen. However, unlike the Fermat

Primality Test, there is a probability "bound" on whether the test classifies a composite number incorrectly (which we prove later).

It is also important to note that we must use an algorithm to calculate the Jacobi Symbol, since our definition of it relies on knowing the prime factors of n. However, using the properties of the Jacobi Symbol defined previously, we can devise an efficient way to calculate the Jacobi symbol of any two integers. The algorithm is as follows:

(1) If the top argument is greater than the bottom argument, then reduce the top argument modulo the bottom argument, by Lemma 2.3.
(2) We can "get rid" of any factors of 2 using Lemma 2.4 and 2.8.
(3) If the top argument is 1, then the Jacobi Symbol evaluates to 1 (1 is always a quadratic residue modulo any number). If the numerator and denominator are not relatively prime (determined by Euclid's Algorithm), then by Lemma 2.5, the Jacobi Symbol becomes 0.
(4) If none of the conditions in step 3 are satisfied, then the top and bottom arguments are now odd positive relatively prime integers. This means we can "flip" the arguments by Lemma 2.6. We can then return to step 1 after we do this and repeat this process.

This algorithm allows us to calculate the Jacobi symbol without knowing the prime factorization of n, and is also quite efficient.

We now will prove that at most $\frac{1}{2}$ of the bases for a composite integer n are Euler liars. The proof comes from [SS77, SS78].

Theorem 3.5 (Solovay–Strassen)**.** *Let n be an odd, positive, composite integer. The set $S = \{a + (n) | a \in \mathbb{Z}_n^* \ \& \ \gcd(a, n) = 1, a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}\}$ is not equal to $\mathbb{Z}_n^*$.*

Proof. We first note that S is a subgroup of $\mathbb{Z}_n^*$, since S only contains some of the elements relatively prime to n. We now see why we only need to prove that $S \neq \mathbb{Z}_n^*$. This is because by Lagrange's Theorem, $|S| \mid |\mathbb{Z}_n^*|$. At maximum, $|S| = |\mathbb{Z}_n^*|/2$, which is less than or equal to $\frac{n-1}{2}$ (since $S \neq \mathbb{Z}_n^*$ contains only all integers relatively prime to n). Therefore, we have the inequality $|S| \leq \frac{|\mathbb{Z}_n^*|}{2} \leq \frac{n-1}{2}$, which is what we are trying to prove.

We try to find a contradiction, by stating that $S = \mathbb{Z}_n^*$. This means that

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}, \tag{3.1}$$

for all a relatively prime to n. We consider cases of n to show this:

Case 1 $n = p^x$, for some prime p and integer x: This means we have:

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

Squaring both sides gives us: $a^{p^x-1} \equiv 1 \pmod{p^x}$. Since $\mathbb{Z}_{p^x}^*$ is cyclic with order $\phi(p^x) = p^{x-1}(p-1)$ by Theorem 2.14, we know that $p^{x-1}(p-1) \mid p^x - 1$. We now

see that $x \leq 1$. This is because $p^{x-1}(p-1) \mid p^x - 1$ implies that there is some integer d such that:

$$d = \frac{p^x - 1}{p^{x-1}(p-1)}.$$

We can simply the fraction giving us:

$$\begin{aligned} d &= \frac{p^x - 1}{p^{x-1}(p-1)} \\ &= \frac{p^{x-1} + p^{x-2} + \ldots + 1}{p^{x-1}} \\ &= 1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^{x-1}}. \end{aligned}$$

In order for this to be an integer, $x \leq 1$, since otherwise, the sum evaluates to a fraction. However, this is a contradiction, since this implies that n is a prime number, however, we defined that n was composite.

Case 2 $n = pq$**, for square-free integers** p **and** q**:** By Equation 1, we know that it implies that:

$$a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}. \tag{3.2}$$

We will now show that the conditions of this case mean:

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n}, \tag{3.3}$$

for all a relatively prime to n. Assume that $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ (the only other possibility). Since p and q are relatively prime, this means we can apply CRT to give us the system of equations:

$$\begin{aligned} b &\equiv 1 \pmod{r} \\ b &\equiv a \pmod{s} \end{aligned}$$

Raising each congruence to the $\frac{n-1}{2}$, we have that:

$$\begin{aligned} b^{\frac{n-1}{2}} &\equiv 1 \pmod{r} \\ b^{\frac{n-1}{2}} &\equiv -1 \pmod{s} \end{aligned}$$

However, this is a contradiction to Equation 2, as both of the equations would either have to be congruent to 1 or -1 to not have a contradiction (by CRT). Therefore, we know that Equation 3 is true. However, Equation 3 (by Euler's Criterion) implies that $\left(\frac{a}{n}\right) = 1$ for all a relatively prime to n, which is false because it is impossible for all relatively prime integers a to n be quadratic residues to it.

Case 3 $n = p^x \cdot q$**, where** $x > 1$**,** p **is an odd prime and** $\gcd(p, q) = 1$**:** This case assumes that n is not square-free. From earlier in the proof, we know that $a^{n-1} \equiv 1 \pmod{n}$, for all a relatively prime to n. By CRT, we know that $a^{n-1} \equiv 1 \pmod{p^x}$,

meaning that $p^{x-1}(p-1) \mid n-1$ (since $\mathbb{Z}_{p^x}^*$) is cyclic and the order is $\phi(p^x)$). Since $x > 1$, this means that $p \mid n-1$ as well as n. However, by Euclid's Algorithm, we know that $\gcd(n-1, n) = 1$, so therefore, this is a contradiction. This means that n is square-free. However, we already have a case covering if n is square-free, which has a contradiction. Thus, we have proved this case.

These three cases encapsulate all the possible forms of a composite number n, and since we have derived a contradiction for each, we have shown that $S \neq \mathbb{Z}_n^*$, our original goal. Therefore, we have proved the theorem. ■

By Theorem 3.5, we know that if we were to run k iterations of the Solovay–Strassen test as outlined in Definition 3.4, then the probability of erroneously classifying a composite integer as a prime is 2^{-k}. This is of course much better than the Fermat Primality test. We now look at a way to make it to determinstic, if n is less than a certain bound.

By using a pre-selected bases, we can treat the Solovay–Strassen test as a determinstic test up till when the test identifies a number n wrong.

Selected bases	Determistic Up To Some Value of n (non-inclusive)
{2}	561
{2, 3}	1729
{2, 3, 5, 7}	399001
{2, 3, 5, 7, 11}	399001
{2, 3, 5, 11}	15841
{2, 3, 5, 7, 11, 13}	15841
{2, 3, 5, 7, 11, 13, 17}	1857421
{2, 3, 5, 7, 11, 13, 17, 19}	6189121
{2, 3, 5, 7, 11, 13, 17, 23}	14469841
{3, 5, 11, 13}	416641
{2, 37}	1729
{2,25}	561
{2, 24}	1729
{24, 88}	15841
{24, 88, 71}	15841
{24, 71}	1729
{26, 71}	217
{2, 26}	561
{2, 200}	561
{2, 300}	1729
{2, 1000}	1729
{2, 1001}	162401
{2, 88}	2047

The values in the table demonstrate that while this is a useful feature for certain n, these bounds are not comparable to size of primes used in cryptography.

3.3. **Miller–Rabin Test.**

Definition 3.6 (Miller Rabin Primality Test)**.** The Miller–Rabin test determines if a number is a strong probable prime, which means that it satisfies the following conditions, given that n is an odd positive integer > 1, and we write $n - 1$ as $2^s \cdot d$, where d is odd:

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

where a is defined to be a random number relatively prime to n. As stated previously, if n passes the test, it is considered a strong probable prime to base a. By contraposition, if n is not a strong probable prime, then n is definitely composite. In this case, the base a is called a "witness" (for the "compositeness" of n). However, some composite numbers n do pass the test, in which case, n is called a strong pseudoprime and a is known as a strong liar.

We now prove that if n is prime, then the test returns that n as a strong probable prime.

Theorem 3.7. *If p is a prime number, then it passes the Miller–Rabin test.*

Proof. Factor $p - 1$ as $2^s \cdot d$, where d is odd. We now use the expression $x^{p-1} - 1$ (where x is relatively prime to p). We can factor this with difference of two squares as so: $(x^{2^{s-1} \cdot d} - 1)(x^{2^{s-1} \cdot d} + 1)$.We can continue to factor $(x^{2^{s-1} \cdot d} - 1)$ using difference of squares, provided that the exponent of x is not odd. Therefore, we can factor $x^{p-1} - 1$ as $(x^d - 1)(x^d + 1)(x^{2d} + 1)(x^{4d} + 1) \dots (x^{2^{s-2} \cdot d} + 1)(x^{2^{s-1} \cdot d} + 1)$. However, note that by Fermat's Little Theorem, we know that $x^{p-1} \equiv 1 \pmod{p}$. We can replace x^{p-1} with a factorization, giving us: $(x^d - 1)(x^d + 1)(x^{2d} + 1)(x^{4d} + 1) \dots (x^{2^{s-2} \cdot d} + 1)(x^{2^{s-1} \cdot d} + 1) \equiv 0 \pmod{p}$. Since p is prime, we know that one of these factors must be $0 \pmod{p}$. Therefore, either $x^d \equiv 1 \pmod{p}$, or $x^{2^r \cdot d} \equiv -1 \pmod{p}$, where $0 \leq r < s$. Therefore, a prime number would pass the test. ∎

As with the Solovay–Strassen test, no composite number can be a strong pseudoprime to all bases (once again contrasting the Fermat Primality test). In fact, at most $\frac{1}{4}$ of the bases relatively prime to n can be strong liars (which will be proven later). While we could try all possible passes a relatively prime to n (and less than n), this would only give a slow, deterministic test. We instead pick the bases randomly, yielding a fast probabilistic test. Instead, we can pick k different values of a (similar to previous test), meaning the probability of a composite number passing the test becomes 4^{-k}, which becomes extremely small very quickly. This makes the Miller–Rabin test a very good probabilistic test, as it is able to produce high accuracy extremely quickly.

We now take a more in-depth look at the time complexity/speed of the algorithm itself. The test has a time complexity of $\mathcal{O}(k(\log(n)))^3$, where n is the number being tested for primality, and k is the amount of iterations run, by using efficient methods for modular

exponentiation. However, we can make the algorithm even more efficient. Using the Harvey-Hoeven algorithm for Fast Fourier Transform(FFT) based multiplication, the Miller Rabin test can be sped up further to $\tilde{\mathcal{O}}(\log^2(n))$, which comes from the fact that the time complexity of the Harvey-Hoeven is $\mathcal{O}(n\log(n))$.

We now look at the accuracy of the Miller–Rabin test, which will prove our claims made previously. The following theorem is inspired by [Sch08].

Theorem 3.8 (Rabin–Monier theorem)**.** *Let n be an odd composite integer greater than 9. We write $n-1=2^k\cdot m$, for some odd integer m. Let $B=\{x\in(\mathbb{Z}/n\mathbb{Z})^* \mid x^m\equiv 1 \pmod n$ or $x^{m\cdot 2^i}\equiv -1 \pmod n$ for some $0\leq i<k\}$. Then we have that $\frac{\#(B)}{\phi(n)}\leq\frac{1}{4}$, where $\phi(n)$ is Euler's Totient function.*

Proof. We let 2^l be the largest power of 2 that divides $p-1$ for all prime divisors p of n. We now create the set $B'=\{x\in(\mathbb{Z}/n\mathbb{Z})^* \mid x^{m\cdot 2^{l-1}}\equiv\pm 1 \pmod n\}$. We prove that $B\subset B'$. If $y\in B$ such that $y^m\equiv 1 \pmod n$, then y must also be an element of B'. This is because $y^{m\cdot 2^{l-1}}\equiv 1 \pmod n$ as well, which can be seen by "taking out" an m from the exponent, and using the fact that $y^m\equiv 1 \pmod n$.

We now deal with the case where $y^{2^i\cdot m}\equiv -1 \pmod n$. We first observe that $y^{2^i\cdot m}\equiv -1 \pmod p$, for any prime p dividing n because of the following:

$$\begin{aligned}
&y^{2^i\cdot m}=nk-1, \text{ for some positive integer } k\\
&y^{2^i\cdot m}+1=nk\\
&y^{2^i\cdot m}+1=cpk, \text{ for some positive integer } c\\
&y^{2^i\cdot m}+1\equiv 0 \pmod p\\
&y^{2^i\cdot m}\equiv -1 \pmod p.
\end{aligned}$$

Therefore, we have $y^{2^i\cdot m}\equiv -1 \pmod p$, for all $p\mid n$. Squaring this equation gives us $y^{2^{i+1}\cdot m}\equiv 1 \pmod p$. This implies that the order t of y modulo p divides $2^{i+1}\cdot m$. By definition, since $y^m\equiv -1 \pmod n$, we know that t and 2^{i+1} share factors. However, we now show that 2^{i+1} is the exact power of 2 dividing t. We prove this in the following lemma:

Lemma 3.9. *2^{i+1} is the exact power of 2 dividing t.*

Proof. Assume that $t=2^c\cdot g$ (we know that t is even), where g is odd and $c\in\mathbb{Z}<i+1$. We try to derive a contradiction to the fact that $y^{2^i\cdot m}\equiv -1 \pmod n$ for some $0\leq i<k$. If the order of y modulo p was $t=2^c\cdot g$, then we know that $y^{2^{c-1}\cdot g}\equiv -1 \pmod p$. We also know that if $2^c\cdot g\mid 2^{i+1}\cdot m$, then $2^c\cdot g\cdot v=2^{i+1}\cdot m$, for some positive integer v. This tells us that v must be even, since $c<i+1$, and g and m are both odd (and therefore do not contribute any factors of 2). Dividing by two on both sides gives us: $2^{c-1}\cdot g\cdot v=2^i\cdot m$. Therefore, raising $y^{2^{c-1}\cdot g}$ to the v power would give us $2^i\cdot m$. Since we have $y^{2^{c-1}\cdot g}\equiv -1 \pmod n$, we have that $y^{2^i\cdot m}\equiv(-1)^v \pmod n$. However, since v is even, we have that $y^{2^i\cdot m}\equiv 1 \pmod n$.

However, this contradicts the fact that $y^{2^{i}\cdot m} \equiv -1 \pmod{n}$ for some $0 \leq i < k$, which is what we assumed in this case. Therefore, we have derived a contradiction and showed that the exact power of 2 dividing t is 2^{i+1} (since this contradiction means $c = i + 1$). ■

The above lemma tells us that 2^{i+1} divides $p - 1$ for p dividing n. We can see this using Fermat's Little Theorem. We know that $y^{p-1} \equiv 1 \pmod{p}$. The order of y modulo p is t, so we have $t \mid p - 1$. However, since $2^{i+1} \mid t$, we have that $2^{i+1} \mid p - 1$. However, we also know that l is the largest power of 2 dividing $p - 1$. Therefore, $l \geq i + 1$. Therefore, we can write $y^{2^{l-1}\cdot m} \pmod{p}$ as $(y^{2^{i}\cdot m})^{2^{l-i-1}} \pmod{p}$, which is $(-1)^{2^{l-i-1}} \pmod{p}$. This is ± 1, depending on whether $l = i + 1$ or $l > i + 1$. It follows that $B \subset B'$.

By the Chinese Remainder Theorem, the number of elements $x \in (\mathbb{Z}/n\mathbb{Z})^*$ for which $x^{2^{l}\cdot m} \equiv 1 \pmod{n}$ is equivalent to the equation $X^{2^{l-1}\cdot m} \equiv \pmod{p}^{p_b}$, where $p \mid n$, p is a prime, p_b is the exact power of p dividing n. We now prove the following lemma:

Lemma 3.10. *All groups stated are finite and abelian. For any $n \in \mathbb{Z}$ and a cyclic group G, we let $s_n(G) := \{g \in G : g^n = 1\}$. Then the above definitions imply $|s_n(G)| = \gcd(n, |G|)$.*

Proof. We let $d = \gcd(n, |G|)$ and $S = s_n(G)$. We know that $S \leq G$, so therefore, since G is cyclic, S must be cyclic as well. This means that $S = \langle a \rangle$ where $a \in G$, and therefore, the multiplicative order of a is the order of group S. Since $a \in S$, $a^n = 1$, and hence, $|a| \mid n$, where $|a|$ denotes the multiplicative order of a. We can also use the fact that since $a \in G$, $a^{|G|} = 1$, so therefore, $|a| \mid |G|$. From these two divisibility requirements for $|a|$, we can see that $|a| \mid \gcd(|G|, n) = d$. Since G is cyclic and d divides $|G|$, there exists some subgroup S' of G of order d. If $g \in S'$, then $g^{|S'|} = g^d = 1$, which implies that $g^n = 1$, which results from the fact that $d \mid n$. Therefore, this shows that $S' \leq S$, and by Lagrange's Theorem, $|S'| \mid |S|$. However, these can be replaced by d and $|a|$, giving us $d \mid |a|$. However, we also know that $|a| \mid d$. Therefore, $|a| = |S| = d$. We have thus proved the lemma. ■

We now use Lemma 3.10 to find the number of solutions to $X^{2^{l-1}\cdot m} \equiv \pmod{p^{p_b}}$. The ossible solutions for X are in $(\mathbb{Z}/p^{p_b}\mathbb{Z})^*$, which is cyclic (since it is modulo a prime power). Therefore, by Lemma 3.10, we have that the number of solutions to the congruence is $\gcd(2^{l-1}\cdot m, |(\mathbb{Z}/p^{p_b}\mathbb{Z})^*|)$, which let d be equal to. Since this is the multiplicative group modulo p^{p_b}, the order of the group is $\phi(p^{p_b}) = p^{p_b-1}(p-1)$. Therefore, $d = \gcd(2^{l-1} \cdot m, p^{p_b-1}(p-1))$, which is the number of solutions to $X^{2^{l-1}\cdot m} \equiv 1 \pmod{p^{p_b}}$. Since $m \nmid p$, we see that the p^{p_b-1} term in the "gcd expression" does not contribute to its value. Therefore, we have that $d = \gcd(p-1, m) \cdot 2^{l-1}$. Therefore, the total number of solutions to $X^{2^{l-1}\cdot m} \equiv 1 \pmod{n}$ is the product of the number of solutions for each of the modular equations modulo a prime power. This gives us the following equation:

$$\#\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid x^{m2^{l-1}} \equiv 1 \pmod{n}\} = \prod_{p|n} \gcd(p-1, m)2^{l-1}.$$

Using the same method as before, we find that the number of solutions to $X^{2^l m} \equiv 1 \pmod{p^{p_b}}$ is $\gcd(p-1,m)2^l$, which is twice the number of solutions to $X^{2^{l-1}m} \equiv 1 \pmod{p^{p_b}}$. Therefore, the number of solutions to $X^{2^{l-1}m} \equiv -1 \pmod{p^{p_b}}$ is also $\gcd(p-1,m)2^{l-1}$. Therefore, we can express the cardinality of B' as:

$$\#(B') = 2\prod_{p|n} \gcd(p-1,m)2^{l-1},$$

and therefore,

$$\frac{\#(B')}{\phi(n)} = 2\prod_{p|n} \frac{\gcd(p-1,m)2^{l-1}}{p^{p_b-1}(p-1)}.$$

The denominator of the product results from the fact thatwe are "breaking down" n into its prime powers. We now try to derive a contradiction by assuming that $\frac{\#(B)}{\phi(n)} > \frac{1}{4}$. Since $B \subset B'$, we have:

$$\prod_{p|n} \frac{\gcd(p-1,m)2^{l-1}}{p^{p_b-1}(p-1)} > \frac{1}{4}. \tag{3.4}$$

We note that $\gcd(p-1,m)2^{l-1}$ divides $\frac{p-1}{2}$, so therefore, we have that $\frac{\gcd(p-1,m)2^{l-1}}{p^{p_b-1}} \leq \frac{1}{2p^{p_b-1}}$. Since $p^{p_b-1} \geq 1$ and we want to minimize the denominator, we have $\frac{1}{2p^{p_b-1}} \leq \frac{1}{2}$. If we let t be the number of prime factors of n, then the maximum value is $2 \cdot 2^{-t} = 2^{1-t}$. Since $2^{1-t} > \frac{1}{4}$, $t \leq 2$. We now do casework on the value of t:

Case 1 t = 2: This means that n has only two prime divisors. We now show that n must be squarefree. If one the divisors has the property such that $p^2 \mid n$, this would mean that the maximum value would be $\frac{1}{2\cdot 3}$ (since p must be an odd prime), which is $\frac{1}{6}$. This is because we have $2^{1-2}/3 = 1/6$, which is a contradiction, since this is less than $\frac{1}{4}$. Rather than 2, if we said that $p^n \mid n$, this would only mean that the maximum value of left hand side would become smaller (and be even less than $\frac{1}{4}$). Therefore $p_b = 1$, and $n = pq$ for distinct primes p and q. We can now transform the

inequality using the fact that $p_b = 1$:

$$\begin{aligned}
2 \cdot \frac{\gcd(p-1,m)2^{l-1}}{p-1} \cdot \frac{\gcd(q-1,m)2^{l-1}}{q-1} &> \frac{1}{4} \\
\frac{\gcd(p-1,m)2^{l}}{p-1} \cdot \frac{\gcd(q-1,m)2^{l-1}}{q-1} &> \frac{1}{4} \\
\frac{p-1}{\gcd(p-1,m)2^{l}} \cdot \frac{q-1}{\gcd(q-1,m)2^{l-1}} &< 4 \\
\frac{p-1}{\gcd(p-1,m)2^{l}} \cdot \frac{q-1}{\gcd(q-1,m)2^{l-1}} \cdot \frac{1}{2} &< 4 \cdot \frac{1}{2} \\
\frac{p-1}{\gcd(p-1,m)2^{l}} \cdot \frac{q-1}{\gcd(q-1,m)2^{l}} &< 2
\end{aligned}$$

We know that each of the left hand side are each integers, so therefore, each of the fractions are 1 (in order to be less than 2). This means that $p-1 = \gcd(p-1,m)2^l$ and $q-1 = \gcd(q-1,m)2^l$. However, since we know that m is odd and $p-1$ is even, the gcd of those two numbers are odd. Therefore, the exact power of 2 dividing $q-1$ and $p-1$ is 2^l. Furthermore, this implies that the odd "parts" of $p-1$ and $q-1$ must divide m. We then use the fact that $n = 2^k \cdot m + 1$, and now replace n with pq, giving us $pq = 2^k \cdot m + 1$. We then take this modulo the odd part of $p-1$, using the fact that $p-1$ is divisible by m. Let $o(x)$ denote the largest odd part of x:

$$\begin{aligned}
pq &= 2^k \cdot m + 1 \pmod{o(p-1)} \\
q &= 1 \pmod{o(p-1)} \\
q - 1 &= 0 \pmod{o(p-1)}.
\end{aligned}$$

However, since $o(p-1)$ is odd(by definition) we can disregard the even part of $q-1$, meaning that the odd part of $p-1$ divides the odd part of $q-1$. By taking the equation modulo $q-1$, we find that $o(q-1) \mid o(p-1)$. Therefore, the odd parts of $p-1$ and $q-1$ are equal. However, since we also established that 2^l is the exact power of 2 dividing both $p-1$ and $q-1$, this means that both the even and odd parts of $p-1$ and $q-1$ are equal. However, this means that $p-1 = q-1$, or $p = q$. However, this contradicts the fact that p and q are distinct primes, so therefore $t = 2$ gives us a contradiction.

Case 2 t = 1: This means that $n = p^a$, where a is an integer $a \geq 2$. The first inequality now states that $p^{a-1} < 4$, meaning that the only solution is $p = 3$ and $a = 2$. This means that $n = 9$, contradicting the fact that we defined that $n > 9$.

Therefore, following from the result that $B' \subset B$, we have $\frac{\#(B)}{\phi(n)} \leq \frac{1}{4}$. We have thus proved the theorem (as we have found contradictions in both cases). ■

This is of course an improvement over the Solovay–Strassen test, and we will see that this makes the test much more effective when choosing bases to make a deterministic test

(as we did with Solovay–Strassen test). The following table compiles the results from [PSW80, Jae93, Fei13].

Selected bases	Deterministic Up To Some Value of n (non-inclusive)
{2}	2,047
{2, 3}	1,373,653.
{31, 73}	9,080,191
{2, 3, 5}	25,326,001
{2, 3, 5, 7}	3,215,031,751
{2, 7, 61}	4,759,123,141
{2, 13, 23, 1662803}	1,122,004,669,633
{2, 3, 5, 7, 11}	2,152,302,898,747
{2, 3, 5, 7, 11, 13}	3,474,749,660,383
{2, 3, 5, 7, 11, 13, 17}	341,550,071,728,321
{2, 3, 5, 7, 11, 13, 17, 19, 23}	3,825,123,056,546,413,051
{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37}	18,446,744,073,709,551,616 = 2^{64}

As we can see, making the Miller–Rabin a deterministic test up to a certain value of n is much more fruitful than the Solovay–Strassen test (which definitely makes sense considering the probability bound for each iteration of each of the tests).

3.4. **Lucas Probable Prime Tests.**

Definition 3.11 (Lucas Probable Prime Test)**.** Theorem 2.17 forms the basis of the Lucas Probable Prime Tests. For a given pair (a, b) such that $a^2 - 4b$ is not a perfect square, and a number n such that $\gcd(n, 2b \cdot \Delta) = 1$, then if n satisfies Theorem 2.17, n is known as a Lucas Probable Prime. If n is composite and satisfies the congruence, then n is a Lucas pseudoprime. However, if n does not satisfy the theorem, then by contraposition, n is composite.

When we perform the Lucas Probable Prime test, we need to pick a value for a and b, since this determines the sequence U_j. However, it is important to keep in mind that we defined Δ to not be a perfect square. This is because if this was the case, then $\Delta = c^2$ for some integer c, implying that $\left(\frac{D}{n}\right) = 1$. This would mean that $a = c + 2$ and $b = c + 1$. Solving for the roots of the equation $x^2 - ax + b$ and using this to create an explicit formula for U_j gives us: $\frac{(c+1)^n - 1}{c+1-1} = \frac{b^n - 1}{b-1}$. For $j = n - 1$, we have that $U_{n-1} = \frac{b^{n-1} - 1}{b-1}$, meaning that the Lucas Probable Prime test becomes an ordinary primality test. Therefore, it is better to have $\left(\frac{\Delta}{n}\right) = -1$. A method of picking Δ created by John Selfridge was to find the first term in the sequence $5, -7, 9, -11, 13, -15, \ldots$ that satisfies $\left(\frac{\Delta}{n}\right) = -1$. We then let $a = 1$ and $b = \frac{1-\Delta}{4}$. However, since this is a primality test, if we find a Δ such that $\left(\frac{\Delta}{n}\right) = 0$, then we can immediately output that n is composite (since Δ shares factors with n besides 1 and n, meaning n is composite). Additionally, if n is a square, this means that the Jacobi Symbol will always greater than -1. We quickly show why this is true, by first recalling that the

formula for the Jacobi Symbol is (where we define n to be factorized as $p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are prime numbers and $a_1, a_2, \ldots, a_k$ are positive integers):

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right)^{a_1} \cdot \left(\frac{b}{p_2}\right)^{a_2} \cdot \ldots \cdot \left(\frac{b}{p_k}\right)^{a_k}. \tag{3.5}$$

Since n is a perfect square, $a_1, a_2, \ldots, a_k$ must all be even, meaning that when we calculate the Jacobi Symbol, each of the terms will be nonnegative. Therefore, if we do not find a suitable Δ after a few tries using Selfridge's method, we should check if n is a square.

Once we find a suitable value of D, we can then choose a and b as outlined above and conduct the Lucas Probable Prime Test as stated in Definition 3.11. However, we can strengthen the test by taking some inspiration from the Miller–Rabin test to create the Strong Lucas Probable Prime Test.

Definition 3.12 (Strong Lucas Probable Prime Test)**.** Let n is an odd composite integer such that the $\gcd(n, \Delta) = 1$. Factor $n - \left(\frac{\Delta}{n}\right)$ as $2^s \cdot d$ where d is odd. The Strong Lucas Probable Prime Test is as follows: If n satisfies at least one of the followign conditions:

$$U_d \equiv 0 \pmod{n}$$
$$V_{d \cdot 2^r} \equiv 0 \pmod{n}, \text{for some } 0 \leq r < s,$$

then n is declared a Strong Lucas Probable Prime. If n is a composite number and passes the test, it is considered a Strong Lucas Probable Prime.

We now prove the following theorem:

Theorem 3.13. *If n is a prime p, then at least one of the conditions are satisfied of the Strong Lucas Probable Prime Test, provided that* $\gcd(p, 2b\Delta) = 1$.

Proof. Since $p \nmid \Delta$, $x^2 - ax + b$ has distinct roots y and z in $\overline{F_p}$. We now divide the proof into two cases:

Case 1 $\left(\frac{\Delta}{p}\right) = 1$**:** If $\left(\frac{\Delta}{p}\right) = 1$, this means that Δ is a quadratic residue modulo p. In other words, Δ is a square in F_p, meaning that $f(x)$ factors modulo p. This means that y, z are roots in F_p, and we can therefore apply Fermat's Last Theorem to get: $y^{p-1} \equiv z^{p-1} \equiv 1 \pmod{p}$. This gives us that: $U_{p-1} \equiv \frac{y^{p-1} - z^{p-1}}{y - z} \equiv 0 \pmod{p}$. We know that $y^{p-1} - z^{p-1} \equiv 0 \pmod{p}$, so we can factor $y^{p-1} - z^{p-1}$ can be factored as follows by difference of two squares:

$$(y^{\frac{p-1}{2}} - z^{\frac{p-1}{2}})(y^{\frac{p-1}{2}} + z^{\frac{p-1}{2}}) \equiv 0 \pmod{p}$$
$$(y^{\frac{p-1}{4}} - z^{\frac{p-1}{4}})(y^{\frac{p-1}{4}} + z^{\frac{p-1}{4}})(y^{\frac{p-1}{2}} + z^{\frac{p-1}{2}}) \equiv 0 \pmod{p}$$
$$\ldots$$
$$(y^d - z^d)(y^d + z^d)(y^{2d} + z^{2d}) \ldots (y^{2^{s-1}d} + z^{2^{s-1}d}) \equiv 0 \pmod{p}$$

Note that one of these factors must be 0 (mod p). Therefore, $y^d - z^d \equiv 0 \pmod{p}$. We know that $U_d \equiv \frac{y^d - z^d}{y-z} \pmod{p}$, and since $y^d - z^d 0 \pmod{p}$, we have that $U_d \equiv 0 \pmod{p}$. Otherwise, $y^{\frac{p-1}{2^r d}} + z^{\frac{p-1}{2^r d}} \equiv 0 \pmod{p}$, for some $0 \leq r < s$. However, notice that this is the definition of $V_{2^r d}$, so therefore, we have that $V_{2^r d} \equiv 0 \pmod{p}$. We have therefore proved the first case.

Case 2 $\left(\frac{\Delta}{p}\right) = -1$**:** This means that the discriminant is not a square in F_p, and therefore, the roots are in the field F_{p^2}, as this means that $f(x)$ is irreducible modulo p. Note that since $y \cdot z = b$ (by Vieta's Formulas) and $b, z \neq 0$, y is nonzero as well. We have that:

$$\begin{aligned} U_{2^s d} \equiv \frac{y^{2^s d} - z^{2^s d}}{y - z} &\equiv 0 \pmod{p} \\ y^{2^s d} - z^{2^s d} &\equiv 0 \pmod{p} \\ y^{2^s d} &\equiv z^{2^s d} \pmod{p} \\ (\frac{y}{z})^{2^s d} &\equiv 1 \pmod{p} \end{aligned}$$

If we take the square root of the final equation, since the only square roots of 1 are 1 and -1, we either have $(y/z)^{2^r d} \equiv -1 \pmod{p}$, or $(y/z)^d \equiv 1 \pmod{p}$. By rearranging the terms of the congruences, we find that the first condition implies that $V_{2^r d} \equiv 0 \pmod{p}$, for some $0 \leq r < s$, and the second condition corresponding to $U_d \equiv 0 \pmod{p}$ (using similar logic as in the previous case). We have therefore proved this case as well.

We have proved both cases and therefore the theorem. ■

Arnault (1997) showed that a composite number n is a pseudoprime to at most $\frac{4}{15}$ of the possible bases, unless n is the product of two twin primes $2^k q_1 \pm 1$ (where q_1 is odd), $\left(\frac{\Delta}{2^k q_1 - 1}\right) = -1$ and $\left(\frac{\Delta}{2^k q_1 + 1}\right) = 1$. For a deeper discussion of the topic and the full proof, see [Arn97].

We now define the Extra Strong Lucas Probable Prime Test:

Definition 3.14 (Extra Strong Lucas Probable Prime Test)**.** Let $U_n = U_n(a, 1)$ and $V_n = V_n(a, 1)$. Therefore, $\Delta = a^2 - 4$. Assume that $\gcd(n, 2\Delta) = 1$, and let $n = 2^s d + \left(\frac{\Delta}{n}\right)$, where d is odd. Then, either one of the following congruences hold:

$$\begin{gathered} U_d \equiv 0 \pmod{n} \text{ and } V_d \equiv \pm 2 \pmod{n} \\ V_{2^r d} \equiv 0 \pmod{n} \text{ for some } 0 \leq r < s - 1. \end{gathered}$$

If n passes the test, then n is known as an Extra Strong Lucas Probable Prime. However, if n is composite and passes the test, then n is known as an Extra Strong Lucas Pseudoprime.

We now prove the following theorem:

Theorem 3.15. *Let p be a prime number. Then it must pass the Extra Strong Lucas Probable Prime Test.*

Proof. We can use the Theorem 3.13 to our advantage. Most of the test is the same, except for some conditions; it suffices to show that $V_{2^{s-1}d} \not\equiv 0 \pmod{p}$, and that if $U_d \equiv 0 \pmod{n}$, then $V_d \equiv \pm 2 \pmod{n}$.

We first prove the latter condition, using the following lemma:

Lemma 3.16. $V_n^2 - \Delta U_n^2 = 4b^n$.

Proof. Let c and d be roots of the polynomial $x^2 - ax + b$ (the recurrence polynomial for the sequences $U_j(a,b)$ and $V_j(a,b)$). We have $V_n = c^n + d^n$ and $U_n = \frac{c^n - d^n}{c-d}$, by our previous definitions of the sequences. This gives us (keeping in mind that $\Delta = (c-d)^2$):

$$\begin{aligned}(c^n + d^n)^2 - (c^n - d^n)^2 &= c^{2n} + 2(cd)^n + d^{2n} - (c^{2n} - 2(cd)^n + d^{2n}) \\ &= 4(cd)^n\end{aligned}$$

Note that since $cd = b$ by Vieta's Formulas, we have that $V_n^2 - \Delta U_n^2 = (c^n + d^n)^2 - (c^n - d^n)^2 = 4b^n$, and we have proved the lemma. ∎

By Lemma 3.16 and the fact that $b = 1$, we have that $V_d^2 - \Delta U_d^2 = 4$. Taking this equation modulo p, we have $V_d^2 - \Delta U_d^2 \equiv 4 \pmod{p}$. Since we are trying to prove that if $U_d \equiv 0 \pmod{p}$, then $V_d \equiv \pm 2 \pmod{p}$, we assume that $U_d \equiv 0 \pmod{p}$. This means that we have that $V_d^2 \equiv 4 \pmod{p}$, or $V_d \equiv \pm 2 \pmod{p}$. Therefore, we have proved the latter condition.

We now prove that $V_{2^{s-1}d} \not\equiv 0 \pmod{p}$. We first assume that g is a root of the polynomial $x^2 - ax + 1$. This would imply that g^{-1} is the other root, since by Vieta's Formulas, the product of the two roots is 1. This means that $V_{2^{s-1}d} = g^{2^{s-1}d} + g^{-2^{s-1}d}$. We now try to derive a contradiction. Suppose that $V_{2^{s-1}d} \equiv 0 \pmod{p}$. This would mean that: $g^{2^{s-1}d} + g^{-2^{s-1}d} \equiv 0 \pmod{p}$, which implies that $g^{2^s d} \equiv -1 \pmod{p}$. We now divide this into two different cases:

- **Case 1** $\left(\frac{\Delta}{n}\right) = 1$**:** This would mean that $2^s \cdot d = p - 1$. However, since $\left(\frac{\Delta}{n}\right) = 1$, we know that $g \in F_p$ (since g is a root of $f(x)$, and $f(x)$ is reducible modulo p). However, this means that FLT holds true, meaning $g^{p-1} \equiv 1 \pmod{p}$. However, we know that $V_{2^{s-1}d} \equiv 0 \pmod{p}$ implies that $g^{2^s d} \equiv -1 \pmod{p}$, or $g^{p-1} \equiv -1 \pmod{p}$. Therefore, we have proved a contradiction.
- **Case 2** $\left(\frac{\Delta}{n}\right) = -1$**:** This implies that $g^p \equiv g^-1 \pmod{p}$, which means that $g^{p+1} \equiv 1 \not\equiv -1 \pmod{p}$, and we have again derived a contradiction.

We have derived contradictions in both of the cases, and therefore have proved the theorem. ∎

3.5. **Baillie–PSW Primality Test.** The Baillie–PSW Primality Test is a combination of two previous tests that have been mentioned in this paper. It combines a base 2 Miller–Rabin test and a standard or strong Lucas Probable Prime test.

Definition 3.17 (Baillie–PSW Primality Test)**.** The Baillie–PSW Primality Test goes as follows:

(1) First perform a Miller–Rabin test with base 2. If the test fails, then n is composite. Otherwise, proceed to the next step.
(2) Perform a Strong Probable Lucas Test, using Definition 3.12. If n succeeds, then n is most likely prime.

Carl Pomerance stated that in an exhaustive search to $25 \cdot 10^9$, no composite number was found to pass the test [Pom84]. In fact, even if the Miller Rabin test base 2 was weakened to a Fermat Probable Prime test base 2, every composite $n \leq 25 \cdot 10^9$ would fail at least one of the conditions. In fact, no examples of any composite number passing the test are known. The Elliptic Curve primality proving program PRIMO has been checking all probable primes with this test for years, and no counterexample has been found yet. This has led M. Martin to conclude that no number with less than 10,000 digits will pass the Baillie-PSW test [Wei18]. However, a heuristic argument by Pomerance indicates that there are an infinite number of counterexamples to the Baillie-PSW Primality test [Pom84].

4. Deterministic Tests

4.1. **AKS Primality Test.** The AKS Primality test was the first general, unconditional, and determinstic primality test to run in polynomial time. While it is of immense theoretical importance, it is not used in practice, rendering it as a galactic algorithm. For example, the Baillie–PSW conjecture runs much faster for 64-bit integers. Furthermore, other algorithms such as Elliptic Curve Primality Proving are also unconditionally correct and are much better than the AKS Primality test. The original primality test was published in 2002 by Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. The AKS Primality Test is based off of the following theorem:

Theorem 4.1. *Given an integer $n \geq 2$ and an integer a relatively prime to n, n is prime if and only if the following congruence*

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

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

This theorem can be easily proven using the binomial theorem, and we in fact do something very similar to this in our proof of Theorem 2.13. While Theorem 4.1 could be its own primality test, verifying it would take exponential time (as we would have to expand $(X+a)^n$ and reduce modulo n).

However, there is a way to make the test a bit faster. We can instead take the polynomial modulo another polynomial, $X^r - 1$, for a small value of r. In other words, the following equation must be satisfied:

$$(X+a)^n - (X^n + a) = (X^r - 1)g(x) + nf(x), \tag{4.1}$$

for some polynomials $f(x)$ and $g(x)$. Note that all primes satisfy this equation, since if we let $g(x) = 0$, then we arrive at Theorem 4.1. The congruence can be checked in polynomial time when r is appropriately chosen as a small value (in other words, r is polynomial to the digits in n). The AKS algorithm evaluates Equation 4.1 for a large range of a values.

We now define the AKS Primality Test algorithm below:

Definition 4.2 (AKS algorithm)**.** The AKS Primality Test is as follows:

(1) Check if $n = a^b$ for for positive integer a and $b > 1$.
(2) Find the smallest r such that $\text{ord}_r(n) > \log_2^2 n$. If r and n are not relatively prime, then output that n is composite.
(3) For all $2 \leq a \leq \min(r, n-1)$, check that $a \nmid n$, if it does, then output that n is composite.
(4) If $n \leq r$, then output that n is prime.
(5) For $a = 1$ to $\left\lfloor \sqrt{\phi(r)} \log_2(n) \right\rfloor$ perform Equation 4.1 with n. If n does not satisfy the equation, then n is composite.
(6) Output that n is prime.

We now prove the following theorem:

Theorem 4.3. *If n is prime, then it passes the AKS Algorithm (4.2)*

Proof. A prime number would of course pass steps 1 and 3 since these are divisibility tests. A prime would also pass step 5 because of Equation 4.1. Therefore, the algorithm would either identify n as a prime in step 4 or 6. ■

We now prove the converse of the Theorem 4.3, through a sequence of lemmas. Note that the following lemmas to come are inspired by [AKS04].

Lemma 4.4. *There exists an $r \leq \max 3, \left\lceil \log_2^5(n) \right\rceil$ such that Step 2 in Definition 4.2 is true.*

Proof. This theorem is of course true when $n = 2$, since this would imply that $r = 3$, which satisfies all the conditions of the problem. Therefore, we assume that $n > 2$. This means that n is at least 3 (since n is an integer), meaning that $\left\lceil \log_2^5(n) \right\rceil > 10$. We now use the following lemma, which will allow us to use this fact in a beneficial way (see [Nai82] for a proof):

Lemma 4.5. *Let m be an integer greater than or equal to 7. Then the following inequality is true:*

$$\text{LCM}(1, 2, 3, \ldots, m) \geq 2^m,$$

where LCM *means the Least Common Multiple of the numbers "passed into" the function.*

Let $B = \lceil \log_2^5(n) \rceil$. Since Lemma 4.5 applies to $m \geq 7$, this means that it also works for B as well. Note that we also have that for an integer $m \geq 2$ and an integer k, and a number of the form $m^k \leq B$, the largest value of k is $\lfloor \log_2(B) \rfloor$. This is because we have that:

$$\begin{aligned} k \cdot \log_2(m) &\leq \log_2(B) \\ k &\leq \frac{\log_2(B)}{\log_2(m)} \\ k &\leq \log_2(B), \end{aligned}$$

where the last step results from the fact that the minimum of the denominator is $\log_2(2) = 1$ (since $m \geq 2$). Therefore, since k is an integer, we have that k can at maximum be $\lfloor \log_2(B) \rfloor$. Note that therefore, this means that $n^{\log_2(B)} \leq B$. We now consider the smallest number r that does not the divide the product

$$n^{\lfloor \log_2(B) \rfloor} \cdot \prod_{i=1}^{\lfloor \log_2^2(n) \rfloor} (n^i - 1).$$

Notice that $\gcd(r, n)$ cannot be divisible by all the prime divisors p_i of r, since this would imply that $r \mid n^{\lfloor \log_2(B) \rfloor}$. This is because this means that $p_i \mid \gcd(r, n)$, and using the fact that $\gcd(r, n) \mid n$, meaning that $p_i \mid n$. This means that n is divisible by all the prime divisors of r and from our observation above, we know that this would imply that $r \mid n^{\lfloor \log_2(B) \rfloor}$, which is a contradiction to the fact that r does not divide the above product. Therefore, $\frac{r}{\gcd(r,n)}$ cannot divide the product as well. We now use the fact that r is the smallest number to not divide the product. If $\gcd(r, n) \neq 1$, this would mean that by our previous observation, $\frac{r}{\gcd(r,n)}$ wouldn't divide the product. However, this contradicts the fact that r is the smallest number to not divide the product. Therefore, $\gcd(r, n) = 1$, or in other words, r is relatively prime to n. Furthermore, since r does not divide $n^i - 1$ for $1 \leq i \leq \lfloor \log_2^2(n) \rfloor$, this means that $\text{ord}_r(n) > \log_2^2(n)$. We now create a nicer bound for $\prod_{i=1}^{\lfloor \log_2^2(n) \rfloor} (n^i - 1)$.

Note that since $n^i - 1 < n^i$, we have that $\prod_{i=1}^{\lfloor \log_2^2(n) \rfloor} (n^i - 1) < \prod_{i=1}^{\lfloor \log_2^2(n) \rfloor} n^i = n^{\frac{\lfloor \log_2^2(n) \rfloor (\lfloor \log_2^2(n) \rfloor + 1)}{2}}$. However, we can replace $\lfloor \log_2^2(n) \rfloor$ with $\log_2^2(n) - 1$. This is because while this would create a value that is less than $n^{\frac{\lfloor \log_2^2(n) \rfloor (\lfloor \log_2^2(n) \rfloor + 1)}{2}}$, the product would still be greater than $\prod_{i=1}^{\lfloor \log_2^2(n) \rfloor} (n^i - 1)$. Therefore, we have that $\prod_{i=1}^{\lfloor \log_2^2(n) \rfloor} (n^i - 1) < n^{\frac{\log_2^2(n)(\log_2^2(n)-1)}{2}}$. We can now

use this to make our original product much "nicer". This gives us the inequality:

$$n^{\lfloor \log_2(B) \rfloor} \cdot \prod_{i=1}^{\lfloor \log_2^2(n) \rfloor} (n^i - 1) < n^{\lfloor \log_2(B) \rfloor + \frac{\log_2^2(n)(\log_2^2(n)-1)}{2}} \leq n^{\log_2^4(n)} \leq 2^{\log_2^5(n)} \leq 2^B.$$

Note that the above inequality only holds for $n \geq 2$. By Lemma 4.5, we know that $\text{LCM}(1, 2, 3, \ldots, B) \geq 2^B$. Therefore, we know that $r \leq B = \lceil \log_2^5(n) \rceil$. Therefore, we proved the lemma. ■

The main importance of the above lemma is to show that $r = \mathcal{O}(\log^5(n))$, which makes the test extremely inefficient. As we shall see later, certain conjectures will speed up this process to find r greatly, and thus reduce the overall time complexity of the algorithm. However, we shall first prove the converse of Theorem 4.3. Since $\text{ord}_r(n) > 1$, there exists a prime divisor of n, p, such that $\text{ord}_r(p) > 1$. We know that $p > r$, otherwise Step 3 or 4 would have already ended the test. Using this fact, we know that $\gcd(rn,) = 1$, we know that $p, r \in \mathbb{Z}_r^*$. For the remainder of the proof, we let p and r be fixed. We also let $c = \left\lfloor \sqrt{\phi(r)} \log_2(n) \right\rfloor$.

Step 5 of the algorithm verifies c equations based on Theorem 4.1. Since the algorithm does not out output whether the number is composite or not in this step, we have:

$$(X + a)^n \equiv X^n + a \pmod{X^r - 1, n}, \tag{4.2}$$

for every $0 \geq a \leq c$. This also gives us

$$(X + a)^n \equiv X^n + a \pmod{X^r - 1, p}, \tag{4.3}$$

for $0 \geq a \leq c$. We also have by Theorem 4.1

$$(X + a)^p \equiv X^p + a \pmod{X^r - 1, p}. \tag{4.4}$$

The previous two equations imply that

$$(X + a)^{n/p} \equiv X^{\frac{n}{p}} + a \pmod{X^r - 1, p}. \tag{4.5}$$

Therefore, n and $\frac{n}{p}$ both behave like p in the above equation. We give a name to this property (the same name as given in the original paper):

Definition 4.6. For a polynomial $f(x)$ and a positive integer m, m is known as *introspective* for $f(x)$ if:

$$[f(X)]^m \equiv f(X^m) \pmod{X^r - 1, p}.$$

From Equations 4.3 and 4.4, we can see that $\frac{n}{p}$ and p are both introspective for $X + a$, when $0 \leq a \leq c$. We now prove the following lemma, which shows that introspective numbers are closed under multiplication.

Lemma 4.7. *If a and b are introspective numbers for $f(X)$, then ab is also introspective for $f(X)$.*

Proof. We first use the property that a is introspective for $f(X)$. This means that we have:

$$[f(X)]^a \equiv f(X^a) \pmod{X^r - 1, p}.$$

We can raise both sides of the congruence to power of b, giving us:

$$[f(X)]^{ab} \equiv [f(X^a)]^b \pmod{X^r - 1, p}. \tag{4.6}$$

However, note that since b is also introspective for $f(X)$, we have that:

$$[f(X^a)]^b \equiv f(X^{ab}) \pmod{X^{ar} - 1, p}.$$

However, since $X^r - 1$ divides into $X^{ar} - 1$, the above equation can become:

$$[f(X^a)]^b \equiv f(X^{ab}) \pmod{X^r - 1, p}. \tag{4.7}$$

Therefore, combining Equations 4.6 and 4.7 and gives us $[f(X)]^{ab} \equiv f(X^{ab}) \pmod{X^r - 1, p}$. Therefore, we have proved the lemma. ■

We also prove that for a number a, the set of polynomials that a is introspective to is also closed under multiplication.

Lemma 4.8. *If m is introspective to $f(X)$ and $g(X)$, then m is introspective to $f(X) \cdot g(X)$.*

Proof. We have

$$[f(X) \cdot g(X)]^m \equiv [f(X)]^m \cdot [g(X)]^m \pmod{X^r - 1, p} \equiv [f(X^m)] \cdot [g(X^m)] \pmod{X^r - 1, p}.$$

The above equation uses the fact that m is both introspective to $f(X)$ and $g(X)$. Therefore, we have proved the lemma. ■

The above two lemmas together imply that the set $I = \{(\frac{n}{p})^i \cdot p^j \mid i, j \geq 0\}$ is introspective for all polynomials in the set $P = \{\prod_{a=0}^{c} (X+a)^{e_a} \mid e_a \geq 0\}$. This is because from our previous observations, we know that p and $\frac{n}{p}$ are both introspective for $X + a$ (where $0 \leq a \leq c$). Therefore, by Lemma 4.7, we know that their product will also be introspective for $X + a$. In set P, since the elements are products of $X + a$, we know that by Lemma 4.8, the elements of I must be introspective to set P. We now define two groups that will important for later lemmas.

We define the group $\mathcal{G}$ to be the set of all residues of I modulo r. Note that this is a subgroup of $\mathbb{Z}_r^*$, because we showed that $\gcd(n, r) = 1$ and $\gcd(r, p) = 1$. We also let $|\mathcal{G}| = t$. $\mathcal{G}$ is generated by n and p (these numbers create I). Since $\text{ord}_r(n) > \log_2^2(n)$, we know that $t > \log_2^2(n)$. This is because we know that the residue of n modulo r is in $\mathcal{G}$, and the order of n must be divisible by t by Lagrange's Theorem. Therefore, $t > \log_2^2(n)$.

We now define the second group using properties of cyclotomic polynomials. We let $Q_r(X)$ be the r^{th} cyclotomic polynomial over F_p. This means that $Q_r(X)$ factorizes into irreducible polynomials of degree $\text{ord}_r(n)$ and also divides $X^r - 1$. We let $k(X)$ be one of the irreducible factors. Since $\text{ord}_r\, p > 1$, the degree of $k(X)$ is greater than one (since each of the factors have a degree equal to $\text{ord}_r\, p > 1$ as stated previously). The second group $\mathcal{H}$ is the set of all polynomials in P modulo $k(X)$ and p (written as $P(X) \pmod{k(X), p}$). This group

is generated by $X, X+1, X+2, \ldots, X+c$ (these are what create the set p) in the field $F = F_p[X]/(k(X))$, and is also a subgroup of the multiplicative group of F. We now prove the following lemma which puts a lower bound on $|\mathcal{H}|$.

Lemma 4.9. $|\mathcal{H}| \geq \binom{t+c}{t-1}$.

Proof. It is important to note that since $k(X)$ is a factor of $Q_r(X)$, X is a primitive r^{th} root of unity in F (all roots of a cyclotomic polynomial are primitive roots of unity).

We now show that any two distinct polynomials of degree less than t in P will map to different elements in $\mathcal{H}$. We let $f(X)$ and $g(X)$ be two polynomials in P. Suppose that $f(X) = g(X)$ in the field F, and let $m \in I$. We therefore have $[f(X)]^m = [g(X)]^m$ in F (since $f(X) = g(X)$ in F). However, note that m is also introspective for both $f(X)$ and $g(X)$ (all elements of I are introspective to the polynomials in P). Therefore, we have that $f(X^m) = g(X^m)$ as well. Subtracting $g(X^m)$ from both sides gives us $f(X^m) - g(X^m) = 0$, meaning that X^m is a root for $Q(Y) = f(Y) - g(Y)$, for every $m \in G$ (we never assumed anything about m). Since $\gcd(m, r) = 1$ ($\mathcal{G} \leq \mathbb{Z}_r^*$, meaning that all elements of $\mathcal{G}$ are relatively prime to r), we know that X^m is a primitive root of unity. This is because at the beginning of the proof, we stated that X was a primitive root of unity, and since $\gcd(m, r) = 1$, this means that X^m is also a primitive root of unity. Therefore, there will be t distinct roots of $Q(Y)$ in F, meaning $\deg(Q(Y)) = t$. However, this contradicts the fact that we chose $f(X)$ and $g(X)$ to have a degree less than t, so their difference could not have produced a new polynomial of degree t. Therefore, $f(X) \neq g(X)$.

Note that y and z in F_p cannot be equal to each other, for $1 \leq y \neq z \leq c$. This is because $c = \sqrt{\phi(r)}\log_2(n) < \sqrt{r}\log_2(n) < r < p$. Therefore, there are more elements in F_p than the value of c, so therefore, $i \neq j$. This means $X, X+1, X+2, \ldots, X+c$ are all distinct. Since $\deg(h(X)) > 1$, $X + a \neq 0$ for $0 \leq a \leq c$ in F. This is because all elements of $\mathcal{H}$ are the polynomials of P (which are products of the polynomials of $X + a$) taken modulo $h(X)$ and p. However, since $\deg(X + a) < \deg(h(X))$, $X + a \neq 0$ in F. This means that there are at least $c + 1$ polynomials of degree 1 in $\mathcal{H}$. Therefore, there are at least $\binom{t+c}{t-1}$ polynomials of degree less than t in $\mathcal{H}$, meaning that $|\mathcal{H}| \geq \binom{t+c}{t-1}$. We have thus proved the lemma. ■

We give an upper bound for $|\mathcal{H}|$:

Lemma 4.10. *If n is not a power of p, then $|\mathcal{H}| \leq n^{\sqrt{t}}$.*

Proof. We first consider a subset of I, which we shall call I':

$$I' = \{(\frac{n}{p})^i \cdot p^j | 0 \leq i, j \leq \sqrt{t}\}.$$

If n is not a power of p (if it were then the $\frac{n}{p}$ would reduce into another power of p), there are $(\lfloor\sqrt{t}\rfloor + 1)^2 > t$ distinct members (since i and j can be any value from 0 to $\lfloor\sqrt{t}\rfloor$, meaning that they have $\lfloor\sqrt{t}\rfloor + 1$ options each). This means that there must be at least two elements in I' that have equal residues modulo r. This is because since I' is larger than $\mathcal{G}$, at least

two of the numbers must share residues, since $\mathcal{G}$ is the set of all residues in I modulo r. We let these numbers be a and b, with $a > b$. Therefore, we have:

$$X^a \equiv X^b \pmod{X^r - 1}.$$

We now let $f(X) \in P$. Since a is introspective to all polynomials in P, we have:

$$\begin{aligned}[f(X)]^a &\equiv f(X^a) \pmod{X^r - 1, p} \\ &\equiv f(X^b) \pmod{X^r - 1, p} \\ &\equiv [f(X)]^b \pmod{X^r - 1, p},\end{aligned}$$

implying that $[f(X)]^a = [f(X)]^b$ in the field of F. This is because if they weren't equal, there wouldn't exist polynomials $g(X)$ and $h(X)$ as outlined in Equation 4.1. Therefore, $f(X) \in \mathcal{H}$ is a root of the polynomial $S(X) = Y^a - Y^b$ in F. Since we picked $f(X)$ from $\mathcal{H}$ with no assumptions, $S(X)$ must have at least $|\mathcal{H}|$ distinct roots in F. We know that the degree of $S(X)$ is a, so $a \leq (n/p \cdot p)^{\lfloor\sqrt{t}\rfloor}$. This follows from the fact that $(n/p \cdot p)^{\lfloor\sqrt{t}\rfloor}$ is the largest element in I', and since a is an element of I', it must be less than or equal to it. However, $(n/p \cdot p)^{\lfloor\sqrt{t}\rfloor}$ is also less than or equal to $n^{\sqrt{t}}$. This means that $|\mathcal{H}| \leq n^{\sqrt{t}}$, and we have proved the lemma. ■

Using these estimates, we can finally prove that if the algorithm outputs that n is prime, then n is truly prime.

Theorem 4.11 (Converse of Theorem 4.3)**.** *If the AKS algorithm outputs that n is prime, then n must be prime.*

Proof. It is important to note that $t > \sqrt{t}\log_2(n)$. This is because we showed earlier that $t > \log_2^2(n)$, which can be transformed into $t > \sqrt{t}\log_2(n)$ (taking the square root of both sides and multiplying by $\sqrt{t}$). We also note that $c > \lfloor t\log_2(n)\rfloor$. This is because we remember that $\mathcal{G}$ is a subgroup of $\mathbb{Z}_r^*$, which has an order of $\phi(r)$, meaning that $|\mathcal{G}| = t \leq \phi(r)$. Therefore, $c > \left\lfloor\sqrt{t}\log_2(n)\right\rfloor$, because $c = \left\lfloor\sqrt{\phi(r)}\log_2(n)\right\rfloor$. Using the above inequalities and Lemma 4.9, we have:

$$\begin{aligned}|\mathcal{H}| &\geq \binom{t+c}{t-1} \\ &\geq \binom{c+1+\lfloor\sqrt{t}\log_2(n)\rfloor}{\lfloor\sqrt{t}\log_2(n)\rfloor} \\ &\geq \binom{2\lfloor\sqrt{t}\log_2(n)\rfloor+1}{\lfloor\sqrt{t}\log_2(n)\rfloor}\end{aligned}$$

We now expand $\binom{2\lfloor\sqrt{t}\log_2(n)\rfloor+1}{\lfloor\sqrt{t}\log_2(n)\rfloor}$, giving us: $\frac{(2\lfloor\sqrt{t}\log_2(n)\rfloor+1)\cdot(2\lfloor\sqrt{t}\log_2(n)\rfloor)\cdot\ldots\cdot(\lfloor\sqrt{t}\log_2(n)\rfloor+2)}{(\lfloor\sqrt{t}\log_2(n)\rfloor)\cdot(\lfloor\sqrt{t}\log_2(n)\rfloor-1)\cdot\ldots\cdot1}$. We now "pair" $2\lfloor\sqrt{t}\log_2(n)\rfloor$ with $\lfloor\sqrt{t}\log_2(n)\rfloor$, and so on to $\lfloor\sqrt{t}\log_2(n)\rfloor+2$ with 2. Therefore,

$2\lfloor\sqrt{t}\log_2(n)\rfloor+1$ is paired with 1. Excluding the pair with $2\lfloor\sqrt{t}\log_2(n)\rfloor+1$, since the quotient of each of these pairs is at least 2, we have $2^{\lfloor\sqrt{t}\log_2(n)\rfloor-1}$. We multiply this by $2\lfloor\sqrt{t}\log_2(n)\rfloor+1$, giving us $2^{\lfloor\sqrt{t}\log_2(n)\rfloor-1}\cdot(2\lfloor\sqrt{t}\log_2(n)\rfloor+1)$. We pull out a 2 from the latter term, giving us $2^{\lfloor\sqrt{t}\log_2(n)\rfloor}\cdot(\lfloor\sqrt{t}\log_2(n)\rfloor+\frac{1}{2})$. $(\lfloor\sqrt{t}\log_2(n)\rfloor+\frac{1}{2})$ can be estimated as 2. Therefore, we have $2^{\lfloor\sqrt{t}\log_2(n)\rfloor+1}$. We can now continue our "inequality chain":

$$\begin{aligned}|\mathcal{H}| &\geq \binom{2\lfloor\sqrt{t}\log_2(n)\rfloor+1}{\lfloor\sqrt{t}\log_2(n)\rfloor}\\ &> 2^{\lfloor\sqrt{t}\log_2(n)\rfloor+1}\\ &\geq n^{\sqrt{t}}.\end{aligned}$$

By Lemma 4.10, $|\mathcal{H}|\leq n^{\sqrt{t}}$ if n is not a power of p. However, we just showed that $|\mathcal{H}|\geq n^{\sqrt{t}}$, meaning that n must be a power of p. Therefore, $n=p^v$, for some integer v greater than 0. However, if $v>1$, then step 1 would have determined n as composite. Therefore, n must be prime and we have proved the theorem. ■

The above theorem definitively shows that the AKS primality test is deterministic. We now look at the time complexity. The time complexity of the algorithm itself was shown to be $\tilde{\mathcal{O}}((\log n)^{12})$. However, if the following widely-held conjecture about the distribution of Sophie-Germain primes were true, then the time complexity would be cut down to $\tilde{\mathcal{O}}((\log n)^6)$. Note that these reductions all come from the fact that we can minimize the size of r, which reduces the amount of computations needed for other steps (especially step 5).

We now give the conjecture:

Conjecture 4.12 (Sophie Germain Prime Density Conjecture)**.** *The number of primes q less than or equal to a number m such that $2q+1$ is also prime is asymptotically $\frac{2C_2m}{\ln^2(m)}$, where C_2 is the twin prime constant (which is approximately 0.66).*

The above conjecture implies that $r=\tilde{\mathcal{O}}(\log^2(n))$. This is because by Conjecture 4.12, we know that there are at least $\log_2^2(n)$ such primes between $8\log_2^2(n)$ and $c\log_2^2(n)(\log_2\log_2 n)$, for a suitable value of c. Note that for any such prime q, the possible orders of n modulo q are $\mathrm{ord}_q(n)\leq 2$ or $\mathrm{ord}_q(n)\geq\frac{q-1}{2}$. If $\mathrm{ord}_q(n)\leq 2$, then q must divide n^2-1, meaning that it is bounded by $\mathcal{O}(\log n)$. This is because there are at most $\ln(n^2-1)$ prime factors of n^2-1, which is approximately $2\ln n$. This implies that there exists an $r=\tilde{\mathcal{O}}(\log^2(n))$, such that $\mathrm{ord}_r(n)>\log_2^2(n)$. This value of r gives us an algorithm of $\tilde{\mathcal{O}}(\log^6(n))$.

5. Future Directions and Conclusion

5.1. **Euler Jacobi Pseudoprimes and Carmichael Numbers.** At the end of Section 3.2, I gave a table that outlines bounds on when the Solovay–Strassen test is deterministic. The results in the table may lead us to the following observation (excluding the last row):

Observation 5.1. *If a pair of pre–selected bases for the Solovay–Strassen contains the number 2, the test is deterministic until some Carmichael Number.*

This observation was disproved by the set $\{2, 88\}$ (in the table), which had a "bound" that was not a Carmichael Number (which was 2047). Analyzing the number of counterexamples to the above observation, specifically the primes, gives us some interesting results/graphs. Below I give step counting functions for the set $\{2, n\}$, where the maximum values of n are $100,000$ in Figure 1 and 2 and $1,000,075$ in Figure 3 and 4(generated by implementing code and graphing my results on Matplotlib). Each of the figures give a "zoomed in" and "zoomed out" plot of our prime counterexamples, to get a better sense for their distribtuion. I also give the approximate ratios for the number of counterexamples to the total amount of numbers tested (they are given in the tables following the figures).

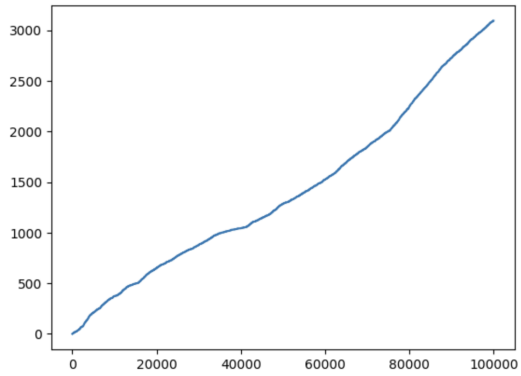

Figure 1. Prime Counterexamples To Our Observation Until 100,000

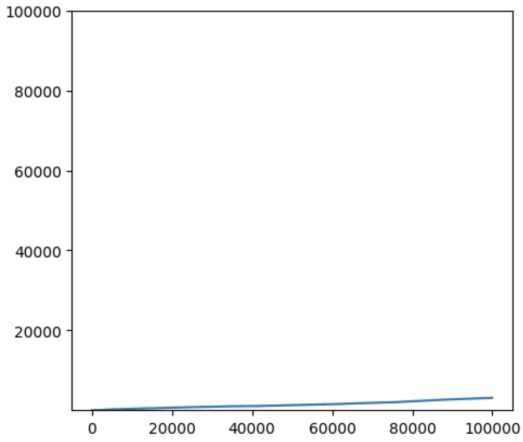

Figure 2. Prime Counterexamples To Our Observation Until 100,000

From the "zoomed in" version of the graph, we can definitely see that there are certain ranges that have fewer amounts of counterexamples to our observation than others. This trend also seems to continue when increase the range of n. In other words, the amount of counterexamples within a given range is relatively inconsistent. However, the zoomed out picture shows us that the graph still increases relatively smoothly asymptotically, which may allow us to create an analogue to the prime counting function for these prime counterexamples.

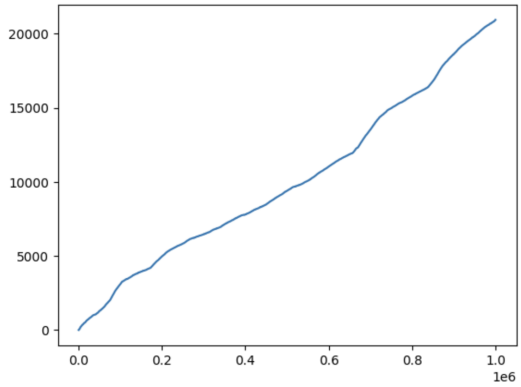

Figure 3. Prime Counterexamples To Our Observation Until 1,000,075

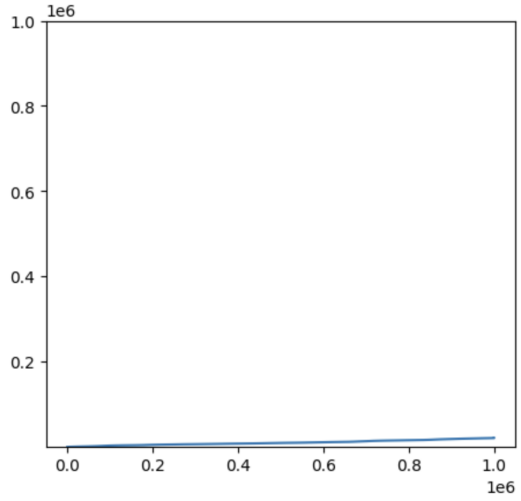

Figure 4. Prime Counterexamples To Our Observation Until 1,000,075

$n \leq 100,000$	Count	Approximated Ratio
Total Counterexamples	36436	36436/100000 = 0.36436
Prime Counterexamples	3093	3093/100000 = 0.03093

$n \leq 1,000,075$	Count	Approximated Ratio
Total Counterexamples	337040	$337040/1000075 = 0.337$
Prime Counterexamples	20930	$20930/1000075 = 0.0209$

As stated previously, the main difficulty in analyzing these counterexamples and the ratios is that the graph does not increase "smoothly". While we do know that each of the above figures are bounded from above by the prime counting function, this is of course not the best estimate. I am currently trying to find a better heuristic estimate to find the number of these prime counterexamples that exist less than a number n. Using these results, I hope to find a method that can generalize this to all counterexamples, and not just the prime counterexamples.

It is also important to note that some of the numbers that are products of twin primes are counterexamples to this hypothesis. I list the first 10 twin prime numbers that are counterexamples to my hypothesis: $143, 323, 3599, 5183, 19043, 32399, 57599, 72899, 97343, 186623$.

To see a comprehensive list of the counterexamples, go to this link that I have created: Counterexamples To Hypothesis.

5.2. **Conclusion.** While we have covered a wide range of primality tests, there are still many others, each with their own merits. These include the Frobenius Tests [Kha20, Gra98], Elliptic Curve Primality Proving [Uzu04], etc. The author encourages the reader to learn about these primality tests as well, as they offer even more unique perspectives on prime numbers and ultimately shows the diversity in the field of Primality Testing.

6. Acknowledgements

The author would like to thank Katherine Martin and Dr. Simon Rubinstein-Salzedo for insightful conversations and guidance.

References

[AGP94] W. R. Alford, Andrew Granville, and Carl Pomerance. There are infinitely many Carmichael numbers. *Ann. Math. (2)*, 139(3):703–722, 1994.

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Ann. Math. (2)*, 160(2):781–793, 2004.

[Arn97] F. Arnault. The Rabin-Monier theorem for Lucas pseudoprimes. *Math. Comput.*, 66(218):869–881, 1997.

[Bur10] David Burton. *Elementary Number Theory*. McGraw Hill, seventh edition, 2010.

[Con16] Keith Conrad. Carmichael Numbers And Korselt's Criterion, 2016.

[CP05] Richard Crandall and Carl Pomerance. *Prime numbers. A computational perspective*. New York, NY: Springer, 2nd ed. edition, 2005.

[Fei13] Jan Feitsma. Tables of pseudoprimes and related data, 2013.

[Gra98] Jon Grantham. A probable prime test with high confidence. *J. Number Theory*, 72(1):32–47, 1998.

[Jae93] Gerhard Jaeschke. On strong pseudoprimes to several bases. *Math. Comput.*, 61(204):915–926, 1993.

[Kha20] Sergei Khashin. Evaluation of the effectiveness of the frobenius primality test, 2020.

[Nai82] M. Nair. On Chebyshev-type inequalities for primes. *Am. Math. Mon.*, 89:126–129, 1982.

[Pom84] Carl Pomerance. ARE THERE ANY COUNTEREXAMPLES TO THE BAILLIE–PSW PRIMALITY TEST, 1984.

[PSW80] Carl Pomerance, J. L. Selfridge, and Samuel S. jun. Wagstaff. The pseudoprimes to $25 \cdot 10^9$. *Math. Comput.*, 35:1003–1026, 1980.

[Sch08] René Schoof. Four primality testing algorithms. In *Algorithmic number theory. Lattices, number fields, curves and cryptography*, pages 101–126. Cambridge: Cambridge University Press, 2008.

[SS77] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM J. Comput.*, 6:84–85, 1977.

[SS78] R. Solovay and V. Strassen. Erratum: A fast Monte-Carlo test for primality. *SIAM J. Comput.*, 7:118, 1978.

[Uzu04] Osmanbey Uzunkol. ATKIN'S ECPP (Elliptic Curve Primality Proving) ALGORITHM. Master's thesis, TECHNICAL UNIVERSITY OF KAISERSLAUTERN, 2004.

[Wei18] Eric W. Weisstein. Tree. From MathWorld—A Wolfram Web Resource, 2018.

Email address: abilak@gmail.com