High School Student Institute of Mathematics and Informatics

Summer Research School Symposium 2021

Primality Testing

Author:

Emilie Ma
University of British Columbia
kewbish@gmail.com

Scientific Advisor:

Pressiana Marinova
Occado Technology Sofia
pressiana.marinova@gmail.com

Abstract

Abstract

1 Introduction

Introduction

1.1 Fermat Primality Test

The Fermat Primality Test is a probablistic primality test based on Fermat's little theorem. Fermat's little theorem, developed by Pierre de Fermat in 1640, states that for any integer a and any prime p, the following holds:

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

If a is not divisible by, or *coprime* to, p, the following is equivalent:

$$a^{(p-1)} \equiv 1 \pmod{p}$$

Proof. Consider $S = \{a, 2a, 3a, \ldots, (p-1) * a\}$. Suppose ra and sa in the set are equal (mod p), so $r \equiv s \pmod{p}$. Therefore, the $p-1$ multiples of a in S are uniquely distinct, and must be congruent to $1, 2, 3, \ldots, (p-1)$ in some order. Multiply these congruences like so:

$$a * 2a * 3a * \ldots * (p-1)a \equiv 1 * 2 * 3 * \ldots (p-1) \pmod{p}$$

This gives:

$$a^{(p-1)} * (p-1)! \equiv (p-1)! \pmod{p}$$

Divide by $(p-1)!$ on each side for:

$$a^{(p-1)} \equiv 1 \pmod{p}$$

To arrive at the alternate form of Fermat's Little Theorem, multiply both sides by a.

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

□

Knowing that $a^{(n-1)} \equiv 1 \pmod{n}$ holds if n is prime, Fermat's primality test chooses k random integers a coprime to n to test if all a are congruent to 1. Because this holds trivially for $a \equiv 1 \pmod{n}$ and if n is odd and $a \equiv -1 \pmod{n}$, a is conventionally chosen such that $1 < a < n-1$. Higher values of k indicate a higher probability that the number is prime.

If n passes these k base tests, it is known as a probable prime. However, not all numbers that pass the Fermat primality test are prime - composite numbers n that pass the test are known as Fermat pseudoprimes. There are infinitely many Fermat pseudoprimes, and several forms of composite numbers that pass the test. For example, Carmichael numbers, composite numbers that satisfy the relation $b^{(n-1)} \equiv 1 \pmod{n}$ for all integers b coprime to n, all pass Fermat's primality test.

1.2 Euler (Solovay-Strassen) Test

The Solovay-Strassen Test is another probablistic test, utilizing the properties of Euler's theorem. Proposed by Leonhard Euler in 1763, Euler's theorem is a generalization of Fermat's little theorem, stating that if a and p are coprime, then the following holds:

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

The function $\phi(n)$ is Euler's totient function. The totient of some number n is the number of positive integers l in the range $1 <= l <= n$ where l is coprime to n.

Proof. Consider $S = \{1 <= l <= n | gcd(l, n) = 1\} = \{l_1, l_2, l_3, \ldots, l_{\phi(n)}\}$. Create a set $aS = \{al_1, al_2, al_3, \ldots, al_{\phi(n)}\}$.
All elements of aS are relatively prime to n, so if all elements of aS are distinct, $aS = S$.

All elements of aS are distinct, as all elements of S are distinct. Therefore, each element of $aS \equiv S \pmod{n}$. Therefore:

$$l_1 * l_2 * l_3 * \ldots * l_{\phi(n)} \equiv al_1 * al_2 * al_3 * \ldots * al_{\phi(n)} \pmod{n}$$

As $l_1 * l_2 * l_3 * \ldots * l_{\phi(n)}$ is relatively prime to n, reducing this gives:

$$a^{\phi(n)} * l_1 * l_2 * l_3 * \ldots * l_{\phi(n)} \equiv l_1 * l_2 * l_3 * \ldots * l_{\phi(n)} \pmod{n}$$

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

Fermat's little theorem is considered a special case of Euler's theorem, because if n is prime, $\phi(n) = n - 1$.

Given that $a^{\phi(n)} \equiv 1 \pmod{n}$, then

$$a^{\phi(n)/2} \equiv \begin{cases} 1 \pmod{n} & \text{when there exists } x \text{ such that } a \equiv x^2 \pmod{n} \\ -1 \pmod{n} & \text{when there is no such integer.} \end{cases}$$

The conditions above form the criteria for the Legendre symbol of a and n. The Legendre symbol $(\frac{a}{n})$ is defined like so:

$$(\frac{a}{n}) \begin{cases} 0 & \text{when } a \equiv 0 \pmod{n} \\ -1 & \text{when } a \not\equiv 0 \pmod{n} \text{ and there exists } x : a \equiv x^2 \pmod{n} \\ -1 & \text{when } a \not\equiv 0 \pmod{n} \text{ and there is no such integer } x. \end{cases}$$

The Jacobi symbol is the generalization of the Legendre symbol to any odd integer n, and is used in the Solovay-Strassen primality test. It is defined as the product of the Legendre symbols of n's prime factors, such that:

$$(\frac{a}{n}) = (\frac{a}{p_1})^{\alpha_1} * (\frac{a}{p_2})^{\alpha_2} * \ldots * (\frac{a}{p_k})^{\alpha_k}$$

for $n = p_1^{\alpha_1} * p_2^{\alpha_2} * \ldots * p_k^{\alpha_k}$.

As with Fermat's primality test, k random bases a are tested. If $a^{(n-1)/2} \equiv (\frac{a}{n}) \pmod{n}$ holds for all k basis, then n is a probable prime.

Similar to Fermat's primality test, the Solovay-Strassen test may pass composite numbers as primes. These are then known as Euler (sometimes Euler-Jacobi) pseudoprimes or liars. All Euler pseudoprimes are also Fermat pseudoprimes.

1.3 Miller-Rabin Primality Test

A third probablistic primality test, the Miller-Rabin primality test was discovered first by Gary Miller in 1976, and subsequently modified by Michael Rabin in 1980. The test relies on two congruence relations that hold when n is an odd prime and rewritten as $2^s * d + 1$, and a is a base such that $0 < a < n$:

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

$$a^{(2^r * d)} \equiv -1 \text{ for some } r \text{ such that } 0 <= r < s$$

Because n is written as $2^s * d + 1$, $n - 1 = 2^s * d$. Therefore, if $a^d \equiv \pm 1 \pmod{n}$, then n is a strong probable prime.

Proof. Given that:

$$a^{(n-1)} \equiv (a^d)^{2^s} \equiv 1 \pmod{n}$$

for all prime n, and because there are no square roots of 1 other than ± 1, the repeated squaring with 2^s doesn't affect the congruence. □

Otherwise, $a^d \pmod{n}$ is squared, for $a^2 d$. If $a^2 d \equiv 1 \pmod{n}$, n is composite, because there are different square roots of $a^2 m \pmod{n}$ other than ± 1. If $a^2 d \equiv -1 \pmod{n}$, then n is a probable prime for similar reasons as above.

These checks are repeated until $a^{(2^{(s-1)} * d)}$ has been reached. If it is ± 1, the result is known by the tests above; however, if not, n is composite, by Fermat's little theorem.

2 Methods

Methods

2.1 Base Analysis

Each primality test was analyzed in a standard way over three trials; the raw data is available in Appendix A. Each trial tested a different k value, and consisted of:

- Generating a random set (S) of 10^4 integers such that $10^6 < x < 2 * 10^6$
- Using SageMath's `is_prime` to check for primality for each integer in S
- Running the primality test with k attempts run on each integer in S with respect to some base a
- Counting all pseudoprimes which passed the primality test but not Sage's primality test
- Repeat for three sub-trials, average results and return lowest number of bases tried (lowest k) that returned the lowest number of pseudoprimes passed

a was a choice of either all random bases, 2, 3, 5, and a pair of 2, 3, or 5. Each trial was timed with the Linux `time` command, recording the real, or total wall time, elapsed.

3 Results

Simplified tables and synthesized figures

The results over three trials of Fermat's Primality Test are shown in Table 1. The results over three trials of Euler's Primality Test are shown in Table 2.

4 Discussion

Discussion of results

5 Conclusion

Conclusion

References

Appendix A Raw Data for Primality Tests

A.1 Fermat's Primality Test

Table 1: Raw data for Fermat's Primality Test Trials

	All Random Bases		
	Trial 1	Trial 2	Trial 3
Running Time	2m45.313s	2m46.200s	2m42.205s
Lowest k required	12	74	93
Pseudoprimes passed at lowest k	0	0.33	0
Range of lowest k required	81		
Range of number of pseudoprimes passed	0.33		
	Base 2		
	Trial 1	Trial 2	Trial 3
Running Time	2m28.057s	2m29.196s	2m31.840s
Lowest k required	45	24	8
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	37		
Range of number of pseudoprimes passed	0		
	Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	2m30.574s	2m46.716s	2m27.309s
Lowest k required	13	60	16
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	44		
Range of number of pseudoprimes passed	0		
	Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	2m27.032s	2m26.897s	2m23.043s
Lowest k required	4	27	7
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	20		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	4m40.323s	5m13.970s	4m51.122s
Lowest k required	19	25	13
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	12		
Range of number of pseudoprimes passed	0		
	Base 3 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	5m6.811s	5m1.727s	4m41.699s
Lowest k required	2	7	6
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	5		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	4m47.168s	5m38.154s	5m26.986s
Lowest k required	6	11	10
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	5		
Range of number of pseudoprimes passed	0		

A.2 Euler's Primality Test

Table 2: Raw data for Euler's Primality Test Trials

	All Random Bases		
	Trial 1	Trial 2	Trial 3
Running Time	1m50.609s	2m4.602s	1m53.909s
Lowest k required	3	5	2
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	3		
Range of number of pseudoprimes passed	0		
	Base 2		
	Trial 1	Trial 2	Trial 3
Running Time	1m45.231s	1m41.760s	1m37.776s
Lowest k required	2	1	3
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	2		
Range of number of pseudoprimes passed	0		
	Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	1m52.067s	1m39.540s	1m37.529s
Lowest k required	2	2	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	1		
Range of number of pseudoprimes passed	0		
	Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	1m51.691s	1m42.775s	1m52.078s
Lowest k required	2	2	2
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	3m32.639s	3m8.813s	3m3.992s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		
	Base 3 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	3m17.024s	2m59.818s	3m5.117s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	3m4.498s	3m14.970s	2m57.338s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		

A.3 Miller-Rabin's Primality Test

Table 3: Raw data for Miller-Rabin's Primality Test Trials

	All Random Bases		
	Trial 1	Trial 2	Trial 3
Running Time	5m59.978s	5m40.792s	5m25.613s
Lowest k required	1	1	3
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	2		
Range of number of pseudoprimes passed	0		
	Base 2		
	Trial 1	Trial 2	Trial 3
Running Time	5m25.738s	6m1.777s	5m7.809s
Lowest k required	2	4	4
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	2		
Range of number of pseudoprimes passed	0		
	Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	5m28.475s	5m47.667s	5m13.659s
Lowest k required	3	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	2		
Range of number of pseudoprimes passed	0		
	Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	5m39.310s	6m8.393s	5m27.674s
Lowest k required	3	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	2		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	11m31.348s	10m57.862s	10m36.092s
Lowest k required	3	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	2		
Range of number of pseudoprimes passed	0		
	Base 3 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	12m36.687s	11m1.823s	10m10.577s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	12m2.218s	10m46.525s	10m17.739s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Range of lowest k required	0		
Range of number of pseudoprimes passed	0		