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	0m18.645s	0m17.844s	0m15.753s
Lowest k required	2	1	4
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.0707	0.0404	0.1111
Range of lowest k required	3		
Range of number of pseudoprimes passed	0		
	Base 2		
	Trial 1	Trial 2	Trial 3
Running Time	0m11.905s	0m12.099s	0m10.469s
Lowest k required	27	16	88
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	3.1616	3.3737	3.3838
Range of lowest k required	72		
Range of number of pseudoprimes passed	0		
	Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	0m11.461s	0m10.760s	0m10.794s
Lowest k required	8	28	3
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	3.3131	3.3131	2.9191
Range of lowest k required	25		
Range of number of pseudoprimes passed	0		
	Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	0m11.109s	0m10.513s	0m10.543s
Lowest k required	5	2	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	2.9595	2.7070	2.9898
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	0m19.564s	0m18.097s	0m16.651s
Lowest k required	1	3	3
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.7070	0.7070	0.6060
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	0m23.712s	0m16.890s	0m16.427s
Lowest k required	1	3	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.5151	0.6767	0.6363
Range of lowest k required	2		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	0m19.252s	0m17.247s	0m16.832s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.7676	0.6767	0.6868
Range of lowest k required	0		

A.2 Euler's (Solovay-Strassen) Primality Test

Table 2: Raw data for Euler's (Solovay-Strassen) Primality Test Trials

	All Random Bases		
	Trial 1	Trial 2	Trial 3
Running Time	0m9.258s	0m10.460s	0m10.214s
Lowest k required	2	1	2
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.0101	0.0	0.0101
Range of lowest k required	1		
Range of number of pseudoprimes passed	0		
	Base 2		
	Trial 1	Trial 2	Trial 3
Running Time	0m9.731s	0m9.428s	0m10.574s
Lowest k required	1	1	5
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	1.5555	1.4242	1.3535
Range of lowest k required	4		
Range of number of pseudoprimes passed	0		
	Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	0m9.572s	0m9.513s	0m10.635s
Lowest k required	1	3	3
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	1.2626	1.5454	1.1212
Range of lowest k required	2		
Range of number of pseudoprimes passed	0		
	Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	0m9.672s	0m9.418s	0m10.831s
Lowest k required	3	2	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	1.2020	1.0303	1.1010
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	0m14.920s	0m15.070s	0m15.584s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.1818	0.2222	0.2222
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	0m15.277s	0m14.959s	0m15.246
Lowest k required	3	2	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.1717	0.1515	0.1919
Range of lowest k required	2		
Range of number of pseudoprimes passed	0		
	Base 2 and Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	0m15.145s	0m14.725s	0m15.836s
Lowest k required	1	2	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.0707	0.0909	0.0404
Range of lowest k required	1		

A.3 Miller-Rabin's Primality Test

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

	All Random Bases		
	Trial 1	Trial 2	Trial 3
Running Time	0m12.835s	0m14.231	0m13.195s
Lowest k required	1	2	2
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.0	0.0404	0.0202
Range of lowest k required	1		
Range of number of pseudoprimes passed	0		
	Base 2		
	Trial 1	Trial 2	Trial 3
Running Time	0m10.604s	0m11.397s	0m10.681s
Lowest k required	3	2	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.7777	0.8282	0.6464
Range of lowest k required	2		
Range of number of pseudoprimes passed	0		
	Base 3		
	Trial 1	Trial 2	Trial 3
Running Time	0m10.732s	0m11.364s	0m10.849s
Lowest k required	4	1	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.8181	0.8989	0.8686
Range of lowest k required	3		
Range of number of pseudoprimes passed	0		
	Base 5		
	Trial 1	Trial 2	Trial 3
Running Time	0m11.549s	0m11.179s	0m10.729s
Lowest k required	4	2	3
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.9292	0.9797	0.7272
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	0m17.325s	0m17.455s	0m17.524s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.1010	0.0707	0.0606
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	0m17.582s	0m17.999s	0m16.950s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.0303	0.0303	0.1414
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	0m17.235s	0m17.694s	0m18.829s
Lowest k required	1	1	1
Pseudoprimes passed at lowest k	0	0	0
Average pseudoprimes passed	0.0505	0.0303	0.0303
Range of lowest k required	0		