Improving the Accuracy of Primality Tests by Enhancing the Miller-Rabin Theorem

Shyam Narayanan

Fourth Annual MIT-PRIMES Conference

Mentor: David Corwin
Project Proposed by Stefan Wehmeier and Ben Hinkle

May 17, 2014

Overview

Outline

Primality Test

Definition

A *primality test* is an algorithm for determining whether an input number is prime.

- Trial division: divide n by every number from 2 until $n - 1$
- Deterministic Primality Tests: Always accurate, but slower
- Probabilistic Primality Tests: faster, but are not accurate.

Fermat Primality Test

- Probabilistic primality test to determine whether a number is a probable prime.
- Fermat's Little Theorem states that $x^{p-1} \equiv 1 \pmod{p}$ for all x relatively prime to a prime p.
- Implementation:
  - For arbitrary integer n, pick random x, where $1 \leq x < n$.
  - If $x^{n-1} \not\equiv 1 \pmod{n}$, then n is composite.
  - If not, then n is probably prime.

False Witnesses

Definition

For integers n and x with $1 \leq x < n$, we say x is a *false witness* to n if n is composite but the Fermat primality test states that n is probably prime in base x.

Weakness of Fermat Primality Test

- High rate of false witnesses
- Carmichael numbers - for any Carmichael number n, every x relatively prime to n is a false witness
- Infinitely many Carmichael numbers

The Miller-Rabin Primality Test

- Stronger version of the Fermat Primality Test.
- Implementation:
  - Write an odd integer n as $n = 1 + 2^e \cdot d$, where d is odd.
  - Then for an integer $x (1 \leq x < n)$, if $x^d \equiv 1 \pmod{n}$, or $x^{d \cdot 2^i} \equiv -1$ for some $0 \leq i \leq e - 1$, then n is probably prime.
  - Else, the integer n is composite.
- Running time: $O(\log^2(n) \cdot \log(\log(n)) \cdot \log(\log(\log(n))))$.
- More accurate than the Fermat primality test but still not always accurate.

Definitions

Strong Psuedoprime and Nonwitness

- If n is composite and $1 \leq x < n$, we say n is a *strong pseudoprime* to the base x if the Miller-Rabin primality test outputs n as probably prime in base x.
- In this case, we say x is a *nonwitness* to n.
- Else, we say x is a *witness* to n.
- Nonwitness for Miller-Rabin, False witness for Fermat

NW(n)

We define $NW(n)$ as the number of nonwitnesses of n.

Sample Test

- Suppose $n = 91$ and $x = 4$.
- $91 = 1 + 2^1 \cdot 45$.
- $4^{45} \equiv 64 \pmod{91}$, and $4^{90} \equiv 1 \pmod{91}$.
- 4 is a false witness for the Fermat Primality Test.
- But it is a witness for the Miller Rabin test.

Outline

Purpose of this Research

- For very large integers, deterministic primality tests are slow and probabilistic primality tests tend to be very inaccurate.
- For example, the probabilistic Miller-Rabin Primality Test often fails to detect composite integers.
- The main goal of this project is to create an improved primality test based on Miller-Rabin.
- The idea: eliminate certain special forms of composite numbers that have many nonwitnesses.
- This research has important applications, as it reduces the number of Miller-Rabin iterations needed.

Outline

Accuracy of Miller-Rabin Test

- The Miller-Rabin Primality Test has significantly fewer nonwitnesses than the Fermat Primality Test.
- Michael O. Rabin proved the following theorem in 1980:

Theorem 1 (Miller-Rabin Theorem)

- Suppose $\frac{NW(n)}{\varphi(n)} = M(n)$.
- Then $M(n) \leq \frac{1}{4}$.

Formula for NW(n)

- Explicit formula for the number of nonwitnesses of n given n's prime factorization.
- This formula was previously stated by Charles R. Greathouse IV, but an original proof is presented in my research paper.

Theorem 2

- Consider an odd composite integer n with m distinct prime factors.
- Suppose that $n - 1 = 2^e \cdot d$ and d is odd.
- Also suppose that $n = \prod_{i=1}^{m} p_i^{q_i}$, and each p_i can be expressed as $2^{e_i} \cdot d_i + 1$, where each d_i is odd.
- The number of nonwitnesses $NW(n)$ equals $\left(\frac{2^{\min(e_i) \cdot m} - 1}{2^m - 1} + 1\right) \cdot \prod_{i=1}^{m} \gcd(d, d_i)$.

Extension of the Miller-Rabin Theorem

Theorem 3 (Main Theorem)

- $M(n) = \frac{1}{4}$ if and only if n is one of two forms:
  1. $n = (2x+1)(4x+1)$, where x is odd and $2x+1$ and $4x+1$ are prime
  2. n is a Carmichael Number of the form pqr, where p, q, r are distinct primes $\equiv 3 \pmod 4$.
- $\frac{1}{6} < M(n) < \frac{1}{4}$ if and only if $n = (2x+1)(4x+1)$, where x is even and $2x+1, 4x+1$ are prime.
- $M(n) = \frac{1}{6}$ if and only if n is of the form $(2x+1)(6x+1)$, where x is odd and $2x+1, 6x+1$ are prime.
- Else, $M(n) \leq \frac{5}{32}$.

New Test

1. Determine if n is of the form $(2x+1)(4x+1)$ for some integer x.
2. Determine if n is of the form $(2x+1)(6x+1)$ for some integer x.
3. Determine if n is a Carmichael number of the form pqr, where $p, q, r \equiv 3 \pmod 4$.
4. Perform the Miller-Rabin Test for a certain base.

Experimental Results about Nonwitnesses

- Define n_a as the smallest composite n so that the first a prime numbers are all nonwitnesses to n.
- All of $n_1, \ldots, n_{11}$ are one of two forms:
  1. $(x+1)(kx+1)$, where $2 \leq k \leq 5$
  2. Carmichael numbers pqr, where $p, q, r \equiv 3 \pmod 4$
- Of the 3773 strong pseudoprimes less than $4 \cdot 10^{12}$, 3187 of them were of the form $(x+1)(kx+1)$, where k is an integer and $x+1$ and $kx+1$ are primes.

Outline

Checking for Carmichael numbers

- There is currently no fast way to check if a number is a Carmichael number.
- However, if n is a Carmichael number of the form pqr, where p, q, r are primes $\equiv 3 \pmod 4$, the following is true:

Lemma Regarding Nonwitnesses

A positive integer x is a nonwitness to n if and only if $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = \left(\frac{x}{r}\right)$

Choosing bases

- Alford, Granville, and Pomerance proved the following Theorem:

Theorem 4

For large enough integers A, and for any set S of $\left\lfloor \log(A)^{1/(3\cdot\log\log\log A)} \right\rfloor$ integers, there are at least $A^{1/(35\cdot\log\log\log(A))}$ Carmichael numbers $n \leq A$ such that i is a nonwitness to n for all $i \in S$.

- Unfortunately, this implies that for any set S of integers, there are infinitely many n for which every element of S is a nonwitness.
- However, certain bases can be chosen to minimize error.

Open Question

- If the Generalized Riemann Hypothesis is true, then for all composite odd n, there exists an integer $i < 2 \cdot log^2(n)$ such that i is a witness.
- For numbers not of the 3 forms given at the outline of the new test, does this bound shrink?

Outline

1. Introduction
2. Purpose
3. Results
4. Problems and Conjectures
5. Summary

Summary and Next Steps

- In this research, we presented a proof for the number of nonwitnesses for n.
- Also, the number of nonwitnesses for a composite odd integer n has been reduced to $\frac{5}{32} \cdot \varphi(n)$, except for a few specific forms of n.
- However, our new primality test requires a method to eliminate effectively Carmichael numbers of the form pqr, where p, q, r are primes $\equiv 3 \pmod 4$.
- This project is expected to be implemented in MATLAB.

Acknowledgements

- I would like to thank my mentor, David Corwin, for the help he has provided me this year, from MATLAB implementations to checking my theorems and progress.
- I would also like to thank Dr. Tanya Khovanova, the lead mentor, for general guidance.
- I would like to thank Stefan Wehmeier and Ben Hinkle from MathWorks, who proposed this project and helped me with MATLAB.
- Finally, I would like to thank the PRIMES-USA program for making this research possible and my parents for all the support they have provided me over the years.

References

- Rabin, Michael O. (1980), "Probabilistic algorithm for testing primality", Journal of Number Theory 12 (1): 128138
- https://oeis.org/A141768
- Carl Pomerance, John L. Selfridge, Samuel S. Wagstaff, Jr. (July 1980). "The pseudoprimes to $25 \cdot 10^9$". Mathematics of Computation 35 (151): 10031026.
- W.R. Alford, A. Granville and C. Pomerance. "On the Difficulty of Finding Reliable Witnesses". Algorithmic Number Theory, Lecture Notes in Comput. Sci. 877, Springer, Berlin, 1994, 1-16.
- E. Bach, Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, MIT Press, Cambridge, Mass., 1985.