Furman University
Electronic Journal of Undergraduate Mathematics
Volume **12, 1 – 4, 2007**

FINDING PRIME NUMBERS: MILLER RABIN AND BEYOND

CHRISTINA MCINTOSH

Abstract. This expository paper motivates and explains the Miller Rabin test and gives some generalizations of it. The Miller Rabin test is a standard probabilistic test used to find large prime numbers quickly.

1. Introduction

How do we know that our personal information is safe when we transfer it over the internet? The truth is most of us don't. But, transferring confidential information over the internet really is safe. Surprisingly, finding large prime numbers plays a significant role in securing our information. This is because in 1978, Rivest, Shamir and Adleman (RSA) created the RSA cryptosystem which uses large primes. The security of this cryptosystem is based on the difficultly of factoring large numbers into their prime decomposition. The RSA cryptosystem has made buying and selling on the internet practical and safe. See [1, 4, 5] for many historical comments on public key cryptography.

It is astonishing that finding prime numbers is easy even though factoring integers is very hard. Our first step in this direction will be Fermat's theorem.

2. Fermat's Theorem

Theorem 2.1. *If p is a prime number and a is an integer, then $a^p = a \bmod p$. Furthermore, if the greatest common divisor of a and p is 1, $a^{p-1} = 1 \bmod p$.*

A proof of this major theorem can be found in any abstract algebra text. See [2] for a sample proof.

Applying Fermat's Theorem to the prime 17 for example, yields

$$3^{16} = 1 \bmod 17.$$

Even more important for our purposes, Fermat's Theorem can also be used to show a number is *not* prime. For instance

$$2^{9699690} = 0100618 \neq 1 \bmod 9699691$$

and we know 9699691 is not prime. For an even more dramatic example, consider $n = 72769523494671107612633$. Then,

$$2^{n-1} = 1382973387568859937483 \neq 1 \bmod n$$

Received by the editors April 10, 2007.
2000 *Mathematics Subject Classification.* 11A51, 11T71, 94A60.
Key words and phrases. prime numbers, Miller Rabin test, Fermat, finite fields, cryptography.
The author of this paper was a sophomore mathematics major at the time the paper was written. This work was done under the supervision of Professor Jeffrey Ehme.

and we see n is composite. As the smallest factor of n is greater than a trillion, it would take considerable time to test for compositeness by trying each prime less than one trillion. It could be hoped that this Fermat test would give an if and only if test for primeness. That is, $a^{n-1} = 1 \bmod n$ iff n is prime where $\gcd(a, n) = 1$. Unfortunately, $561 = (3)(11)(17)$ and yet $2^{560} = 1 \bmod 561$. It is actually worse than this. In fact, $a^{560} = 1 \bmod 561$ for all a with $\gcd(a, 561) = 1$.(Such a number is called a Carmichael number [4].) The question is how often does Fermat fail? Not often. In fact, for $a = 2$, it only fails for forty numbers less than one million [7].

3. Miller Rabin Test

There is a relatively simple extension of Fermat's Theorem that allows one to test for primality with a much higher probability than Fermat's theorem. It is based on the two following facts:

1. Over a field, the quadratic equation $x^2 = 1$ has exactly two solutions: 1 and -1.
2. Z_n, the integers $\bmod n$, form a field precisely when n is a prime number.

The Miller Rabin test works as follows:

Let n be an odd number we wish to test for primeness.

1. Factor $n - 1$ in the form $2^s m$ where m is odd and s is the number of twos that were factored from n. (This step is very easy.) As $n - 1$ is even, $1 \leq s$.
2. Choose an integer a to be the "base" and compute the following sequence of numbers:

$$(*) \qquad a^m \bmod n,\ (a^m)^2 \bmod n,\ ...(a^m)^{2^s} \bmod n$$

This completes the calculation. Now it remains to interpret the result. By construction

$$(a^m)^{2^s} = a^{n-1} = 1 \bmod n \text{ by Fermat if } \gcd(a, n) = 1.$$

(Note: If $\gcd(a, n) > 1$, n is not prime and we actually have a factor of n.) Thus, the sequence of numbers (*) needs to end with a 1 or else n is definitely not prime. Assuming we ended with 1, consider the number that proceeded it. We'll call that number x. By the way we constructed the sequence, $x^2 = 1$. If n is prime, then Z_n is a field which implies $x = -1$ or 1 . Thus a 1 must always be proceeded by a 1 or -1. If this happens, we conclude the number is "probably" prime.

It can be proved that this test gives an incorrect answer for at most $\frac{1}{4}$ of the a values less than n [3]. If n is a composite number and the above test using the base a yields the output "prime", then n is called a strong pseudoprime to the base a. In practice, such numbers are extremely rare [7].

4. First Variation of the Miller Rabin Test

We now would like to consider a variation on the standard Miller Rabin test. If factoring out twos works, how about factoring out threes? More specifically, write $n - 1 = 3^s m$ where $\gcd(m, 3) = 1$. (This is possible for $\frac{1}{3}$ of the numbers n). Next, choose a base number a and compute the following sequence:

$$a^m \bmod n, (a^m)^3 \bmod n, ..., (a^m)^{3^s} \bmod n.$$

As before, by construction $(a^m)^{3^s} = a^{3^s m} = a^{n-1} = 1 \bmod n$. By Fermat, if n is prime and $\gcd(a, n) = 1$, the sequence must end in a 1.

Consider the number x that proceeds a 1. By the way the sequence is constructed, $x^3 = 1$. If n is prime, Z_n is a field, which implies $x^3-1 = (x-1)(x^2+x+1)$ which in turn implies $x = 1$ or x is a solution to $x^2 + x + 1 = 0$. Even though we have no idea which numbers besides 1 are cube roots of 1 in Z_n, we do have a simple test for such numbers. Compute $x^2 + x + 1$ and see if it is 0. Thus, to perform our test, we do the following:

1. Check to see if the sequence ends with a 1.
2. Check to see if each number proceeding a 1 is a 1 or a solution to $x^2+x+1 = 0$. (This is easy to perform).

For example, let $n = 321503175$. Then $n - 1 = 3^4(39691750)$. With $s = 4$ and $a = 2$, the sequence of numbers becomes

$$858624235, -689818282, 514160435, 1, 1.$$

It can be noticed that $514160435^2 + 514160435 + 1 \neq 0 \bmod n$. This yields n is not a prime number. It should be noted, using the standard Miller Rabin test with $a = 2$ for this number yields the incorrect result that n is prime.

5. Second Variation of the Miller Rabin Test

Let F be a finite field and choose $a \neq 0$. A standard theorem from Abstract Algebra implies $F^* = F \setminus \{0\}$ is a cyclic group under multiplication. Suppose $|F| = m$. Then, $|F^*| = m - 1$, Hence $a^{m-1} = 1$. This is very similar to Fermat's Theorem. This can be used to develop a test for primeness.

Suppose n is a number we wish to test for primeness. First we will build a field. We do this by constructing a polynomial that is irreducible $\bmod n$. Call it $p(x)$. Then $Z_n[x]/p(x)$ is a field and $|Z_n[x]/p(x)| = n^{\deg p(x)}$. This means if $m = n^{\deg p(x)}$ and if $f(x)$ is in the element of $Z_n[x]/p(x)$ it follows $f(x)^{m-1} = 1 \bmod p(x)$. This gives a test for n being prime. We list the steps below.

1. Choose an irreducible quadratic $p(x)$ over $Z_n[x]$ [1].
2. Choose a base polynomial in $Z_n[x]/p(x)$. Say $x+1$ is our base polynomial.
3. Write $m - 1 = 2^s q$ where q is odd. Compute the sequence $(x + 1)^q, ((x + 1)^q)^2, ..., ((x + 1)^q)^{2^s} = (x + 1)^{m-1} \bmod p(x)$.

This 2^s sequence of polynomials should end in a 1. Each 1 should be proceeded by a 1 or -1 because $x^2 = 1$ has exactly two solutions in the field F, as before.

For example, suppose $n = 593858003$. Then if n is prime, then $p(x) = x^2+8x+1$ is irreducible in $Z_n[x]$. Then $s = 3$ using $x + 1$ as our base, the sequence in $Z_n[x]/x^2 + 8x + 1$ becomes

$$-162631050x - 14803387, -31552933x - 126211732, -1, 1, 1$$

and the test yields n is prime.

[1]Finding an irreducible quadratic in $Z_n[x]$ is itself an interesting problem, but we leave that for another paper.

6. References

1. Boneh, Dan, *Twenty Years of Attacks on the RSA Cryptosystem*, Notices of the American Mathematical Society (AMS), Vol. 46, No. 2, pp. 203–213, 1999.
2. Fraleigh, John, A First Course in Abstract Algebra, Pearson Education, Inc. 2003.
3. Koblitz, Neal. Graduate Texts in Mathematics: A Course in Number Theory and Cryptography. 2nd Edition. Springe Verlag. New York: 1994.
4. Mollin, Richard, RSA and Public-Key Cryptography, Chapman & Hall, CRC, 2003.
5. Mollin, Richard, An Introduction to Cryptography, Chapman & Hall, CRC, 2000.
6. Pomerance, C.; Selfridge, J. L.; and Wagstaff, S. S. Jr. "The Pseudoprimes," 1980. http://mpqs.free.fr/ThePseudoprimesTo25e9.pdf.
7. "The On-Line Encyclopedia of Integer Sequences", http//www.research.att.com/unjas/sequences.

Department of Mathematics,, Spelman College, Atlanta, GA 30314
E-mail address: cmcintosh@spelman.edu

Sponsor: Jeffrey Ehme, Department of Mathematics,, Atlanta, GA 30314
E-mail address: jehme@spelman.edu