Primality Tests Based on Fermat's Little Theorem

Manindra Agrawal

Department of Computer Science
Indian Institute of Technology, Kanpur
manindra@iitk.ac.in

Abstract. In this survey, we describe three algorithms for testing primality of numbers that use Fermat's Little Theorem.

1 Introduction

Pierre de Fermat, a 17th century mathematician, is famous for the *Fermat's Last Theorem*:

Theorem (Fermat's Last Theorem) *For any number $n > 2$, there is no integer solution of the equation $x^n + y^n = z^n$.*

Fermat did not give a proof of this theorem and it remained a conjecture for more than three hundred years. The quest for a proof of this theorem resulted in the development of several branches of mathematics. The eventual proof of the theorem is more than a hundred pages long [6]. A less well known contribution of Fermat is the *Fermat's Little Theorem*:

Theorem (Fermat's Little Theorem) *For any prime number n, and for any number a, $0 < a < n$, $a^{n-1} = 1 \pmod{n}$.*

Unlike Fermat's Last Theorem, this theorem has a very simple proof. At the same time, the theorem has had a great influence in algorithmic number theory as it has been the basis for some of the most well-known algorithms for primality testing – one of the fundamental problems in algorithmic number theory. In this article, we describe three such algorithms: *Solovay-Strassen Test*, *Miller-Rabin Test*, and *AKS Test*. The first two are randomized polynomial time algorithms and are widely used in practice while the third one is the only known deterministic polynomial time algorithm.

2 Preliminaries

The proofs in next section use basic properies of finite groups and rings which can be found in any book on finite fields (see, e.g., [2]). For numbers r and n, (r, n) equals the gcd of r and n. If $(r, n) = 1$ then $O_r(n)$ equals the order of

r modulo n, or, in other words, $O_r(n)$ is the smallest number $\ell > 0$ such that $n^\ell = 1 \pmod{r}$.

For number n, $\phi(n)$ denotes Euler's totient function which equals the number of a's between 1 and n that are relatively prime to n. If $n = p^k$ for some prime p then $\phi(n) = p^{k-1}(p-1)$.

3 Solovay-Strassen Test

The test was proposed by Solovay and Strassen [5] and was the first efficient algorithm for primality testing. Its starting point is a restatement of Fermat's Little Theorem:

Theorem (Fermat's Little Theorem, Restatement 1) *For any odd prime number n, and for any number a, $0 < a < n$, $a^{\frac{n-1}{2}} = \pm 1 \pmod{n}$.*

It is an easy observation that for prime n, a is a *quadratic residue* (in other words, $a = b^2 \pmod{n}$ for some b) if and only if $a^{\frac{n-1}{2}} = 1 \pmod{n}$. The *Legendre symbol* $\left(\frac{a}{n}\right)$ equals 1 if a is a quadratic residue modulo n else equals -1 for prime n. Therefore, for prime n,

$$\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod{n}.$$

Legendre symbol can be generalized to composite numbers by defining:

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

where $n = \prod_{i=1}^{k} p_i^{e_i}$, p_i is prime for each i. This generalization is called *Jacobi symbol*. Jacobi symbol satisfies *quadratic reciprocity law*:

$$\left(\frac{a}{n}\right) \cdot \left(\frac{n}{a}\right) = (-1)^{\frac{(a-1)(n-1)}{4}}.$$

This, along with the property that $\left(\frac{a}{n}\right) = \left(\frac{a+n}{n}\right)$ gives an algorithm to compute $\left(\frac{a}{n}\right)$ that takes only $O(\log n)$ arithmetic operations.

For composite n, it is no longer neccessary that $\left(\frac{a}{n}\right) = 1$ iff a is a quadraric residue modulo n or that $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod{n}$. This suggests that checking if $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod{n}$ may be a test for primality of n. Solovay and Strassen showed that this works with high probability when a is chosen randomly. To see this, let n have at least two prime divisors and $n = p^k \cdot m$ with $(p, m) = 1$, p a prime, and k odd. (If every prime divisor of n occurs with even exponent then n is a perfect square and can be handled easily.) Let

$$A = \{a \pmod{p^k} \mid (a, p) = 1\}.$$

Clearly, $|A| = p^{k-1}(p-1)$ and exactly $\frac{1}{2}p^{k-1}(p-1)$ numbers in A are quadratic non-residues modulo p. Let $a_0 \in A$ be a quadratic residue modulo p and $b_0 \in A$

be a non-residue modulo p. Pick any number c, $0 < c < m$ and $(c, m) = 1$, and let a, b be the unique numbers between 0 and n such that $a = b = c \pmod m$ and $a = a_0 \pmod{p^k}$, $b = b_0 \pmod{p^k}$. Then,

$$\left(\frac{a}{n}\right) = \left(\frac{a_0}{p}\right)^k \cdot \left(\frac{c}{m}\right) = \left(\frac{c}{m}\right) = -\left(\frac{b}{n}\right).$$

If $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \pmod n$ and $b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right) \pmod n$ then $a^{\frac{n-1}{2}} = -b^{\frac{n-1}{2}} \pmod n$. This implies

$$c^{\frac{n-1}{2}} \pmod m = a^{\frac{n-1}{2}} \pmod m = -b^{\frac{n-1}{2}} \pmod m = -c^{\frac{n-1}{2}} \pmod m.$$

This is impossible since $(c, m) = 1$. Hence, either $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \pmod n$ or $\left(\frac{b}{n}\right) \neq b^{\frac{n-1}{2}} \pmod n$. Therefore, for a random choice of a between 0 and n, either $(a, n) > 1$ or with probability at least $\frac{1}{2}$, $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \pmod n$.

The above analysis implies that the following algorithm works.

Input n.

1. If $n = m^k$ for some $k > 1$ then output COMPOSITE.
2. Randomly select a, $0 < a < n$.
3. If $(a, n) > 1$, output COMPOSITE.
4. If $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod n$ then output PRIME.
5. Otherwise output COMPOSITE.

The test requires $O(\log n)$ arithmetic operations and hence is polynomial time.

4 Miller-Rabin Test

This test was proposed by MIchael Rabin [4] slightly modifying a test by Miller [3]. The starting point is another restatement of Fermat's Little Theorem:

Theorem (Fermat's Little Theorem, Restatement 2) *For any odd prime $n = 2^s \cdot t$ with t odd, and for any number a, $0 < a < n$, the sequence $a^t \pmod n$, $a^{2t} \pmod n$, $a^{2^2 t} \pmod n$, …, $a^{2^s t} \pmod n$ either has all 1's or the pair $-1, 1$ occurs somewhere in the sequence.*

If n is composite, then the sequence may not satisfy the above property. Miller proved that, assuming Extended Riemann Hypothesis, for at least one a between 1 and $\log^2 n$, the above sequence fails to satisfy the property when n is composite but not a prime power. Miller proved that the same holds with high probability for a random a without any hypothesis. We will give Miller's argument.

Assume that n is composite but not a prime power. Let p and q be two odd prime divisors of n. Let k be the largest power of p dividing n. Let $p-1 = 2^v \cdot w$ where w is odd.

We first analyze the case when there is a -1 somewhere in the sequence. Define set A_u as:

$$A_u = \{a \mid (0 < a < n) \ \wedge \ (a^{2^u \cdot t} = -1 \pmod{n})\}$$

for some $0 \leq u < s$.

Then $a^{2^u \cdot t} = -1 \pmod{p^k}$ for every $a \in A$. Let

$$A_{p,u} = \{a \pmod{p^k} \mid a \in A_u\}.$$

Since the size of the multiplicative group modulo p^k is $p^{k-1}(p-1)$, for every $a \in A_{p,u}$, $a^{p^{k-1}\cdot(p-1)} = 1 \pmod{p^k}$. Therefore, $a^{(p^k\cdot(p-1), 2^{u+1}\cdot t)} = 1 \pmod{p^k}$. Prime p does not divide t since otherwise it divides $n-1 = -1 \pmod{p}$ which is absurd. Hence, $a^{(p-1, 2^{u+1}\cdot t)} = 1 \pmod{p^k}$. Since t is odd and $p-1 = 2^v \cdot w$, $a^{2^{\min\{v,u+1\}}\cdot(w,t)} = 1 \pmod{p^k}$. If $v \leq u$ then we get $a^{2^u\cdot t} = 1 \pmod{p^k}$ which is not possible. Hence, $v > u$ implying that $a^{2^u\cdot(w,t)} = -1 \pmod{p^k}$. It is easy to see that the equation $x^\ell = \pm 1 \pmod{p^k}$ for $\ell \mid (p-1)$ has at most ℓ solutions. It follows that $|A_{p,u}| \leq 2^u \cdot (w,t) \leq 2^u \cdot t \leq \frac{1}{2^{u-v}}(p-1)$.

An identical argument shows that $|A_{q,u}| \leq \frac{1}{2^{u-v'}}(q-1)$ for $u < v'$ where $A_{q,u}$ is defined similarly to $A_{p,u}$ and $q-1 = 2^{v'} \cdot w'$ for odd w'. By Chinese Remainder Theorem, it follows that $|A_u| \leq \frac{1}{4^{u-v''}}(n-1)$ if $u < v'' = \min\{v, v'\}$, 0 otherwise. Hence,

$$\sum_{0 \leq u < s} |A_u| \leq \sum_{0 \leq u < v''} \frac{n-1}{4^{u-v''}} = (\frac{1}{3} - \frac{1}{3 \cdot 4^{v''}}) \cdot (n-1).$$

For the case when the whole sequence is all 1's, one can argue exactly as above to obtain that the number of a's giving rise to such a sequence is at most $\frac{1}{4^{v''}}(n-1)$. Hence the probability that the sequence generated by a randomly chosen a satisfies either of the two properties is less than $\frac{1}{2}$.

The above analysis implies that the following algorithm works.

Input n.

1. If $n = m^k$ for some $k > 1$ then output COMPOSITE.
2. Randomly select a, $0 < a < n$.
3. If $(a, n) > 1$ output COMPOSITE.
4. Let $n - 1 = 2^s \cdot t$.
5. Compute the sequence $a^t \pmod{n}$, $a^{2t} \pmod{n}$, ..., $a^{2^s\cdot t} \pmod{n}$.

```
6.  If The sequence is all 1's or has a −1 followed by a 1 then output PRIME.
7.  Otherwise output COMPOSITE.
```

The test requires $O(\log n)$ arithmetic operations and hence is polynomial time.

5 AKS Test

This test was proposed by Agrawal, Kayal and Saxena [1]. It is the only known deterministic polynomial time algorithm known for the problem. The starting point of this test is a slight generalization of Fermat's Little Theorem.

Theorem (Fermat's Little Theorem, Generalized) *If n is prime then for any $r > 0$ and any a, $0 < a < n$,*

$$(x+a)^n = x^n + a \pmod{n, x^r - 1}.$$

On the other hand, if n is composite and not a prime power, then it appears unlikely that the above equation holds for several a's. This can be proven formally as follows.

Suppose that n is not a prime power and let p be a prime divisor of n. Suppose that $(x+a)^n = x^n + a \pmod{n, x^r - 1}$ for $0 < a \leq 2\sqrt{r}\log n$ and r is such that $O_r(n) > 4\log^2 n$. Define the two sets

$$A = \{m \mid (x+a)^m = x^m + a \pmod{p, x^r - 1}, 0 < a \leq 2\sqrt{r}\log n\},$$

and

$$B = \{g(x) \mid g(x)^m = g(x^m) \pmod{p, x^r - 1}, m \in A\}.$$

Clearly, p, $n \in A$ and $x + a \in B$ for $0 < a \leq 2\sqrt{r}\log n$. Moreover, it is straightforward to see that both sets A and B are closed under multiplication and hence are infinite. We now define two finite sets associated with A and B. Let

$$A_0 = \{m \pmod{r} \mid m \in A\},$$

and

$$B_0 = \{g(x) \pmod{p, h(x)} \mid g(x) \in B\}$$

where $h(x)$ is an irreducible factor of $x^r - 1$ over F_p such that the field $F = F_p[x]/(h(x))$ has x as a primitive rth root of unity.

We now estimate the sizes of these sets. Let $t = |A_0|$. Since elements of A_0 are residues modulo r, $t \leq \phi(r) < r$. Also, since $O_r(n) \geq 4\log^2 n$ and A_0 contains all powers of n, $t \geq 4\log^2 n$.

Let $T = |B_0|$. Since elements of B_0 are polynomials modulo $h(x)$ and degree of $h(x) \leq r - 1$, $T \leq p^{r-1}$. The lower bound on T is a little more involved. Consider any two polynomials $f(x), g(x) \in B$ of degree $< t$. Suppose $f(x) =$

$g(x) \pmod{p, h(x)}$. Then $f(x^m) = f(x)^m = g(x)^m = g(x^m) \pmod{p, h(x)}$ for any $m \in A_0$. Therefore, the polynomial $f(y) - g(y)$ has at least t roots in the field F (as x is a primitive rth root of unity). Since the degree of $f(y) - g(y)$ is less than t, this is possible only if $f(y) = g(y)$. This argument shows that all polynomials of degree $< t$ in B map to distinct elements in B_0. The number of polynomials in B of degree $< t$ is at least $\binom{2\sqrt{r}\log n + t - 1}{t-1} \geq \binom{4\sqrt{t}\log n}{2\sqrt{r}\log n} > 2^{2\sqrt{t}\log n}$. This follows because B_0 has at least $2\sqrt{r}\log n$ distinct degree 1 polynomials assuming that $p > 2\sqrt{r}\log n$. Therefore, $T > 2^{2\sqrt{t}\log n}$.

With the above lower bound on T, we can now complete the proof. Since $|A_0| = t$, there exist $(i_1, j_1) \neq (i_2, j_2)$, $0 \leq i_1, j_1, i_2, j_2 \leq \sqrt{t}$ such that $n^{i_1}p^{j_1} = n^{i_2}p^{j_2} \pmod{r}$. Let $g(x) \in B_0$. Then

$$g(x)^{n^{i_1}p^{j_1}} = g(x^{n^{i_1}p^{j_1}}) = g(x^{n^{i_2}p^{j_2}}) = g(x)^{n^{i_2}p^{j_2}} \pmod{p, h(x)}.$$

Hence, the polynomial $y^{n^{i_1}p^{j_1}} - y^{n^{i_2}p^{j_2}}$ has at least $|B_0| = T > 2^{2\sqrt{t}\log n}$ roots in the field F. The degree of this polynomial is at most $n^{2\sqrt{t}}$, and therefore the polynomial is zero. This implies $n^{i_1}p^{j_1} = n^{i_2}p^{j_2}$ which means that n is a power of p. This is not possible by assumption.

The above argument shows that the following test works.

Input n.

1. If $n = m^k$ for some $k > 1$ then output COMPOSITE.
2. Find the smallest r such that $O_r(n) > 4\log^2 n$.
3. For every a, $0 < a \leq 2\sqrt{r}\log n$, do
   If $(a, n) > 1$, output COMPOSITE.
   If $(x + a)^n \neq x^n + a \pmod{n, x^r - 1}$, output COMPOSITE.
4. Output PRIME.

The test requires $O(r^{\frac{3}{2}}\log^2 n \log r)$ arithmetic operations. An easy counting arguments shows that $r = O(\log^5 n)$ and hence the algorithm works in polynomial time.

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, 2004.

[2] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications.* Cambridge University Press, 1986.

[3] G. L. Miller. Riemann's hypothesis and tests for primality. *J. Comput. Sys. Sci.*, 13:300–317, 1976.

[4] M. O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, 12:128–138, 1980.

[5] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM Journal on Computing*, 6:84–86, 1977.

[6] A. Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 141:443–551, 1995.