METHODS OF PRIMALITY TESTING

ZIXING WANG*

Abstract. Primality testing plays an increasingly important role as the introduction of public-key cryptography. In this article, I listed some historically typical algorithms for primality testing and evaluated their pros and cons, including trial division algorithm, Fermat primality test, Lucas primality test, Solovay–Strassen primality test and AKS primality test.

1. Introduction

The interest in primality testing has grown rapidly in the past two decades since the introduction of public-key cryptography. The security of this type of cryptography primarily relies on the difficulty involved in factoring very large numbers. Therefore, the mathematics and computer science communities have begun to address the problem of primality testing with increased vigor. There are many algorithms for testing primality, and in this article I will list a few typical algorithms.

2. Algorithms in primality testing

2.1. **Trial division algorithm.**

Theorem 2.1 (Trial division algorithm)**.** *Let $p > 1$ be an integer. Then p has no prime divisor less than or equal to $\sqrt{p}$ if and only if p is prime.*

Trial division is the most laborious but easiest to understand of the integer factorization algorithms. It takes $O(\sqrt{n})$ which is impractical for large n, but it serves as a useful base case for more sophisticated recursive methods that we will consider. Trial division was first described by Fibonacci in his book Liber Abaci (1202).

2.2. **Fermat primality test.**

Fermat's Little Theorem is first appeared in a letter written by Fermat in 1640. It was stated without proof, though it is speculated that Fermat's proof relied on the binomial theorem. Nearly one hundred years after Fermat stated this theorem, Euler published the first proof in Proceedings of the St. Petersburg Academy in 1736.

2010 *Mathematics Subject Classification.* Primary 11A41.

Key words and phrases. prime number, primality test, algorithm.

* Corresponding author.

Theorem 2.2 (Fermat's Little Theorem)**.** *Let p be a prime and a any integer with $(a, p) = 1$. Then*

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

Proof. We begin by listing the $p-1$ distinct nonzero elements of $\mathbb{Z}_p$:

$$1, 2, 3, \ldots, p-2, p-1 \tag{2.1}$$

By multiplying each member of (**??**) by some fixed nonzero $a \in \mathbb{Z}_p$ we obtain a new list:

$$1a, 2a, 3a, \ldots, (p-2)a, (p-1)a \tag{2.2}$$

Since $\mathbb{Z}_p$ is closed under multiplication, each member of (**??**) is in $\mathbb{Z}_p$. Moreover, each member of (**??**) is distinct. Since products in $\mathbb{Z}_p$ are commutative and associative, we may form the product of the elements in each list and obtain the congruence

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

Finally, multiplication by the inverse of $(p-1)!$ yields the desired result. □

We can use the contrapositive of Fermat's Little Theorem to test not for primality, but instead for compositeness. Letting $n > 2$ be odd, if we can find a base a relatively prime to n for which $a^{n-1} \not\equiv 1 \pmod{n}$, then n is necessarily composite.

The algorithm can be written as follows:

Inputs:

n : a value to test for primality, $n > 3$;

k: a parameter that determines the number of times to test for primality

Output:

Repeat k times:

Pick a randomly in the range $[2, n-2]$. If $a^{n-1} \not\equiv 1 \pmod{n}$, then return **composite**.

If composite is never returned: return **probably prime**.

Complexity:

Using fast algorithms for modular exponentiation, the running time of this algorithm is $\mathrm{O}\left(k \log^3 n\right)$, where k is the number of different values of a we test.

Example 2.3. Consider $n = 5461$. Choosing the base $a = 680$ at random, we find that $(a, n) = 1$. Now we compute

$$680^{5460} \equiv 1162 \not\equiv 1 \pmod{5461}$$

which shows that n is composite. In fact, $n = 43 \cdot 127$.

Notice that if we had chosen the base $a = 16$, we would have again had $(a, n) = 1$, but we would have computed

$$16^{5460} \equiv 1 \pmod{5461}$$

and we would not have been able to make a conclusive decision regarding the compositeness of n.

Unfortunately, our example outlines the fact that there are composites n which can satisfy Fermat's Little Theorem for a particular base a with $(a, n) = 1$. This leads us to the following definition.

Definition 2.4. Let a and n be integers with $(a, n) = 1$. Then n is a pseudoprime to the base a if n is composite, yet we still have $a^{n-1} \equiv 1 \pmod{n}$.

The existence of pseudoprimes means that the converse of Fermat's Little Theorem does not hold true. One would hope that for a particular base a, there are only finitely many pseudoprimes. This is not the case. Actually, there are infinitely many pseudoprimes to the base 2. The base 2 is not the only base troubled by pseudoprimes; each base has infinitely many pseudoprimes associated to it. Worse yet, there are composites which are pseudoprimes to every possible base. These troublesome composites were studied by Carmichael and are named for him.

Definition 2.5. Let a and n be integers. Then n is a Carmichael number if n is composite and $a^{n-1} \equiv 1 \pmod{n}$ for all a with $(a, n) = 1$.

In 1912 , Carmichael conjectured that there are infinitely many Carmichael numbers. Eighty years later, Alford, Granville and Pomerance proved it. Though Carmichael numbers appear less frequently than primes, their infinitude still provides an infinite amount of trouble in testing for compositeness using Fermat's Little Theorem.

2.3. **Lucas primality test.** We saw that the converse of Fermat's Little Theorem does not hold true. However, Lucas showed in a work published in 1876 that an additional condition can be placed on the converse of Fermat's Little Theorem so that it does hold true.

Theorem 2.6 (Lucas' converse of Fermat's Little Theorem)**.** *Let n be a positive integer. If $a^{n-1} \equiv 1 \pmod{n}$ and there is an integer a for every prime divisor p_i of $n-1$ satisfies $a^{(n-1)/p_i} \neq 1 \pmod{n}$, then n is prime.*

Proof. We show that n is prime by verifying that $\phi(n) = n - 1$. By the previous theorem, our first hypothesis means that $\mathrm{ord}_n(a) \mid n - 1$. Now suppose $\mathrm{ord}_n(a) \neq n - 1$, then $n - 1 = k \cdot \mathrm{ord}_n(a)$ for some integer $k > 1$. Let p_i be any prime divisor of k, then

$$a^{(n-1)/p_i} = a^{k \cdot \mathrm{ord}_n(a)/p_i} = \left(a^{\mathrm{ord}_n(a)}\right)^{k/p_i} \equiv 1 \pmod{n}$$

which contradicts our second hypothesis. Thus, $\mathrm{ord}_n(a) = n - 1$. Now by definition, $\mathrm{ord}_n(a) \leq \phi(n)$ and $\phi(n) \leq n - 1$, and since $\mathrm{ord}_n(a) = n - 1$, this means that $\phi(n) = n - 1$ and therefore n is prime. □

This theorem allows us to derive a test which is stronger than the test derived from Fermat's Little Theorem since it is capable of detecting both primes and composites. This new test is well-suited for application to n for which $n-1$ is easy to factor. The following example illustrates this.

Example 2.7. Consider $n = 65537$. The prime factorization of $n-1$ is $65536 = 2^{16}$. Choosing the base $a = 44188$ at random, we find that $(a, n) = 1$. We then compute

$$44188^{65536} \equiv 1 \pmod{65537}$$

which gives evidence that n is prime. Continuing the test, we now compute

$$44188^{65536/2} = 44188^{32768} \equiv -1 \not\equiv 1 \pmod{65537}$$

and then by Lucas' converse of Fermat's Little Theorem, n is prime.

2.4. **Solovay–Strassen primality test.** The Solovay–Strassen primality test, developed by Robert M. Solovay and Volker Strassen in 1977, is a probabilistic test to determine if a number is composite or probably prime. The idea behind the test was discovered by M. M. Artjuhov in 1967. This test has been largely superseded by the Baillie-PSW primality test and the Miller–Rabin primality test, but has great historical importance in showing the practical feasibility of the RSA cryptosystem. The Solovay–Strassen test is essentially an Euler–Jacobi pseudoprime test.

Theorem 2.8 (Euler–Jacobi method)**.** *For any prime number p and any integer a,*

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

This contrasts with the Fermat primality test, for which the proportion of witnesses may be much smaller. Therefore, there are no odd composite n without many witnesses, unlike the case of Carmichael numbers for Fermat's test.

Using fast algorithms for modular exponentiation, the running time of this algorithm is $\mathrm{O}\left(k \log^3 n\right)$, where k is the number of different values of a we test.

2.5. **Miller–Rabin primality test.** The Miller–Rabin primality test is a primality test: an algorithm which determines whether a given number is likely to be prime, similar to the Fermat primality test and the Solovay–Strassen primality test. Gary L. Miller discovered it in 1976; Miller's version of the test is deterministic, but its correctness relies on the unproven extended Riemann hypothesis. Michael O. Rabin modified it to obtain an unconditional probabilistic algorithm in 1980.

Theorem 2.9 (Miller–Rabin primality test)**.** *Suppose $n = 2^s d + 1$, if we can find an a such that $a^d \not\equiv 1 \pmod{n}$ and*

$$a^{2^r d} \not\equiv -1 \pmod{n}$$

for all $0 \leq r \leq s-1$, *then* n *is not prime.*

Proof. Suppose n be prime, and $n > 2$. It follows that $n-1$ is even and we can write it as $2^s d$, where s and d are positive integers and d is odd. For each a in $\mathbb{Z}_n$, either

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

or

$$a^{2^r \cdot d} \equiv -1 \pmod{n}$$

for some $0 \leq r \leq s-1$. To show that one of these must be true, we can use Fermat's little theorem, that for a prime number n : $a^{n-1} \equiv 1 \pmod{n}$. If we keep taking square roots of a^{n-1}, we will get either 1 or -1. If we get -1 then the second equality holds and it is done. If we never get -1, then when we have taken out every power of 2, we are left with the first equality. □

We call a a witness for the compositeness of n. Otherwise a is called a strong liar, and n is a strong probable prime to base a. The term "strong liar" refers to the case where n is composite but nevertheless the equations hold as they would for a prime.

Using repeated squaring, the running time of this algorithm is $\mathrm{O}\left(k \log^3 n\right)$, where k is the number of different values of a we test.

The error made by the primality test is measured by the probability for a composite number to be declared probably prime. The more bases a are tried, the better the accuracy of the test. It can be shown that if n is composite, then at most $\frac{1}{4}$ of the bases a are strong liars for n. As a consequence, if n is composite then running k iterations of the Miller-Rabin test will declare n probably prime with a probability at most 4^{-k}.

2.6. **AKS primality test.** The AKS primality test is a deterministic primality-proving algorithm created and published by Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, computer scientists at the Indian Institute of Technology Kanpur, on August 6, 2002, in an article titled "PRIMES is in P".

Lemma 2.10. *Let* $n > 1$ *be an integer and* a *any integer with* $(a, n) = 1$. *Then* n *is prime if and only if*

$$(x+a)^n \equiv x^n + a \pmod{n}$$

Proof. First note that

$$\begin{aligned}(x+a)^n - (x^n + a) &= C_n^0 a^n + C_n^1 a^{n-1} x + \cdots + C_n^{n-1} a x^{n-1} + C_n^n x^n - x^n - a \\ &= a^n - a + \sum_{0<i<n} C_n^i a^{n-i} x^i\end{aligned}$$

Suppose n is prime. Then each binomial coefficient in the sum is zero, so this case reduces to Fermat's Little Theorem.

Conversely, suppose n is composite. Then n has a prime divisor q, so let $q^k \| n$. We can prove that the coefficient $C_n^q a^{n-q}$ of x^q in $(x+a)^q$ is not divisible by n and therefore, doing a term-by-term comparison, the congruence

cannot hold. Since $(a, n) = 1$, then $(a, q) = 1$ and consequently $\left(a^{n-q}, q^k\right) = 1$. □

While the lemma constitutes a primality test in itself, verifying it takes exponential time: the brute force approach would require the expansion of the $(x + a)^n$ polynomial and a reduction mod$n$ of the resulting $n + 1$ coefficients.

The congruence is an equality in the polynomial ring $\mathbb{Z}_n[x]$. Evaluating in a quotient ring of $\mathbb{Z}_n[x]$ creates an upper bound for the degree of the polynomials involved. The AKS evaluates the equality in $\mathbb{Z}_n[x]/\left(x^r - 1\right)$, making the computational complexity dependent on the size of r. For clarity, this is expressed as the congruence

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

Note that all primes satisfy this relation. This congruence can be checked in polynomial time when r is polynomial to the digits of n.

The AKS algorithm evaluates this congruence for a large set of a values, whose size is polynomial to the digits of n. The proof of validity of the AKS algorithm shows that one can find an r and a set of a values with the above properties such that if the congruences hold then n is a power of a prime.

The algorithm can be written as follows:

Input:

Integer $n > 1$.

Output:

1. If $n = a^b$ for $a \in \mathbb{N}$ and $b > 1$, return **composite**.
2. Find the smallest r such that $\mathrm{ord}_r(n) > (\log_2 n)^2$.
3. If $1 < (a, n) < n$ for some $a \leq r$, return **composite**.
4. If $n \leq r$, return **prime**.
5. For $a = 1$ to $\lfloor \sqrt{\phi(r)} \log_2 n \rfloor$ do
   if $(x + a)^n \neq x^n + a \pmod{x^r - 1, n}$, return **composite**;
6. Return **prime**.

Complexity:

In the first version of the paper, the authors proved the asymptotic time complexity of the algorithm to be $\tilde{O}\left(\log^{12} n\right)$. However, this upper bound was rather loose; a widely-held conjecture about the distribution of the Sophie Germain primes would, if true, immediately cut the worst case down to $\tilde{O}\left(\log^6 n\right)$.

While the algorithm is of immense theoretical importance, it is not used in practice, for it is more complex, time-consuming and space-consuming than other algorithms like Miller–Rabin primality test.

References

[1] Jones, Gareth A, and J. Mary Jones. Elementary Number Theory. London: Springer, 1998.
[2] M.O. Rabin, Probablistic algorithm for testing primality, Journal of Number Theory 12 (1980), 128–138.
[3] M. Agrawal, N. Kayal, N. Saxena, PRIMES is in P, Annals of Mathematics160, 781-793, 2004.

School of Mathematical Sciences, Shanghai Jiao Tong University, 800 Dongchuan Road, 200240 Shanghai, China
Email address: nbwzx@126.com