CSL 758: Advanced Algorithms
Primality Testing

Professor: Kavitha Telikepalli
Scribe: Arindam Pal

Lecture #10
February 18, 2008

---

1 Introduction

Determining whether a number is prime or not is an important problem in number theory. This problem has many applications in computer science – both theoretical and practical. One of the major application of prime numbers is in the design of secure cryptosystems such as the RSA cryptosystem. The security of such a cryptosystem depends on our ability to efficiently find large prime numbers and on our inability to efficiently factorize large composite numbers. Note that this is the decision version of the factorization problem.

2 The Problem

Input: An integer n.
Output: PRIME if n is prime, COMPOSITE otherwise.
Goal: Design an algorithm whose running time is polynomial in $\log n$.

Note that the input size is $\lceil \log_2(n+1) \rceil = \Theta(\log n)$ bits. Hence, the simple algorithm of dividing n by $1, 2, \ldots, \sqrt{n}$ is not a polynomial time algorithm, as its running time is $\sqrt{n} = 2^{\log n/2}$, which is an exponential time algorithm in $\log n$.

3 Preliminaries

Before proceeding further, we need to introduce some terminologies.

Definition 1 *A* group $(G, \circ)$ *is a set* G *with a binary operation* $\circ$ *that satisfies the following four axioms:*

1. Closure*:* $\forall a, b \in G, a \circ b \in G$.
2. Associativity*:* $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$.
3. Existence of Identity*:* $\exists e \in G : \forall a \in G, e \circ a = a \circ e = a$.
4. Existence of Inverse*:* $\forall a \in G, \exists a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e$.

The set of integers $\mathbb{Z}$ forms a group under the normal addition operator $+$. The set of integers $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ forms a group under the modulo addition operator $+_n$ defined as $a +_n b = (a + b) \bmod n$.

Definition 2 *The order of an element* a *in a group* G *is the least positive integer* k *such that* $a^k = e$. *If no such* k *exists, then the order of* a *is said to be infinity.*

Theorem 1 (Lagrange's Theorem) *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.*

Proof Let $g \in G$. The *left coset* of H containing g is defined as

$$gH = \{gh : h \in H\}.$$

The set of left cosets of H forms a partition of the elements of G, i.e. two distinct left cosets g_1H and g_2H satisfy

$$g_1H \cap g_2H = \emptyset \quad (1)$$

$$\bigcup_{g \in G} gH = G \quad (2)$$

(1) can be proved as follows. Suppose, $g_1H \cap g_2H \neq \emptyset$. Then there exists $h_1, h_2 \in H$ such that $g_1h_1 = g_2h_2$. Hence, $g_1h = g_2h_2h_1^{-1}h$ for all $h \in H$. Since H is a subgroup of $G, h_2h_1^{-1}h \in H$. Hence, $g_1h \in g_2H$ for all $h \in H$. In other words, $g_1H \subseteq g_2H$. Similarly, $g_2H \subseteq g_1H$. Hence, $g_1H = g_2H$, contradicting the assumption that they are distinct.

(2) can be proved as follows. Consider any $g \in G$. Let $g_1 = gh^{-1}$. Since $g_1h = g, g \in g_1H$. Thus, every $g \in G$ is in some left coset of H.

Moreover, $H = eH$ and $|gH| = |H|, \forall g \in G$. Thus, if there are k left cosets of H, $k|H| = |G|$. So, $|H|$ divides $|G|$. ■

Theorem 2 (Fermat's Little Theorem) *If p is a prime and a is any integer such that $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof Let $G = \{1, 2, \ldots, p-1\}$. It is easy to verify that under the operation of multiplication modulo p, G forms a group. Let $a \in G$ and let k be the order of a, so that $a^k \equiv 1 \pmod{p}$. By Lagrange's theorem, k divides $|G| = p - 1$. So $p - 1 = km$ for some positive integer m. Therefore,

$$a^{p-1} \equiv a^{km} \equiv (a^k)^m \equiv 1^m \equiv 1 \pmod{p}.$$ ■

Let $\mathbb{Z}_n^*$ be the set of integers between 1 and n which are *relatively prime* to n. It is easy to verify that $\mathbb{Z}_n^*$ forms a group under the modulo multiplication operator $*_n$ defined as $a *_n b = (ab) \bmod n$.

4 A Simple Algorithm

Here is a simple randomized algorithm for primality testing.

1. choose a number a uniformly at random from the set $\mathbb{Z}_n^+ = \{1, 2, \ldots, n-1\}$.
2. **if** $\gcd(a, n) \neq 1$ return COMPOSITE
   else compute $r \equiv a^{n-1} \pmod{n}$
   if $b \neq 1$ return COMPOSITE
   else return PRIME

If n is prime, our algorithm will *always* return PRIME. We will show that if n is composite, our algorithm will return COMPOSITE with probability *at least* $\frac{1}{2}$. For this we need the following lemma.

Lemma 3 *If there is an integer $a \in \mathbb{Z}_n^*$ such that $a^{n-1} \not\equiv 1 \pmod{n}$, then at least $\frac{1}{2}|\mathbb{Z}_n^*|$ elements of $\mathbb{Z}_n^*$ satisfy $a^{n-1} \not\equiv 1 \pmod{n}$.*

Proof Lets define the following sets:

$$\begin{aligned} H &= \{a \in \mathbb{Z}_n^* : a^{n-1} \equiv 1 \pmod{n}\} \\ S &= \{a \in \mathbb{Z}_n^* : a^{n-1} \not\equiv 1 \pmod{n}\} \end{aligned}$$

Clearly, $H \cup S = \mathbb{Z}_n^*$ and $H \cap S = \emptyset$. Hence, $|H| + |S| = |\mathbb{Z}_n^*|$. Since, H is a subgroup of $\mathbb{Z}_n^*$, $|H|$ divides $|\mathbb{Z}_n^*|$. By the assumption in the lemma, $|S| \geq 1$. Thus, $|H| < |\mathbb{Z}_n^*|$. Hence, $|H| \leq \frac{1}{2}|\mathbb{Z}_n^*|$, meaning that $|S| \geq \frac{1}{2}|\mathbb{Z}_n^*|$. ■

It is clear from the above lemma that the error probability for our algorithm is at most $\frac{1}{2}$. Unfortunately, the existence of a certain type of numbers makes matters more complicated. This is captured in the next definition.

Definition 3 *A* Carmichael number *is a composite positive integer n such that*

$$a^{n-1} \equiv 1 \pmod{n}, \forall a \in \mathbb{Z}_n^*.$$

Our algorithm will not work if n is a Carmichael number.