Theoretical Cryptography, Lecture 12

Instructor: Manuel Blum
Scribe: Ryan Williams

Feb 27, 2006

1 Introduction

Today we'll try to cover several topics. Those that we don't finish will be covered in the following lecture.

- Pseudo-Primality Tests
- Carmichael Numbers
- Randomized Primality Tests
- Generation of Random n-Bit Primes

Let's recall some basic number-theoretic definitions and facts. Let $n > 0$ be an integer.

$$\begin{aligned} \mathbb{Z}_n &:= \{0, \ldots, n-1\}, \\ \mathbb{Z}_n^+ &:= \mathbb{Z}_n - \{0\}, \\ \mathbb{Z}_n^* &:= \{a \in Z_n^* \mid (a, n) = 1\}, \end{aligned}$$

where (a, b) is the gcd of a and b.

Fact 1.1 *$\mathbb{Z}_n^*$ is a group under multiplication modulo n.*

Definition 1.1 *H is a subgroup of G iff $H \subseteq G$, the identity $1 \in H$, and H is a group under the same operations as G.*

Theorem 1.1 (Lagrange) *If G is a group and H is a subgroup of G, then $|H|$ divides $|G|$; that is, $\frac{|G|}{|H|}$ is an integer.*

Proof. For $a, b \in G$, define a relation $a \equiv b \iff a \cdot b^{-1} \in H$. This is an equivalence relation since $a \equiv a$, $a \equiv b \implies b \equiv a$, and $(a \equiv b) \wedge (b \equiv c) \implies a \equiv c$, by the properties of a group.

Let $C_1, \ldots, C_k$ be the list of all equivalence classes with respect to $\equiv$ above, for some integer $k > 0$. We claim that for all i, $|C_i| = |H|$ (proof left to the reader). Since they are equivalence classes, $C_i \cap C_j = \varnothing$ for $i \neq j$, and $\bigcup_i C_i = G$. It follows that $|G| = \sum_{i=1}^{k} |C_i| = k|H|$. □

We define $\phi(n) := |\mathbb{Z}_n^*|$.

Fact 1.2 *If the prime factorization of n is $n = p_1^{e_1} \cdots p_k^{e_k}$ where p_i are prime, then $\phi(n) = p_1^{e_1-1}(p_1-1)\cdots p_k^{e_k-1}(p_k-1)$.*

Let's consider some examples of the above fact.

When n is prime, $\phi(n) = n-1$. This makes sense, because when n is prime, $\mathbb{Z}_n^* = \{1, \ldots, n-1\}$: all these numbers are relatively prime to n.

When $n = p^2$ for prime p, $\phi(n) = p(p-1)$. For a proof of this, consider the list of integers

$$1, \ldots, p-1, p, p+1, \ldots, 2p-1, 2p, 2p+1, \ldots\ldots, p^2-1.$$

Each integer of the form kp is not relatively prime to n, but the rest on the list are relatively prime. Removing these bad integers from the list yields

$$1, \ldots, p-1, p+1, \ldots, 2p-1, 2p+1, \ldots\ldots, p^2-1,$$

which is a list of $p(p-1)$ integers.

For one final example, consider $n = 6$. $\mathbb{Z}_6^* = \{1, 5\}$, and $\phi(6) = 2^0(2-1)\cdot 3^0 \cdot (3-1) = 2$.

Fact 1.3 *For all primes p, $\mathbb{Z}_p^*$ has a generator,* i.e. *an element g such that for every $i \in Z_p$, there is a k such that $g^k = i$.*

We will prove this fact in the next lecture.

2 Pseudo-Primality Tests

We know that Fermat's little theorem says that if a number is prime, then for all integers b, $b^{n-1} \equiv 1 \bmod n$. Therefore, considering the contrapositive, if one finds a b such that $b^{n-1} \neq 1 \bmod n$, then one has a proof that a number is composite.

We will look at two kinds of pseudoprimes, defined below. The first kind is weaker than the second.

Definition 2.1 *A number n is a* base-b pseudoprime *iff n is not prime and $b^{n-1} \bmod n \equiv 1$.*

E.g. the smallest base-2 pseudoprime is $341 = 11 \times 31$.

Definition 2.2 *A number n is a* Carmichael number *iff for all $b \in Z_n^*$, n is a base-b pseudoprime.*

For example, the smallest Carmichael number is $561 = 3 \times 11 \times 17$.

Pseudoprimes are counterexamples for the following primality test:

> Let $b > 1$ be an integer.
> If $b^{n-1} \bmod n \equiv 1$ then return "probably prime" else return "n is not prime".

Clearly, this primality test is not perfect, since base-b pseudoprimes are composite, yet the above returns "probably prime" for them. Carmichael numbers are fairly rare, but we'd like a primality test that has no bad instances, and want the algorithm to work with high probability. That is, we currently have a deterministic algorithm that works on most instances– instead, we want a randomized algorithm that, on most of its runs, works on *all* instances.

3 Randomized Test for Primes or Carmichael Numbers

We start by giving a randomized polynomial time algorithm with the following input-output specification:

> **Input:** Positive integer n and parameter k.
>
> **Output:** Either "n is probably prime or Carmichael" or "n is not prime and not Carmichael", with probability of error at most $1/2^k$.

After giving an algorithm for the above, we will show how to get rid of the "or Carmichael" exception, resulting in a randomized primality test.

Let n be a positive integer. Define $A_n = \{a \in \mathbb{Z}_n^* \mid a^{n-1} \bmod n \equiv 1\}$. (Note if n is composite, then A_n is the set of bases b such that n is a base-b pseudoprime.)

Lemma 3.1 *A_n is a subgroup of $\mathbb{Z}_n^*$.*

Proof. A_n is closed under multiplication: for $a, b \in A_n$, $(ab)^{n-1} = a^{n-1} \cdot b^{n-1} \equiv 1 \bmod n$. A_n has the identity, since $1^{n-1} \bmod n \equiv 1$. Finally, for $a \in A_n$, a^{-1} is in A_n as well:

$$1 = 1^{n-1} = (a \cdot a^{-1})^{n-1} = a^{n-1} \cdot (a^{-1})^{n-1} \equiv (a^{-1})^{n-1} \bmod n,$$

where the third equality follows from commutativity of multiplication. □

The fact that A_n is a subgroup implies that if there is just one element not in A_n, then *at least half* of $\mathbb{Z}_n^*$ is not in A_n.

Lemma 3.2 *If $\mathbb{Z}_n^*$ has a b such that $b^{n-1} \bmod n \neq 1$, then $|A_n| \leq |\mathbb{Z}_n^*|/2$.*

Proof. The existence of such a b implies that $|A_n| < |Z_n^*|$. Thus $|\mathbb{Z}_n^*|/|A_n| > 1$. Since A_n is a subgroup, $|A_n|$ divides $|\mathbb{Z}_n^*|$ by Lagrange's theorem. Therefore $|\mathbb{Z}_n^*|/|A_n| \geq 2$. □

The above lemma is very useful for a randomized test:

- If n is a prime or a Carmichael number, then for all $b \in Z_n^*$, $b^{n-1} \bmod n \equiv 1$, by Fermat's little theorem and definition of a Carmichael number.
- If n is not prime and not Carmichael, then there is a b such that $b^{n-1} \bmod n \neq 1$. The above lemma implies that $b^{n-1} \bmod n \neq 1$ for at least $1/2$ of the $b \in \mathbb{Z}_n^*$.

These two conditions suggest a natural randomized algorithm.

Repeat k times:
  Choose $c \in \{1, \ldots, n\}$ uniformly at random.
  If $(c, n) \neq 1$ then return **composite**.
  (After this point, can assume c is chosen uniformly at random from $\mathbb{Z}_n^*$.)
  If $c^{n-1} \bmod n \neq 1$, then return **not prime and not Carmichael**.
Return **probably prime or Carmichael**.

- If n is prime or Carmichael, then it is always the case that $c^{n-1} \bmod n \equiv 1$. Therefore, the test will always report *probably prime or Carmichael* in this case.
- If n is not prime and not Carmichael, then with probability at least $1/2$, a randomly chosen $c \in \mathbb{Z}_n^*$ is such that $c^{n-1} \bmod n \neq 1$. Repeating the test k times means that with probability at least $1 - 1/2^k$, at least one c chosen is such that $c^{n-1} \bmod n \neq 1$, so the test reports *not prime and not Carmichael* with this probability.

4 Randomized Primality Test

Of course, we do not yet have a full primality test. How can we fix the above, so that it is not fooled by Carmichael numbers?

Unfortunately, the test that Manuel gave in lecture is not correct. This space will be filled with a correct version of the Miller-Rabin test later.