REU 2006 · Discrete Math · Lecture 10

Instructor: László Babai
Scribe: Elizabeth Beazley
Editors: Eliana Zoque and Elizabeth Beazley

July 24, 2006. Last updated July 25, 2006 at 1:22 p.m.
NOT PROOF-READ

Today's topic will be Primality Testing. Assume that we have a large number with thousands of digits, and we want to know whether or not it is prime. For a long time, this problem was equated with factoring a number. Factoring, however, remains intractible with no efficient algorithms for computer computations. We shall discuss efficient algorithms for determining whether a number is prime.

10 The Monte Carlo Algorithm

We shall discuss algorithms of the following form. We input a number n, and the outcome is either prime or it is composite. Compositeness will be certified and a proof that n is composite, or *certificate*, is presented. The prime outcome, by contrast, is correct $\leq 50\%$ of the time. To improve this probability, we can use this algorithm repeatedly with the same number n. Note that there is nothing random about the input number. The number n is either prime or it is not. The challenge becomes to think of certificates of compositeness that are somehow easy to find.

10.1 Mersenne and Fermat Primes

The largest known prime number is a **Mersenne prime**, or a prime number of the form $2^p - 1$. Numbers of the form $2^p - 1$ are called **Mersenne numbers**, not all of which are prime. For example, $2^{11} - 1$ is not prime.

Exercise 10.1.1. If $2^k - 1$ is prime, then k is prime.

There are special methods to test Mersenne numbers for primality. The exponents can be in the millions, and there exist algorithms that can determine whether a given Mersenne number is prime.

Exercise 10.1.2. If 2^k+1 is prime, then $k = 2^m$ for some m. Numbers of the form $2^{(2^m)}+1$ are called **Fermat numbers**.

The first five Fermat numbers are all prime: 3, 5, 17, 257, 65,537. We strongly believe that only a finite number of Fermat numbers are prime. By contrast, we believe strongly that infinitely many of the Mersenne numbers are prime.

Let's think about how we can prove that the sixth Fermat number $F_6 = 2^{32} + 1$ is composite. Recall that by Fermat's Little Theorem we have that $3^{p-1} \equiv 1 \mod p$. Thus, if we could prove that $3^{F_6-1} \not\equiv 1 \mod F_6$, we would know that F_6 is not prime. Let us call this the "Fermat Test": Given n and a, is $a^{n-1} \equiv 1 \mod n$? If $1 \leq a \leq n-1$ and (n, a) fails the Fermat test, then we will say that "a is a Fermat witness of compositeness of n." By Fermat's Little Theorem, if a number n has a Fermat witness, then n is composite.

10.2 Carmichael Numbers

Definition 10.2.1. An integer n is a **Carmichael number** if $(\forall a)(\gcd(a, n) = 1$ then $a^{n-1} \equiv 1 \mod n)$ and n is not a prime.

Equivalently, note that n is a Carmichael number if n is composite, but has no Fermat witness.

We shall proceed with "worst-case analysis" of primality. Specifically, we assume that the number n is given by an adversary who knows what algorithm we are going to use to decide whether or not n is prime. We are interested both in guaranteeing that the computation can be carried out in finite time and that the outcome will be correct.

Suppose we have a number that is composite, but not Carmichael, so there is a Fermat witness. Assume that n is a k-digit integer, where $k \approx 1000$. How do we find a Fermat witness?

If $n = pq$ for two distinct primes p and q, then how many numbers are there that are relatively prime to n? We can compute that $\dfrac{\varphi(pq)}{pq} = (1 - \dfrac{1}{p})(1 - \dfrac{1}{q})$, so that the density of integers from 1 to pq that are not relatively prime to pq is $\dfrac{1}{p} + \dfrac{1}{q} - \dfrac{1}{pq}$. There are better algorithms than testing every number smaller than n, as this calculation might suggest.

Observation 10.2.2. Consider $\mathbb{Z}_n^\times$, the multiplicative group of integers mod n. Concretely, $\mathbb{Z}_n^\times = \{i \mid 1 \leq i \leq n,\ \gcd(i, n) = 1\}$. Note that $|\mathbb{Z}_n^\times| = \varphi(n)$.

Exercise 10.2.3. Prove that $\mathbb{Z}_n^\times$ is a group under multiplication mod n.

Theorem 10.2.4 (Lagrange's Theorem). *If $H \leq G$ is a subgroup of a group G, then $|H|$ divides $|G|$.*

Corollary 10.2.5. In particular, if $H \neq G$, then $|H| \leq \frac{1}{2}|G|$.

Now define $\mathbb{Z}_n^\times \supset M := \{\text{non-witnesses}\} = \{i \in \mathbb{Z}_n^\times \mid i^{n-1} \equiv 1 \mod n\}$.

Claim 10.2.6. *$M \leq \mathbb{Z}_n^\times$ is a subgroup.*

Proof. Note that the subset is closed under multiplication. Since $1 \in M$, then if $i, j \in M$, then $(ij)^{n-1} = i^{n-1}j^{n-1} \equiv 1 \cdot 1 = 1 \mod n$. □

Is it possible that $M = \mathbb{Z}_n^\times$? Yes, exactly if n is a Carmichael number.

Here is another possible algorithm for testing primality. Input an integer n, and pick a random number a such that $1 \leq a \leq n-1$. Then,

1. if $\gcd(a, n) = 1$, output "COMPOSITE"
2. if $a^{n-1} \not\equiv 1 \mod n$, output "COMPOSITE".
3. else, output "PRIME OR CARMICHAEL".

Theorem 10.2.7. *If n is not prime or Carmichael, then $P(\text{output "COMPOSITE"}) \geq \frac{1}{2}$.*

Proof. If a does not catch the compositeness of n, then $a \in M$. Thus, the probability that this algorithm won't catch compositeness is $\frac{|M|}{n} < \frac{1}{2}$, since $|M| \leq \frac{\varphi(n)}{2} < \frac{n}{2}$. □

Exercise 10.2.8. Carmichael numbers exist.

1. Show that 561 is a Carmichael number.
2. Show that 561 is the smallest Carmichael number.
3. Find the second smallest Carmichael number. (Hint: It is less than 2000!)

Theorem 10.2.9. *There are infinitely many Carmichael numbers.*

Exercise 10.2.10. If $n = pq$ for p, q prime, then n is not a Carmichael number.

10.3 Carmichael Numbers are Square-Free

Theorem 10.3.1. *If n is Carmichael, then n is square-free; i.e., n is a product of distinct primes.*

Definition 10.3.2. Let G be a group, and $a \in G$. The **order** of a is the smallest $k \geq 1$ such that $a^k = 1$. We shall denote the order by $o_G(a)$.

Claim 10.3.3. $a^t = 1 \iff o_G(a) | t$.

Proof. Suppose that $o_G(a)|t$. Then $a^t = (a^{o_G(a)})^s = 1^s = 1$. Conversely, suppose that $a^t = 1$. Then the Division Algorithm says that we may write $t = o_G(a)q + r$, where $0 \leq r \leq o_G(a) - 1$. Thus, $a^{t-r} = a^{o_G(a)q} = 1$ and so $1 = a^t = a^r a^{t-r} = a^r$ and in particular, $a^r = 1$. But since $r < o_G(a)$, this contradicts the definition of t as $o_G(a)$. □

Proof of Theorem 10.3.1. We shall proceed by contradiction. Suppose that $p^2|n$ for some prime p and that $n = p^s m$, where $\gcd(m, p) = 1$. Consider $o_{p^2}(pm + 1)$, where we denote by o_{p^2} the order in the group $\mathbb{Z}_{p^2}^{\times}$. Note that p does not divide $pm + 1$, and any other prime divisor of n is a divisor of m, and so it does not divide $pm + 1$. Thus we see that $\gcd(pm+1, n) = 1$. Therefore, $(pm+1)^{n-1} \equiv 1 \mod n$, since n is Carmichael by hypothesis. Further, $(pm + 1)^{n-1} \equiv 1 \mod p^2$, and so $o_{p^2}(pm + 1)|n - 1$.

Now, $(pm+1)^p = (1+pm)^p = 1+p^2m+\binom{p}{2} p^2m^2+\cdots \equiv 1 \mod p^2$. Thus $o_{p^2}(pm+1)|p$. But note that $o_{p^2}(pm + 1) = 1 \iff pm + 1 \equiv 1 \mod p^2$; *i.e.*, $p^2|pm$ and so $p|m$, which is a contradiciton. Thus, $o_{p^2}(pm + 1) = p$ and so $p|n - 1$, which can only happen if $p|1$ since $p|n$, our final contradiction. □

10.4 Quadratic Residues

One of Gauss's great early discoveries, the Theorem of Quadratic Reciprocity, shall now be of use to us. We now review the basic properties and definitions of quadratic residues.

Definition 10.4.1. Let p be a prime. We say that a is a **quadratic residue** $\mod p$ if $(\exists x)(x^2 \equiv a \mod p \text{ and } x \not\equiv 0 \mod p)$.

Example 10.4.2. In the integers $\mod 5$, we have $x = \pm 1, \pm 2$ and so $x^2 = 1, 4$. The residues are $\{1, 4\}$. The **non-residues** are $\{2, 3\}$.

Example 10.4.3. If we compute $\mod 7$, then we have $x = \pm 1, \pm 2, \pm 3$, so that $x^2 = 1, 4, 2$. The quadratic residues are $\{1, 2, 4\}$, and the non-residues $\mod 7$ are $\{3, 5, 6\}$.

Claim 10.4.4. *The number of quadratic residues is $\frac{p-1}{2}$ and so the number of non-residues is also $\frac{p-1}{2}$.*

Exercise 10.4.5. Prove that if $x^2 = y^2 \mod p$, then $x \equiv \pm y \mod p$.

Definition 10.4.6. The **Legendre symbol** is defined to be

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a non-residue mod } p \\ 0 & \text{if } a \equiv 0 \mod p \end{cases}$$

Exercise* 10.4.7. $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \mod 4$

Exercise* 10.4.8. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$

Theorem 10.4.9. *The Legendre symbol is multiplicative; i.e.,* $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Proof. If $\left(\frac{a}{p}\right)$ or $\left(\frac{b}{p}\right) = 0$, then $p|ab$ as well. Assume that p does not divide a or b. Then we have four cases:

1. If $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$, then $x^2 \equiv a \mod p$ and $y^2 \equiv b \mod p$. Thus we need to find a z such that $z^2 \equiv ab \mod p$. Take $z = xy$.

2. If $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{b}{p}\right) = -1$, then we need to prove that $\left(\frac{ab}{p}\right) = -1$. Assume that $\left(\frac{ab}{p}\right) = 1$. Then we have $x^2 \equiv a \mod p$ and $y^2 \equiv ab \mod p$ and we need to find a z such that $z^2 \equiv b \mod p$. Take $z = \frac{y}{x}$. Then $xz \equiv y \mod p$, and we can solve for z.

3. If $\left(\frac{a}{p}\right) = -1$ and $\left(\frac{b}{p}\right) = 1$, the argument is the same as in Case (2).

4. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$, and we need to prove that $\left(\frac{ab}{p}\right) = 1$. Let R denote the set of quadratic residues $\mod p$ and N the set of non-residues. Consider the set of numbers $\{1, 2, \ldots, p-1\} = R \cup N$. Then $aR \subset N$ by the previous case, and since R and N have the same cardinality, we may conclude that $aR = N$. Similarly, $aN = R$, since there is no room for more numbers in N. (Here we have used the basic fact that multiplication by a permutes the set $\{1, 2, \ldots, p-1\} \mod p$.)

   Another proof of this uses Group Theory. Let R and N be as above.

   Claim 10.4.10. $R \leq \mathbb{Z}_p^\times$.

   Further, note that the index of R in $\mathbb{Z}_p^\times$ is $[\mathbb{Z}_p^\times : R] = \dfrac{|\mathbb{Z}_p^\times|}{|R|} = \dfrac{p-1}{\frac{p-1}{2}} = 2$. So for $a \notin R$, we have that $\mathbb{Z}_p^\times = R \cup aR$, and aR is the only coset. Therefore $aN = R$.

□

Theorem 10.4.11 (Law of Quadratic Reciprocity). *If p, q, are odd primes, then* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Example 10.4.12. Euler's Formula: $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Example 10.4.13. Gauss's Formula: $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Example 10.4.14. $\left(\dfrac{83}{107}\right) = \left(\dfrac{107}{83}\right)(-1)^{\frac{107-1}{2}\frac{83-1}{2}} = -\left(\dfrac{107}{83}\right) = -\left(\dfrac{24}{83}\right) = -\left(\dfrac{2}{83}\right)^3\left(\dfrac{3}{83}\right) = \left(\dfrac{3}{83}\right) = \left(\dfrac{83}{3}\right)(-1)^{\frac{83-1}{2}\frac{3-1}{2}} = -\left(\dfrac{83}{3}\right) = -(\dfrac{2}{3}) = 1$. (Here we have used that $\left(\frac{2}{83}\right) = (-1)^{\frac{83^2-1}{8}} = -1$.) Thus we see that 83 is indeed a quadratic residue $\mod 107$.

Exercise 10.4.15. The number of rounds in Euclid's algorithm for two integers a and b is $< 2\log_2 a$.