REU 2006 · Discrete Math · Lecture 11

Instructor: László Babai
Scribe: Travis Schedler
Editor: Duru Türkoğlu

July 26, 2006. Last updated July 28, 2006 at 1:15 p.m.
NOT PROOF-READ

11 Primality Test (Continued)

11.1 Chinese Remainder Theorem for Primality Test

Theorem 11.1.1 (Chinese Remainder Theorem). *Consider the equations:*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_1 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

If $(\forall i \neq j)(\gcd(m_i, m_j) = 1)$*, then there exists a solution* x*.*

Exercise 11.1.2. Prove the Chinese Remainder Theorem.

Now, we consider the equation $x^2 \equiv 1 \pmod{m}$.

Question 11.1.3. When does this congruence have solutions other than $\pm 1 \pmod{m}$?

1. No nontrivial solution exists if m is prime.

   Proof. $x^2 \equiv 1 \pmod{p}$ which by definition implies

   $$p \mid x^2 - 1 = (x-1)(x+1)$$

   Therefore,

   $$p \mid x+1 \Rightarrow x \equiv -1 \pmod{p} \quad \text{or} \quad p \mid x-1 \Rightarrow x \equiv 1 \pmod{p}$$

   □

2. No nontrivial solution exists if $m = 2p$.
   For $p = 2$, x is odd implies $x \equiv \pm 1 \pmod 4$.
   For $p \neq 2$ we have $2p \mid (x-1)(x+1)$, which is equivalent to $2 \mid (x-1)(x+1)$ and $p \mid (x-1)(x+1)$. By the first part,

$$2 \mid (x-1)(x+1) \Leftrightarrow x \equiv \pm 1 \pmod 2$$
$$p \mid (x-1)(x+1) \Leftrightarrow x \equiv \pm 1 \pmod p$$

   Therefore, there are altogether two solutions (modulo $2p$):

$$\left.\begin{array}{ll} x \equiv 1 & \pmod p \\ x \equiv 1 & \pmod 2 \end{array}\right\} \Leftrightarrow x \equiv 1 \pmod{2p}; \tag{11.1.1}$$

$$\left.\begin{array}{ll} x \equiv -1 & \pmod p \\ x \equiv -1 & \pmod 2 \end{array}\right\} \Leftrightarrow x \equiv -1 \pmod{2p}. \tag{11.1.2}$$

3. Does a nontrivial solution exist if $m = 4p$, p is an odd prime?
   We need $4p \mid (x-1)(x+1)$.

   Claim 11.1.4. *If $n = 4p, p \geq 3$ prime, then $\exists$ nontrivial solution.*

   Proof.

$$x^2 \equiv 1 \pmod{4p} \Leftrightarrow \begin{cases} x^2 \equiv 1 \pmod 4 & \Leftrightarrow x \equiv \pm 1 \pmod 4 \\ x^2 \equiv 1 \pmod p & \Leftrightarrow x \equiv \pm 1 \pmod p \end{cases} \tag{11.1.3}$$

   Choose $x \equiv 1 \pmod 4$ and $x \equiv -1 \pmod p$: then there exists a nontrivial x to satisfy Eq. 11.1.3, by Theorem 11.1.1 (CRT). □

Theorem 11.1.5. *If $n = r \cdot s$, $\gcd(r, s) = 1$, and $r, s \geq 3$, then a nontrivial x exists to satisfy $x^2 \equiv 1 \pmod n$.*

The proof follows in the lines of the proof of the third case. The cases which are NOT covered by the above theorem are: p^k and $2 \cdot p^k$.

Exercise 11.1.6. Decide the status of these numbers (status means the truth value of ($\exists$nontrivial x)($x^2 \equiv 1 \pmod n$).)

Now, the purpose of all this: PRIMALITY TEST. Remember that if p is prime, $p \nmid a$, then by Fermat's ℓittle Theorem (FℓT),

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p, \tag{11.1.4}$$

because

$$a^{p-1} \equiv 1 \pmod p. \tag{11.1.5}$$

Here we think of $a^{\frac{p-1}{2}}$ as x and a^{p-1} as x^2.

11.2 A Simple Primality Test

The PRIMALITY TEST goes as follows: Given an odd integer $n \geq 3$. Pick random integers $a_1, \ldots, a_k$ such that $1 \leq a_i \leq n-1$. Then

1. if $(\exists i)(\gcd(a_i, n) \neq 1)$ halt COMPOSITE
2. else if $(\forall i)(a_i^{\frac{n-1}{2}} \equiv 1 \pmod{n})$ halt COMPOSITE
3. else if $(\forall i)(a_i^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n})$ halt PRIME
4. else halt COMPOSITE

Note that this algorithm can make both types of mistakes: can either say a number is composite if it is prime, or say that a number is prime if it is not. Nonetheless,

Theorem 11.2.1. $(\forall n)(\Pr(\textit{error}) \leq \frac{1}{2^k})$.

Proof. Case (a): n is prime. An error cannot occur in line 1. We cannot reach line 4 because $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. So $\Pr(\text{error}) = \Pr(\text{error in line 2}) = \frac{1}{2^k}$. Because half of the numbers have a quadratic residue 1.

Case(b) n is composite. Before going on, let us make the definitions

$$\mathbb{Z}_n^\times = \{a \mid 1 \leq a \leq n-1, \gcd(a, n) = 1\} \tag{11.2.1}$$

$$R = \{a \mid a^{n-1} \equiv 1 \pmod{n}\} \tag{11.2.2}$$

$$H = \{a \mid a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}\} \tag{11.2.3}$$

$$K = \{a \mid a^{\frac{n-1}{2}} \equiv 1 \pmod{n}\} \tag{11.2.4}$$

Exercise 11.2.2. $K \leq H \leq R \leq \mathbb{Z}_n^\times$. Here $\leq$ means "is a subgroup of".

Lemma 11.2.3. *If n is composite and $K \neq H$ then $H \neq \mathbb{Z}_n^\times$.*

We use this lemma for the error estimate:

Passing line 2 and exiting in line 3 guarantees $K \neq H$. So we deduce that $H \neq \mathbb{Z}_n^\times$: that is $(\exists x)(x^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}, \gcd(x, n) = 1)$. So

$$\Pr(\text{random } x \text{ satisfies } x^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}) \geq \frac{1}{2}. \tag{11.2.5}$$

Hence $\Pr(\text{all } a_i \in H) \leq \frac{1}{2^k}$. □

Proof. (Lemma). Case 1: n is not square free, by previous class

$$(\exists x)(\gcd(x, n) = 1, x^{n-1} \not\equiv 1 \pmod{n})$$

(i.e. it violates the Fermat test.) Then $R \lneq \mathbb{Z}_n^\times$, i.e. $H \neq \mathbb{Z}_n^\times$ because $H \leq R$.

Case 2: n is square free, composite $\Rightarrow n = r \cdot s, \gcd(r,s) = 1, r, s \geq 3$. By $K \neq H$, $(\exists x)$ such that

$$x^{\frac{n-1}{2}} \equiv -1 \pmod{n} \Rightarrow x^{\frac{n-1}{2}} \equiv -1 \pmod{r}$$

Also trivially,

$$1^{\frac{n-1}{2}} \equiv 1 \pmod{n} \Rightarrow 1^{\frac{n-1}{2}} \equiv 1 \pmod{s}$$

By CRT we can find z such that $z \equiv x \pmod{r}$ and $z \equiv 1 \pmod{s}$. Now,

$$\left.\begin{aligned} z^{\frac{n-1}{2}} &\equiv -1 \pmod{r} \\ z^{\frac{n-1}{2}} &\equiv 1 \pmod{s} \end{aligned}\right\} \Rightarrow z^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{rs}. \tag{11.2.6}$$

Also

$$\left.\begin{aligned} \gcd(z,r) &= 1 \\ \gcd(z,s) &= 1 \end{aligned}\right\} \Rightarrow \gcd(z,n) = 1. \tag{11.2.7}$$

Hence $z \in \mathbb{Z}_n^\times \setminus H \Rightarrow H \neq \mathbb{Z}_n^\times$. □

11.3 Jacobi Symbol and Quadratic Reciprocity

Recall from the last lecture,

Definition 11.3.1. The Legendre symbol for p an odd prime is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue} \\ -1 & a \text{ is a non-quadratic residue} \\ 0, & a \equiv 0 \pmod{p}. \end{cases} \tag{11.3.1}$$

Theorem 11.3.2 (Quadratic Reciprocity). *If p, q are odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{11.3.2}$$

That is,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \Leftrightarrow p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4}. \tag{11.3.3}$$

Example 11.3.3. $\left(\frac{31}{83}\right) = -\left(\frac{83}{31}\right) = -\left(\frac{21}{31}\right)$, since $83 = 2 \cdot 31 + 21$. Then this is $\pm\left(\frac{31}{21}\right)$? To figure it out, write $-\left(\frac{21}{31}\right) = -\left(\frac{3}{31}\right)\left(\frac{7}{31}\right)$, and use $\left(\frac{31}{21}\right) := \left(\frac{31}{3}\right)\left(\frac{31}{7}\right)$.

Here in the above example we are using factoring. But it is highly believed that factoring is hard, hence we cannot calculate the Legendre symbol efficiently. Instead we analyse Quadratic Reciprocity for the Jacobi symbol as defined below.

Definition 11.3.4 (Jacobi Symbol). The Jacobi symbol for odd $m = \prod p_i^{k_i}$ is

$$\left(\frac{a}{m}\right) = \prod \left(\frac{a}{p_i}\right)^{k_i} \tag{11.3.4}$$

Exercise 11.3.5 (Quadratic Reciprocity for Jacobi Symbol). Let $r, s \geq 3$ odd, with $\gcd(r, s) = 1$. Then the Quadratic Reciprocity holds for the Jacobi symbol:

$$\left(\frac{r}{s}\right)\left(\frac{s}{r}\right) = (-1)^{\frac{r-1}{2}\cdot\frac{s-1}{2}}. \tag{11.3.5}$$

Corollary 11.3.6. The Jacobi symbol is computable as fast as gcd.

Exercise 11.3.7. If $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$, then $(\exists x)(x^2 \equiv a \pmod{pq})$. (CRT)

More about the Jacobi symbol: E.g., if we have two factors, then $\left(\frac{a}{pq}\right) = 1$ if either a is a quadratic residue modulo both p and q, or neither.

Exercise 11.3.8. (Practice) $m = p \cdot q$, $\left(\frac{a}{pq}\right) = 1 = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$ then $\{x^2 \pmod{pq}, \gcd(x, pq) = 1\} \leq \mathbb{Z}_{pq}^{\times}$.

This hopefully gives us a bit of understanding about the Jacobi symbol.

11.4 Solovay-Strassen Primality Test

Given n odd, ≥ 3, pick a at random, $1 \leq a \leq n-1$.

1. if $\gcd(a, n) \neq 1$, halt COMPOSITE.
2. else if $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)$ (Jacobi symbol), halt PRIME.
3. else halt COMPOSITE.

Claim 11.4.1. *If n is prime, then there is no error. If n is composite, then $Pr(error) \leq \frac{1}{2}$.*

Proof. (Incomplete)

Case (a): n is prime. Then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$. (This is 1 if a is a quadratic residue.) Clearly we pass line 1 and at line 2 we halt and output PRIME.

Case (b): n is composite. We could divide into cases n is square-free and not, but there is a better way. Let $H^* := \{a \mid a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}, \gcd(a, n) = 1\}$, and let $K^* := K \cap H^*$.

Exercise 11.4.2. $K^* \leq H^* \leq R \leq \mathbb{Z}_n^{\times}$.

Exercise 11.4.3. Complete the proof (we are out of time).

□