

**Math 104B, Number Theory, Winter 2003.**

**Lecture 8. Solution of  $x^2 \equiv a \pmod{p}$ .**

**Last Time** we introduced quadratic residues and for  $p$  an odd prime we introduced the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } p|a. \end{cases}$$

We showed that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

**Proposition 9.1.9. (Euler's Criterion).** Let  $p$  be an odd prime and  $a$  an integer such that  $(a, p) = 1$ ; then

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

In particular,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

We also introduced the following results which will be proved later: For distinct odd primes  $p$  and  $q$ ,

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

Also

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

**Proof of Euler's Criterion.** Recall that we showed that if  $g$  is a primitive root modulo  $p$ , then

$$\left(\frac{g^m}{p}\right) = (-1)^m.$$

Now  $g^{p-1} \equiv 1 \pmod{p}$  and  $g^{(p-1)/2}$  has order 2 modulo  $p$ , so  $g^{(p-1)/2} \equiv -1 \pmod{p}$ . Hence

$$\left(\frac{g^m}{p}\right) = (-1)^m \equiv (g^{(p-1)/2})^m \equiv (g^m)^{(p-1)/2} \pmod{p}.$$

Since any  $a$  with  $(a, p) = 1$  can be written as  $a \equiv g^m \pmod{p}$  for some  $m$ , this proves Euler's criterion.

Now assume  $\left(\frac{a}{p}\right) = 1$ . We wish to solve the equation  $x^2 \equiv a \pmod{p}$ . The easy case is the case when  $p \equiv 3 \pmod{4}$ . In this case,  $p - 1 = 2s$  with  $s$  odd. By Euler's criterion,

$$a^{(p-1)/2} = a^s \equiv 1 \pmod{p}.$$

Hence

$$a^{s+1} \equiv a \pmod{p}.$$

Now we use the fact that  $s$  is odd. We can set

$$x = a^{(s+1)/2},$$

and then  $x^2 \equiv a \pmod{p}$ .

**Example.** Solve  $x^2 \equiv 5 \pmod{11}$ . We have  $11 - 1 = 2 \cdot 5$ . Taking  $s = 5$  we have  $(s + 1)/2 = 3$ . The solution is

$$x \equiv 5^3 = 125 \equiv 4 \pmod{11}.$$

We can check that  $4^2 = 16 \equiv 5 \pmod{11}$ .

This method does not work in the case when  $p \equiv 1 \pmod{4}$ . We will show the main new idea in that case by solving the equation

$$(*) \quad x^2 \equiv -1 \pmod{p}.$$

(Notice that you can only solve this when  $p \equiv 1 \pmod{4}$  because when  $p \equiv 3 \pmod{4}$   $-1$  is not a quadratic residue.) The idea is to find an element  $z$  whose order is divisible by 4. Once we have such an element, we are done. Indeed, if the order of  $z$  is  $4r$ , then the order of

$$x \equiv z^r \pmod{p}$$

is 4. But this implies that  $x^2$  has order 2 modulo  $p$ , and the only element of order 2 modulo  $p$  is  $-1$ , so  $x$  is a square root of  $-1$ . Now the question is, how do we find an element whose order is divisible by 4? A primitive root would work, since  $\phi(p) = p - 1$  is divisible by 4, but it is not so easy to find a primitive root. For large primes it can take a lot of calculation. The important observation is that we can use any quadratic non-residue. Since half the invertible elements are quadratic non-residues, we can find these quickly by choosing numbers at random. It also turns out that we do not even need to calculate the order of the quadratic non-residue precisely to find the square root of  $-1$ , because we have the following lemma:

**Lemma 9.2.3.** If  $p - 1 = 2^r s$  where  $s$  is odd, and if  $n$  is a quadratic non-residue modulo  $p$ , then  $z = n^s$  has order precisely  $2^r$ . In fact the set

$$S_{2^r} = \{z, z^2, z^3, \dots, z^{2^r}\}$$

gives all the elements (modulo  $p$ ) whose order modulo  $p$  divides  $2^r$ , i.e. which satisfy the equation  $y^{2^r} \equiv 1 \pmod{p}$ .

We followed the proof in the book.

**Example.** Solve  $x^2 \equiv -1 \pmod{13}$ .

**Solution.** Notice that  $13 - 1 = 4 \cdot 3$ . We first search for a quadratic non-residue modulo 13.

$$\left(\frac{2}{13}\right) = (-1)^{(13-1)(13+1)/8} = (-1)^{3 \cdot 7} = -1.$$

Hence  $n = 2$  is a quadratic non-residue. Now calculate  $z = n^3$  and get  $z \equiv 8 \pmod{13}$ . By the Lemma,  $z$  has order 4, and is thus  $x = z = 8$  a solution of  $x^2 \equiv -1 \pmod{13}$ . (Indeed,  $8^2 = 64 = 65 - 1 = 13 \cdot 5 - 1$ .)

Now we put the two ideas together to solve the general equation  $x^2 \equiv a \pmod{p}$  when  $\left(\frac{a}{p}\right) = 1$  and  $p \equiv 1 \pmod{4}$ . First we write  $p - 1 = 2^r s$  with  $s$  odd. Set

$$x_0 \equiv a^{(s+1)/2} \pmod{p}.$$

Then

$$x_0^2 \equiv a^s a \equiv b_0 a \pmod{p},$$

where

$$b_0 \equiv a^s \pmod{p}.$$

We wish to solve

$$y^2 b_0 \equiv 1 \pmod{p}$$

since then we get

$$(x_0 y)^2 \equiv a \pmod{p}.$$

The important observation is that the order of  $b_0$  divides  $2^{r-1}$ . Indeed,

$$b_0^{2^{r-1}} \equiv a^{2^{r-1}s} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$$

since  $a$  is a quadratic residue. Hence choosing  $n$  to be a quadratic non-residue modulo  $p$  and  $z \equiv n^s \pmod{p}$ , by the Lemma we can write

$$b_0 = z^m, \pmod{p}$$

for some  $m < 2^r$ , and we see that  $m$  must be even. Hence  $y = z^{2^{r-1}-m/2}$  solves

$$y^2 b_0 \equiv z^{2^r} z^{-m} z^m \equiv 1 \pmod{p}$$

and  $x_0y$  is the solution.

**Example.** Solve  $x^2 \equiv 2 \pmod{41}$ .

**Solution.** We see that  $n = 3$  is a quadratic non-residue. Indeed,

$$\left(\frac{3}{41}\right) = (-1)^{\frac{21-1}{2} \frac{3-1}{2}} \left(\frac{41}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

We take

$$z \equiv 3^5 \equiv -3 \pmod{41}.$$

Now  $41 - 1 = 2^3 \cdot 5$ . Set

$$x_0 \equiv 2^{(5+1)/2} \equiv 2^3 = 8.$$

Then

$$b_0 \equiv 2^5 \equiv 32 \pmod{41}.$$

Now

$$S_8 = \{-3 \equiv 38, 9, -27 \equiv 14, -1 \equiv 40, 3, -9 \equiv 32, 27, 1\}.$$

We see that  $32 \equiv (-3)^6$  and so we want to take

$$y = (-3)^{2^{3-1}-6/2} = (-3)^{4-3} = -3,$$

and

$$x = 8 \cdot (-3) = -24 \equiv 17.$$

Note  $17^2 = 289 = 7 \cdot 41 + 2$ .