

Math 104B, Number Theory, Winter 2003.

Lecture 7. Quadratic Residues.

We want to understand the solutions to the equation $ax^2 + bx + c \equiv 0 \pmod{m}$. Suppose $(m, a) = 1$ and $(m, 2) = 1$. Then multiplying by $2a$ we get $4a^2 + 4abx + 4ac \equiv 0 \pmod{m}$. Completing the square, this becomes $(2a + b)^2 \equiv b^2 - 4ac \pmod{m}$. Setting $y = 2a + b$ and $d = b^2 - 4ac$, we seek the solution to $y^2 \equiv d \pmod{m}$.

If $(m, a) = 1$, then a is a **quadratic residue** modulo m if the equation $x^2 \equiv a \pmod{m}$ has a solution. Otherwise a is a *quadratic nonresidue*.

From now on solutions to congruences will mean solutions in a fixed complete residue system.

The first problem is to understand the solutions when m is prime.

Example. Squares modulo 11.

k	1	2	3	4	5	6	7	8	9	10
$k^2 \pmod{11}$	1	4	9	5	3	3	5	9	4	1

Notice the pattern. There are exactly $5 = (11 - 1)/2$ quadratic residues, 1, 3, 4, 5, 9 and 5 quadratic nonresidues, 2, 6, 7, 8, 10. The case for a general prime is similar:

Lemma 9.1.3. Let p be an odd prime.

(a). If $(a, p) = 1$, then the equation $x^2 \equiv a \pmod{p}$ either has no solutions or exactly 2 solutions. If x_0 is a solution then $-x_0 \equiv p - x_0 \pmod{p}$ is the other solution.

(b). There are $(p - 1)/2$ quadratic residues and $(p - 1)/2$ quadratic non-residues.

The proof of (a) follows the book.

For the proof of (b), set $S = \{1, 2, \dots, (p - 1)/2\}$. Then for every x , there is an element y of S such that either x or $-x$ is congruent to y modulo p . Furthermore, for all $x, y \in S$, we have $x \not\equiv -y \pmod{p}$. Hence we see that in the standard residue system the quadratic residues are precisely

$$a_1 = 1^2 \pmod{p}, \quad a_2 = 2^2 \pmod{p}, \quad \dots, \quad a_{(p-1)/2} = \left(\frac{p-1}{2}\right)^2 \pmod{p}.$$

For a second proof of (b) we follow Lemma 9.1.4. In particular we proved the fact that if g is a primitive root modulo p , then

$$g^k \text{ is a quadratic residue modulo } p \quad \Leftrightarrow \quad k \text{ is even.}$$

Definition 9.1.5. Let p be an odd prime. The **Legendre symbol** is

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

For example,

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1.$$

and

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1.$$

Proposition 9.1.7 Let p be an odd prime and let a, b be two integers such that $(p, ab) = 1$. Then

$$(a) \quad \left(\frac{a^2}{p}\right) = 1$$

$$(b) \quad \text{If } a \equiv b \pmod{p}, \text{ then } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

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

We followed the proof in the book. This lemma enables us to reduce the computation of $\left(\frac{-1}{p}\right)$ that of $\left(\frac{2}{p}\right)$, $\left(\frac{a}{p}\right)$, and $\left(\frac{q}{p}\right)$ for $q < p$ prime. For example,

$$\left(\frac{87}{31}\right) = \left(\frac{25}{31}\right) = \left(\frac{5}{31}\right)^2 = 1.$$

$$\left(\frac{28}{37}\right) = \left(\frac{4}{37}\right) \left(\frac{7}{37}\right) = \left(\frac{7}{37}\right).$$

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

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

We will discuss the proof in the book next time. As a corollary we get

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

Example.

$$\left(\frac{31}{67}\right) = \left(\frac{-1}{67}\right) \left(\frac{36}{67}\right) = (-1)^{33} \left(\frac{6}{67}\right)^2 = -1.$$

In chapters 17.1 and 17.2 we will prove the quadratic reciprocity theorem. If p and q are distinct odd primes, then

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

In addition we will show that

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

With these we can compute Legendre symbols fast. For example,

$$\begin{aligned} \left(\frac{40}{23}\right) &= \left(\frac{4}{23}\right) \left(\frac{2}{23}\right) \left(\frac{5}{23}\right) \\ &= (-1)^{(23-1)(23+1)/8} \left(\frac{23}{5}\right) (-1)^{\frac{23-1}{2} \frac{5-1}{2}} \\ &= (-1)^{66} \left(\frac{3}{5}\right) (-1)^{22} = \left(\frac{3}{5}\right) = -1. \end{aligned}$$