

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

**Lecture 14. Quadratic Reciprocity.**

Last time we proved:

**Theorem 17.2.4.** Let  $p, q$  be odd primes and suppose  $p \equiv \pm q \pmod{4a}$  where  $a > 0$  is an integer. Then

$$\left(\frac{a}{p}\right) \equiv \left(\frac{a}{q}\right) \pmod{p}.$$

It is easy to deduce quadratic reciprocity from this. Indeed,

**Proposition.** (a). If  $p \equiv q \pmod{4}$  then  $\left(\frac{p}{q}\right) = \left(\frac{-q}{p}\right)$ .

(b). If  $p \equiv -q \pmod{4}$  then  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ .

**Proof.** (a). Now

$$p \equiv q \pmod{4} \Rightarrow p - q = 4a \Rightarrow p \equiv q \pmod{4a},$$

and so

$$\left(\frac{p}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{-q}{p}\right).$$

(a). Similarly,

$$p \equiv -q \pmod{4} \Rightarrow p + q = 4a \Rightarrow p \equiv -q \pmod{4a},$$

and so

$$\left(\frac{p}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{q}{p}\right).$$

From the proposition part (a) we see that

$$p \equiv q \pmod{4} \Rightarrow \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = \left(\frac{-1}{q}\right) = \begin{cases} 1 & p \equiv q \equiv 1 \pmod{4}, \\ -1 & p \equiv q \equiv 3 \pmod{4}, \end{cases}$$

while

$$p \not\equiv q \pmod{4} \Rightarrow \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = 1.$$

This proves quadratic reciprocity.

**Example.** Characterize the primes  $p$  which divide  $x^2 - 10$  for some  $x$ .

**Solution.** We follow the discussion in the book to find those primes  $p$  for which  $\left(\frac{10}{p}\right) = 1$ . We have

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{8}, \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$$

1

and

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{5} \\ -1 & p \equiv \pm 3 \pmod{5}. \end{cases}$$

Hence

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{5}{p}\right) = \begin{cases} 1 & \begin{cases} p \equiv \pm 1 \pmod{8}, p \equiv \pm 1 \pmod{5} \\ p \equiv \pm 3 \pmod{8}, p \equiv \pm 3 \pmod{5} \end{cases} \\ -1 & \begin{cases} p \equiv \pm 1 \pmod{8}, p \equiv \pm 3 \pmod{5} \\ p \equiv \pm 3 \pmod{8}, p \equiv \pm 1 \pmod{5}. \end{cases} \end{cases}$$

Thus  $\left(\frac{10}{p}\right) = 1$  if and only if  $p \equiv \pm 1$  or  $\pm 3, \pmod{40}$ .

**The Jacobi Symbol.** We saw how to calculate the Legendre symbol by factorizing the numerator and then using the quadratic reciprocity law, for example

$$\left(\frac{21}{31}\right) = \left(\frac{3}{31}\right) \left(\frac{7}{31}\right) = \left(\frac{31}{3}\right) \left(\frac{31}{7}\right) = \left(\frac{1}{3}\right) \left(\frac{3}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -1.$$

For large numerator this may be a lengthy procedure because of the need to factorize. The algorithm will be shorter once we have extended the Legendre symbol to allow non-prime odd denominators. Then we will have instead

$$\left(\frac{21}{31}\right) = \left(\frac{31}{21}\right) = \left(\frac{10}{21}\right) = \left(\frac{2}{21}\right) \left(\frac{5}{21}\right) = (-1)^{20 \cdot 22/8} \left(\frac{5}{21}\right) = -\left(\frac{21}{5}\right) = -\left(\frac{1}{5}\right) = -1.$$

**Definition.** If  $m$  is odd with prime factorization  $m = p_1 \dots p_k$ , the the Jacobi symbol  $\left(\frac{a}{m}\right)$  is defined by

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right).$$

**Lemma.** If  $m, n$  are odd then

$$(a) \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right),$$

$$(b) \quad \left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right),$$

$$a \equiv b \pmod{m} \quad \Rightarrow \quad \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right).$$

$$(d) \quad \left(\frac{-1}{m}\right) = (-1)^{(m-1)/2},$$

$$(e) \quad \left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8},$$

$$(f) \quad \left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4},$$

**Note** that  $\left(\frac{a}{m}\right)$  does not in general determine whether  $a$  is a quadratic residue modulo  $p$ . Indeed, if  $m = p_1 \dots p_k$  is the prime factorization then

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right) = 1 \Leftrightarrow \#\left\{j : \left(\frac{a}{p_j}\right) = -1\right\} \text{ is even.}$$

But  $a$  is a quadratic residue modulo  $m$  if and only if  $a$  is a quadratic residue modulo  $p_j$  for every  $j$  which holds if and only if  $\left(\frac{a}{p_j}\right) = 1$  for every  $j$ .