Elementary Number Theory
Math 17500, Section 30
Autumn Quarter 2008

John Boller, e-mail: boller@math.uchicago.edu
website: http://www.math.uchicago.edu/∼boller/M175

Quadratic Residues and Quadratic Reciprocity

Definition 0.0.1 Fix $m > 1$ and suppose $(a, m) = 1$. If there exists $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{m}$, then a is called a *quadratic residue (mod m)*. If there does not exist such an $x \in \mathbb{Z}$, then a is called a *quadratic nonresidue (mod m)*.

Definition 0.0.2 If p is an odd prime, then the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as follows:

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

Theorem 0.0.3 Let p be an odd prime. Then:

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

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

iii. $a \equiv b \pmod{p}$ implies that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

iv. If $(a, p) = 1$, then $\left(\frac{a^2}{p}\right) = 1$ and $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

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

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

For the last main theorem, Quadratic Reciprocity, we first need a Eisenstein's Lemma.

Definition 0.0.4 If x is a real number, then we denote by $[x]$ the greatest integer less than or equal to x. This is sometime known as the *floor function*.

To prove Eisenstein's Lemma, we first prove the following four lemmas. For these lemmas, we use the ad hoc notation that if $2 \leq u \leq p-1$ is an even integer, then $r(u)$ is the least positive residue of $qu \pmod{p}$.

Lemma 0.0.5 The number $(-1)^{r(u)}r(u)$ is even.

Lemma 0.0.6 The two sets $\{2, 4, \ldots, p-1\}$ and $\{(-1)^{r(2)}r(2), (-1)^{r(4)}r(4), \ldots, (-1)^{r(p-1)}r(p-1)\}$ are identical.

Lemma 0.0.7 $q^{(p-1)/2} \equiv (-1)^{r(2)+r(4)+\cdots+r(p-1)} \pmod{p}$

Lemma 0.0.8 $\dfrac{qu}{p} = \left[\dfrac{qu}{p}\right] + \dfrac{r(u)}{p}$

Theorem 0.0.9 (Eisenstein's Lemma) If p and q are distinct odd primes, then:

$$\left(\frac{q}{p}\right) = (-1)^S, \text{ where } S = \sum_{\substack{u=2 \\ u\,:\,\text{even}}}^{p-1} \left[\frac{qu}{p}\right].$$

To prove Quadratic Reciprocity, we keep in mind the result of Eisenstein's Lemma and first prove the following lemmas. We make the following ad hoc definitions:

$$\begin{array}{rcl} P & = & \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid 0 < x < p,\ \ 0 < y < q\} \\ P_1 & = & \{(x,y) \in P_0 \mid 0 < y < qx/p,\ \ x \text{ is even}\} \\ P_2 & = & \{(x,y) \in P_0 \mid 0 < x < p/2,\ \ 0 < y < qx/p\} \\ P_3 & = & \{(x,y) \in P_0 \mid 0 < y < q/2,\ \ 0 < x < py/q\} \end{array}$$

(Hint: It may help to consider the statements geometrically.)

Lemma 0.0.10 $S = |P_1|$ where S is the sum in Eisenstein's Lemma.

Lemma 0.0.11 $P_1 \equiv P_2 \pmod{2}$

Lemma 0.0.12 $\left(\dfrac{q}{p}\right) = (-1)^{|P_2|}$

Lemma 0.0.13 $\left(\dfrac{p}{q}\right) = (-1)^{|P_3|}$ (Hint: Simliar!)

Lemma 0.0.14 $|P_2 \cup P_3| = \frac{p-1}{2} \cdot \frac{q-1}{2}$ and $P_2 \cap P_3 = \emptyset$

Theorem 0.0.15 (Quadratic Reciprocity) If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$