

Math 104B, Number Theory, Winter 2003.

Lecture 13. Quadratic Reciprocity.

Theorem 17.1.2. If p is an odd prime then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv 1, 7, \pmod{8} \\ -1 & p \equiv 3, 5 \pmod{8}. \end{cases}$$

Proof. Recall last time we showed that $\left(\frac{a}{p}\right) = (-1)^n$ where the number n is obtained as follows: Write the elements of

$$S = \left\{ a, 2a, \dots, \frac{(p-1)a}{2} \right\}$$

in the absolute least residue system to obtain the set S' . Then n is the number of negative elements in S' . Let's apply this in the case $a = 2$. Then

$$S = \{2, 4, 6, \dots, (p-1)\}.$$

We want to figure out which of these elements are negative in the absolute least residue system and this is easy, since elements in $(0, \frac{p}{2})$ are positive and elements in $(\frac{p}{2}, p)$ are negative. We hence want to count the number of even elements in $(\frac{p}{2}, p)$, that is

$$\#\{\ell \in \mathbb{Z} : \frac{p}{2} < 2\ell < p\} = \#\{\ell \in \mathbb{Z} : \frac{p}{4} < \ell < \frac{p}{2}\} = \#\text{ integers in } \left(\frac{p}{4}, \frac{p}{2}\right).$$

Lemma. If a and b are not integers then the number of integers in the interval (a, b) is $\lfloor b \rfloor - \lfloor a \rfloor$.

We do not prove this, just check that it holds for the number of integers in the interval $(1\frac{1}{2}, 1\frac{3}{4})$, for the number of integers in the interval $(\frac{1}{2}, 1\frac{1}{2})$ and for the number of integers in the interval $(\frac{1}{2}, 5\frac{1}{2})$.

Now n is the number of integers in the interval $(\frac{p}{4}, \frac{p}{2})$ which is

$$\left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor,$$

and so

$$\left(\frac{2}{p}\right) = (-1)^{\left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor}.$$

However, we claim that if we replace $p \equiv r \pmod{8}$ then

$$(-1)^{\left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor} = (-1)^{\left\lfloor \frac{r}{2} \right\rfloor - \left\lfloor \frac{r}{4} \right\rfloor}.$$

Indeed, if $p = 8q + r$ then

$$\left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor = \left\lfloor \frac{r}{2} + 4q \right\rfloor - \left\lfloor \frac{r}{4} + 2q \right\rfloor = \left\lfloor \frac{r}{2} \right\rfloor - \left\lfloor \frac{r}{4} \right\rfloor + (4q - 2q) = \left\lfloor \frac{r}{2} \right\rfloor - \left\lfloor \frac{r}{4} \right\rfloor + 2q.$$

Computing for the numbers $r = 1, 3, 5, 7$ we find that

$$\left\lfloor \frac{r}{2} \right\rfloor - \left\lfloor \frac{r}{4} \right\rfloor = \begin{cases} \left\lfloor \frac{1}{2} \right\rfloor - \left\lfloor \frac{1}{4} \right\rfloor = 0 - 0 = 0 & r = 1 \\ \left\lfloor \frac{3}{2} \right\rfloor - \left\lfloor \frac{3}{4} \right\rfloor = 1 - 0 = 1 & r = 3 \\ \left\lfloor \frac{5}{2} \right\rfloor - \left\lfloor \frac{5}{4} \right\rfloor = 2 - 1 = 1 & r = 5 \\ \left\lfloor \frac{7}{2} \right\rfloor - \left\lfloor \frac{7}{4} \right\rfloor = 3 - 1 = 2 & r = 7. \end{cases}$$

Hence we get

$$\left(\frac{2}{p} \right) = \begin{cases} 1 & p \equiv 1, 7, \pmod{8} \\ -1 & p \equiv 3, 5 \pmod{8}. \end{cases}$$

The proof given above can be extended to prove the following result:

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

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

Proof. If $p|a$ then $p|q$ so $p = q$ and the result clearly holds. We will find an expression for $\left(\frac{a}{p} \right)$. As usual let

$$S = \left\{ a, 2a, \dots, \frac{(p-1)a}{2} \right\} = \left\{ al : \ell \in \mathbb{Z}, \quad 0 < al < \frac{ap}{2} \right\}.$$

We want to count the elements of S which are negative in the absolute least residue system modulo p . But we remarked last time that m is negative in the absolute least residue system modulo p if and only if there exists an odd j with

$$\frac{jp}{2} < m < \frac{(j+1)p}{2}.$$

Hence

$$n = \sum_{j=1, \text{ odd}}^{a-1} A_j,$$

where

$$A_j = A_j(p) = \left\{ al : \ell \in \mathbb{Z}, \quad \frac{jp}{2} < al < \frac{(j+1)p}{2} \right\} = \left\{ \ell \in \mathbb{Z} : \frac{jp}{2a} < \ell < \frac{(j+1)p}{2a} \right\}.$$

Now the endpoints of the interval $(\frac{jp}{2a}, \frac{(j+1)p}{2a})$ are never integers. This is clear if $j < a - 1$, since $(p, a) = 1$ and $a \nmid j$ and $a \nmid j + 1$. If $j = a - 1$ then again $a \nmid j$, so the lower endpoint is not an integer, and the upper endpoint is $p/2$ which is not an integer. Hence

$$A_j = \left\lfloor \frac{(j+1)p}{2a} \right\rfloor - \left\lfloor \frac{jp}{2a} \right\rfloor.$$

All we need to show now is that

$$p \equiv \pm q \pmod{4a} \Rightarrow A_j(p) \equiv A_j(q) \pmod{2},$$

for this will imply $n(p) = n(q) \pmod{2}$ so $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. (Here $n(p)$ denotes the value of n for the prime p and $n(q)$ denotes the value of n for the prime q .)

First suppose that $q \equiv p \pmod{4a}$. Then writing $q = p + 4ak$ we have

$$\begin{aligned} A_j(q) &= \left\lfloor \frac{(j+1)(p+4ak)}{2a} \right\rfloor - \left\lfloor \frac{j(p+4ak)}{2a} \right\rfloor = \left\lfloor \frac{(j+1)p}{2a} + 2(j+1)k \right\rfloor - \left\lfloor \frac{jp}{2a} + 2jk \right\rfloor \\ &= \left\lfloor \frac{(j+1)p}{2a} \right\rfloor - \left\lfloor \frac{jp}{2a} \right\rfloor + 2k = A_j(p) + 2k. \end{aligned}$$

Now suppose that $q \equiv -p \pmod{4a}$. Then $q = 4ak - p$ and using the fact that if s is not an integer then $\lfloor -s \rfloor = -1 - \lfloor s \rfloor$ we get that

$$\begin{aligned} A_j(q) &= \left\lfloor \frac{(j+1)(4ak-p)}{2a} \right\rfloor - \left\lfloor \frac{j(4ak-p)}{2a} \right\rfloor = \left\lfloor 2(j+1)k - \frac{(j+1)p}{2a} \right\rfloor - \left\lfloor 2jk - \frac{jp}{2a} \right\rfloor \\ &= 2(j+1)k - 1 - \left\lfloor \frac{(j+1)p}{2a} \right\rfloor - \left(2jk - 1 - \left\lfloor \frac{jp}{2a} \right\rfloor \right) = 2k - A_j(p). \end{aligned}$$

Since this is congruent to $A_j(p)$ modulo 2, this completes the proof.