March 27 – Lemma's for quadratic reciprocity

We will prove the two lemmas needed in order to prove quadratic reciprocity.

We want to prove

Theorem 1 (Quadratic reciprocity)**.** Let p and q be primes with $p \neq q$, then

- if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.
- if $p \equiv q \equiv 3 \pmod 4$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Let's try some examples:

Question 1 $\left(\frac{11}{47}\right) = -1 * \left(\frac{47}{11}\right)$. *We can reduce* $47 \equiv 3 \pmod{11}$, *which*

Multiple Choice:

(a) *is* ✓

(b) *is not*

a quadratic residue modulo 11. Thus, $\left(\frac{11}{47}\right) = -1$ *and* $\left(\frac{47}{11}\right) = 1$.

Question 2 $\left(\frac{3}{107}\right) = -1 * \left(\frac{107}{3}\right)$. *We can reduce* $107 \equiv 2 \pmod 3$, *which*

Multiple Choice:

(a) *is*

(b) *is not* ✓

a quadratic residue modulo 3. Thus, $\left(\frac{107}{3}\right) = -1$ *and* $\left(\frac{3}{107}\right) = 1$.

Learning outcomes:
Author(s):

We are going to restate quadratic reciprocity as

Theorem 2 (Restatement of quadratic reciprocity)**.** Let p and a be odd primes with $p \neq q$. Then

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

Theorem 3. The restatement of quadratic reciprocity implies quadratic reciprocity.

Proof Let p and q be odd primes with $p \neq q$. We assume that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ is true. Then we have two cases:

- $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$ [To show $\left(\frac{p}{q}\right) = 1 * \left(\frac{q}{p}\right)$.]

  Without loss of generality, we assume $p \equiv 1 \pmod 4$. Then there exists a $k \in \mathbb{Z}$ such that $p = 4k + 1$. This implies that $\dfrac{p-1}{2} = 2k$. Thus,

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

  Thus, we have that $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ must either both be $+1$ or both be -1.

- $p \equiv q \equiv 3 \pmod 4$[To show $\left(\frac{p}{q}\right) = -1 * \left(\frac{q}{p}\right)$.] There exists $k, m \in \mathbb{Z}$ such that $p = 4k + 3$ and $q = 4m + 3$. This implies that $\dfrac{p-1}{2} = 2k + 1$ and $\dfrac{q-1}{2} = 2k + 1$. Thus,

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

  Thus, we have that exactly one of $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ is $+1$ and the other is -1.

■

In order to prove this, we first need to prove two rather technical lemmas. Then we will use a geometric proof to finish.

Theorem 4 (Gauss's lemma)**.** Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$. Let n be the number of least positive residues of the integers $a, 2a, \ldots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$. Then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Question 3 *Use Gauss's lemma to find* $\left(\frac{6}{11}\right)$. *We need to find* n, *the number of least nonnegate positive residues of the integers* $6, 2*6, 3*6, 4*6, 5*6$ *greater that* 5.5 *We have*

$$\begin{aligned} 6 &\equiv 6 \pmod{11} \\ 2*6 &\equiv 1 \pmod{11} \\ 3*6 &\equiv 7 \pmod{11} \\ 4*6 &\equiv 2 \pmod{11} \\ 5*6 &\equiv 8 \pmod{11} \end{aligned}$$

Thus, $n = 3$ *and* $(-1)^n = -1$.

We now prove Gauss's lemma.

Proof Let $r_1, r_2, \ldots r_n$ be the least nonnegative residues of the integers $a, 2a, \ldots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$ and $s_1, s_2, \ldots, s_m$ be the least nonnegative residues that are less that $\frac{p}{2}$. Note that no r_i or s_j is 0, since p does not divide any of $a, 2a, \ldots \frac{p-1}{2}$. Consider the $\frac{p-1}{2}$ integers given by

$$p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m.$$

We want to show that these integers are the integers from 1 to $\frac{p-1}{2}$ inclusive in some order. Since each integer is less than or equal to $\frac{p-1}{2}$, it suffices to show that no two of these integers are congruent modulo p.

If $p - r_i \equiv p - r_j \pmod{p}$ for some $i \neq j$, then $r_i \equiv r_j \pmod{p}$, but this implies that there exists some $k_i, k_j \in \mathbb{Z}$ such that $r_i = k_i a \equiv k_j a = r_j \pmod{p}$ with $k_i \neq k_j$ and $1 \leq k_i, k_j \leq \frac{p-1}{2}$. Since

Multiple Choice:

(a) $p \nmid a$ ✓

(b) $p \mid a$

we know that the multiplicative inverse of a modulo p

Multiple Choice:

(a) exists ✓

(b) does not exist

and thus $k_i \equiv k_j \pmod{p}$, a contradiction. Thus, no two of the first n integers are congruent modulo p.

Similarly, no two of the second m integers are congruent. Now, if $p - r_i \equiv s_j \pmod{p}$, for some i and j, then $-r_i \equiv s_j \pmod{p}$. Thus, there exists $k_i, k_j \in \mathbb{Z}$ such that $-r_i = -k_i a \equiv k_j a = s_j \pmod{p}$ with $k_i \neq k_j$ and $1 \leq k_i, k_j \leq \frac{p-1}{2}$. Since $p \nmid a$, we know that the multiplicative inverse of a modulo p exists, and thus $-k_i \equiv k_j \pmod{p}$, a contradiction. Thus, the $\frac{p-1}{2}$ integers $p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m$ are the integers $1, 2, \ldots, \frac{p-1}{2}$ in some order.

Then,

$$(p - r_1)(p - r_2) \cdots (p - r_n) s_1 s_2 \cdots s_m \equiv \frac{p-1}{2}! \pmod{p}$$

implies that

$$(-1)^n r_1 r_2 \cdots r_n s - 1 s_2 \cdots s_m \equiv \frac{p-1}{2}! \pmod{p}.$$

By the definition of r_i and s_j, we have

$$(-1)^n a(2a)(3a) \cdots (\frac{p-1}{2}a) \equiv \frac{p-1}{2}! \pmod{p}.$$

By reordering, we have

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

Thus, $(-1)^n a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, and $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$. By Euler's criterion, we get that $\left(\frac{a}{p}\right) \equiv (-1)^n \pmod{p}$. Since both sides of the congruence must be ± 1, we have $\left(\frac{a}{p}\right) = (-1)^n$. ■

We are going to prove a result about $\left(\frac{2}{p}\right)$ before our next technical lemma.

Theorem 5. Let p be an odd prime. Then

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

Proof By Gauss's Lemma, we have that $\left(\frac{2}{p}\right) = (-1)^n$, where n is the number of least positive residues of the integers $2, 2*2, 2*3, \ldots, \frac{p-1}{2}$ that are greater than $\frac{p}{2}$. Let $k \in \mathbb{Z}$ with $1 \leq k \leq \frac{p-1}{2}$. Then $2k < \frac{p}{2}$ if and only if $k < \frac{p}{4}$; so $\left\lfloor \frac{p}{4} \right\rfloor$ of the integers $2, 2*2, 2*3, \ldots, \frac{p-1}{2}$ that are less than $\frac{p}{2}$, where $\lfloor \cdot \rfloor$ is the greatest integer (or floor) function. So, $\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$ of these integers are greater than $\frac{p}{2}$, from which

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

by Gauss's Lemma. For the first equality, it suffices to show that

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} \pmod 2.$$

If $p \equiv 1 \pmod 8$, the $p = 8k+1$ for some $k \in \mathbb{Z}$. That gives us

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{(8k+1)-1}{2} - - \left\lfloor \frac{8k+1}{4} \right\rfloor = 4k - 2k = 2k \equiv 0 \pmod 2$$

and

$$\frac{p^2-1}{8} = \frac{8k+1)^2-1}{8} = 8k^2 + 2k \equiv 0 \pmod 2.$$

Thus, holds when $p \equiv 1 \pmod 8$. The rest of the cases are part of homework 9. ■

Theorem 6 (Rephrased textbook Theorem 3.3)**.** Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$ and a odd. If

$$N = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor,$$

then

$$\left(\frac{a}{p}\right) = (-1)^N.$$

Where $\lfloor \cdot \rfloor$ is the greatest integer (or floor) function. This gives us another way of computing Legendre symbols. Let's look at an example before diving into the technical proof.

Question 4 *Use this lemma to find* $\left(\frac{7}{11}\right)$. *We have*

$$\begin{aligned} N &= \sum_{j=1}^{5} \left\lfloor \frac{j7}{11} \right\rfloor = \left\lfloor \frac{7}{11} \right\rfloor + \left\lfloor \frac{14}{11} \right\rfloor + \left\lfloor \frac{21}{11} \right\rfloor + \left\lfloor \frac{28}{11} \right\rfloor + \left\lfloor \frac{35}{11} \right\rfloor \\ &= 0 + 1 + 1 + 2 + 3 \\ &= 7 \end{aligned}$$

So $\left(\frac{7}{11}\right) = (-1)^7 = -1$.

Proof Let $r_1, r_2, \ldots, r_n$ are the least nonnegative representatives of $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ modulo p which are greater than $\frac{p}{2}$ and $s_1, s_2, \ldots, s_m$ be the least nonnegative representatives of $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ modulo p which are less than $\frac{p}{2}$. Then for each $j = 1, 2, \ldots, \frac{p-1}{2}$ we have that

$$ja = p\left\lfloor \frac{ja}{p} \right\rfloor + (\text{remainder depending on } j)$$

where each of $r_1, r_2, \ldots, r_n, s_1, s_2, \ldots, s_m$ appears exactly once as a remainder. By adding the $\frac{p-1}{2}$ equations above, we get

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j \tag{1}$$

The integers $p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m$ are precisely the integers from 1 to $\frac{p-1}{2}$ in some order, so we have

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{n}(p - r_j) + \sum_{j=1}^{m} s_j = pn - \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j \tag{2}$$

We subtract (**??**) from (**??**) to get

$$\begin{aligned}\sum_{j=1}^{\frac{p-1}{2}} ja - \sum_{j=1}^{\frac{p-1}{2}} j &= \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j - \left(pn - \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j \right) \\ &= \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor - pn + 2\sum_{j=1}^{n} r_j.\end{aligned}$$

Now, we can factor the left hand side to get

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor - pn + 2\sum_{j=1}^{n} r_j.$$

Reducing both sides of the equation modulo 2 gives

$$0 \equiv \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor - n \pmod 2$$

since $p \equiv 1 \pmod 2$. Equivalently $n \equiv \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor \pmod 2$.

Thus, $n \equiv N \pmod 2$, thus $\left(\frac{a}{p}\right) = (-1)^n = (-1)^N$. ■