Quadratic Reciprocity continued

October 23, 2012

1 Recall next Hour-and-a-half Exam:

November 5.

2 Reading:

Read Chapter 5 of [**I-R**].

3 Recall the statement of Quadratic Reciprocity for odd primes $p \neq q$.

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

4 Recall Gauss's Lemma

(Define: *least residue.*) If a is prime to p form the $\frac{p-1}{2}$ distinct congruence classes mod p:

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a.$$

Now pass to the "least residues" of these $\frac{p-1}{2}$ classes. So we have a collection of $\frac{p-1}{2}$ integers, some positive, some negative. Let μ be the number of positive ones, and ν the number of negative ones, so

$$\mu + \nu = \frac{p-1}{2}.$$

Proposition 1 (Gauss's Lemma)

$$\left(\frac{a}{p}\right) = (-1)^{\nu},$$

I.e., if there's an odd number of negative least residues in the set

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

then

$$\left(\frac{a}{p}\right) = -1;$$

and if not, then

$$\left(\frac{a}{p}\right) = +1.$$

4.1 Geometric proof of Quadratic Reciprocity

Here p, q re odd, distinct primes.

Theorem 1 *Let*

$$S(q,p) = S_{\text{Gauss}}(q,p) = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor.$$

Then $S(q,p) \equiv \nu$ *modulo* 2.

The proof of this is by first writing, for each k—whichever of the two following formulas work:

$$kq = p\lfloor \frac{kq}{p} \rfloor + \ell_k$$

or

$$kq = p\lfloor \frac{kq}{p} \rfloor + (p - \ell_k)$$

with $\ell_k \leq (p-1)/2$.

and the summing over $k \leq (p-1)/2$ and reducing mod 2 to get:

$$\frac{p^2-1}{8} \equiv S(q,p) + \nu \cdot p + \frac{p^2-1}{8}$$

which proves the theorem.

Note that a geometric argument gives us:

Theorem 2

$$S(q,p) + S(p,q) = (\frac{p-1}{2})(\frac{q-1}{2}).$$

Putting the two previous theorems together gives (at least the odd prime part of) the Quadratic reciprocity theorem.

5 Eisenstein's version of Gauss's Lemma

Definition 1 *For p an odd prime, the "Eisenstein residues" (I just made up the name) consists in the even numbers in the range $[-(p-1), +(p-1)]$.*

So, writing

$$x = p \cdot \langle \frac{x}{p} \rangle \pm u(x)$$

with $u(x)$ the Eisenstein residue of x the sign in this equality depends on the parity of $u(x)$, which is equal to the parity of $\langle \frac{x}{p} \rangle$. We have a slightly different version of Gauss' Lemma:

Proposition 2 (Eisenstein's Gauss's Lemma)

$$\left(\frac{a}{p}\right) = (-1)^m,$$

where m is equivalently:

1. *the number of negative numbers in the Eisenstein residues (mod p) of the collection*

$$a, 2a, 4a, 6a, \ldots, (p-1) \cdot a,$$

   or:

2. $m = \sum_{k=1}^{\frac{p-1}{2}} u(2k \cdot a)$, *or:*

3. $m = S_{\text{Eis}}(q,p) := \sum_{k=1}^{\frac{p-1}{2}} \langle \frac{2k \cdot a}{p} \rangle$.

I.e., if there's an odd number of negative Eisenstein residues in the set

$$a, 2a, 4a, 6a, \ldots, (p-1) \cdot a.$$

then

$$\left(\frac{a}{p}\right) = -1;$$

and if not, then

$$\left(\frac{a}{p}\right) = +1.$$

The proof is almost identical to the proof of Gauss's Lemma. Also, note that we have the equation:

$$2kq = p \cdot [\frac{2kq}{p}] + s(2kq)$$

so (since p is odd) $[\frac{2kq}{p}] \equiv s(2kq)$ modulo 2.

6 Summary

6.1 Different representative systems for $\mathbf{Z}/pZ^*$

for p an odd prime. Here are three of them:

1. **standard:** $\{1, 2, 3, \ldots, p-1\}$
2. **least residue:** $\{-\frac{p-1}{2}, 1-\frac{p-1}{2}, \ldots, -2, -1, +1, +2, \ldots \frac{p-1}{2}-1, \frac{p-1}{2}\}$
3. **Eisenstein:** $\{1-p, 3-p, \ldots, -4, -2, +2, +4, \ldots, p-3, p-1\}$

Any number x not divisible by p can (of course) be put in any of these three forms:

1. **standard:** $x = mp + s(x)$ with $1 \leq s \leq p-1$; note that m is the floor function $[\frac{x}{p}]$; or
2. **least residue:** $x = m'p + \ell(x)$ with
$$\frac{p-1}{2} \leq \ell \leq +\frac{p-1}{2}$$
3. **Eisenstein:** $x = m''p + Eis(x)$ with $Eis(x)$ even and $1-p \leq Eis(x) \leq p-1$.

6.2 Different ways of describing $\left(\frac{p}{q}\right)$

Let p, q be distinct odd primes. We have been collecting loads of different ways of describing the Legendre symbol. To add to this assortment, here is a list of some numbers m such that

$$\left(\frac{p}{q}\right) = (-1)^m,$$

i.e.,such that the parity of m tells us whether p is a square mod q. We can take m (mod 2 is all that is germaine) to be:

1. the number of *negative* least residues of
$$q, 2q, 3q, \ldots, \frac{p-1}{2}q.$$

2. The number of *negative* Eisenstein residues of

$$2q, 4q, 6q, \ldots, (p-1) \cdot q.$$

3. The number of *odd* standard residues of

$$2q, 4q, 6q, \ldots, (p-1) \cdot q.$$

4. $S_{\text{Gauss}}(q, p)$

5. $S_{\text{Eis}}(q, p)$.

7 Jacobi symbol version of Quadratic reciprocity

8 Yet another proof of QR

Let us imagine that you can concoct a function $F : \mathbf{Q}/\mathbf{Z} \to \mathbf{C}$ that has these properties:

- F is odd $F(-z) = -F(z)$, and vanishes only on $\mathbf{Z}$,
- For any positive integer n,

$$\frac{F(nz)}{F(z)} = \prod_{k=1}^{\frac{n-1}{2}} F(z + \frac{k}{n}) F(z - \frac{k}{n}).$$

Claim: If so, then you get yourself a proof of Quadratic Reciprocity.

Lemma 1 *If $(a, p) = 1$, then $\prod_{k=1}^{\frac{p-1}{2}} F(\frac{ak}{p}) = \binom{a}{p} \cdot \prod_{k=1}^{\frac{p-1}{2}} F(\frac{k}{p})$. Or, better:*

$$\prod_{k=1}^{\frac{p-1}{2}} \frac{F(\frac{ak}{p})}{F(\frac{k}{p})} == \binom{a}{p}$$

Proof: Gauss's Lemma argument.

So, by (2) above,

$$\binom{a}{p} = \prod_{k=1}^{\frac{p-1}{2}} \prod_{\ell=1}^{\frac{q-1}{2}} F(\frac{\ell}{q} + \frac{k}{p}) F(\frac{\ell}{q} - \frac{k}{p})$$