Yet more Quadratic Reciprocity; Introduction to Gauss sums

October 26, 2012

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

November 6.

2 Homework set due November 1

- If p is a prime congruent to 1 modulo 7, then 3 is a seventh power mod p if $3^{(p-1)/7}$ has what property?
- Page 64: Exercises 25-28.
- Page 77: Exercise 11.

3 Don't hand in, but these are good exercises to do, and tothink about

Page 77: Exercise 10, 12-14.

4 Yet another ever-so-slightly different version of a proof of QR

4.1 Recall yet again: different representative systems for $(\mathbf{Z}/p\mathbf{Z})^*$

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 $1-p \leq Eis(x) \leq p-1$.

4.2 Different ways of describing $\binom{p}{q}$

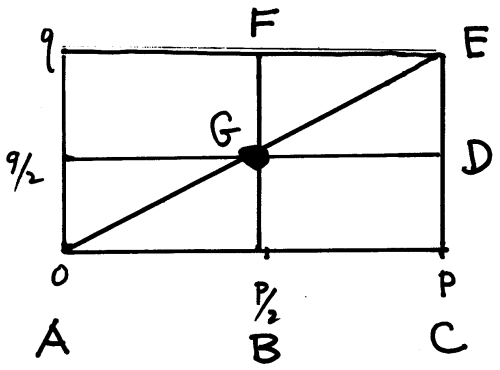
Let p, q be distinct odd primes. We have been collecting loads of different ways of describing the Legendre symbol. To add to this assortment, here is a list of some numbers w such that
$$\binom{p}{q} = (-1)^w,$$
i.e., such that the parity of w tells us whether p is a square mod q. We can take w (mod 2) 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. The *sum* of the *odd* standard residues of
$$2q, 4q, 6q, \ldots, (p-1)\cdot q.$$
That is, we can take w to be
$$\sum_{k=1}^{\frac{p-1}{2}} s(2kq).$$
Or, recalling 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,

5. we can take w to be

$$\sum_{k=1}^{\frac{p-1}{2}}[\frac{2kq}{p}].$$

6. In the diagram in the Euclidean plane below, we shall describe any polygon in it by listing its vertices going counterclockwise.



If we put an absolute value around the name of the polygon, we will mean the number of lattice points in the interior. The subscript *even*s or *odd* will mean the number of lattice points in the figure with *even* or *odd* x-coordinates, respectively. We can take w to be

$$\sum_{k=1}^{\frac{p-1}{2}}[\frac{2kq}{p}] = |ACE|_{\text{even}} = |ABG|_{\text{even}} + |BCEG|_{\text{even}}$$

7. Since

$$|BCEG|_{\text{even}} \equiv |GEF|_{\text{even}}$$

modulo 2, we can take w to be

$$|ABG|_{\text{even}} + |GEF|_{\text{even}}$$

.

8. **Lemma 1** $|GEF|_{\text{even}} = |ABG|_{\text{odd}}$

Proof: The transformation of the plane $(x, y) \mapsto (p-x, q-y)$ sends GEF isomorphically onto ABG (and the other way around too), inducing a one:one correspondence on lattice points, but it sends lattice points with x-coordinate even onto lattice points with x-coordinate odd, and vice versa.

So we can take w to be

$$|ABG|_{\text{even}} + |ABG|_{\text{odd}} = |ABG|.$$

9. I.e., we have the formula:

$$\binom{p}{q} = (-1)^{|ABG|}.$$

10. Interchanging x, and y axes, and switching p and q, we have

$$\binom{q}{p} = (-1)^{|AGH|}.$$

11. Putting these together we have

$$\binom{p}{q}\binom{q}{p} = (-1)^{|ABG|+|AGH|} = (-1)^{|ABGH|} = \frac{p-1}{2}\frac{q-1}{2}.$$

5 And yet another proof of QR

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

- $F(z+1) = F(z)$ for all $z \in \mathbf{Q}$,
- F is odd; i.e., $F(-z) = -F(z)$,
- $F(z)$ vanishes only on $\frac{1}{2}\mathbf{Z}$,
- For any positive odd 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. Here's the proof. Let p be an odd prime.

Lemma 2 *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. Write each $ak = m \cdot p + \ell(ak)$ so

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

$$= \prod_{k=1}^{\frac{p-1}{2}} F(\pm\frac{|\ell(ak)|}{p})$$

where the signs $\pm|\ell(ak)|$ keep track of which ones are positive and negative. Now the number of those negative signs we called μ, so we have

$$\prod_{k=1}^{\frac{p-1}{2}} F(\pm\frac{|\ell(ak)|}{p}) = (-1)^{\mu} \prod_{k=1}^{\frac{p-1}{2}} F(\frac{|\ell(ak)|}{p})$$

since F is odd, and also by the same argument as we saw in Gauss' lemma, we have

$$\prod_{k=1}^{\frac{p-1}{2}} F(\frac{|\ell(ak)|}{p}) = \prod_{k=1}^{\frac{p-1}{2}} F(\frac{k}{p}).$$

Corollary 1

$$\binom{q}{p} = \prod_{k=1}^{\frac{p-1}{2}} \frac{F(\frac{qk}{p})}{F(\frac{k}{p})} = \prod_{j=1}^{\frac{q-1}{2}} F(\frac{k}{p} + \frac{j}{q}) F(\frac{k}{p} - \frac{j}{q}),$$

and therefore, also:

$$\binom{p}{q} = \prod_{j=1}^{\frac{q-1}{2}} \frac{F(\frac{pj}{q})}{F(\frac{j}{q})} = \prod_{k=1}^{\frac{p-1}{2}} F(\frac{j}{q} + \frac{k}{p}) F(\frac{j}{q} - \frac{k}{p}).$$

For, by the second bullet at the beginning of this section, we do get the equalities above:

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

and

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

One can pass from the RHS of **(*)** to the RHS of **(**)** by switching the $\frac{p-1}{2}\frac{q-1}{2}$ signs in the arguments of the

$$F(\frac{\ell}{q} - \frac{k}{p})$$

terms in the the RHS of **(*)**. But since $F(-z) = F(z)$, this, in effect, multiplies the RHS of **(**)** by

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

Theorem 2 *Quadratic reciprocity for two odd primes p, q*

Given all the above discussion, to get a proof of QR we only need the existence of some F satisfying the bullets above.

Lemma 3 *The function*

$$F(z) = e^{2\pi iz} - e^{-2\pi iz}$$

is such a function (i.e., it satisfies the four bullets listed at the beginning of this section).

6 Introduction to Quadratic Gauss Sums

6.1 The ring $\mathbf{Z}[\zeta_p]$

Use Eisenstein's criterion to prove the theorem of Gauss:

Theorem 3 *Let p be prime. Then the polynomial $f(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ is irreducible over $\mathbf{Q}$.*

7 Quadratic Gauss Sums

Let p be an odd prime, and choose a primitive root of unity ζ_p. Say: $\zeta_p = e^{2\pi i/p}$.

For a not divisible by p, put

$$g_a := \sum_{k=0}^{p-1} \binom{k}{p} \zeta_p^{ka}.$$

Recall "where" g_a lives (i.e., in $\mathbf{Z}[\zeta_p]$).

Put $g := g_1$. The two basic facts about these quadratic Gauss sums:

1. **Proposition 1** $g_a = \left(\frac{a}{p}\right) g$,

   and

2. **Proposition 2** $g_a^2 = (-1)^{(p-1)/2} p$.

In other words, put $p^* := (-1)^{(p-1)/2} p$ so we can say that g_a is a *square root* of p^*. In particular, a square root of p^* lives in $\mathbf{Z}[\zeta_p]$.

Proof of Proposition 2. Evaluate $g_a g_{-a} = \left(\frac{-1}{p}\right) g^2$ if $(a,p) = 1$; and $= 0$ if p divides a. Now we deal with $\sum_a g_a g_{-a}$ in two ways:

(a) $\sum_a g_a g_{-a} = (p-1)\left(\frac{-1}{p}\right) g^2$.

(b) Also,

$$\sum_a g_a g_{-a} = \sum_a \sum_x \sum_y \binom{x}{p} \binom{y}{p} \zeta^{a(x-y)}.$$

$$= \sum_x \sum_y \binom{x}{p} \binom{y}{p} \sum_a \zeta^{a(x-y)}.$$

Here the summations are over (i.e., the variables a, x, y run through) a full set of residue classes mod p. Now, if $x - y \not\equiv 0 \bmod p$ then $\sum_a \zeta^{a(x-y)} = 0$, while if $x - y \equiv 0 \bmod p$ then $\sum_a \zeta^{a(x-y)} = p$ so the above triple sum becomes

$$\sum_a g_a g_{-a} = \sum_{x=y} \binom{x}{p} \binom{y}{p} \cdot p = (p-1)p.$$

So: $g^2 = \left(\frac{-1}{p}\right) p$; that is:

$g = \pm\sqrt{p}$ if $p \equiv 1 \bmod 4$, and
$g = \pm i\sqrt{p}$ if $p \equiv -1 \bmod 4$.

With what *sign*?