Quadratic Reciprocity

Robert Hines

October 16, 2015

Contents

1 Proofs Using the Quadratic Gauss Sum

Definition. *A Gauss sum $g(a,\chi)$ associated to a character χ of modulus n (a homomorphism $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}$ extended to $\mathbb{Z}$, $\chi(k) = 0$ if $(k,n) > 1$) is*

$$g(a,\chi) = \sum_{k=1}^{n-1} \chi(k) e^{2\pi iak/n}$$

Observe that for $(a,n) = 1$

$$g(a,\chi) = \sum_{k=1}^{n-1} \chi(k) e^{2\pi iak/n} = \sum_{l=1}^{n-1} \chi(l)\bar{\chi}(a) e^{2\pi il/n} = \bar{\chi}(a) g(1,\chi)$$

with $l = ka$. Also observe that

$$\overline{g(a,\chi)} = \sum_k \bar{\chi}(k) e^{-2\pi iak/n} = \bar{\chi}(-1) g(a,\bar{\chi}).$$

Proposition. *For a non-principal character χ of prime modulus p and $(a,p) = 1$ we have*

$$|g(a,\chi)|^2 = p.$$

Proof. We evaluate $\sum_a g(a,\chi)\overline{g(a,\chi)}$ two different ways:

$$\sum_a g(a,\chi)\overline{g(a,\chi)} = \sum_{a,k,l} \chi(kl^{-1})e^{2\pi i a(k-l)/p} = \sum_{k,l}\chi(kl^{-1})\sum_a e^{2\pi i a(k-l)/p}$$
$$= \sum_{k,l}\chi(kl^{-1})p\delta_{kl} = p(p-1),$$

$$\sum_a g(a,\chi)\overline{g(a,\chi)} = \sum_a \bar{\chi}(a)g(1,\chi)\chi(a)\overline{g(1,\chi)}$$
$$= (p-1)|g(1,\chi)|^2.$$

□

For χ real, the above says $g(1,\chi)^2 = \chi(-1)p$, which we will use below.

Theorem (Quadratic Reciprocity)**.** *For odd primes p, q we have*

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

where $\left(\frac{\cdot}{l}\right)$ is the Legendre symbol, $\left(\frac{a}{l}\right) = \pm 1$ according as $x^2 \equiv a(l)$ has a solution or not.

Proof 1. Let χ be the quadratic character mod p, ψ the quadratic character mod q, $g = g(1,\chi)$, and $p^* = g^2 = \chi(-1)p$. We have

$$g^q = (p^*)^{(q-1)/2}g \equiv \psi(p^*)g \mod q$$

and also

$$g^q = \left(\sum_k \chi(k)e^{2\pi i k/p}\right)^q \equiv \sum_k \chi(k)^q e^{2\pi i kq/p} \equiv g(q,\chi) \equiv \chi(q)g \mod q$$

(noting that $\chi(k)^q = \chi(k)$ and $\bar{\chi} = \chi$). Hence (the numbers being ± 1 makes the congruence mod q an equality)

$$\chi(q) = \psi(p^*) = \psi(\chi(-1)p) = \psi((-1)^{(p-1)/2}p) = (-1)^{(p-1)(q-1)/2}\psi(p)$$

as desired (using $\chi(-1) = (-1)^{(p-1)/2}, \psi(-1) = (-1)^{(q-1)/2}$). □

Proof 2. Here is another proof in a similar vein. By the above, $K = \mathbb{Q}(\zeta_p)$ contains a square root of $p^* = (-1)^{(p-1)/2}p$ (namely g). [Another way to see this is by noting that

$$\frac{x^p-1}{x-1} = \prod_{i=1}^{p-1}(x-\zeta_p^i) \Rightarrow p = \prod_{i=1}^{p-1}(1-\zeta_p^i)$$

(evaluating at $x=1$) and combining the $\pm i$ terms $(1-\zeta_p^{-i})(1-\zeta_p^i) = -\zeta_p^{-i}(1-\zeta_p^i)^2$ so that

$$p = (-1)^{(p-1)/2}\zeta_p^b \prod_{i=1}^{(p-1)/2}(1-\zeta_p^i)^2$$

where $b = -\sum_{k=1}^{(p-1)/2} k$. Let $2c \equiv 1 \bmod p$ so that $\zeta_p^b = (\zeta_p^{bc})^2$ to get a square root of p^*.]

In any case, let $\tau^2 = p^*$ and let σ_q be the automorphism of $\mathbb{Q}(\zeta_p)$ induced by $\zeta_p \mapsto \zeta_p^q$. Then $\sigma_q \tau = \pm\tau$. We have $G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/(p))^\times$ (in the obvious way) and $H = \mathrm{Gal}(K/\mathbb{Q}(\tau))$ is the uniqe index two subgroup, i.e. the squares in $(\mathbb{Z}/(p))^\times$. Hence

$$\sigma_q \tau = \left(\frac{q}{p}\right) \tau$$

($\pm$ depending on whether or not σ_q fixes τ). Let $\mathfrak{Q}|q$, so that σ_q is the Frobenius of $\mathfrak{Q}$. In particular we have

$$\sigma_q \tau \equiv \tau^q \mod \mathfrak{Q}.$$

Thus

$$\left(\frac{q}{p}\right) \tau \equiv \sigma_q \tau \equiv \tau^q \equiv (p^*)^{(q-1)/2} \tau \mod \mathfrak{Q}$$

and (since $1 \not\equiv -1 \mod \mathfrak{Q}$)

$$\left(\frac{q}{p}\right) = (p^*)^{(q-1)/2} = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right).$$

□

2 Some Related Lemmata and a Few More Proofs

Lemma (Gauss' lemma). *Let p be an odd prime and $(a, p) = 1$. Then*

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

where n is the number of $a, 2a, \ldots, \frac{p-1}{2}a$ greater than $p/2$ modulo p.

Proof. Evaluate

$$Z = a \cdot 2a \cdot 3a \ldots \frac{p-1}{2} a \mod p$$

in two different ways. The obvious gives $Z = a^{(p-1)/2} \cdot 2 \cdot 3 \ldots \frac{p-1}{2}$. For the second, if $ka > p/2$, write it as $-(p - ka)$, and note that all of the ka are distinct ($ka \equiv la \Rightarrow k = l$ since $0 \leq k, l \leq (p-1)/2$). Hence $Z = (-1)^n \cdot 2 \cdot 3 \cdots (p-1)/2$ and the result follows. □

Lemma (Eisenstein's lemma). *For an odd prime p and $(a, p) = 1$*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_n \lfloor an/p \rfloor}$$

where the sum is over even $n = 2, 4, \ldots, p-1$.

Proof. For each n considered, let $an = qp + r(n)$ (quotient plus remainder as a function of n). Multiplying all of the an together (modulo p) gives

$$a^{\frac{p-1}{2}} \prod_n n = \prod_n an = \prod_n r(n) = \prod_n (-1)^{r(n)} r(n) = (-1)^{\sum_n r(n)} \prod_n n \text{ (modulo } p)$$

where we leave $r(n) = (-1)^{r(n)}$ alone if $r(n)$ is even and write it as $r(n) = -(p - r(n)) = (-1)^{r(n)}$ if $r(n)$ is odd. This holds because all of the $(-1)^{r(n)}$ are distinct modulo p, else

$$(-1)^{r(n)} an = (-1)^{r(m)} am \Rightarrow m = \pm n$$

which is impossible for even $2 \leq m, n \leq p - 1$ unless $m = n$.

Finally, considering $an = qp + r(n)$ modulo 2, we see that $qp \equiv q \equiv \lfloor an/p \rfloor \equiv r(n)$ (2) and the result follows. $\square$

Lemma (Zolotarev's lemma)**.** *For p an odd prime, $(a, p) = 1$,*

$$\left(\frac{a}{p}\right) = \epsilon(\pi_a)$$

the sign of the permutation of $1, 2, \ldots, p-1$ induced by multiplication by a.

Proof. In a finite group G, π_g has $|G|/|g|$ disjoint cycles each of length $|g|$. π_g is even unless there are an odd number of even cycles, i.e. $|g|$ is even and $|G|/|g|$ is odd. Let x be a primitive root modulo p (i.e. $\langle x \rangle = (\mathbb{Z}/(p))^\times$). Suppose $a = x^j$ so that the order of a is $k = (p-1)/(j, p-1)$ and the index of $\langle a \rangle$ is $i = (p-1, j)$. We have $\left(\frac{a}{p}\right) = -1$ iff j is odd iff k is even and i is odd. $\square$

We now present some proofs of quadratic reciprocity.

Proof (using the Gauss lemma). Here is a proof due to Eisenstein (using the Gauss lemma above). First a trigonometric lemma.

Lemma. *Let $f(z) = 2i \sin(2\pi z)$. Then for odd n we have*

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

Proof. For n odd and ζ a primitive nth root of unity, we have

$$x^n - y^n = \prod_{k=0}^{n-1} (x - \zeta^k) = \prod_{k=0}^{n-1} (x - \zeta^{-2k}) = \zeta^{-n(n-1)/2} \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y) = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y).$$

With $\zeta = e^{2\pi i/n}, x = e^{2\pi i z}, y = e^{-2\pi i z}$ this becomes

$$f(nz) = \prod_{k=0}^{n-1} f(z + k/n).$$

The function f is 1-periodic so that

$$f(z + k/n) = f(z - (n - k)/n)$$

and as k runs from $(n + 1)/2$ to $n - 1$, $n - k$ runs from $(n - 1)/2$ to 1. Thus

$$\begin{aligned}\frac{f(nz)}{f(z)} &= \prod_{k=1}^{(n-1)/2} f(z + k/n) \prod_{(n+1)/2}^{n-1} f(z - (n - k)/n) \\ &= \prod_{k=1}^{(n-1)/2} f(z + k/n) f(z - k/n).\end{aligned}$$

$\square$

Now let $n = q \neq p$ be an odd prime and $z = l/p$. Using the above and taking the product over l gives

$$\prod_{l=1}^{(p-1)/2} \prod_{k=1}^{(q-1)/2} f(l/p + k/q) f(l/p - k/q) = \prod_{l=1}^{(p-1)/2} \frac{f(ql/p)}{f(l/p)}.$$

The right-hand side is $\left(\frac{q}{p}\right)$ as follows. Similar to what we noted in the proof of the Gauss lemma, the collection of numbers

$$\left\{ la : 1 \leq a \leq \frac{p-1}{2} \right\}, \left\{ \pm l : 1 \leq l \leq \frac{p-1}{2} \right\}$$

are the same, and $(-1)^\delta = \left(\frac{a}{p}\right)$ where δ is the number of minus signs occuring (this is the Gauss lemma). Because f is an odd 1-periodic function we see that

$$\prod_{l=1}^{(p-1)/2} \frac{f(al/p)}{f(l/p)} = \left(\frac{a}{p}\right).$$

To obtain quadratic reciprocity, we compare

$$\prod_{l=1}^{(p-1)/2} \prod_{k=1}^{(q-1)/2} f(l/p+k/q) f(l/p-k/q) = \left(\frac{q}{p}\right), \prod_{l=1}^{(q-1)/2} \prod_{k=1}^{(p-1)/2} f(l/q+k/p) f(l/q-k/p) = \left(\frac{p}{q}\right)$$

recalling the fact that f is odd. Hence

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

$\square$

Proof (using the Eisenstein lemma). Here is another proof due to Eisenstein (using the Eisenstein lemma above). Consider lattice points strictly inside the rectangle with diagonal $(0,0),(p,q)$ (and note that there are no lattice points on the diagonal itself). The number of lattice points below the diagonal with even x-coordinate is $\sum_n \lfloor qn/p \rfloor$. The number of lattice points below the diagonal with even x-coordinate and $p/2 < x < p$ has the same parity as the number of lattice points above the diagonal with even x-coordinate and $p/2 < x < p$. Reflecting these twice (about $x = p/2, y = q/2$) gives the lattice points below the diagonal with odd x-coordinate and $0 < x < p/2$. Hence the parity of $\sum_n \lfloor an/p \rfloor$ is the same as the number of total latice points below the diagonal with $0 < x < p/2$. The same argument shows that the parity of $\sum_n \lfloor pn/q \rfloor$ is the same as the total number of total latice points above the diagonal with $0 < y < q/2$. Hence

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}} = (-1)^{\sum_n \lfloor qn/p \rfloor}(-1)^{\sum_n \lfloor pn/q \rfloor}$$

since the total number of latice points with $0 < x < p/2$ and $0 < y < q/2$ is $\frac{p-1}{2}\frac{q-1}{2}$. □

Proof (using the Zolotarev lemma). asdf □

3 A Proof Using Jacobi Sums

We begin with some preliminaries.

Definition (Jacobi Sum). *Let $\chi_i, 1 \leq i \leq l$ be characters mod p. The* Jacobi sum *is defined as*

$$J(\chi_1, \ldots, \chi_l) = \sum_{t_1 + \cdots + t_l = 1} \chi_1(t_1) \ldots \chi_l(t_l).$$

If the Gauss sum is a finite field equivalent of the gamma function, then the Jacobi sum is analogue of the beta function. Here is the property of J we will use.

Proposition. *Let $\chi_i, 1 \leq i \leq l$ be characters mod p. If the χ_i are all nontrivial and $\prod_i \chi_i$ is also nontrivial, then*

$$J(\chi_1, \ldots, \chi_l) = \frac{\prod_i g(\chi_i)}{g(\prod_i \chi_i)}.$$

Proof. We have

$$\begin{aligned}
\prod_i g(\chi_i) &= \prod_i \sum_{t_i} \chi_i(t_i)\zeta^{t_i} = \sum_a \sum_{\sum_i t_i = a} \prod_i \chi_i(t_i)\zeta^a \\
&= J_0(\chi_1, \ldots, \chi_l) + \sum_{a \neq 0} \zeta^a \prod_i \chi_i(a) J(\chi_1, \ldots, \chi_l) \\
&= J_0(\chi_1, \ldots, \chi_l) + J(\chi_1, \ldots, \chi_l) g(\prod_i \chi_i),
\end{aligned}$$

where $J_0(\chi_1,\ldots,\chi_l)\sum_{\sum_i t_i=0}\prod_i \chi_i(t_i)$, which we want to show is zero. We have

$$\begin{aligned} J_0(\chi_1,\ldots,\chi_l) &= \sum_s \chi_l(s) \sum_{t_1+\cdots+t_{l-1}=-s} \chi_1(t_1)\ldots\chi_{l-1}(t_{l-1}) \\ &= \left(\prod_{i=1}^{l-1}\chi_i\right)(-1)J(\chi_1,\ldots,\chi_{l-1})\sum_{s\neq 0}\left(\prod_i \chi_i\right)(s) = 0, \end{aligned}$$

using the fact that $\prod_i \chi_i$ is nontrivial. $\square$

Since q is odd and $\chi^q=\chi$ is nontrivial, by the preceding proposition we have

$$J(\chi,\ldots,\chi) = g(\chi)^{q-1} = (g(\chi)g(\bar\chi))^{\frac{q-1}{2}} = (\chi(-1)p)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}},$$

where we've used the fact that

$$p = g(\chi)\overline{g(\chi)} = \sum_{x,y}\chi(x)\bar\chi(y)\zeta^{x-y} = \sum_x \chi(x)\zeta^x\sum_y \bar\chi(-y)\zeta^y = \bar\chi(-1)g(\chi)g(\bar\chi).$$

Modulo q the Jacobi sum is

$$J(\chi,\ldots,\chi) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \bmod q.$$

There is an action of the cyclic group of order q on the the q-tuples indexing the Jacobi sum, and only one fixed point, $x_i = q^{-1}\text{mod } p$, so that

$$J(\chi,\ldots,\chi) \equiv \chi(q^{-1})^q \equiv \bar\chi(q) \equiv \chi(q) \equiv \left(\frac{q}{p}\right) \bmod p$$

using the fact that χ is real along the way. Hence

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \bmod q$$

and quadratic reciprocity follows.

4 The Quadratic Character of 2 and −1

Tying up loose ends:

Proposition. *for p an odd prime, we have*

$$\begin{aligned} \left(\frac{-1}{p}\right) &= (-1)^{\frac{p-1}{2}} \\ \left(\frac{2}{p}\right) &= (-1)^{\frac{p^2-1}{8}}. \end{aligned}$$

Proof. The first statement is trivial. For the second, we work over the cyclotomic field $\mathbb{Q}(\zeta)$ where $\zeta^8 = 1$ is a primitive eigth root of unity. Then $(\zeta + \zeta^{-1})^2 = 2$ and

$$2^{\frac{p-1}{2}} = (\zeta + \zeta^{-1})^{p-1} = \frac{(\zeta + \zeta^{-1})^p}{\zeta + \zeta^{-1}} \equiv \frac{\zeta^p + \zeta^{-p}}{\zeta + \zeta^{-1}} \mod p.$$

If $p \equiv \pm 1 \mod 8$ we get $\left(\frac{2}{p}\right) = 1$ and if $p \equiv \pm 3 \mod 8$ we get $\left(\frac{2}{p}\right) = -1$.

Or (similarly), working in $\mathbb{Z}[i]$, we have $(1+i)^2 = 2i, (2i)^{\frac{p-1}{2}} = (1+i)^{p-1} \equiv \frac{1+i^p}{1+i} \mod p$, and considering the various cases gives the result. $\square$

5 Appendix: Sign of the Quadratic Gauss Sum

For no good reason, we find the sign of the quadratic Gauss sum ($g(1,\chi)$ with χ the Legendre symbol). We have

$$g(1,\chi) = 1 + \sum_R e^{2\pi i R/q} - \sum_N e^{2\pi i N/q} = 1 + 2\sum_R e^{2\pi i R/q}$$

since

$$0 = 1 + \sum_R e^{2\pi i R/q} + \sum_N e^{2\pi i N/q}$$

(here R and N are the quadratic residues and non-residues mod q). Also,

$$1 + 2\sum_R e^{2\pi i R/q} = \sum_{x=0}^{q-1} e^{2\pi i x^2/q}$$

since x^2 takes on each quadratic residue twice and 0 once. We have the following.

Proposition.

$$S = S(N) = \sum_{x=0}^{N-1} e^{2\pi i x^2/N} = \begin{cases} (1+i)\sqrt{N} & N \equiv 0(4) \\ \sqrt{N} & N \equiv 1(4) \\ 0 & N \equiv 2(4) \\ i\sqrt{N} & N \equiv 3(4) \end{cases}.$$

Proof. Consider the restiction of a continuous $f : \mathbb{R} \to \mathbb{R}$ to $[0,1]$. We have $\tilde{f} = f$ except at $x = 0, 1$ where $\tilde{f}(0) = \tilde{f}(1) = \frac{f(0)+f(1)}{2}$ where $\tilde{f}(x) = \sum_n \left(\int_0^1 f(t)e^{-2\pi i n t}dt\right) e^{2\pi i n x}$. Repeating this for $f_k(x) = f(x+k)$ with $A \le k \le B$ and summing the results gives

$$\sum_{k=A}^{B} \tilde{f}_k(x) = \sum_{k=A}^{B}\sum_n \left(\int_0^1 f(t+k)e^{-2\pi i n t}dt\right) e^{2\pi i n x} = \sum_n \left(\int_A^B f(t)e^{-2\pi i n t}dt\right) e^{2\pi i n x}.$$

Evaluating at $x = 0$ gives

$$\sum_{k=A}^{B} f(k) - \frac{f(A)+f(B)}{2} = \sum_n \left(f \cdot \mathbf{1}_{[A,B]}\right)^{\wedge}(n).$$

We apply this to the function $f(x) = e^{2\pi i x^2/N}$ with $A = 0, B = N$. This gives (noting $(f(0) + f(N))/2 = f(0) = 1$)

$$\begin{aligned}
S(N) &= \sum_n \int_0^N e^{2\pi i x^2/N - 2\pi i n x} dx \\
&= N \sum_n e^{-\pi i N n^2/2} \int_0^1 e^{2\pi i N (y-n/2)^2} dy \\
&= N \sum_n e^{-\pi i N n^2/2} \int_{-n/2}^{1-n/2} e^{2\pi i N y^2} dy \\
&= N \sum_n \int_{-n}^{1-n} e^{2\pi i N y^2} dy + N i^{-N} \sum_n \int_{-n-1/2}^{-n+1/2} e^{2\pi i N y^2} dy \\
&= N(1 + i^{-N}) \int_{-\infty}^{\infty} e^{2\pi i N y^2} dy \\
&= N^{1/2}(1 + i^{-N}) \int_{-\infty}^{\infty} e^{2\pi i z^2} dz \\
&= N^{1/2} \frac{1 + i^{-N}}{1 - i} \left(\text{setting } N = 1, S(1) = 1 \text{ to find } \int_{-\infty}^{\infty} e^{2\pi i z^2} dz = \frac{1}{1 - i} \right).
\end{aligned}$$

□

References

[1] Davenport, *Multiplicative Numbver Theory*, Third Edition, GTM Vol. 74, Springer

[2] Ireland and Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition, GTM Vol. 84, Springer

[3] Serre, *A Course in Arithmetic*, GTM Vol. 7, Springer