THE QUADRATIC RECIPROCITY LAW OF DUKE-HOPKINS

PETE L. CLARK

Circa 1870, G. Zolotarev observed that the Legendre symbol $(\frac{a}{p})$ can be interpreted as the **sign** of multiplication by a viewed as a permutation of the set $\mathbb{Z}/p\mathbb{Z}$. He used this observation to give a strikingly original proof of quadratic reciprocity [2]. We shall not discuss Zolotarev's proof *per se*, but rather a 2005 paper of W. Duke and K. Hopkins which explores the connection between permutations and "quadratic symbols" in a more ambitious way. En route, we explore quadratic reciprocity as expressed in terms of the Kronecker symbol.

1. The Kronecker Symbol

The **Jacobi symbol** $(\frac{a}{n})$ is an extension of the Legendre symbol $(\frac{a}{p})$ which is defined for any positive odd integer n by $(\frac{a}{1}) = 1$ for all $a \in \mathbb{Z}$; if $n = \prod_{i=1}^r p_i$, then

$$\left(\frac{a}{n}\right) = \prod_{i=1}^r \left(\frac{a}{p_i}\right).$$

For an integer a, define

$$\left(\frac{a}{2}\right) = \left\{ \begin{array}{ccc} 0 & a \equiv 0 & (\mathrm{mod}\ 2) \\ 1 & a \equiv 1,7 & (\mathrm{mod}\ 8) \\ -1 & a \equiv 3,5 & (\mathrm{mod}\ 8) \end{array} \right\},$$

$$\left(\frac{a}{-1}\right) = \left\{ \begin{array}{cc} 0 & a = 0 \\ 1 & a > 0 \\ -1 & a < 0 \end{array} \right\},$$

$$\left(\frac{a}{0}\right) = \left\{ \begin{array}{cc} 0 & a \neq 1 \\ 1 & a = 1 \end{array} \right\}.$$

With these additional rules there is a unique extension of the Jacobi symbol to a symbol $(\frac{n}{a})$ defined for any $n, a \in \mathbb{Z}$ such that for all integers n, a, b, we have $(\frac{n}{ab}) = (\frac{n}{a})(\frac{n}{b})$. One also has $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$, i.e., the symbol is **bi-multiplicative**. This extension of the Jacobi symbol is known as the **Kronecker symbol**.

When n is **not** odd and positive, some authors (e.g. [1]) define $(\frac{a}{n})$ only when $a \equiv 0, 1 \pmod 4$. It is not worth our time to discuss these two conventions, but we note that all of our results involve only this"restricted" Kronecker symbol.

For odd $n \in \mathbb{Z}^+$, define $n^* = (-1)^{\frac{n-1}{2}} n$. **Full quadratic reciprocity** – i.e., the usual QR law together with its First and Second Supplements – is equivalent to one elegant identity: for $a \in \mathbb{Z}$ and an odd positive $n \in \mathbb{Z}$,

$$\left(\frac{a}{n}\right) = \left(\frac{n^*}{a}\right). \tag{1}$$

2. The Duke-Hopkins Reciprocity Law

Let G be a finite commutative group (written multiplicatively) of order n. We define an action of $(\mathbb{Z}/n\mathbb{Z})^\times$ on G, by

$$(a \pmod n) \bullet g := g^a.$$

By Lagrange's Theorem, $g^n = 1$, so that $g^a = g^{a'}$ if $a \equiv a' \pmod n$ and $a\bullet$ is well defined. It is immediate that each $a\bullet$ gives a homomorphism from G to G; moreover, since $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, there exists $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $ab \equiv 1 \pmod n$, and then $a\bullet \circ b\bullet = b\bullet \circ a\bullet = \mathrm{Id}_G$, so that each $a\bullet$ is an automorphism of G.

As for any group action on a set, this determines a homomorphism from $(\mathbb{Z}/n\mathbb{Z})^\times$ to the group $\mathrm{Sym}(G)$ of permutations of G, the latter group being isomorphic to S_n, the symmetric group on n elements. Recall that there is a unique homomorphism from S_n to the cyclic group Z_2 given by the **sign** of the permutation. Therefore we have a composite homomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Sym}(G) \to Z_2$$

which we will denote by

$$a \pmod n \mapsto \left(\frac{a}{G}\right).$$

Example 2.1 (Zolotarev): Let p be an odd prime and $G = Z_p$ is the cyclic group of order p. The mapping $(\mathbb{Z}/p\mathbb{Z})^\times \to Z_2$ given by $a \mapsto \left(\frac{a}{Z_p}\right)$ is nothing else than the usual Legendre symbol $a \mapsto (\frac{a}{p})$. Indeed, the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of even order, so admits a unique surjective homomorphism to the group $Z_2 = \{\pm 1\}$: if g is a primitive root mod p, we send g to -1 and hence every odd power of g to -1 and every even power of g to $+1$. This precisely describes the Legendre symbol $a \mapsto (\frac{a}{p})$. Thus it suffices to see that for some $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ we have $\left(\frac{a}{Z_p}\right) = -1$, i.e., the sign of the permutation $n \in Z_p \mapsto n^a$ is -1. To see this, switch to additive notation, viewing Z_p as the isomorphic group $(\mathbb{Z}/p\mathbb{Z}, +)$; the action in question is now just multiplication by a nonzero element a. If g is a primitive root modulo p, multiplication by g fixes 0 and cyclically permutes all $p-1$ nonzero elements, so is a cycle of even order and hence an odd permutation: thus $(\frac{g}{Z_p}) = -1$.

The next result shows that the symbol $(\frac{a}{G})$ is also bi-multiplicative.

Proposition 1. *For $i = 1, 2$ let G_i be a finite commutative group of order n_i and $a \in (\mathbb{Z}/n_1n_2\mathbb{Z})^\times$. Then*

$$\left(\frac{a}{G_1 \times G_2}\right) = \left(\frac{a \pmod{n_1}}{G_1}\right)\left(\frac{a \pmod{n_2}}{G_2}\right).$$

Proof: If $a \in (\mathbb{Z}/n_1n_2\mathbb{Z})^\times$, then

$$a \bullet (g_1, g_2) = (g_1^a, g_2^a) = (g_1^{a \pmod{n_1}}, g_2^{a \pmod{n_2}}).$$

After identifying G_1 (resp. G_2) with the subset $G_1 \times e_{G_2}$ (resp. $e_{G_1} \times G_2$) of $G_1 \times G_2$, the permutation that a induces on $G_1 \times G_2$ is the product of the permutation that $a \pmod n)_1$ induces on G_1 with the permutation that $a \pmod n)_2$ induces on G_2.

Let us now consider the action of -1 on $\mathrm{Sym}(G)$. Let r_1 be the number of fixed

points of $-1\bullet$. More concretely, $-1 \bullet g = g^{-1} = g$ iff g has order 1 or 2. Note that $r_1 \geq 1$ because of the identity element. The $n - r_1$ other elements of G are all distinct from their multiplicative inverses, so there exists a positive integer r_2 such that $n - r_1 = 2r_2$.

Definition: We put $G^* = (-1)^{r_2}|G|^{r_1} = (-1)^{r_2}n^{r_1}$.

Lemma 2. *For any finite commutative group G, we have $G^* \equiv 0$ or $1 \pmod 4$.*

Proof: Let $n = |G|$. If n is odd, then by Lagrange the only g with $g^{-1} = g$ is the identity, so that $r_1 = 1$ and $r_2 = \frac{n-1}{2}$. In this case $G^* = |G|^* = (-1)^{\frac{n-1}{2}}n \equiv 1 \pmod 4$. If n is even, then $n - r_1 = 2r_2 \equiv 0 \pmod 2$, so r_1 is even and hence is at least 2, so $G^* = (-1)^{r_2}n^{r_1} \equiv 0 \pmod 4$.

So the Kronecker symbol $\left(\frac{G^*}{a}\right)$ is always defined (even in the "restricted" sense).

Theorem 3. *(Duke-Hopkins Reciprocity Law) For a finite commutative group G and an integer a, we have*

$$\left(\frac{a}{G}\right) = \left(\frac{G^*}{a}\right).$$

The proof will be given in the next section.

Corollary 4. *a) Suppose G has odd order n. Then for any $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have*

$$\left(\frac{a}{G}\right) = \left(\frac{n^*}{a}\right).$$

b) Taking $G = Z_n$ we recover (1).
c) We have $(\frac{a}{G}) = 1$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ iff n is a square.

Proof of Corollary 4: In the proof of Lemma 2 we saw that $G^* = n^*$; part a) then follows immediately from the reciprocity law. By part a), the symbol $(\frac{a}{G})$ can be computed using any group of order n, so factor n into a product $p_1 \cdots p_r$ of not necessarily distinct primes and apply Example 2.1: we get $(\frac{a}{G}) = \prod_{i=1}^r (\frac{a}{p_i}) = (\frac{a}{n})$. This gives part b). Finally, using the Chinese Remainder Theorem it is easy to see that there is some a such that $(\frac{a}{n}) = -1$ iff n is not a square.

3. The Proof

Enumerate the elements of G as $g_1, \ldots, g_n$ and the characters of G as $\chi_1, \ldots, \chi_n$. Let M be the $n \times n$ matrix whose (i, j) entry is $\chi_i(g_j)$.

Since any character $\chi \in X(G)$ has values on the unit circle in $\mathbb{C}$, we have $\chi^{-1} = \overline{\chi}$. Therefore the number r_1 of fixed points of -1 on G is the same as the number of characters χ such that $\overline{\chi} = \chi$, i.e., real-valued characters. Thus the effect of complex conjugation on the character matrix M is to fix each row corresponding to a real-valued character and to otherwise swap the ith row with the jth row where $\chi_j = \overline{\chi_i}$. In all r_2 pairs of rows get swapped, so

$$\det(\overline{M}) = \det(M) \cdot (-1)^{r_2}.$$

Moreover, with $M^* = (\overline{M})^t$, we have

$$MM^* = nI_n,$$

so that

$$\det(M)\det(\overline{M}) = n^n,$$

so

$$\det(M)^2 = (-1)^{r_2}n^n = (-1)^{r_2}n^{r_1}n^{2r_2} = \ell^2 G^*, \tag{2}$$

where $\ell = n^{r_2}$. (In particular $\det(M)^2$ is a positive integer. Note that $\det(M)$ itself lies in $\mathbb{Q}(\sqrt{G^*})$, and is not rational if n is odd.) So for any $a \in \mathbb{Z}$, we have

$$\left(\frac{\det(M)^2}{a}\right) = \left(\frac{G^*}{a}\right). \tag{3}$$

The character matrix M has values in the cyclotomic field $\mathbb{Q}(\zeta_n)$, which is a Galois extension of $\mathbb{Q}$, with Galois group isomorphic to (what a concidence!) $(\mathbb{Z}/n\mathbb{Z})^\times$, an explicit isomorphism being given by making $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ correspond to the unique automorphism σ_a of $\mathbb{Q}(\zeta_n)$ satisfying $\sigma_a(\zeta_n) = \zeta_n^a$. (All of this is elementary Galois theory except for the more number-theoretic fact that the cyclotomic polynomial Φ_n is irreducible over $\mathbb{Q}$.) In particular the group $(\mathbb{Z}/n\mathbb{Z})^\times$ also acts by permutations on the character group $X(G)$, and indeed in exactly the same way it acts on G:

$$\forall\ g \in G,\ (a \bullet \chi)(g) = \chi(g^a) = (\chi(g))^a = \chi^a(g),$$

so $a \bullet \chi = \chi^a$. This has the following beautiful consequence:

For $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, applying the Galois automorphism σ_a to the character matrix M induces a permutation of the rows which is "the same" as the permutation $\bullet a$ of G. In particular the signs are the same, so

$$\det(\sigma_a M) = \det(M) \cdot \left(\frac{a}{G}\right). \tag{4}$$

Combining (2) and (4), we get that for all $a \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\sigma_a(\sqrt{G^*}) = \left(\frac{a}{G}\right)\sqrt{G^*}.$$

Now, by the multiplicativity on both sides it is enough to prove Theorem 3 when $a = p$ is a prime not dividing n and when $a = -1$.

Proposition 5. *Let p be a prime not dividing n. TFAE:*
a) $\sigma_p(\sqrt{G^*}) = \sqrt{G^*}$.
b) p splits in $\mathbb{Q}(\sqrt{G^*})$.
c) $(\frac{G^*}{p}) = 1$.

The proof of this – a standard result in algebraic number theory – is omitted for now.

We deduce that

$$\left(\frac{G^*}{p}\right) = \left(\frac{p}{G}\right).$$

Finally, when $a = -1$, σ_{-1} is simply complex conjugation, so

$$\left(\frac{-1}{G}\right)\sqrt{G^*} = \sigma_{-1}(\sqrt{G^*}) = \left\{ \begin{array}{cc} \sqrt{G^*} & G^* > 0 \\ -\sqrt{G^*} & G^* < 0 \end{array} \right\} = \left(\frac{G^*}{-1}\right)\sqrt{G^*},$$

so

$$\left(\frac{-1}{G}\right) = \left(\frac{G^*}{-1}\right).$$

This completes the proof of Theorem 3.

4. In fact...

...the "real" Duke-Hopkins reciprocity law is an assertion about a group G of order n which is not necessarily commutative. In this case, the map $g \mapsto g^a$ need not be an automorphism of G, so a more sophisticated approach is needed. Rather, one considers the action of $(\mathbb{Z}/n\mathbb{Z})^\times$ on the **conjugacy classes** $\{C_1, \ldots, C_m\}$ of G: if $g = xhx^{-1}$ then $g^a = xh^a x^{-1}$, so this makes sense. We further define r_1 to be the number of "real" conjugacy classes $C = C^{-1}$ – and assume that in our labelling $C_1, \ldots, C_{r_1}$ are all real – and define r_2 by the equation $m = r_1 + 2r_2$. Then in place of our G^* (notation which is not used in [1]), one has the **discriminant**

$$d(G) = (-1)^{r_2} n^{r_1} \prod_{j=1}^{r_1} |C_j|^{-1}.$$

The Duke-Hopkins reciprocity law asserts that for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\left(\frac{a}{G}\right) = \left(\frac{d(G)}{a}\right).$$

The proof is very similar, except the group $X(G)$ of one-dimensional characters gets replaced by the set $\{\chi_1, \ldots, \chi_m\}$ of characters (i.e., trace functions) of the irreducible complex representations of G. Perhaps surprisingly, the only part of the proof which looks truly deeper is the claim that $d(G) \equiv 0, 1 \pmod 4$ which is required, according to the conventions of [1], for the Kronecker symbol $(\frac{d(G)}{a})$ can be defined. Duke and Hopkins suggest this as an analogue of Stickelberger's theorem in algebraic number theory which asserts that the discriminant of any number field is an integer which is 0 or 1 modulo 4; moreover they adapt a 1928 proof of that theorem due to Issai Schur.

References

[1] W. Duke and K. Hopkins, *Quadratic reciprocity in a finite group*. Amer. Math. Monthly 112 (2005), no. 3, 251–256.

[2] G. Zolotarev, *Nouvelle démonstration de la loi de réciprocité de Legendre*. Nouvelles Ann. Math. (2) 11 (1872) 354-362.