(*March 19, 2024*)

Another presentation of basic Quadratic Reciprocity

Paul Garrett garrett@umn.edu https://www-users.cse.umn.edu/~garrett/

Earlier *ad hoc* examples of quadratic reciprocity for 2 mod p, -3 mod p, and 5 mod p, used the presence of $\sqrt{2}$, $\sqrt{-3}$, and $\sqrt{5}$ in fields generated by roots of unity, to obtain expressions for the quadratic symbols that were manifestly periodic as functions of p. We systematize this:

[0.1] Claim: Fix an odd prime p. There is an explicit linear combination of p^{th} roots of unity equal to $\sqrt{\pm p}$. Specifically,

$$\Big(\sum_{a\in(\mathbb{Z}/p)^\times} \chi(a)\cdot\psi(a)\Big)^2 \;=\; \Big(\frac{-1}{p}\Big)_2\cdot p$$

where $\chi(a) = \big(\frac{a}{p}\big)_2$, and $\psi(a) = e^{2\pi i a/p} = \omega_p^a$, where ω_p is a primitive p^{th} root of unity.

[0.2] Remark: $g = \sum_{a\in(\mathbb{Z}/p)^\times} \chi(a)\cdot\psi(a)$ is an instance of a *Gauss sum*.

Proof: Since $(\mathbb{Z}/p)^\times$ is *cyclic*, we have Euler's expression

$$\chi(a) \;=\; a^{\frac{p-1}{2}} \bmod p$$

Thus, the map $a \to \chi(a) = \big(\frac{a}{p}\big)_2$ is a *group homomorphism* $(\mathbb{Z}/p)^\times \to \{\pm1\} \subset \mathbb{C}^\times$. Then

$$g^2 \;=\; \Big(\sum_{a\in(\mathbb{Z}/p)^\times} \chi(a)\cdot\psi(a)\Big)^2 \;=\; \sum_{a,b\in(\mathbb{Z}/p)^\times} \chi(a)\cdot\psi(a)\cdot\chi(b)\cdot\psi(b)$$

Make a change of variables in the group $(\mathbb{Z}/p)^\times$: replace a by ab, so the previous becomes

$$\sum_{a,b\in(\mathbb{Z}/p)^\times} \chi(ab)\cdot\psi(ab)\cdot\chi(b)\cdot\psi(b) \;=\; \sum_{a,b\in(\mathbb{Z}/p)^\times} \chi(a)\chi(b)\cdot\psi(ab)\cdot\chi(b)\cdot\psi(b) \;=\; \sum_{a,b\in(\mathbb{Z}/p)^\times} \chi(a)\cdot\psi((a+1)b)$$

since $\chi(b)^2 = (\pm1)^2 = 1$. We prove the following after this proof:

[0.3] Claim: *Cancellation Lemma* For a group homomorphism $\varphi : G \to \mathbb{C}^\times$,

$$\sum_{g\in G} \varphi(g) \;=\; \begin{cases} 0 & \text{for } \varphi \text{ non-trivial} \\ \#G & \text{for } \varphi \text{ trivial} \end{cases}$$

This cancellation lemma will be applied twice, both to $G = \mathbb{Z}/p$ with addition, and to $G = (\mathbb{Z}/p)^\times$. First, for fixed $a \in (\mathbb{Z}/p)^\times$, the inner sum over b is

$$\sum_{b\in(\mathbb{Z}/p)^\times} \psi((a+1)b) = \sum_{b\in\mathbb{Z}/p} \psi((a+1)b) - \sum_{b=0} 1 = \begin{cases} 0-1 & b \to \psi((a+1)b) \text{ non-trivial} \\ p-1 & b \to \psi((a+1)b) \text{ trivial} \end{cases} = \begin{cases} -1 & a \neq -1 \\ p-1 & a = -1 \end{cases}$$

Thus, the whole sum is

$$g^2 \;=\; \sum_{a\in(\mathbb{Z}/p)^\times,\, a\neq -1} \chi(a)\cdot(-1) \;+\; \sum_{a=-1} \chi(a)\cdot(p-1) \;=\; -\sum_{a\in(\mathbb{Z}/p)^\times} \chi(a) \;+\; p\cdot\chi(-1)$$

Again invoking the cancellation lemma, the first sum is 0, so the whole is indeed

$$\Big(\sum_{a\in(\mathbb{Z}/p)^\times} \chi(a)\cdot\psi(a)\Big)^2 \;=\; p\cdot\chi(-1) \;=\; p\cdot\left(\frac{-1}{p}\right)_2$$

as claimed. ///

Returning to the main argument for Quadratic Reciprocity: using Euler's criterion: since $g^2 = \left(\frac{-1}{p}\right)_2\cdot p = \chi(-1)\cdot p$, not just p, compute

$$\left(\frac{\chi(-1)\cdot p}{q}\right)_2 \;=\; \Big(\chi(-1)\cdot p\Big)^{\frac{q-1}{2}} \;=\; \Big(\sum_{a\in(\mathbb{Z}/p)^\times} \chi(a)\cdot\psi(a)\Big)^{q-1} \qquad (\text{mod } q, \text{ in } \mathbb{Z}[\omega])$$

To use the fact that inner binomial coefficients $\binom{q}{k}$, with $0<k<q$, are divisible by q, multiply both sides by the Gauss sum g again, so

$$g\cdot\left(\frac{\chi(-1)\cdot p}{q}\right)_2 \;=\; \Big(\sum_{a\in(\mathbb{Z}/p)^\times} \chi(a)\cdot\psi(a)\Big)^{q} \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} \chi(a)^q\cdot\psi(a)^q \qquad (\text{mod } q \text{ in } \mathbb{Z}[\omega])$$

Since $\chi(a)=\pm1$ and q is odd, $\chi(a)^q=\chi(a)$. So

$$\sum_{a\in(\mathbb{Z}/p)^\times} \chi(a)^q\cdot\psi(a)^q \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} \chi(a)\cdot\psi(qa)$$

Note that now we are discussing this sum without thinking about reduction mod q in $\mathbb{Z}[\omega]$. Since q is a unit in $(\mathbb{Z}/p)^\times$, we can change variables, replacing a by aq^{-1}, obtaining

$$\sum_{a\in(\mathbb{Z}/p)^\times} \chi(aq^{-1})\cdot\psi(a) \;=\; \chi(q^{-1})\sum_{a\in(\mathbb{Z}/p)^\times} \chi(a)\cdot\psi(a) \;=\; \chi(q)\cdot g$$

since $\chi(q)=\pm1$. Altogether,

$$g\cdot\left(\frac{\chi(-1)\cdot p}{q}\right)_2 \;=\; \chi(q)\cdot g \;=\; \left(\frac{q}{p}\right)_2\cdot g \qquad (\text{mod } q \text{ in } \mathbb{Z}[\omega])$$

Since $g^2=\pm p$, it is a unit mod q, so we can cancel, to obtain

$$\left(\frac{\left(\frac{-1}{p}\right)_2\cdot p}{q}\right)_2 \;=\; \left(\frac{q}{p}\right)_2$$

In many regards, this is the most natural presentation of the argument for the main part of Quadratic Reciprocity over $\mathbb{Z}$. ///

To recover the more typical assertion of the main part of Quadratic Reciprocity over $\mathbb{Z}$, we realize that we can interpolate

$$\left(\frac{-1}{p}\right)_2 \;=\; (-1)^{\frac{p-1}{2}}$$

And, since the quadratic symbol is a group homomorphism in the upper argument

$$\left(\frac{\left(\frac{-1}{p}\right)_2\cdot p}{q}\right)_2 \;=\; \left(\frac{(-1)^{\frac{p-1}{2}}\cdot p}{q}\right)_2 \;=\; \left(\frac{-1}{q}\right)_2^{\frac{p-1}{2}} q\cdot\left(\frac{p}{q}\right)_2 \;=\; (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\left(\frac{p}{q}\right)_2$$

Thus,

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \binom{p}{q}_2 \;=\; \binom{q}{p}_2$$

And now, the proof of the Cancellation Lemma:

Proof: For a finite group G, and group homomorphism $\varphi : G \to \mathbb{C}^time s$, when φ is the trivial homomorphism, then, of course, $\sum_g \varphi(g) = \sum_g 1 = \#G$. Otherwise, for φ non-trivial, there is $h \in G$ such that $\varphi(h) \neq 1$. Then $\sum_g \varphi(g) = \sum_g 1 = \#G$. Otherwise, for φ non-trivial, there is $h \in G$ such that $\varphi(h) \neq 1$. Changing variables in the sum, replacing g by hg,

$$\sum_g \varphi(g) \;=\; \sum_g \varphi(hg) \;=\; \sum_g \varphi(h)\varphi(g) \;=\; \varphi(h)\sum_g \varphi(g)$$

Subtracting the right-hand side from both sides:

$$(1-\varphi(h))\cdot\sum_g \varphi(g) \;=\; 0$$

Since $1-\varphi(h) \neq 0$, the sum is 0, finishing the proof of the Cancellation Lemma. ///
