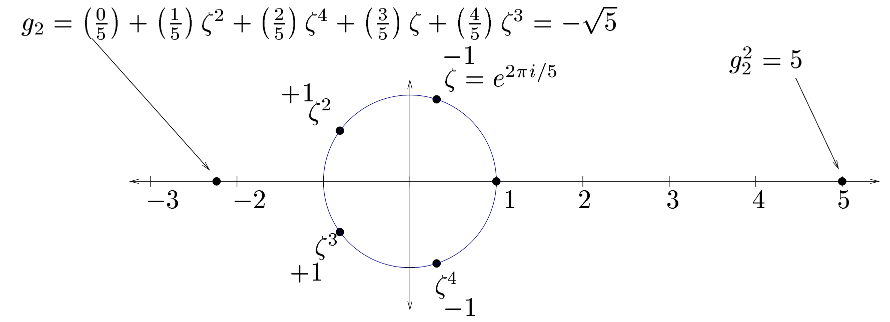

FIGURE 6.2. Gauss sum g_2 for $p = 5$

Definition 6.4.1 (Root of Unity). An nth *root of unity* is a complex number ζ such that $\zeta^n = 1$. A root of unity is a *primitive* nth root of unity if n is the smallest positive integer such that $\zeta^n = 1$.

Since for θ a real number, $e^{i\theta} = \cos(\theta) + i\sin(\theta)$, the complex number $e^{2\pi i/n}$ is a primitive nth root unity. For the rest of this section, fix a prime p and a primitive pth root ζ of unity, e.g., $\zeta = e^{2\pi i/p}$.

Definition 6.4.2 (Gauss Sum). The *Gauss sum* associated to an integer a is

$$g_a = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{an}.$$

(Note that p is implicit in the definition of g_a. If we were to change p, then the Gauss sum g_a associated to a would be different.)

Figure 6.2 illustrates the Gauss sum g_2 for $p = 5$. The Gauss sum is got by adding the points on the unit circle, with signs as indicated, to obtain the real number $-\sqrt{5}$. This suggests the following proposition, whose proof will require some work.

Proposition 6.4.3. *For any a not divisible by p,*

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

In order to prove the proposition, we introduce a few lemmas.

Lemma 6.4.4. *For any integer a,*

$$\sum_{n=0}^{p-1} \zeta^{an} = \begin{cases} p, & \text{if } a \equiv 0 \pmod{p} \\ 0, & \text{otherwise.} \end{cases}$$

Proof. If $a \equiv 0 \pmod{p}$, then $\zeta^a = 1$, so the sum equals the number of summands, which is p. If $a \not\equiv 0 \pmod{p}$, we use the telescopic identity $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$ with $x = \zeta^a$. We have $\zeta^a \neq 1$, so

$\zeta^a - 1 \neq 0$ and

$$\sum_{n=0}^{p-1} \zeta^{an} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = 0.$$

□

Lemma 6.4.5. *Let x and y be integers and let $\delta(x, y)$ be 1 if $x \equiv y \pmod{p}$ or 0 otherwise. Then*

$$\sum_{n=0}^{p-1} \zeta^{(x-y)n} = p \cdot \delta(x, y).$$

Proof. This follows immediately from Lemma 6.4.4 by setting $a = x - y$. □

Lemma 6.4.6. *Let p be a prime. Then*

$$g_0 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) = 0.$$

Proof. By Proposition 6.2.5, the map

$$\left(\frac{\bullet}{p}\right) : (\mathbb{Z}/p)^\times \to \{\pm 1\}$$

is a surjective homomorphism of groups. Thus exactly half the elements of $(\mathbb{Z}/p)^\times$ map to $+1$ and half map to -1 (the subgroup that maps to $+1$ has index 2). Since $\left(\frac{0}{p}\right) = 0$, the sum in the statement of the lemma is 0. □

Lemma 6.4.7. *Let p be a prime and a any integer. Then*

$$g_a = \left(\frac{a}{p}\right) g_1.$$

Proof. When $a \equiv 0 \pmod{p}$ the lemma follows immediately from Lemma 6.4.6, so suppose that $a \not\equiv 0 \pmod{p}$. Then

$$\left(\frac{a}{p}\right) g_a = \left(\frac{a}{p}\right) \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{an} = \sum_{n=0}^{p-1} \left(\frac{an}{p}\right) \zeta^{an} = \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta^{m} = g_1.$$

Now multiply both sides by $\left(\frac{a}{p}\right)$ and use that $\left(\frac{a}{p}\right)^2 = 1$. □

We now have enough lemmas to prove Proposition 6.4.3.

Proof of Proposition 6.4.3. We evaluate the sum $\sum_{a=0}^{p-1} g_a g_{-a}$ in two different ways. By Lemma 6.4.7, since $a \not\equiv 0 \pmod{p}$ we have

$$g_a g_{-a} = \left(\frac{a}{p}\right) g_1 \left(\frac{-a}{p}\right) g_1 = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)^2 g_1^2 = (-1)^{(p-1)/2} g_1^2,$$

where the last step follows from Proposition 6.2.1 and the fact that $\left(\frac{a}{p}\right) \in \{\pm 1\}$. Thus

$$\sum_{a=0}^{p-1} g_a g_{-a} = (p-1)(-1)^{(p-1)/2} g_1^2. \tag{6.1}$$

On the other hand, by definition

$$\begin{aligned} g_a g_{-a} &= \sum_{n=0}^{p-1}\left(\frac{n}{p}\right)\zeta^{an} \cdot \sum_{m=0}^{p-1}\left(\frac{m}{p}\right)\zeta^{-am} \\ &= \sum_{n=0}^{p-1}\sum_{m=0}^{p-1}\left(\frac{n}{p}\right)\left(\frac{m}{p}\right)\zeta^{an}\zeta^{-am} \\ &= \sum_{n=0}^{p-1}\sum_{m=0}^{p-1}\left(\frac{n}{p}\right)\left(\frac{m}{p}\right)\zeta^{an-am}. \end{aligned}$$

Thus by Lemma 6.4.5,

$$\begin{aligned} \sum_{a=0}^{p-1} g_a g_{-a} &= \sum_{a=0}^{p-1}\sum_{n=0}^{p-1}\sum_{m=0}^{p-1}\left(\frac{n}{p}\right)\left(\frac{m}{p}\right)\zeta^{an-am} \\ &= \sum_{n=0}^{p-1}\sum_{m=0}^{p-1}\left(\frac{n}{p}\right)\left(\frac{m}{p}\right)\sum_{a=0}^{p-1}\zeta^{an-am} \\ &= \sum_{n=0}^{p-1}\sum_{m=0}^{p-1}\left(\frac{n}{p}\right)\left(\frac{m}{p}\right) p\delta(n,m) \\ &= \sum_{n=0}^{p-1}\left(\frac{n}{p}\right)^2 p = p(p-1). \end{aligned}$$

Equating (6.1) and the above equality then canceling $(p-1)$ shows that

$$g_1^2 = (-1)^{(p-1)/2} p.$$

Since $a \not\equiv 0 \pmod{p}$, we have $\left(\frac{a}{p}\right)^2 = 1$, so by Lemma 6.4.7,

$$g_a^2 = \left(\frac{a}{p}\right)^2 g_1^2 = g_1^2,$$

and the proposition is proved. □

6.4.1 Proof of Quadratic Reciprocity

We are now in a position to prove Theorem 6.1.3 using Gauss sums.

Proof. Let q be an odd prime with $q \neq p$. Set $p^* = (-1)^{(p-1)/2}p$ and recall that Proposition 6.4.3 asserts that $p^* = g^2$, where $g = g_1 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^n$ is a Gauss sum with $\zeta = e^{2\pi i/p}$ a primitive pth root of unity.

Proposition 6.2.1 trivially implies that

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

We have $g^{q-1} = (g^2)^{(q-1)/2} = (p^*)^{(q-1)/2}$, so multiplying both sides of the displayed equation by g yields a congruence

$$g^q \equiv g\left(\frac{p^*}{q}\right) \pmod{q}. \tag{6.2}$$

But what does this congruence *mean*, given that g^q is not an integer? In Exercise 8, you will prove that every $\mathbb{Z}$-linear combination of powers of ζ can be written uniquely as a $\mathbb{Z}$-linear combination of elements of $B = \{1, \zeta, \ldots, \zeta^{p-2}\}$. The above congruence means that if we write g^q and $g\left(\frac{p^*}{q}\right)$ as $\mathbb{Z}$-linear combinations of the elements of B then the coefficients of the linear combination are congruent modulo q.

Another useful property of congruences, which you will prove in Exercise 9, is that if x and y are two $\mathbb{Z}$-linear combinations of powers of ζ, then $(x+y)^p \equiv x^p + y^p \pmod{p}$. Applying this in our current situation, we see (also using that q is odd) that

$$g^q = \left(\sum_{n=0}^{p-1}\left(\frac{n}{p}\right)\zeta^n\right)^q \equiv \sum_{n=0}^{p-1}\left(\frac{n}{p}\right)^q \zeta^{nq} \equiv \sum_{n=0}^{p-1}\left(\frac{n}{p}\right)\zeta^{nq} \equiv g_q \pmod{q}.$$

By Lemma 6.4.7,

$$g^q \equiv g_q \equiv \left(\frac{q}{p}\right) g \pmod{q}.$$

Combining this with (6.2) yields

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \pmod{q}.$$

Since $g^2 = p^*$ and $p \neq q$, we can cancel g from both sides to find that $\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod{q}$. Since both residue symbols are ± 1 and q is odd, it follows that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$. Finally, we note using Proposition 6.2.1 that

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

□