Gauss Sums

As we have seen, there is a close connection between Legendre symbols of the form

$$\left(\frac{-3}{p}\right)$$

and cube roots of unity. Specifically, if ω is a primitive cube root of unity, then

$$\omega - \omega^2 \;=\; \pm\, i\sqrt{3}$$

and hence

$$\left(\omega - \omega^2\right)^2 \;=\; -3$$

In fact, this last equation holds for any element ω of order 3 in any field $\mathbb{F}$, and hence -3 is a perfect square in any field that has elements of order 3.

There are similar considerations for other primes. For example, if ω is a primitive 5th root of unity, then

$$\omega - \omega^2 - \omega^3 + \omega^4 \;=\; \pm\sqrt{5}.$$

and hence

$$\left(\omega - \omega^2 - \omega^3 + \omega^4\right)^2 \;=\; 5.$$

Again, it is possible to show that this last equation holds for any element ω of order 5 in any field $\mathbb{F}$, and therefore 5 is a perfect square in any field that has elements of order 5.

Gauss discovered a beautiful generalization of these formulas.

Theorem 1 Gauss Sum Formula

Let $p > 2$ be prime, and let ω be a primitive pth root of unity. Then

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\omega^k \;=\; \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ \pm\, i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

The sum

$$g_p(\omega) = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\omega^k = \omega + \left(\frac{2}{p}\right)\omega^2 + \left(\frac{3}{p}\right)\omega^3 + \cdots + \left(\frac{p-1}{p}\right)\omega^{p-1}$$

is known as a **Gauss sum**. According to the theorem

$$g_p(\omega)^2 = \begin{cases} p & \text{if } p \equiv 1 \pmod{4}, \\ -p & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

for any primitive pth root of unity ω. Equivalently, we can write this formula as

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

EXAMPLE 1 Gauss Sum for $p = 7$

It is easy to check that the quadratic residues modulo 7 are $\{1, 2, 4\}$, while $\{3, 5, 6\}$ are quadratic non-residues. Therefore, by the Gauss sum formula

$$\omega + \omega^2 - \omega^3 + \omega^4 - \omega^5 - \omega^6 = \pm i\sqrt{7}$$

for any primitive 7th root of unity ω.

It is not too hard to check that this is correct. Squaring the Gauss sum gives

$$\begin{aligned}&\left(\omega + \omega^2 - \omega^3 + \omega^4 - \omega^5 - \omega^6\right)^2 \\ &\qquad = \omega^2 + 2\omega^3 - \omega^4 + \omega^6 - 6\omega^7 + \omega^8 - \omega^{10} + 2\omega^{11} + \omega^{12}\end{aligned}$$

and using the identity $\omega^7 = 1$ to reduce the powers of ω simplifies this to

$$\left(\omega + \omega^2 - \omega^3 + \omega^4 - \omega^5 - \omega^6\right)^2 = -6 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6.$$

But $1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 = \Phi_7(\omega) = 0$, and hence

$$\left(\omega + \omega^2 - \omega^3 + \omega^4 - \omega^5 - \omega^6\right)^2 = -7.$$

■

EXAMPLE 2 Gauss Sum for $p = 11$

It is easy to check that the quadratic residues modulo 11 are $\{1, 3, 4, 5, 9\}$, while $\{2, 6, 7, 8, 10\}$ are quadratic non-residues. Therefore, by the Gauss sum formula

$$\omega - \omega^2 + \omega^3 + \omega^4 + \omega^5 - \omega^6 - \omega^7 - \omega^8 + \omega^9 - \omega^{10} = \pm i\sqrt{11}$$

for any primitive 11th root of unity ω.

Again, we can use simple algebra to show that this is correct. Squaring the Gauss sum and applying the identity $\omega^{11} = 1$ gives the formula

$$\begin{aligned}&\left(\omega - \omega^2 + \omega^3 + \omega^4 + \omega^5 - \omega^6 - \omega^7 - \omega^8 + \omega^9 - \omega^{10}\right)^2 \\ &\qquad = -10 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 + \omega^7 + \omega^8 + \omega^9 + \omega^{10}\end{aligned}$$

But $1 + \omega + \omega^2 + \cdots + \omega^{10} = \Phi_{11}(\omega) = 0$, and hence

$$\left(\omega - \omega^2 + \omega^3 + \omega^4 + \omega^5 - \omega^6 - \omega^7 - \omega^8 + \omega^9 - \omega^{10}\right)^2 = -11. \qquad \blacksquare$$

EXAMPLE 3 Gauss Sum for $p = 13$

It is easy to check that the quadratic residues modulo 13 are $\{1, 3, 4, 9, 10, 12\}$, while $\{2, 5, 6, 7, 8, 11\}$ are quadratic non-residues. Therefore, by the Gauss sum formula

$$\omega - \omega^2 + \omega^3 + \omega^4 - \omega^5 - \omega^6 - \omega^7 - \omega^8 + \omega^9 + \omega^{10} - \omega^{11} + \omega^{12} = \pm\sqrt{13}$$

for any primitive 13th root of unity ω.

Since $13 \equiv 1 \pmod 4$, the algebra for checking this goes a little differently. Squaring the Gauss sum and then reducing powers of ω modulo 13 gives

$$\begin{aligned}&\left(\omega - \omega^2 + \omega^3 + \omega^4 - \omega^5 - \omega^6 - \omega^7 - \omega^8 + \omega^9 + \omega^{10} - \omega^{11} + \omega^{12}\right)^2 \\ &\qquad = 12 - \omega - \omega^2 - \omega^3 - \omega^4 - \omega^5 - \omega^6 - \omega^7 - \omega^8 - \omega^9 - \omega^{10} - \omega^{11} - \omega^{12}.\end{aligned}$$

But $1 + \omega + \omega^2 + \cdots + \omega^{12} = \Phi_{13}(\omega) = 0$, and hence

$$\left(\omega - \omega^2 + \omega^3 + \omega^4 - \omega^5 - \omega^6 - \omega^7 - \omega^8 + \omega^9 + \omega^{10} - \omega^{11} + \omega^{12}\right)^2 = 13. \qquad \blacksquare$$

Of course, the Gauss sum formula gives two possible values of $g_p(\omega)$ in each case, so a natural question to ask is which of these two values $g_p(\omega)$ is equal to. For example, if $p \equiv 1 \pmod 4$, is $g_p(\omega)$ equal to $\sqrt{p}$ or $-\sqrt{p}$. The answer is that it depends on which primitive pth root of unity ω we choose. However, in the case where $\omega = e^{2\pi i/p}$, Gauss was able to prove that

$$g_p(\omega) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

For example, if $\omega = e^{2\pi i/7}$ then

$$\omega + \omega^2 - \omega^3 + \omega^4 - \omega^5 - \omega^6 = i\sqrt{7},$$

and if $\omega = e^{2\pi i/13}$ then

$$\omega - \omega^2 + \omega^3 + \omega^4 - \omega^5 - \omega^6 - \omega^7 - \omega^8 + \omega^9 + \omega^{10} - \omega^{11} + \omega^{12} = \sqrt{13}.$$

This result is actually much more difficult than the Gauss sum formula, and we will not prove it here.

Proof of the Gauss Sum Formula

Throughout this section, let $p > 2$ be a prime, and let ω be a primitive pth root of unity. Let $g_p(x)$ be the **Gauss polynomial**

$$g_p(x) \;=\; \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) x^k.$$

Our goal is to prove that

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

Extension of the Legendre Symbol

For convenience, we will use the convention that

$$\left(\frac{a}{p}\right) \;=\; 0 \quad \text{if } p \mid a.$$

Using this notation,

$$g_p(x) \;=\; \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) x^k,$$

where the sum starts at $k = 0$ instead of $k = 1$.

Squaring the Gauss Sum

Observe first that

$$g_p(\omega)^2 \;=\; \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \left(\frac{j}{p}\right) \left(\frac{k}{p}\right) \omega^{j+k}.$$

Since $\omega^p = 1$, we can reduce each power of ω modulo p and then combine like terms. This yields an equation of the form

$$g_p(\omega)^2 \;=\; a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-1}\omega^{p-1} \tag{1}$$

where

$$a_n \;=\; \sum_{\substack{j+k\,\equiv\, n \\ (\mathrm{mod}\ p)}} \left(\frac{j}{p}\right) \left(\frac{k}{p}\right) \tag{2}$$

for each $n \in \mathbb{Z}_p$.

Sum of the Coefficients

Note first that

$$g_p(1) \;=\; \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \;=\; 0$$

since $\mathbb{Z}_p^\times$ has an equal number of quadratic residues and quadratic non-residues. It follows that $g_p(1)^2 = 0$, so the sum of the coefficients in $g_p(x)^2$ is equal to 0. Therefore,

$$a_0 + a_1 + \cdots + a_{p-1} \;=\; 0. \tag{3}$$

Value of a_0

It is not hard to determine the value of a_0. By equation (2), we have

$$a_0 \;=\; \sum_{\substack{j+k\,\equiv\,0 \\ (\mathrm{mod}\ p)}} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right) \;=\; \sum_{j=0}^{p-1} \left(\frac{-j}{p}\right)\left(\frac{j}{p}\right).$$

But

$$\left(\frac{-j}{p}\right)\left(\frac{j}{p}\right) \;=\; \left(\frac{-1}{p}\right)\left(\frac{j^2}{p}\right) \;=\; \begin{cases} 0 & \text{if } j = 0, \\ \left(\dfrac{-1}{p}\right) & \text{otherwise.} \end{cases}$$

and thus

$$a_0 \;=\; \sum_{j=1}^{p-1} \left(\frac{-1}{p}\right) \;=\; \left(\frac{-1}{p}\right)(p-1). \tag{4}$$

Equality of the Remaining Coefficients

Let $n \in \mathbb{Z}_p^\times$. By equation (2), we have that

$$a_n \;=\; \sum_{\substack{j+k\,\equiv\,n \\ (\mathrm{mod}\ p)}} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right).$$

If we make the substitution $j = nj'$ and $k = nk'$, then $j' + k' \equiv 1 \pmod{p}$, and indeed

$$a_n \;=\; \sum_{\substack{j'+k'\,\equiv\,1 \\ (\mathrm{mod}\ p)}} \left(\frac{nj'}{p}\right)\left(\frac{nk'}{p}\right).$$

But

$$\left(\frac{nj'}{p}\right)\left(\frac{nk'}{p}\right) \;=\; \left(\frac{n^2}{p}\right)\left(\frac{j'}{p}\right)\left(\frac{k'}{p}\right) \;=\; \left(\frac{j'}{p}\right)\left(\frac{k'}{p}\right)$$

and hence

$$a_n = \sum_{\substack{j'+k' \equiv 1 \\ (\mathrm{mod}\ p)}} \left(\frac{j'}{p}\right)\left(\frac{k'}{p}\right) = a_1$$

for all $n \in \{1, \ldots, p-1\}$. Thus

$$a_1 = a_2 = \cdots = a_{p-1}. \tag{5}$$

End of the Proof

Equations (3) and (5) are

$$a_0 + a_1 + \cdots + a_{p-1} = 0 \qquad \text{and} \qquad a_1 = a_2 = \cdots = a_{p-1}$$

and combining these together gives

$$a_n = -\frac{a_0}{p-1}$$

for each $n \in \{1, \ldots, p-1\}$. Substituting in the value of a_1 obtained in (4), we deduce that

$$a_n = -\left(\frac{-1}{p}\right)$$

for each $n \in \{1, \ldots, p-1\}$. Thus equation (1) becomes

$$g_p(\omega)^2 = \left(\frac{-1}{p}\right)\Big((p-1) - \omega - \omega^2 - \cdots - \omega^{p-1}\Big).$$

But

$$1 + \omega + \omega^2 + \cdots + \omega^{p-1} = \Phi_p(\omega) = 0$$

so

$$\omega + \omega^2 + \cdots + \omega^{p-1} = -1.$$

and hence

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

This completes the proof of the Gauss sum formula.

Symmetry of Gauss Sums

The Gauss sum formula tells us that

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

for *any* primitive pth root of unity ω. The following formula tells us how the sign of $g_p(\omega)$ changes when we use different pth roots of unity.

Proposition 2 Symmetry of the Gauss Sum

Let $p > 2$ be a prime, let ω be a primitive pth root of unity, and let

$$g_p(x) \;=\; \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) x^k.$$

Then for each $n \in \{1, \ldots, p-1\}$,

$$g_p(\omega^n) \;=\; \left(\frac{n}{p}\right) g_p(\omega).$$

PROOF Observe that

$$g_p(\omega^n) \;=\; \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) x^{nk} \;=\; \left(\frac{n}{p}\right) \sum_{k=1}^{p-1} \left(\frac{nk}{p}\right) x^{nk}.$$

But as k runs over the set $\{1, \ldots, p-1\}$, the product $m = nk$ also runs over the elements of this set. Hence we can substitute $m = nk$ to get

$$g_p(\omega^n) \;=\; \left(\frac{n}{p}\right) \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) x^m \;=\; \left(\frac{n}{p}\right) g_p(\omega).$$

■

EXAMPLE 4 Consider the polynomial

$$g_7(x) \;=\; x + x^2 + x^4 - x^3 - x^5 - x^6.$$

If $\omega = e^{2\pi i/7}$, then it is easy to check that

$$g_7(\omega) \;=\; \omega + \omega^2 + \omega^4 - \omega^3 - \omega^5 - \omega^6 \;=\; i\sqrt{7}.$$

According to the formula above, it follows that

$$g_7\big(\omega^n\big) \;=\; \left(\frac{n}{p}\right)g_7(\omega) \;=\; \left(\frac{n}{p}\right)i\sqrt{7}$$

for any $n \in \mathbb{Z}_p^\times$. For example,

$$\begin{aligned} g_7\big(\omega^2\big) \;&=\; \big(\omega^2\big) + \big(\omega^2\big)^2 + \big(\omega^2\big)^4 - \big(\omega^2\big)^3 - \big(\omega^2\big)^5 - \big(\omega^2\big)^6 \\ &=\; \omega^2 \;+\; \omega^4 \;+\; \omega \;-\; \omega^6 \;-\; \omega^3 \;-\; \omega^5 \;=\; g_7(\omega) \;=\; i\sqrt{7} \end{aligned}$$

since 2 is a quadratic residue modulo 7, and

$$\begin{aligned} g_7\big(\omega^3\big) \;&=\; \big(\omega^3\big) + \big(\omega^3\big)^2 + \big(\omega^3\big)^4 - \big(\omega^3\big)^3 - \big(\omega^3\big)^5 - \big(\omega^3\big)^6 \\ &=\; \omega^3 \;+\; \omega^6 \;+\; \omega^5 \;-\; \omega^2 \;-\; \omega \;-\; \omega^4 \;=\; -g_7(\omega) \;=\; -i\sqrt{7} \end{aligned}$$

since 3 is a quadratic non-residue modulo 7. ■