Gauss Sums and Reciprocity Laws

Lev Kruglyak and Ignasi Segura Vicente

March 2022

Our goal for this talk is to explain how we can study multiplicative characters by associating them to a natural quantity called a Gauss sum. These Gauss sums can be thought of as a compressed representation of the character, and applying their algebraic properties to certain characters gives rise to many powerful reciprocity laws.

1 Quadratic Reciprocity

Let p be an odd prime and consider the cyclotomic field $\mathbb{Q}[\zeta_p]$. Recall that the extension $\mathbb{Q}[\zeta_p]/\mathbb{Q}$ is Galois, with a cyclic Galois group $\mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q}) = \mathbb{F}_p^\times$ of order $p-1$. The group $\mathbb{F}_p^\times$ has a unique subgroup of index 2, generated by an element ℓ with order $(p-1)/2$. By the fundamental theorem of Galois theory the field fixed by the automorphisms $\zeta \mapsto \zeta^{a\ell}$ is the unique quadratic subfield of $\mathbb{Q}[\zeta_p]$.

We've shown on a previous problem set that for any odd prime p, we have

$$\sqrt{(-1)^{\frac{p-1}{2}}p} \in \mathbb{Q}[\zeta_p].$$

The quantity $(-1)^{\frac{p-1}{2}}p$ is especially important, so we'll refer to it as p^* from now on. This means that $\mathbb{Q}[\sqrt{p^*}]$ is the unique quadratic subfield of $\mathbb{Q}[\zeta_p]$. Something sneaky is going on here, so perhaps investigating this quadratic subfield further will give us deeper insight into the behavior of quadratic residues. There are a few methods to calculate explicitly this square root in terms of roots of unity.

1.1 Discriminant approach

One method is to use the discriminant. Recall that for an odd prime p, the discriminant of the cyclotomic number field $\mathbb{Q}[\zeta_p]$ is

$$\Delta_{\mathbb{Q}[\zeta_p]} = p^* p^{p-3}.$$

Since the discriminant of a number field is the square of the determinant of a matrix, we can write $p^* p^{p-3} = \alpha^2$ where $\alpha = |\zeta^{ij}|_{1\le i,j\le p-1}$. Thus,

$$p^* = (p^{-\frac{p-3}{2}}\alpha)^2.$$

For example if $p = 5$, $p^* = 5$ and $\alpha = 10\zeta^3 + 10\zeta^2 + 1$ so $\sqrt{p^*} = 2\zeta^3 + 2\zeta^2 + 1 = -(\zeta - \zeta^2 - \zeta^3 + \zeta^4)$. While this method to calculate a generator for the quadratic subfield works, it's a bit too tricky to work with to get meaningful results. To obtain a useful form for $\sqrt{p^*}$, we'll use Legendre symbols.

1.2 Legendre symbols

Let's briefly review some theory associated to quadratic residues modulo an odd prime.

Theorem 1. *(Euler's criterion) Let p be an odd prime. Define the* **Legendre symbol** *by setting it for any $a \in \mathbb{F}_p$:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \textit{if there is some } x \in \mathbb{F}_p \textit{ with } x^2a \\ 0 & \textit{if } a = 0 \\ -1 & \textit{otherwise} \end{cases}$$

Then for any a coprime to p we have

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Proof. Can be found in any number theory textbook. □

A nice corollary of Euler's criterion is that the Legendre symbol is multiplicative, i.e. for $a, b \in \mathbb{F}_p$ we have

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Also we have

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

1.3 Quadratic Gauss sum

We're finally ready to define the quadratic Gauss sum.

Definition 2. For any odd prime p, the ***quadratic Gauss sum*** at $a \in \mathbb{F}_p$ is the quantity:

$$g_a = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{an} \in \mathbb{Q}[\zeta_p].$$

Notice that it suffices to consider $g = g_1$ because of the relation (for $a \neq 0$):

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

since an ranges over all of $\mathbb{F}_p$ when $a \neq 0$. To prove that this Gauss sum is what we're looking for, let's square it.

Proposition 3. *For any odd prime p, we have $g^2 = p^*$.*

Proof. Let $S = \sum_{a=0}^{p-1} g_{-a}g_a$. Then $g_{-a}g_a = \left(\frac{-a}{p}\right)\left(\frac{a}{p}\right) g^2 = \left(\frac{-1}{p}\right) g^2$ so

$$S = \sum_{a=0}^{p-1} \left(\frac{-1}{p}\right) g^2 = (p-1)\left(\frac{-1}{p}\right) g^2.$$

Approaching S from the other side, we also have

$$g_{-a}g_a = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \zeta^{-ax} \sum_{y=0}^{p-1} \left(\frac{y}{p}\right) \zeta^{ay}.$$

Then we have

$$\begin{aligned} S = \sum_{a=0}^{p-1} \sum_{x,y=1}^{p-1} \left(\frac{xy}{p}\right) \zeta^{a(x-y)} = \sum_{x,y=0}^{p-1} \left(\frac{xy}{p}\right) \sum_{a=0}^{p-1} \zeta^{a(x-y)} &= \sum_{x=0}^{p-1} \left(\frac{x^2}{p}\right) p \\ &= (p-1)p. \end{aligned}$$

where the penultimate equality can be seen geometrically. So cancelling on both sides, we get $g^2 = p^*$. □

So the Gauss sum g is a generator for the unique quadratic subfield of $\mathbb{Q}[\zeta_p]$. To see how powerful this is, we'll provide a simple proof of the law of quadratic reciprocity.

1.4 Quadratic reciprocity

Often called one of the first "crowning achievements" of number theory, Gauss's quadratic reciprocity law tells us that whether a prime p is a quadratic residue modulo q is closely related to whether or not a prime q is a quadratic residue modulo p.

Theorem 4 (Quadratic reciprocity)**.** *Given odd distinct primes p, q, we have*

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

Proof. Since g is a linear combination of pth roots of unity, it is an algebraic integer, and so we are able to take the residue of g modulo q in $\mathbb{A}$. We will be working modulo q.

Firstly, note that $g^q = gg^{q-1} = g(g^2)^{\frac{q-1}{2}} = (gp^*)^{q-1/2}$. Because p^* is an integer coprime with q, this means

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

On the other hand, recall that $g = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^t$. By the multinomial Theorem, q divides $\binom{q}{a_1, a_2, \ldots a_q}$ for all $a_1, \ldots a_q$ such that more than one is nonzero. This means

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

Because $\left(\frac{n}{p}\right) \in \mathbb{Z}$ for all $n \in \mathbb{F}_p^\times$, by Fermat's little theorem, $\left(\frac{n}{p}\right)^q \equiv \left(\frac{n}{p}\right) \mod q$, so the previous result becomes

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

Combining the two expressions we have obtained for $g^q \mod q$ and multiplying by g on both sides, we have

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

Because p^*, $\left(\frac{p^*}{q}\right)$ and $\left(\frac{q}{p}\right)$ are all integers coprime with q, we can cancel out p^*, and then, because $\left(\frac{p^*}{q}\right)$ and $\left(\frac{q}{p}\right)$ are either 1 or -1, we have

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

This completes the proof. □

2 Generalizing Gauss sums

Quadratic reciprocity is an incredibly powerful theorem, and the ease with which we proved it using Gauss sums might lead one to wonder what other theorems we could squeeze out of Gauss sum like structures. The crucial property of the Legendre symbol that we used was its multiplicativity, so we might try choosing some general multiplicative function and forming the same weighted sum of roots of unity as in the quadratic Gauss sum.

2.1 Characters

A simple collection of multiplicative functions we can work with is:

Definition 5. A ***character*** is a multiplicative function $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$.

This definition might seem trivially simple, but it hides a very deep structure underneath. First of all, we can let $\mathcal{C}(\mathbb{F}_p^\times)$ be the set of all characters. This can be given a natural group structure by multiplying characters pointwise. In the same way we get inverses. Now note that for any character χ, we have $\chi(1) = 1$, and for any $a \in \mathbb{F}_p^\times$, $\chi(a)$ is a $(p-1)$-th root of unity. This means that if $a \in \mathbb{F}_p^\times$ is a generator, the values of χ are completely determined by $\chi(a)$. Yet $\chi(a)$ is a $(p-1)$-th root of unity, so we have an isomorphism

$$\mathcal{C}(\mathbb{F}_p^\times) \cong \mu_{p-1}$$

where μ_{p-1} is the group of $(p-1)$-th roots of unity. There is some character χ with $\chi(a) = \zeta_{p-1}$ which generates $\mathcal{C}(\mathbb{F}_p^\times)$.

2.2 Characters and the behavior of $f(x) = x^n$

Now here's a truly remarkable fact.

Proposition 6. *The Legendre symbol is the unique character of order* 2 *in* $\mathcal{C}(\mathbb{F}_p^\times)$.

Proof. For some character $\chi \in \mathcal{C}(\mathbb{F}_p^\times)$ with $\chi^2 = 1$, note that $\chi(a) = \pm 1$ for all $a \in \mathbb{F}_p^\times$. If a is some generator of $\mathbb{F}_p^\times$, then clearly $\chi(a) = -1$. Then for every element a^m, $\chi(a^m) = (-1)^m$. If a^m is a quadratic residue, say $x^2 \equiv a^m \mod p$, then $1 = a^{m(p-1)/2} \mod p$ so $m(p-1)/2 \equiv 0 \mod p-1$ and so $2 \mid m$. Thus $\chi(a^m) = 1$ for quadratic residues. Otherwise, $\chi(a^m) = -1$, so χ is exactly the Legendre symbol. □

Proposition 7. *More generally, an order n character in $\mathcal{C}(\mathbb{F}_p^\times)$ corresponds exactly to the behavior of $f(x) = x^n$ in $\mathbb{F}_p^\times$.*

This shows that characters are a natural generalization of Legendre symbols, so let's attempt to study their structure in the same way that we studied Legendre symbols using Gauss sums.

2.3 Gauss sums associated to a character

First of all, we can extend any character $\chi \in \mathcal{C}(\mathbb{F}_p^\times)$ to $\mathbb{F}_p$ by setting $\chi(0) = 0$ if χ is nontrivial, and $\chi(0) = 1$ if $\chi = \epsilon$, the trivial character taking every element to 1.

Definition 8. For any character $\chi \in \mathcal{C}(\mathbb{F}_p^\times)$, the Gauss sum associated to χ is defined as

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

As before, we use g to denote g_1.

We can then prove many of the same properties as we did for quadratic Gauss sums.

Proposition 9. *For any $\chi \neq \epsilon$ and $a \in \mathbb{F}_p^\times$, $g_a(\chi) = \chi(a^{-1})g_1(\chi)$. Meanwhile, $g_0(\chi) = 0$, $g_a(\epsilon) = p$, and $g_0(\epsilon) = 0$.*

Similarly, we have the relationship to $\sqrt{p}$:

Proposition 10. *For any $\chi \neq \epsilon$, $|g| = \sqrt{p}$.*

2.4 The duality between characters and their Gauss sums

To further see why Gauss sums are so useful for understanding characters, we can show that the singular element $g(\chi) \in \mathbb{C}$ is enough to recover all values of the underlying character χ. To make this more explicit, let χ be a character of order k in $\mathcal{C}(\mathbb{F}_p^\times)$. Then χ takes on values in the field $\mathbb{Q}[\zeta_k]$ which is a degree $\phi(k)$ extension over $\mathbb{Q}$. Thus the Gauss sum $g(\chi)$ is an element of the field $\mathbb{Q}[\zeta_k, \zeta_p]$, which is a degree $\phi(p) = p - 1$ degree extension over $\mathbb{Q}[\zeta_k]$. This means that $\mathbb{Q}[\zeta_k, \zeta_p]$ is a $(p-1)$-dimensional vector space over $\mathbb{Q}[\zeta_k]$ with basis $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$. Since the Gauss sum is some linear combination of these elements, it's coefficients must be determined uniquely. This means that the value of the Gauss sum determines χ completely.

In the proof of reciprocity laws, it is often not g, but rather g^k that is computed. Nevertheless, χ can be recovered completely from g^k as well: g is among the kth roots of g^k, which equal $g, \zeta_k g, \ldots, \zeta_k^{k-1} g$. Now, because $\chi(1) = 1$, the coefficient of ζ_p in the expression of g as a linear combination of $\zeta_p, \ldots \zeta_p^{p-1}$ is 1, whereas the coefficients of ζ_p in each of $\zeta_k g, \ldots \zeta_k^{k-1} g$ are $\zeta_k, \ldots \zeta_k^{k-1}$, respectively. Therefore, the value of g^k encapsulates χ completely.

3 Cubic Reciprocity

To generalize quadratic reciprocity in order to find cubic residues, we'll need to change our setting slightly. When proving quadratic reciprocity, we used the fact that the quadratic

Gauss sum's square was a member of the ring of integers, so we could include it in congruence relations. This is not the case in higher reciprocity laws, so we'll expand our domain to the ring $\mathbb{Z}[\omega]$ where $\omega = \frac{-1+\sqrt{-3}}{2}$.

3.1 Properties of $\mathbb{Z}[\omega]$

The ring $\mathbb{Z}[\omega]$ is a nice setting to work in, indeed it is a principal ideal domain. To get more familiar in this setting, let's investigate some basic properties.

Proposition 11. *The only units in $\mathbb{Z}[\omega]$ are $1, -1, \omega, -\omega, \omega^2, -\omega^2$.*

Lastly, we'll investigate the primes in this ring.

Proposition 12. *There are three types of primes in $\mathbb{Z}[\omega]$.*

- *If $p \in \mathbb{Z}$ is a rational prime with $p \equiv 1 \mod 3$, then $p = \pi\overline{\pi}$ for a prime $\pi \in \mathbb{Z}[\omega]$.*
- *If $p \in \mathbb{Z}$ is a rational prime with $p \equiv 2 \mod 3$, then p stays prime in $\mathbb{Z}[\omega]$.*
- *$3 = -\omega^2(1-\omega)^2$ is totally ramified and $1-\omega$ is prime in $\mathbb{Z}[\omega]$.*

This last case makes sense since $\Delta_{\mathbb{Z}[\omega]} = -3$.

Proof. See Ireland and Rosen. □

Just like in quadratic reciprocity where we consider positive primes only, we'll only consider primes congruent to $2 \mod 3$ in this case, these are called ***primary primes***.

Now since $\mathbb{Z}[\omega]$ is a Euclidean domain, this means that for any prime $\pi \in \mathbb{Z}[\omega]$, the quotient $\mathbb{Z}[\omega]_\pi = \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a field. Let's thus defined congruence to be $a, b \in \mathbb{Z}[\omega]$ satisfy $a \equiv b \mod \pi$ if $a - b \in \pi\mathbb{Z}[\omega]$.

Proposition 13. *Let π be a prime in $\mathbb{Z}[\omega]$. Then the field $\mathbb{Z}[\omega]_\pi$ has $N(\pi)$ elements.*

Proof. Casework on types of primes, lattice geometry, and division algorithm. □

3.2 The cubic character

Now that we're familiar with the space $\mathbb{Z}[\omega]$, let's define an appropriate character to study using generalized Gauss sums. Since $\mathbb{Z}[\omega]_\pi^\times$ has $N(\pi)$ elements, then for any $\alpha \in \mathbb{Z}[\omega]$ with $\pi \nmid \alpha$ we have $\alpha^{N(\pi)-1} \equiv 0 \mod \pi$. It follows that $N(\pi) - 1 \equiv 0 \mod 3$, and so we are justified in the following definition:

Definition 14. Let $\pi \in \mathbb{Z}[\omega]$ be a prime with $N(\pi) \neq 3$. The cubic character, $\chi_\pi(\alpha)$ is defined as 0 if $\pi \mid \alpha$, otherwise is the member of $\{1, \omega, \omega^2\}$ such that

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \chi_\pi(\alpha) \mod \pi.$$

Then $\chi_\pi(\alpha)$ is well defined and multiplicative.

This is a natural character to consider because:

Proposition 15. $\chi_\pi(\alpha) = 1$ *if and only if $x^3 = \alpha$ has a solution in $\mathbb{Z}[\omega]_\pi$.*

We are now ready to state the law of cubic reciprocity.

3.3 Proof outline of cubic reciprocity

First we'll prove a useful lemma. Note that if π is a non-integer prime with norm $N(\pi) \equiv 1 \mod 3$ then $\mathbb{Z}[\omega]_\pi$ is naturally isomorphic to $\mathbb{F}_{N(\pi)}$. We can thus view χ_π as a member of $\mathcal{C}(\mathbb{F}_{N(\pi)}^\times)$.

Proposition 16. *Let π be a primary prime in $\mathbb{Z}[\omega]$ with $N(\pi) \equiv 1 \mod 3$. Then,*

$$g(\chi_\pi) = \pi N(\pi).$$

Proof. This proof is a bit tricky, but ultimately boils down to computations involving Gauss sums. There is also a notion of a Jacobi sum, which could be interesting to look into. □

Theorem 17. *Let π, π_2 be primary primes in $\mathbb{Z}[\omega]$. Then*

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

Proof. There are three cases we need to consider:
Case 1: $\pi_1 = p, \pi_2$ are integer primes congruent to $2 \mod 3$.

Case 2: π_1 is an integer prime congruent to $2 \mod 3$ and π_2 divides an integer prime congruent to $1 \mod 3$.

Case 3: π_1, π_2 divide integer primes congruent to $1 \mod 3$

The first case turns out to be quite easy, the second two use Gauss sum manipulations and the proposition. We omit them for the sake of brevity, see Ireland and Rosen for a full proof. □