Gauss Sums

Mark Sellke

This handout is based on *A Classical Introduction to Modern Number Theory* by Ireland and Rosen.

1 Quadratic Gauss Sums

Definition 1. For an odd prime $p > 2$ and integer a define the *quadratic Gauss sum*

$$g_a = \sum_{t \in \mathbb{Z}_p} \left(\frac{t}{p}\right) \zeta_p^{at}$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$. Hence g_a is a complex number. (Note that $\left(\frac{0}{p}\right) = 0$ by definition.)

Exercise 1.1. *Show* $g_a = \left(\frac{a}{p}\right) g_1$.

Exercise 1.2. *Show that* $g_1 = \sum_t \zeta_p^{t^2}$.

Exercise 1.3. *Show* $g_1^2 = (-1)^{\frac{p-1}{2}} p$. *If you know some Galois theory/algebraic number theory, try to explain why this makes sense.*

At this point you might think that these things are boring, since we've just written $\sqrt{\pm p}$ in a funny way. However, here are a couple applications that might impress you.

Problem 1.4. *Prove quadratic reciprocity for odd primes by considering* g_1^q *modulo* q *and using the preceding. Don't worry too much about being careful with rigor if that's an issue, we can talk about it.*

Exercise 1.5 (If you're comfortable with finite fields...)**.** *Find which primes satisfy* $\left(\frac{2}{p}\right) = 1$ *by considering* $\zeta_8 + \zeta_8^{-1}$ *in the algebraic closure of* $\mathbb{F}_p$ *and determining whether it actually lies in* $\mathbb{F}_p$. *Phrase the argument for the main case of QR using this idea. (You can think of* $2\zeta_8 + 2\zeta_8^{-1}$ *as a Gauss sum mod* 8*.)*

Problem 1.6. *Show that*

$$\left|\sum_{t=k}^{\ell} \left(\frac{t}{p}\right)\right| < \sqrt{p} \log p.$$

2 Basics on Characters

To do more stuff we need to extend Gauss sums beyond the Legendre symbol. The important property of the Legendre symbol was the multiplicativity; this property defines a *character*.

Definition 2. A *character* on $\mathbb{F}_p$ is a function

$$\chi : \mathbb{F}_p \to \mathbb{C}$$

such that $\chi(1) = 1$ and $\chi(ab) = \chi(a)\chi(b)$. The *trivial character* ε is 1 on all non-zero elements, but all other characters χ must satisfy $\chi(0) = 0$.

Nothing below is that exciting, so you might want to skim for now and go to the next section. You can use the below as a reference and think about things when they come up.

Exercise 2.1. *Show that $\chi(a)$ is a $p-1$st root of unity, and $\chi(a^{-1}) = \overline{\chi(a)}$.*

Exercise 2.2. *If χ is non-trivial, then $\sum_t \chi(t) = 0$.*

Exercise 2.3. *Show that the characters form a group isomorphic to $\mathbb{Z}_{p-1}$. You can use the fact that $\mathbb{F}_p^\times$ is like this.*

Exercise 2.4. *Show that for all a we have $\sum_{\chi \text{ is a character}} \chi(a) = 0$.*

Exercise 2.5. *Show that $N(x^n = a) := |\{x : x^n = a\}| = \sum_{\chi^n = \varepsilon} \chi(a)$.*

3 Gauss and Jacobi Sums

Definition 3. For a character χ, define $g_a(\chi) = \sum_t \chi(t)\zeta_p^{at}$. Let $g(\chi) = g_1(\chi)$.

Exercise 3.1. *Show again that $g_a(\chi) = \chi(a)^{-1} g(\chi)$ and $|g(\chi)| = \sqrt{p}$, except that $g(\varepsilon) = p$.*

Exercise 3.2. *Use Gauss sums to show that $x^2+y^2 = p$ has solutions for $p \equiv 1 \pmod 4$ and $x^2-xy+y^2 = p$ has solutions for $p \equiv 1 \pmod 3$.*

Now let's say we want to count solutions to an polynomial equation like $N(x^2 + y^2 = 1)$. Since $N(x^2 = a) = 1 + \left(\frac{a}{p}\right)$ we get

$$N(x^2 + y^2 = 1 = \sum_{a+b=1} \left(1 + \left(\frac{a}{p}\right) + \left(\frac{b}{p}\right) + \left(\frac{ab}{p}\right)\right).$$

For larger values of 2 we'd get a similar expression with more terms. But a miracle occurs:

Definition 4. For characters χ, λ let the *Jacobi sum* be

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b).$$

Exercise 3.3. *Suppose χ, λ are non-trivial. We have:*

1. *$J(\varepsilon, \varepsilon) = p$.*
2. *$J(\varepsilon, \chi) = 0$.*
3. *$J(\chi, \chi^{-1}) = -\chi(-1)$.*
4. *If $\chi\lambda \neq \varepsilon$ then $J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.*

Corollary 3.4. *If $\chi, \lambda, \chi\lambda$ are non-trivial then $|J(\chi, \lambda)| = \sqrt{p}$.*

Exercise 3.5. *Find $N(x^2 + y^2 = 1)$.*

Exercise 3.6. *Show that $\left(\left(\frac{t}{p}\right), \left(\frac{t+1}{p}\right)\right) \in \{\pm 1\}^2$ is equidistributed up to $O(1)$ error for large p.*

Exercise 3.7. *Show that $|N(x^3 + y^3 = 1) - p + 2| \leq 2\sqrt{p}$.*

Exercise 3.8 (ISL 2012)**.** *Show that $f(x, y) = x^2 + y^5$ is surjective mod p for all primes $p > 100$.*

Remark. There's much more in Ireland and Rosen. They do similar square-root cancellation for longer sums $\sum_i a_i x_i^{e_i} = b$ by analyzing higher-order Jacobi sums; it's interesting that square-root cancellation is what you'd expect if the terms of these sums were "random." They also prove cubic/quartic reciprocity, and do lots of other things.