More Quadratic Gauss sums and their uses

October 30, 2012

1 Recall next Hour-and-a-half Exam:

November 6.

2 Reading:

Make sure that you have read sections 1-3 of Chapter 6. Read all of Chapter 7.

3 Recall Quadratic Gauss Sums

Use Eisenstein's criterion to prove the theorem of Gauss:

Theorem 1 *Let p be prime. Then the polynomial $f(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ is irreducible over* $\mathbf{Q}$.

Let p be an odd prime, and choose a primitive root of unity ζ_p. Say: $\zeta_p = e^{2\pi i/p}$.

For a not divisible by p, put

$$g_a := \sum_{k=0}^{p-1} \binom{k}{p} \zeta_p^{ka}.$$

Recall "where" g_a lives (i.e., in $\mathbf{Z}[\zeta_p]$).

Put $g := g_1$. The two basic facts about these quadratic Gauss sums:

3.1 Computation that $|g| = \sqrt{p}$

1. **Proposition 1** $g_a = \left(\frac{a}{p}\right) g$,
   and
2. **Proposition 2** $g_a^2 = (-1)^{(p-1)/2} p$.

In other words, put $p^* := (-1)^{(p-1)/2} p$ so we can say that g_a is a *square root* of p^*. In particular, a square root of p^* lives in $\mathbf{Z}[\zeta_p]$.

Proof of Proposition 2. Evaluate $g_a g_{-a} = \left(\frac{-1}{p}\right) g^2$ if $(a,p) = 1$; and $= 0$ if p divides a. Now we deal with $\sum_a g_a g_{-a}$ in two ways:

(a) $\sum_a g_a g_{-a} = (p-1)\left(\frac{-1}{p}\right) g^2$.

(b) Also,

$$\sum_a g_a g_{-a} = \sum_a \sum_x \sum_y \binom{x}{p} \binom{y}{p} \zeta^{a(x-y)}.$$

$$= \sum_x \sum_y \binom{x}{p} \binom{y}{p} \sum_a \zeta^{a(x-y)}.$$

Here the summations are over (i.e., the variables a, x, y run through) a full set of residue classes mod p. Now, if $x - y \not\equiv 0 \bmod p$ then $\sum_a \zeta^{a(x-y)} = 0$, while if $x - y \equiv 0 \bmod p$ then $\sum_a \zeta^{a(x-y)} = p$ so the above triple sum becomes

$$\sum_a g_a g_{-a} = \sum_{x=y} \binom{x}{p} \binom{y}{p} \cdot p = (p-1)p.$$

So: $g^2 = \left(\frac{-1}{p}\right) p$; that is:

$g = \pm\sqrt{p}$ if $p \equiv 1 \bmod 4$, and
$g = \pm i\sqrt{p}$ if $p \equiv -1 \bmod 4$.

With what *sign*?

3.2 Discussion of the Kronecker-Weber Theorem

4 Recall: Algebraic numbers and algebraic integers

Discuss the basic tool for both concepts. Let $V \subset \mathbf{C}$ be a finitely generated module of rank $d > 0$ over $\mathbf{Q}$ (resp. $\mathbf{Z}$). Let $\alpha \in \mathbf{C}$ such that multiplication by α stabilizes V. Then α is an algebraic number (resp., algebraic integer) of degree $\leq d$. **Sketch of proof:** Choose a basis $x_1, x_2, \ldots, x_d$ and express α as a matrix (a_{ij}) relative to this basis noting that

$$\det(\alpha\delta_{ij} - a_{ij}) = 0$$

gives the relation that α satisfies to show it to be an algebraic number (resp., algebraic integer) of degree $\leq d$. Note also that any algebraic number is of the form α/D where α is an algebraic integer and $D \in \mathbf{Z}$ is a positive number.

5 Brief "recall" of field extensions, degree, and constructions

6 Cyclotomic Polynomials; cyclotomic fields in general

Discuss separability issues. Recall the theorem of Gauss that the cyclotomic polynomial $f_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ is irreducible over $\mathbf{Q}$. Discuss automorphism groups.

7 Finite Fields

Construct finite fields crudely as cyclotomic field extensions of prime fields. Now use the appropriate power of "Frobenius" to show that it is what you want. Prove that $\mathbf{F}_{p^d} = \mathbf{F}_p[\mu_{p^d-1}]$.

Theorem 2 *The polynomial*

$$X^{p^n} - X$$

is the product of all monic irreducible polynomials in $\mathbf{F}_p[X]$ *of degrees dividing* n.

Letting $N_d :=$ the number of monic irreducible polynomials in $\mathbf{F}_p[X]$ of degree d, then we have

$$p^n = \sum_{d \mid n} dN_d$$

and therefore, by Moebius inversion

$$N_n = \frac{1}{n} \sum_{d \mid n} \mu(n/d) p^d.$$

8 Proof of Quadratic Reciprocity via Gauss sums

Let p, q be odd (and different) primes. Let $g = g_1$ be the Gauss sum relative to the prime p (as above, so it is living in $\mathbf{Z}[\zeta_p]$). But watch out: we will be working in $\mathbf{Z}[\zeta_p]$ *modulo* $q \cdot \mathbf{Z}[\zeta_p]$ *in a moment. This is the ring*

$$\mathbf{Z}[\zeta_p]/q\mathbf{Z}[\zeta_p] = \mathbf{Z}/q\mathbf{Z}[X]/(f_p(X)) = \mathbf{F}_q[X]/(f_p(X))$$

where $f_p(X)$ is the cyclotomic polynomial as in section 6 above. Note that in this ring we have the Frobenius endomorphism $z \mapsto z^q$ and this will be playing a role. But let's go on for a second, in the ring $\mathbf{Z}[\zeta_p]$:

Form $g^{q-1} = (p^*)^{(q-1)/2}$ noting that it is an ordinary integer in $\mathbf{Z}[\zeta_p]$. Now pass to its image in $\mathbf{F}_q[X]/(f_p(X))$ and note that it is nothing more nor less than $\binom{p^*}{q} \in \mathbf{F}_q \subset \mathbf{F}_q[X]/(f_p(X))$.

Now multiply by g to get:

$$g^q = \binom{p^*}{q} g,$$

We evaluate g^q as the image under the Frobenius endomorphism of g, i.e.,

$$g^q = (\sum_{k=0}^{p-1} \binom{k}{p} \zeta_p^k)^q = \sum_{k=0}^{p-1} \binom{k}{p} \zeta_p^{qk} \equiv g_q = \binom{q}{p} g,$$

so

$$\binom{q}{p} g \;=\; \binom{p^*}{q} g.$$

We're not yet done because we want to get rid of the factor g, but no problem: multiply by g to get:

$$\binom{q}{p} p^* = \binom{q}{p} g^2 \;=\; \binom{p^*}{q} g^2 = \binom{p^*}{q} p^*,$$

and since p^* is a unit mod q, we're done.

Note: we could have done all this work in a finite field extension of $\mathbf{F}_q$ that contains the values of the Gauss sum g. This is the content of Section 3 of Chapter 7 of [**I-R**].