Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Lectures 28-29: Gauss Sums and Class Numbers
November 7-9, 2001

Reference. Lang, *Algebraic Number Theory*, Chapter IV, or Washington, *Introduction to Cyclotomic Fields*, Chapter 6. (Washington gives slightly more general results than we will.)

Outline of lectures.

Throughout, let ζ_n denote a primitive n-th root of unity, let p be a prime, let m be an integer not divisible by p, let l be the order of p mod m, let $q = p^l$, and let $\mathbb{F}_q$ be the finite field of q elements.

1. By a *character* we will mean a homomorphism $\chi : \mathbb{F}_q^* \to \mathbb{Q}(\zeta_{p(q-1)})^*$, which we extend to $\mathbb{F}_q$ by setting $\chi(0) = 0$. For any character χ, define the Gauss sum

$$G(\chi) = \sum_{a \in \mathbb{F}_q^*} \chi(a) \zeta_p^{\mathrm{Trace}(a)}$$

where the trace is from $\mathbb{F}_q$ to $\mathbb{F}_a$. For example, if $q = p$, we could take χ to be the quadratic character $\chi(a) = \left(\frac{a}{p}\right)$ and get back the usual Gauss sum. Note that if χ has order dividing m, then $G(\chi)$ takes values in $\mathbb{Q}(\zeta_{pm})$.

2. Work out some basic properties of the Gauss sums:
   (a) $G(\overline{\chi}) = \chi(-1)\overline{G(\chi)}$;
   (b) for $\chi \neq 1$, $g(\chi)g(\overline{\chi}) = \chi(-1)q$;
   (c) for $\chi \neq 1$, $g(\chi)\overline{g(\chi)} = q$;
   (d) $G(\chi^p) = G(\chi)$.

3. Given characters χ_1 and χ_2, define the Jacobi sum

$$J(\chi_1, \chi_2) = -\sum_{a \in \mathbb{F}_q} \chi_1(a)\chi_2(1-a).$$

Work out some basic properties of the Jacobi sums:
   (a) $J(1,1) = 2 - q$;
   (b) $J(1,\chi) = J(\chi, 1) = 1$ if $\chi \neq 1$;
   (c) $J(\chi, \overline{\chi}) = \chi(-1)$ if $\chi \neq 1$;
   (d) $G(\chi_1)G(\chi_2) = J(\chi_1,\chi_2)G(\chi_1\chi_2)$ if $\chi_1\chi_2 \neq 1$.

4. Note that if χ_1 and χ_2 have order dividing m that $G(\chi_1)G(\chi_2)/G(\chi_1\chi_2)$ is an algebraic integer in $\mathbb{Q}(\zeta_m)$ (not just in $\mathbb{Q}(\zeta_{pm})$).

5. Choose a prime $\mathfrak{p}$ of $\mathbb{Q}(\zeta_{pm})$ above (p) and a prime $\mathfrak{q}$ of $\mathbb{Q}(\zeta_{p(q-1)})$ above $\mathfrak{p}$, choose an isomorphism of the residue field of $\mathfrak{q}$ with $\mathbb{F}_q$, and let $\chi_{\mathfrak{q}}$ be the character such that $\chi_{\mathfrak{q}}(a) \equiv a^{-1} \pmod{\mathfrak{q}}$.

6. For $1 \leq \nu < q-1$, let $s(\nu)$ be the sum of the base p digits of ν. For future reference, observe that
$$s(\nu) = (p-1)\sum_{i=0}^{l-1} \left\{ \frac{p^i \nu}{q-1} \right\},$$
where the braces denote fractional part.

7. Show that $v_{\mathfrak{q}}(G(\chi_{\mathfrak{q}}^{\nu})) = s(\nu)$, by induction on ν, by checking that $v_{\mathfrak{q}}(\chi_{\mathfrak{q}}) = 1$ and that $v_{\mathfrak{q}}(J(\chi_{\mathfrak{q}}^{\nu-1}, \chi_{\mathfrak{q}})) = 0$ if ν is not divisible by p. This gives us an explicit formula for the prime factorization of the ideal $(G(\chi))$ for any character χ.

8. Let G be the Galois group of $\mathbb{Q}(\zeta_m)$ and let $\mathbb{Z}[G]$ and $\mathbb{Q}[G]$ be the group algebras of G over $\mathbb{Z}$ and $\mathbb{Q}$, respectively. (That is, these algebras are free with generators $[g]$ for each $g \in G$, multiplied by the rule $[g_1][g_2] = [g_1 g_2]$.) Define $\mathfrak{a}^{\beta}$ for $\mathfrak{a}$ a fractional ideal of $\mathbb{Q}(\zeta_m)$ and $\beta \in \mathbb{Z}[G]$ as follows: if $\beta = \sum z_i [g_i]$, then $\mathfrak{a}^{\beta} = \prod g_i(\mathfrak{a})^{z_i}$. Define the *Stickelberger element* of $\mathbb{Q}[G]$ by
$$\theta = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^*} \left\{ \frac{a}{m} \right\} \sigma_a^{-1},$$
where σ_a denotes the automorphism $\zeta_m \mapsto \zeta_m^a$.

9. Check that
$$(G(\chi_{\mathfrak{q}}^{(q-1)/m})) = \prod_{a \in (\mathbb{Z}/m\mathbb{Z})^*} \sigma_a^{-1}(\mathfrak{p})^{s(a(q-1)/m)},$$
where a runs over $(\mathbb{Z}/m\mathbb{Z})^*$. Deduce that $(G(\chi_{\mathfrak{q}}^{(q-1)/m})^m) = \mathfrak{p}^{m\theta}$. Then note that the generator of the ideal on the left actually lies in $\mathbb{Q}(\zeta_m)$. (It generates an extension of $\mathbb{Q}(\zeta_m)$ which is only ramified above primes dividing m, whereas $\mathbb{Q}(\zeta_{pm})/\mathbb{Q}(\zeta_m)$ is totally ramified above primes dividing p.)

10. Prove Stickelberger's theorem: if $\beta \in \mathbb{Z}[G]$ is such that $\beta\theta \in \mathbb{Z}[G]$ as well, then $\mathfrak{a}^{\beta\theta}$ is principal for any fractional ideal $\mathfrak{a}$ of $\mathbb{Q}(\zeta_m)$. It suffices to check this for $\mathfrak{a}$ prime and coprime to m (since such ideals generate the full class group; see a prior homework). In fact, if $\mathfrak{a} = \mathfrak{p} \cap \mathbb{Q}(\zeta_m)$, we have now shown that $\mathfrak{a}^{\beta\theta}$ is generated by $G(\chi_{\mathfrak{q}}^{(q-1)/m})^{\beta\theta}$. (The more general statement of the theorem is that the same thing happens in any subfield of $\mathbb{Q}(\zeta_m)$.)