ALGEBRAIC NUMBER THEORY W4043

Homework, week 8, due November 12

Refer to last week's homework for Dirichlet characters. However, this time we change notation: χ_0 is the unique Dirichlet character mod 1; in other words, $\chi_0(n) = 1$ for all n.

Let ζ be a primitive pth root of 1. For any $a \in \mathbb{F}_p{}^\times$ and any Dirichlet character χ modulo p (or χ_0 mod 1) define the *Gauss sum*

$$g_a(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x)\zeta^{ax}.$$

1. Show that $g_a(\chi) = \bar{\chi}(a) g_1(\chi)$. Show that $\overline{g_1(\chi)} = \chi(-1) g_1(\bar{\chi})$.

2. Show that $|g_1(\chi)|^2 = p$ if $\chi \neq \chi_0$, and thus that $|g_a(\chi)|^2 = p$ if $\chi \neq \chi_0$ for any a. (Hint: start out by writing

$$\begin{aligned}(p-1)|g_1(\chi)|^2 &= \sum_{a \in \mathbb{F}_p{}^\times} |g_a(\chi)|^2 = \sum_{a \in \mathbb{F}_p{}^\times} g_a(\chi)\overline{g_a(\chi)} \\ &= \sum_{a \in \mathbb{F}_p{}^\times} [\sum_{x \in \mathbb{F}_p} \chi(x)\zeta^{ax} \sum_{y \in \mathbb{F}_p} \bar{\chi}(y)\zeta^{-ay}] \ldots\end{aligned}$$

and then use the relations proved in last week's assignment.)

3. Let m be an integer prime to p such that $\chi^m = \chi_0$ (on elements of $\mathbb{F}_p{}^\times$). We let ζ_m be a primitive mth root of unity. For b any integer prime to m define $\sigma_b \in Gal(\mathbb{Q}(\zeta_m, \zeta)/\mathbb{Q})$ by $\sigma_b(\zeta_m) = \zeta_m^b$, $\sigma_b(\zeta) = \zeta$. Show that

$$g_1(\chi)^{b - \sigma_b} = \frac{g_1(\chi)^b}{\sigma_b(g_1(\chi))}$$

belongs to $\mathbb{Q}(\zeta_m)$. Conclude that $g_1(\chi)^m \in \mathbb{Q}(\zeta_m)$. Now let χ and λ be two Dirichlet characters mod p (or mod 1). Define the *Jacobi sum*

$$J(\chi, \lambda) = \sum_{a \in \mathbb{F}_p} \chi(a)\lambda(1-a).$$

4. Show that $J(\chi_0, \chi_0) = p$ and $J(\chi_0, \chi) = 0$ if $\chi \neq \chi_0$.

5. Show that $J(\chi, \chi^{-1}) = -\chi(-1)$ if $\chi \neq \chi_0$).

6. Show that if $\chi \neq \chi_0$, $\lambda \neq \chi_0$, and $\chi\lambda \neq \chi_0$, then

$$J(\chi, \lambda) = \frac{g_1(\chi) g_1(\lambda)}{g_1(\chi\lambda)}.$$

In particular

$$|J(\chi, \lambda)| = \sqrt{p}.$$

7. Let $a \in \mathbb{F}_p$ and let $N(x^n = a)$ denote the number of solutions in $\mathbb{F}_p$ to the equation $x^n = a \pmod{p}$. Suppose $n \mid (p-1)$. By classifying the various $a \in \mathbb{F}_p$, show that

$$N(x^n = a) = \sum_{\chi^n = \chi_0} \chi(a).$$

Let $p \equiv 1 \pmod{3}$ be a prime number. Let $\chi \neq \chi_0$ be a Dirichlet character mod p such that $\chi^3 = \chi_0$. Then χ_0, χ, and $\bar{\chi} = \chi^2$ are the three characters with the property $\chi^3 = \chi_0$. Let $N(x^3 + y^3 = 1)$ be the set of pairs $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ such that $x^3 + y^3 = 1$. Observe that

$$N(x^3 + y^3 = 1) = \sum_{a \in \mathbb{F}_p} N(x^3 = a) N(y^3 = 1 - a).$$

Using Jacobi sums, show that

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

In particular, the equation $x^3 + y^3 = 1$ has solutions mod p for all sufficiently large p.