ALGEBRAIC NUMBER THEORY W4043

Homework, week 8, due November 8

Dirichlet characters, continued

Notation is as in last week's homework.

1. We show that $X(p)$ is a cyclic group of order $p-1$ and that, for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, $a \neq 1$. there exists $\chi \in X(p)$ such that $\chi(a) \neq 1$.

(a) Bearing in mind that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group, show that $X(p)$ has at most $p-1$ elements.

(b) Show that $X(p)$ has the structure of abelian group.

(c) Let g be a cyclic generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and define a function $\lambda : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ by

$$\lambda(g^k) = e^{\frac{2\pi i k}{p-1}};\ \lambda(0) = 0.$$

Show that $\lambda \in X(p)$ and that, if n is the smallest positive integer such that $\lambda^n = \chi_0$, then $n = p-1$. Conclude that λ is a cyclic generator of $X(p)$.

(d) If $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $a \neq 1$ then $\lambda(a) \neq 1$.

2. Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, $a \neq 1$. Show that $\sum_{\chi \in X(p)} \chi(a) = 0$.

3. Let d be a divisor of $p-1$. Show that the set of $\chi \in X(p)$ such that $\chi^d = \chi_0$ is a subgroup of order d.

Congruences

4. Let n be a positive integer. A *quadratic form* in n variables $x_1, \ldots, x_n$ is a homogeneous polynomial Q of degree 2 in $x_1, \ldots, x_n$.

(a) For every $n > 0$, find a quadratic form Q_n in n variables with coefficients in $\mathbb{Z}$ such that the only rational solution to the equality

$$Q_n(a_1, \ldots, a_n) = 0$$

is the zero solution $a_1, \ldots, a_n$.

(b) Let $n \geq 3$ and p be a prime number, and let Q be a quadratic form in n variables with coefficients in $\mathbb{Z}$. Show that the congruence

$$Q(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

has a solution with $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ and not all a_i divisible by p.

(c) Let $Q(x, y)$ be a quadratic form in 2 variables with coefficients in $\mathbb{Z}$, let p be a prime number, and $a \in \mathbb{Z}$ an integer not divisible by p. Show that the congruence

$$Q(x, y) \equiv a \pmod{p}$$

has a solution.

(d) Find a homogeneous polynomial $F(X, Y, Z)$ of degree 3 with coefficients in $\mathbb{Z}$, with the property that, if

$$F(a, b, c) \equiv 0 \pmod{2}$$

with $a, b, c \in \mathbb{Z}$, then a, b, and c are all divisible by 2.