Mathematics W4043 Algebraic Number Theory
Assignment # 8

Benjamin Church

Worked With Matthew Lerner-Brecher

November 8, 2017

1. (a) Because $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, take a generator $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ then for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ we have that $a = g^n$ for some n so $\chi(a) = \chi(g)^n$. Thus for any Dirichlet character, χ is determined by $\chi(g)$ because $\chi(0) = 0$. However, $\chi(g)$ is a $(p-1)$-st root of unity in $\mathbb{C}$ so there are at most $p-1$ possible values of $\chi(g)$ and thus at most $p-1$ characters.

   (b) Take $\chi_1, \chi_2 \in X(p)$ and define $\chi_1 \cdot \chi_2$ to be the Dirichlet character $\chi_1 \cdot \chi_2 : a \mapsto \chi_1(a)\chi_2(b)$. This is a character because,

$$\chi_1 \cdot \chi_2 : ab \mapsto \chi_1(ab)\chi_2(ab) = \chi_1(a)\chi_2(a)\chi_1(b)\chi_2(b) = (\chi_1 \cdot \chi_2)(a)(\chi_1 \cdot \chi_2)(b)$$

   and since $(\chi_1 \cdot \chi_2)(a) \mapsto 0$ if and only if $\chi_1(a) = 0$ or $\chi_2(a) = 0$ if and only if $(a,p) \neq 1$. Furthermore, this operation is assoicative and commutative by properties of complex multiplication. For any $\chi \in X(p)$, the character $\chi \cdot \chi_0 = \chi$ because if $(a,p) = 1$ then $(\chi \cdot \chi_0)(a) = \chi(a)\chi_0(a) = \chi(a)$ and if $(a,p) \neq 1$ then $\chi(a) = 0$ and so $(\chi \cdot \chi_0)(a) = 0$. Also, consider the character $\bar{\chi} : a \mapsto \overline{\chi(a)}$ which is a character because $z \mapsto \bar{z}$ is an automorphism of $\mathbb{C}$. Futhermore, if $(a,p) = 1$ then $(\chi \cdot \bar{\chi})(a) = \chi(a)\overline{\chi(a)} = 1$ because $\chi(a)$ is a root of unity in $\mathbb{C}$ and therefore lies on the unit circle. If $(a,p) \neq 1$ then $(\chi \cdot \bar{\chi})(a) = \chi(a)\overline{\chi(a)} = 0$ so $\chi \cdot \bar{\chi} = \chi_0$. Thus, $X(p)$ contains an identity and inverses.

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

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

   Suppose that $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ then $ab, (\mathbb{Z}/p\mathbb{Z})^\times$ so we can write $a = g^n$ and $b = g^m$ so $ab = gn + m$ and thus,

$$\lambda(ab) = e^{\frac{2\pi i(n+m)}{p-1}} = e^{\frac{2\pi i n}{p-1}} e^{\frac{2\pi i m}{p-1}} = \lambda(a)\lambda(b)$$

   Furthermore, if $a = 0$ or $b = 0$ then $ab = 0$ so $\lambda(ab) = 0 = \lambda(a)\lambda(b)$. Thus for any $a, b \in \mathbb{Z}/ : \mathbb{Z}\lambda(ab) = \lambda(a)\lambda(b)$. Furthermore, if $a \equiv b \pmod p$ then if $p \mid a$ then $p \mid b$ so $\lambda(a) = 0 \iff \lambda(b) = 0$. If the residue class is nonzero, then $a \equiv g^n \pmod p$ and $b \equiv g^m \pmod p$ so $p \mid g^n - g^m = g^n(g^{n-m} - 1)$ so $g^{n-m} \equiv 1 \pmod{}$ and therefore, because g is a generator, $p-1 \mid n-m$ and thus,

$$\lambda(a) = e^{\frac{2\pi i n}{p-1}} = e^{\frac{2\pi i(m+(p-1)k)}{p-1}} = e^{\frac{2\pi i m}{p-1}} e^{2\pi i k} = e^{\frac{2\pi i m}{p-1}} = \lambda(b)$$

   By definition, $\lambda(a) = 0$ if and only if $a \notin (\mathbb{Z}/p\mathbb{Z})^\times$ if and only if $(a,p) \neq 1$. Thus, $\lambda \in X(p)$. Suppose that $\lambda^n = \chi_0$ then in particular, $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ so $\lambda^n(g) = 1$ and thus,

$(e^{\frac{2\pi i}{p-1}})^n = 1$ which holds when $n = p-1$ but if $n < p-1$ then $\lambda^n(g) = e^{2\pi i x}$ for $0 < x < 1$ which cannot equal 1. Thus, $\text{ord}(\lambda) = p-1$ and there are exactly $p-1$ elements of $X(p)$ so λ generates the group.

(d) Write $\lambda(g^k) = \zeta_{p-1}^k$ and $\lambda(0) = 0$. Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $a \neq 1$ then $a = g^k$ for $k < p-1$ and thus, $\lambda(g) = \zeta_{p-1}^k \neq 1$ because ζ_{p-1} is primitive.

2. Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $a \neq 1$. Because $X(p)$ is generated by λ,

$$\sum_{\chi \in X(p)} \chi(a) = \sum_{n=0}^{p-2} \lambda^n(a)$$

Write $a = g^k$ then plugging in for the action of λ,

$$\sum_{\chi \in X(p)} \chi(a) = \sum_{n=0}^{p-2} (\zeta_{p-1}^k)^n = \frac{(\zeta_{p-1}^k)^{p-1} - 1}{\zeta_{p-1}^k - 1}$$

However, ζ_{p-1}^k is a $(p-1)$-st root of unity and therefore a root of the polynomial $X^{p-1} - 1$. Furthermore, $a \neq 0$ so $\lambda(a) = \zeta_{p-1}^k \neq 1$ Thus, ζ_{p-1}^k is a root of $X^{p-1} - 1$ but not of $X - 1$ and therefore, ζ_{p-1}^k is a root of the polynomial,

$$\frac{X^{p-1} - 1}{X - 1}$$

so,

$$\sum_{\chi \in X(p)} \chi(a) = \frac{(\zeta_{p-1}^k)^{p-1} - 1}{\zeta_{p-1}^k - 1} = 0$$

3. Let $d \mid p-1$. Because $X(p)$ is a cylic it is abelian so by Lemma 0.1, $X(p)$ contains a subgroup H of all $\chi \in X(p)$ such that $\chi^d = \chi_0$. Furthermore, since $X(p)$ is cyclic, H is also cyclic. Also, $\kappa = \lambda^{\frac{p-1}{d}}$ has order d so $\kappa \in H$ and it has the maximum order because every elemet of H satisifies $\chi^d = \chi_0$ so κ generates H which thus must have order d.

4. (a) For $n > 0$, take $Q_n(X_1, \cdots, X_n) = X_1^2 + \cdots + X_n^2$ then if $Q_n(a_1, \cdots, a_n) = 0$ in $\mathbb{Z}$ we must have each $a_1 = 0$ because every term is positive.

(b) Let $n \geq 3$ and p be prime. Let Q be a quadratic form in n variables with coeficients in $\mathbb{Z}$. Because Q is quadratic, $\deg Q = 2 < n$ so we may apply Chevalley-Warning to conclude that the number of solutions to $Q(x_1, \cdots, x_n) = 0$ in $\mathbb{F}_p$ or equivalently, to $Q(x_1, \cdots, x_n) \equiv 0 \pmod{p}$ with solutions equal modulo p, is divisible by p. However, Q is homogeneous order 2 so $Q(0, \cdots, 0) = 0$ and thus, the number of solutions is non-zero and thus must be at least p. Therefore, there is a solution distinct modulo p from $(0, \cdot, 0)$ which must have the form $(a_1, \cdots, a_n)$ with not every $a_i \equiv 0 \pmod{p}$ i.e. not every $a_i \in \mathbb{Z}$ divisible by p.

(c) We want to prove that for any quadratic form $Q(x, y) = a^2 + bxy + cy^2$ the congruence $Q(x, y) \equiv m \pmod{p}$ has a solution for any integer $m \in \mathbb{Z}$ such that $p \not| a$.

I claim this proposition only holds under the assumption that $\Delta = b^2 - 4ac \not\equiv 0 \pmod{p}$. For example, $x^2 + 2xy + y^2 \equiv 2 \pmod{3}$ has no solutions becaue $x^2 + 2xy + y^2 = (x+y)^2$ is a square but 2 is not. This is because $b^2 - 4ac = 0$ which is divisible by p.

Under this assumption, the proof goes as follows. Consider the quadratic form in three variables, $\tilde{Q}(x,y,z) = ax^2 + bxy + cy^2 - mz^2$. Consider, $\tilde{Q}(x,y,z) \equiv 0 \pmod{p}$. Now, we want to show that this congruence has a soution with nonzero z in $\mathbb{F}_p$. Suppose that $(x,y,0)$ is a solution, then, $\mathbb{Q}(x,y) \equiv 0 \pmod{p}$.

First, consider the case that $p \mid a$. Then, $bxy + cy^2 \equiv 0 \pmod{p}$. The solutions are $(0,0,0)$ and $(-b^{-1}cy, y, 0)$ for any $y \in \mathbb{F}_p$ because $b^2 - 4ac \not\equiv 0 \pmod{p}$ and $p \mid a$ implies that $p \not| b$ and thus b^{-1} exists modulo p. Therefore, there are $p+1$ solutions.

In the case that $p \not| a$, if $y = 0$ then $ax^2 \equiv 0 \pmod{p}$ and $p \not| a$ so $x = 0$. This is one solution, $(0,0,0)$. If $y \neq 0$ then let $z \equiv xy^{-1} \pmod{p}$ then $az^2 + bz + c \equiv 0 \pmod{p}$ implies that $z = (2a)^{-1}\left[-b \pm \sqrt{b^2 - 4ac}\right]$. This has two solutions when $b^2 - 4ac$ is a square modulo p and no solutions otherwise. Now, $(zy, y, 0)$ is a solution. Therefore, the number of solutions is either 1 if $b^2 - 4ac$ is not a square (only the trivial solution) or $1 + 2(p-1) = 2p - 1$ (two for each nonzero y) when $b^2 - 4ac$ is a square.

In every case, the number of solutions with $z = 0$ is not divisible by p. However, because $\deg \tilde{Q} = 2 < 3$, by Chevalley-Warning, the total number of solutions is divisible by p. Thus, there exist solutions with $z \neq 0$ to $\tilde{Q}(x,y,z) \equiv 0 \pmod{p}$. Take such a solution (x,y,z). Then, $ax^2 + bxy + cy^2 - mz^2 \equiv 0 \pmod{p}$ so let $x' = z^{-1}x$ and $y' = z^{-1}y$ where the inverses exist because $z \not\equiv 0 \pmod{p}$. Thus, $(ax'^2 + bx'y' + cy'^2 - m)z^2 \equiv 0 \pmod{p}$ but $z \not\equiv 0 \pmod{p}$ so $ax'^2 + bx'y' + cy'^2 \equiv m \pmod{p}$. Therefore, there exists a solution to $Q(x,y) \equiv m \pmod{p}$.

(d) Let $F(X,Y,Z) = X^3 + Y^3 + Z^3 + XY^2 + YZ^2 + ZX^2 + XYZ$ which is homogeneous of order 3. I claim that the only solution in $\mathbb{F}_2$ to $F(a,b,c) = 0$ is $(0,0,0)$. Eqivalently, that if

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

for $a,b,c \in \mathbb{Z}$ then $2 \mid a,b,c$. We can check this property by considering the 8 possibilities for the residues of a,b,c modulo 2.

$$\begin{array}{ll}
(a,b,c) \equiv_2 (0,0,0) & F(a,b,c) \equiv_2 0+0+0+0+0+0+0 \equiv_2 0 \\
(a,b,c) \equiv_2 (1,0,0) & F(a,b,c) \equiv_2 1+0+0+0+0+0+0 \equiv_2 1 \\
(a,b,c) \equiv_2 (0,1,0) & F(a,b,c) \equiv_2 0+1+0+0+0+0+0 \equiv_2 1 \\
(a,b,c) \equiv_2 (0,0,1) & F(a,b,c) \equiv_2 0+0+1+0+0+0+0 \equiv_2 1 \\
(a,b,c) \equiv_2 (1,1,0) & F(a,b,c) \equiv_2 1+1+0+1+0+0+0 \equiv_2 1 \\
(a,b,c) \equiv_2 (0,1,1) & F(a,b,c) \equiv_2 0+1+1+0+1+0+0 \equiv_2 1 \\
(a,b,c) \equiv_2 (1,0,1) & F(a,b,c) \equiv_2 1+0+1+0+0+1+0 \equiv_2 1 \\
(a,b,c) \equiv_2 (1,1,1) & F(a,b,c) \equiv_2 1+1+1+1+1+1+1 \equiv_2 1
\end{array}$$

Therefore, the only solution modulo 2 is $(0,0,0)$.

Lemmas

Lemma 0.1. *Let A be an abelian group. For $n \in \mathbb{N}$, $A_n = \{a \in A \mid a^n = e\}$ is a subgroup of A.*

Proof. For any $n \in \mathbb{N}$, we have $e^n = e$ so $e \in A_n$. Also, if $a, b \in A$ then $(ab)^n = a^n b^n = e$ so $ab \in A_n$. Also, $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$ so $a^{-1} \in A_n$. Thus A_n is a subgroup of A. $\square$