Mathematics W4043 Algebraic Number Theory
Assignment # 7

Benjamin Church
Worked With Matthew Lerner-Brecher

December 13, 2017

1. (a) Take the quadratic form $aX^2 + bXY + cY^2$ with discriminant $\Delta = b^2 - 4ac = -7$ and $a \le \sqrt{|\Delta|/3} \approx 1.53$. Because $-7 \equiv 1 \pmod 4$ we know that b is odd. For $b = 1$, we have $1 - 4ac = -7$ so $4ac = 8$ and therefore, $ac = 2$. Thus, $a = 1$ and $c = 2$ under the requirement that $|b| \le a \le c$. We have the reduced solution $(1, 1, 2)$. No other values are possible because $|b| \le a \le \sqrt{|\Delta|/3}$ implies that $b = \pm 1$ or $b = 0$. However, b must be odd and in both cases when $|b| = 1$ we have $a = |b| = 1$ so $b \le 0$ by the definition of a reduced form.

   (b) Let $K = \mathbb{Q}(\sqrt{-7})$ and I be an ideal of $\mathcal{O}_K$ with a $\mathbb{Z}$ basis $\{\alpha_1, \alpha_2\}$. On assignment # 4, we proved that
$$q_I(a, b) = \frac{\mathrm{N}^K_{\mathbb{Q}}(a\alpha_1 + b\alpha_2)}{\mathrm{N}(I)}$$
is a quadratic form with discriminant $\Delta_I = \Delta_N$ where Δ_N is the discriminant of the quadratic form given by the norm over the standard basis $\{1, \delta\}$ where $\delta = \frac{1+\sqrt{-7}}{2}$ because $-7 \equiv 1 \pmod 4$. However, for $d \equiv 1 \pmod 4$ the field $K = \mathbb{Q}(\sqrt{d})$ has discriminant d (which equals the discriminant of the form $\mathrm{N}^K_{\mathbb{Q}}(x)$). Thus, $\Delta_I = -7$. However, by part (a), there is a single equivalence class of ideals with discriminant $\Delta = -7$. In particular, q_I must be equivalent to the reduced form $q(X, Y) = X^2 + XY + 2Y^2$. Therefore, there exist integers $r, s, t, u \in \mathbb{Z}$ such that $q(a, b) = q_I(ar + bs, at + bu)$. Let $a = 1$ and $b = 0$ then $q(a, b) = a^2 + ab + 2b^2 = 1$ and thus,
$$q_I(r, t) = \frac{\mathrm{N}^K_{\mathbb{Q}}(r\alpha_1 + t\alpha_2)}{\mathrm{N}(I)} = 1$$
Thus, $\mathrm{N}^K_{\mathbb{Q}}(r\alpha_1 + t\alpha_2) = \mathrm{N}(I)$. Let $\beta = r\alpha_1 + t\alpha_2$. Because $\alpha_1, \alpha_2 \in I$ we have that $\beta \in I$ so $(\beta) \subset I$ and therefore there exists and ideal J such that $(\beta) = IJ$. Thus, $\mathrm{N}(\beta\mathcal{O}_K) = \mathrm{N}(I)\mathrm{N}(J)$ but $\mathrm{N}(\beta\mathcal{O}_K) = \mathrm{N}^K_{\mathbb{Q}}(\beta) = \mathrm{N}(I)$ so $\mathrm{N}(J) = 1$. Therefore, $J = \mathcal{O}_K$ so $(\beta) = I\mathcal{O}_K = I$ so I is a pricipal ideal. Since every ideal of $\mathcal{O}_K$ is therefore principal, the class number of $K = \mathbb{Q}(\sqrt{-7})$ is 1.

   (c) The prime p can be represented by a quadratic form if and only if Δ, the discriminant, is a square modulo $4p$. If Δ is a square modulo $4p$, then Δ is a square modulo p and 4. Conversely, suppose that Δ is a square modulo 4 and modulo p (for odd p) then there are numbers a, b s.t. $\Delta \equiv a^2 \pmod 4$ and $\Delta \equiv b^2 \pmod p$ so by CRT there is a solution modulo $4p$ to $x \equiv a \pmod 4$ and $x \equiv b \pmod p$. Thus, $x^2 \equiv \Delta \pmod 4$ and $x^2 \equiv \Delta \pmod p$ so $x^2 \equiv \Delta \pmod{4p}$. For the case that $\Delta = -7$, because $-7 \equiv 1 \pmod 4$

is a square, p is represented iff $\left(\frac{\Delta}{p}\right) = 1$ or $\left(\frac{\Delta}{p}\right) = 0$. By quadratic reciprociy,

$$\left(\frac{\Delta}{p}\right) = \left(\frac{-7}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{7}{p}\right) = (-1)^{\frac{-8}{2}}\left(\frac{p}{7}\right) = \left(\frac{p}{7}\right)$$

Thus, p is represented iff $p \equiv 0, 1, 2, 4 \pmod{7}$. We have excluded $p = 2$ from the previous discussion and will now consider whether 2 is represented. Since $-7 \equiv 1 \pmod 8$ we have that -7 is a square modulo $4p$ for $p = 2$ so 2 is represented. Since an odd prime p is split in $\mathbb{Q}(\sqrt{d})$ iff $\left(\frac{d}{p}\right) = 1$, we have that every split prime is represented but $p = 7$ is ramified rather than split although 7 is also represented. Because $-7 \equiv 1 \pmod 8$, the prime $p = 2$ is split so we have that every prime excluding 7 is split if and only if it is represented.

2. Let $\chi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ be a Dirichlet character modulo p. Then for $1 \in \mathbb{Z}/p\mathbb{Z}$ we have $1 \cdot 1 = 1$ so $\chi(1)\chi(1) = \chi(1)$. Since $\mathbb{C}$ is a field, either $\chi(1) = 0$ or $\chi(1) = 1$. However, $(1, p) = 1$ so $\chi(1) \neq 0$ therefore $\chi(1) = 1$. By Lagrange's theorem, $\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times : a^{p-1} = 1$ therefore $\chi(a)^{p-1} = \chi(a^{p-1}) = \chi(1) = 1$ so $\chi(a)$ is a $(p-1)$-st root of unity.

3. Take $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ then $\exists a^{-1} \in (\mathbb{Z}/p\mathbb{Z})^\times$ so $\chi(a)\chi(a^{-1}) = \chi(aa^{-1}) = 1$. Because $\mathbb{C}$ is a field, $\chi(a^{-1}) = \chi(a)^{-1}$. However, for $z \in \mathbb{C}$, we have $z^{-1} = \frac{1}{|z|^2} \cdot \bar{z}$. However, $\chi(a)$ is a root of unity so, because the magnitude is multiplicative, $\chi(a)$ has magnitude 1. Thus, $\chi(a^{-1}) = \chi(a)^{-1} = \bar{\chi}(a)$.

4. Suppose that $\chi \neq \chi_0$. Now, $[a] \notin (\mathbb{Z}/p\mathbb{Z})^\times \iff (a, p) \neq 1 \iff \chi(a) = 0$ so,

$$\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(a)$$

However, $(\mathbb{Z}/p\mathbb{Z})^\times$ is a finite multiplicative subgroup of a field and therefore is cyclic. Take a generator $g \in (\mathbb{Z}/p\mathbb{Z})^\times$. Now, $(\mathbb{Z}/p\mathbb{Z})^\times = \{g^k \mid 0 \le k \le p-2\}$ so the sum is,

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(a) = \sum_{k=0}^{p-2} \chi(g^k) = \sum_{k=0}^{p-2} \chi(g)^k = \frac{\chi(g)^{p-1} - 1}{\chi(g) - 1}$$

However, $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ so $\chi(g)$ is a $(p-1)$-st root of unity and therefore a root of the polynomial $X^{p-1} - 1$. Furthermore, if $\chi(g) = 1$, then $\chi(a) = \chi(g^k) = \chi(g)^k = 1$ so $\chi = \chi_0$ which we assumed was false. Thus, $\chi(g)$ is a root of $X^{p-1} - 1$ but not of $X - 1$ and therefore, $\chi(g)$ is a root of the polynomial,

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

In full,

$$\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(a) = \sum_{k=0}^{p-2} \chi(g^k) = \sum_{k=0}^{p-2} \chi(g)^k = \frac{\chi(g)^{p-1} - 1}{\chi(g) - 1} = 0$$

5. Let $\chi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ be given by $\chi : a \mapsto \left(\frac{a}{p}\right)$ if $(p, a) = 1$ and $a \mapsto 0$ otherwise. The definining properties of a Dirichlet character follow from basic properties of the Legendre Symbol. First,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod p \implies \left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

Also, $p \mid ab \iff p \mid a$ or $p \mid b$ therefore $(ab, p) = 1 \iff (a, p) = 1$ and $(b, p) = 1$. Thus, $\chi(ab) = \chi(a)\chi(b)$ since if $(a, p) \neq 1$ then $(ab, p) \neq 1$ so $\chi(ab) = 0 = \chi(a)\chi(b)$. Furthermore, let $a \equiv b \pmod p$ then, if $p \mid a$ then $p \mid b$ and

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod p$$

Therefore, $\chi(a) = \chi(b)$. Finally, a and p have a common factor if and only if $p \mid a$ if and only if $\chi(a) = 0$. Thus, χ is a Dirichet character. Also, the kernel of the function $s : a \mapsto a^2$ has order 2 so the image of the function cannot be the entire ring $\mathbb{Z}/p\mathbb{Z}$. Therefore, there exists at least one quadratic non-residue so $\mathrm{Im}(\chi) = \{0, \pm 1\}$ so this function must be distinct from χ_0 which has image $\{0, 1\}$.