Primes - Problem Sheet 8 - Solutions

Genus theory revisited

Q1) Let $p \equiv 1 \pmod 8$ be prime.

i) Let $\mathcal{C}(-4p)$ be the class group of discriminant $D = -4p < 0$. Use genus theory to prove that

$$\mathcal{C}(-4p) \cong (\mathbb{Z}/2^a\mathbb{Z}) \times G\,,$$

where $\#G$ is odd, and $a \geq 1$. And hence $2 \mid h(-4p)$. Hint: recall the fundamental theorem for finitely generated abelian groups. How many elements of order 2 are in $\mathcal{C}(-4p)$?

ii) Use Gauss's definition of genus to show that

$$2x^2 + 2xy + ((p+1)/2)y^2$$

is in the principal genus. Hint: it is easier to use the Jacobi symbol, not the Legendre symbol.

iii) Use Theorem 8.4 to show $\mathcal{C}(-4p)$ has en element of order 4, hence conclude $4 \mid h(-4p)$.

Solution: i) Since $D = -4p$, $n = p \equiv 1 \pmod 8$, in particular $n \equiv 1 \pmod 4$. We have $\mu = r+1$, here $r = 1$ is the number of odd prime divisors of D. Hence $\mathcal{C}(D)$ has exactly $2^{\mu-1} = 2^1 = 2$ elements of order ≤ 2.

We can write $\mathcal{C} = (\mathbb{Z}/2\mathbb{Z})^{n_1} \times \cdots \times (\mathbb{Z}/2^l\mathbb{Z})^{n_l} \times G$, where $\#G$ odd, and $n_l \geq 1$.

An element of order 2 in $\mathcal{C}$ is $(0, \ldots, 0, 2^{l-1}, 0)$, so along with the identity we exhaust the 2 elements of order ≤ 2. There can be no more elements of order 2. Hence $n_1 = \ldots = n_{l-1} = 0$ (else take $n_i > 0$ and 2^{i-1} as the entry in coordinate i.) Similarly $n_l = 1$, else $n_l \geq 2$ and we can take $(x, \ldots x, g)$ for $x = 0, 2^{l-1}$ to get $2^{n_l} \geq 4$ elements of order ≤ 2.

So $\mathcal{C} = (\mathbb{Z}/2^a\mathbb{Z}) \times G$, with $a \geq 1$ (to get an element of order 2), and $\#G$ odd.

ii) This form certainly represents $(p+1)/2$. As $p = 8k+1$, the result $(p+1)/2 = 4k+1$ is odd, and not divisible by p, hence $\gcd(D, (p+1)/2) = 1$. We can therefore apply Gauss's complete character to the value $(p+1)/2$.

Now $D = -4p$ has $r = 1$ odd prime divisor, and $p = 8k+1 \equiv 1 \pmod 4$, so $\mu = r+1$. We therefore assign characters $\chi_1(a) = \left(\frac{a}{p}\right)$, and $\delta(a) = (-1)^{(a-1)/2}$.

Since $p = 8k+1$, we have $(p+1)/2 = 4k+1$. We compute

$$\delta(4k+1) = (-1)^{(4k)/2} = 1\,,$$

and

$$\chi_1(4k+1) = \left(\frac{4k+1}{p}\right) = 1\,.$$

It is easier to use the properties of the Jacobi symbol this time

$$\left(\frac{4k+1}{p}\right) = \left(\frac{p}{4k+1}\right)(-1)^{(p-1)/2(4k+1-1)/2} = \left(\frac{8k+1}{4k+1}\right) = \left(\frac{-1}{4k+1}\right) = (-1)^{(4k+1-1)/2} = 1$$

So this has the same complete character as the principal form x^2+py^2, which represents 1, and trivially has $\chi_1(1) = \delta(1) = 1$.

Thus $2x^2 + 2xy + ((p+1)/2)y^2$ is in the principal genus.

iii) We know that the forms in the principal genus arise by duplication, so already $f(x, y) = 2x^2 + 2xy + ((p + 1)/2)y^2 = g \circ g$, for some g. But since $p \equiv 1 \pmod 8$, we see $(p + 1)/2 = (8k + 2)/2 = 4k + 1$, $k \geq 1$, so is ≥ 5. The form $2x^2 + 2xy + ((p+1)/2)y^2$ is therefore reduced, and of discriminant $-4p$.

The form $2x^2 - 2xy + ((p + 1)/2)y^2$ is the inverse of this form, but is not reduced, as $|b| = a$, but $b < 0$. It is therefore properly equivalent to the original. So $f \circ f =$ principal, and in particular $g^{\circ 4} = f^{\circ 2} =$ principal. So the form which squares to $f(x, y)$ has order 4. Hence $4 \mid h(-4p)$.