Primes - Problem Sheet 6

Class number 1 and genus theory

Class number 1

Q1) Suppose $m > 1$ is an integer, and $m \neq p^r$ is not a prime power. Show that we can write $m = ac$, where $1 < a < c$, and $\gcd(a, c) = 1$.

Q2) In this exercise we will prove that $h(-4n) = 1$, for $n > 0$ if and only if $n = 1, 2, 3, 4, 7$.

i) Show that $h(-4n) = 1$ for these n, by listing the reduced forms.

ii) Suppose that n is not a prime power. Use the previous exercises to write down a second reduced form of discriminant $-4n$. Hint: $b = 0$.

iii) Suppose that $n = 2^r$. If $r \geq 4$, show that

$$4x^2 + 4xy + (2^{r-2} + 1)y^2$$

is reduced, and is primitive. Check that $h(-4n) > 1$, for $r = 3$, also.

iv) Suppose now that $n = p^r$, p an odd prime. Suppose $n + 1 = ac$, where $2 \leq a < c$, and $\gcd(a, c) = 1$. Show that

$$ax^2 + 2xy + cy^2$$

is reduced of discriminant $-4n$.

v) Finally, suppose that $n = p^r$, but that $n + 1 = 2^s$. If $s \geq 6$, show that

$$8x^2 + 6xy + (2^{s-3} + 1)y^2$$

is a reduced form of discriminant $-4n$. What happens for $s = 1, 2, 3, 4, 5$?

vi) Conclude that $h(-4n) = 1$ if and only if $n = 1, 2, 3, 4, 7$.

Elementary genus theory

Q3) Apply the idea from $p = x^2 + 5y^2$ from Example 6.6, or the general result from Theorem 6.11, to obtain congruence conditions for

- $p = x^2 + 6y^2$ and the other form of discriminant -24,
- $p = x^2 + 8y^2$ and the other form of discriminant -32,
- $p = x^2 + 21y^2$, and the other 3 forms of discriminant -84,
- $p = x^2 - 3y^2$, and the other form of discriminant 12,
- $p = x^2 - 10y^2$ and the other form of discriminant 40.
- $p = x^2 - 15y^2$ and the other 7 forms of discriminant 60.

Q4) It is not possible to obtain a congruence condition for $p = x^2 + 56y^2$, even by using the genus theory Theorem 6.11. What is the best result you can obtain for $p = x^2 + 56y^2$, and the other 7 forms of discriminant -224? Hint: it *is* possible to give congruence conditions for some of the forms.

Q5) Show that the values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$, a form of discriminant $D \equiv 1 \pmod 4$ form a coset of H (the values of the principal form), in $\ker \chi$.

Q6) It appears that this is more difficult than I expected!
~~Suppose that $f(x, y)$ and $g(x, y)$ are two binary quadratic forms of discriminant D. Suppose that $f(x, y)$ and $g(x, y)$ are $\mathrm{GL}_2(\mathbb{Q})$-equivalent, via a matrix whose entries have denominators all coprime to $2D$. Show that $f(x, y)$ and $g(x, y)$ represent the same values in $(\mathbb{Z}/N\mathbb{Z})^*$, for all non-zero N. Conclude that $f(x, y)$ and $g(x, y)$ are in the same genus.~~

Q7) Recall that $x^2 + 14y^2$ and $2x^2 + 7y^2$ are in the same genus, since they both represent $\{ 1, 9, 15, 23, 25, 39 \} \subset (\mathbb{Z}/56\mathbb{Z})^*$. Show that $x^2 + 14y^2$ and $2x^2 + 7y^2$ are $\mathrm{GL}_2(\mathbb{Q})$-equivalent, as forms over the rational numbers. (Hint: denominator 5 works.) Conclude, in particular, that congruence conditions can never separate the primes represented by $x^2 + 14y^2$ and $2x^2 + 7y^2$.

Q8) Show that $2x^2 + 9x^2$ and $x^2 + 18y^2$ are $\mathrm{GL}_2(\mathbb{Q})$-equivalent, as forms over the rational numbers. (Hint: denominator 9 works.) Show however, that $2x^2 + 9y^2$ and $x^2 + 18y^2$ are in different genera. (If they represent the same vaues in $(\mathbb{Z}/72\mathbb{Z})^*$, then the same holds for any divisor of 72.) What differs from the previous exercise?