Primes - Problem Sheet 6 - Solutions

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 $\gcd(a, c) = 1$.
Solution: If $m \neq p^r$, then it has ≥ 2 prime factors. Write $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then $k \geq 2$, and we take $a = p_1^{e_1}$ and $c = p_2^{e_2} \cdots p_k^{e_k}$. If $a > c$, then swap the two factors. We also have $\gcd(a, c) = 1$ since no prime is shared between a and c.

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.
Solution: This was dealt with on the previous solution sheet.

ii) Suppose that n is not a prime power. Use the previous exercises to write down a second reduced form of discriminant $-4n$. Hint: $b = 0$.
Solution: If $n \neq p^r$, then we can write $n = ac$, with $a < c$ and $\gcd(a, c) = 1$. Then $ax^2 + cy^2$ is a reduced form of discriminant $0^2 - 4ac = -4n$.

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.
Solution: On the previous sheet, we saw $h(-32) = 2$ which has $r = 3$.
We see that $\gcd(4, 4, 2^{r-2} + 1) = 1$, since $2^{r-2} + 1$ is odd. So this form is primitive.
To be reduced, we need $|b| \leq a \leq c$. For $r \geq 4$, we get $c \geq 2^2 + 1 = 5$. Since $b = 4 > 0$, the edge case automatically holds.
So we get $r = 0, 1, 2$ corresponding to $n = 1, 2, 4$.

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 $-4n$.
Solution: We certainly have $\gcd(a, 2, c) = 1$ since $\gcd(a, c) = 1$. So the form is primitive. It is reduced since $2 \leq a < c$ by hypothesis. Finally, the discriminant is $D = b^2 - 4ac = 2^2 - 4ac = 4 - 4(n + 1) = -4n$.

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 $s = 1, 2, 3, 4, 5$?

Solution: It is primitive, since the first coefficients are even, and the last coefficient is odd. (2^{s-3} is even, when $s \geq 4$.) It is reduced as $b = 6 < a = 8 < 2^3 + 1 = 9 \leq c$. THe discriminant is

$$6^2 - 4 \cdot 8 \cdot (2^{s-3} + 1) = 4 - 4 \cdot 2^s = 4 - 4(n+1) = -4n\,.$$

The cases $s = 1, 2, 3, 4, 5$ correspond to $n = 1, 3, 7, 15, 31$. Since 15 is not a prime power, it is deal with by the previous part. Finally $h(-4 \cdot 31) = 3$ by explicit computation.

vi) Conclude that $h(-4n) = 1$ if and only if $n = 1, 2, 3, 4, 7$.
Solution: The explicit check shows that $n = 1, 2, 3, 4, 7$ implies $h(-4n) = 1$. We have also deal with the other cases: if n is not a prime power, $h > 1$. If n is a prime power, then either $n + 1$ is not, and $h > 1$ when $n \neq 1, 2, 4$. Or $n + 1$ is, and so it must be 2^r and $h > 1$ when $n \neq 1, 3, 7$.
Thus $h(-4n) = 1$ iff $n = 1, 2, 3, 4, 7$, as claimed.

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.

Solution: We treat only $x^2 + 21y^2$ because the other cases are similar. The 4 forms are

$$x^2 + 21y^2, 2x^2 + 2xy + 11y^2, 3x^2 + 7y^2, 5x^2 + 4xy^2 + 5y^2\,.$$

Using QR, we have $\left(\frac{-84}{p}\right) = 1$ iff $p \equiv 1, 5, 11, 17, 19, 23, 25, 31, 37, 41, 55, 71 \pmod{84}$.

Reducing modulo 3 and 7, we see $p = x^2 + 21y^2$ must be $1 \pmod 3$ and $1, 2, 4$ mod $*\,7$. This means $p = x^2 + 21y^2$ represents (at most) $1, 25, 37 \pmod{84}$. There are 4 forms, each representing at most 3 values. But we have 12 values to hit. So each form represents a distinct coset, and each coset has size 3. The second form represents 11, so would give the coset $11\,\{\,1, 25, 37\,\} = \{\,11, 23, 71\,\}$. The fourth form represents 5, so gives the coset $5\,\{\,1, 25, 37\,\} = \{\,5, 17, 41\,\}$. The third form therefore must represent the remaining values, i.e. the coset $\{\,19, 31, 55\,\}$.

By the genus theory theorem, we obtain for $p \neq 2, 3, 7$, that

$$\begin{aligned} p = x^2 + 21y^2 &\iff p \equiv 1, 25, 37 \pmod{84} \\ p = 2x^2 + 2xy + 11y^2 &\iff p \equiv 11, 23, 71 \pmod{84} \\ p = 3x^2 + 7y^2 &\iff p \equiv 19, 31, 55 \pmod{84} \\ p = 5x^2 + 4xy + 5y^2 &\iff p \equiv 5, 17, 41 \pmod{84} \end{aligned}$$

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.
Solution: Using genus theory, we obtain the following

$$p = \begin{cases} x^2 + 56y^2 \\ 8x^2 + 8xy + 9y^2 \end{cases} \iff p \equiv 1, 9, 25, 57, 65, 81, 113, 121, 137, 169, 177, 193 \pmod{224}$$

$$p = \begin{cases} 4x^2 + 4xy + 15y^2 \\ 7x^2 + 8y^2 \end{cases} \iff p \equiv 15, 23, 39, 71, 79, 95, 127, 135, 151, 183, 191, 207 \pmod{224}$$

which can't be improved upon.

But we also obtain

$$p = \left\{ 3x^2 \pm 2xy + 19y^2 \right. \iff p \equiv 3, 19, 27, 59, 75, 83, 115, 131, 139, 171, 187, 195 \pmod{224}$$

$$p = \left\{ 5x^2 \pm 4xy + 12y^2 \right. \iff p \equiv 5, 13, 45, 61, 69, 101, 117, 125, 157, 173, 181, 213 \pmod{224}$$

both of which give pure congruence conditions valid for each of the individual forms: the forms differing by $\pm$ obviously represent the same values.

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 $\ker \chi$.
Solution: Form $f(x, y) = ax^2 + bxy + cy^2$ has discriminant $D \equiv 1 \pmod 4$. So b is odd, write $b = 2b' - 1$. Then we have

$$af(x, y) = (ax + b'y)^2 + (ax + b'y)(-y) + n(-y)^2 ,$$

and the same argument as before works.

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.~~
Solution: ~~If $f(ax + by, cx + dy) = g(x, y)$ for some matrix $\frac{1}{m}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$, then by reducing modulo N, where $N \nmid m$, where m is the denominator lcm, we see they represent the same values in $(\mathbb{Z}/N\mathbb{Z})$.~~

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 $2x^2 + 7y^2$.
Solution: We have $(\frac{-6}{5}x - \frac{7}{5}y)^2 + 14(\frac{1}{5}x - \frac{3}{5}y)^2 = 2x^2 + 7y^2$, adn the matrix

$$\frac{1}{5}\begin{pmatrix} -6 & -7 \\ 1 & -3 \end{pmatrix}$$

has determinant 1, so is in $\mathrm{GL}_2(\mathbb{Q})$. Since the denominator 5 is coprime to $2 \cdot D = -2^3 \cdot 7$, the previous exercise applies, and shows that $x^2 + 14y^2$ and $2x^2 + 7y^2$ represent the same values in $(\mathbb{Z}/N\mathbb{Z})^*$. So congruences can not separate them.

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?

Solution: We have $2(\frac{-6}{9}x - \frac{9}{9}y)^2 + 9(\frac{1}{9}x - \frac{12}{9}y)^2 = x^2 + 18y^2$. Moreover, the matrix

$$\frac{1}{9}\begin{pmatrix} -6 & 9 \\ 1 & 12 \end{pmatrix}$$

has determinant $1 \neq 0$, so is in $\mathrm{GL}_2(\mathbb{Q})$.

However, modulo 3, we see that $2x^2 + 9x^2 \equiv 2x^2 \pmod 3$ so represents $2 \cdot 1^2 = 2$. Whereas $x^2 + 18y^2 \equiv x^2 \pmod 3$ so represents $1^2 = 1$. These two forms can't be in the same genus.