Primes - Problem Sheet 5 - Solutions

Class number, and reduction of quadratic forms

Positive-definite

Q1) Apply the proof of Theorem 5.5 to find reduced forms equivalent to the following, also give matrices which show the equivalence:

- $6x^2 - 2xy + y^2$
- $10x^2 - 10x + 3y^2$
- $5x^2 - 10xy + 6y^2$
- $5x^2 + 6xy + 3y^2$
- $2x^2 + 4xy + 5y^2$
- $x^2 + 2xy + 7y^2$
- $8x^2 - 2xy + y^2$

Solution: These are all very similar, so we only treat the first part.

- We can make a smaller by applying S to get

$$x^2 + 2xy + 6y^2 \, .$$

Now we can make b smaller by applying T^{-1}, giving

$$x^2 + 5y^2 \, .$$

And this is reduced.
We applied $ST^{-1} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix} \right)$. So we find

$$f(y, -x + y) = x^2 + 5y^2$$

under this change of basis.

Q2) Check that the following, for discriminant $D < 0$ are always reduced forms

- For $D \equiv 0 \pmod 4$, the form $x^2 - \frac{D}{4}y^2$,
- For $D \equiv 1 \pmod 4$, the form $x^2 + xy + \frac{1-D}{4}y^2$.

These are called the *principal forms*. For $D > 0$, these forms are not reduced, but we still call them the *principal forms*. (These forms correspond to the principal ideal class in quadratic number fields. See handout 2.)

Solution: This is a direct check of what reduced means: $|b| \leq a \leq c$ holds for the first since $|b| = |0| = 0 \leq a = 1 \leq c = -D/4$, since $-D/4 \geq 1$. $D < 0$ so $-D > 0$, and $-D/4$ is an integer. Since $b = 0$, the edge cases hold automatically.

Similarly for the second case $|b| = 1 \leq a = 1$, and $a = 1 \leq c = (1 - D)/4$, since $D < 0$, and $(1 - D)/4$ is an integer. Since $b = 1 > 0$, the edge cases also hold.

Q3) Suppose that $f(x) = ax^2 + bxy + cy^2$ is a positive-definite binary quadratic form of discriminant $D < 0$. Suppose $a < \sqrt{-D/4}$ and $-a < b \leq a$. Show that f is reduced.

Solution: The conditions for reduced require $|b| \leq a$ and $a \leq c$, with some edge cases. From the hypothesis, we get $|b| \leq a$, and if $|b| = a$, then $b = a > 0$.

Now we have

$$c = \frac{b^2 - D}{4a} \geq -D/4a > a^2/a = a\,,$$

and there is no edge case to check with $a = c$.

So f is reduced.

Q4)

- Verify the following table of class numbers (in the positive definite case), by listing all reduced forms of the given discriminant.

D	$h(D)$	D	$h(D)$
-3	1	-4	1
-7	1	-8	1
-11	1	-12	1
-15	2	-16	1
-19	1	-20	2
-23	3	-24	2
-27	1	-28	1
-31	3	-32	2
-35	2	-36	2
-39	4	-40	2

- Write a computer program to extend this to all discriminants $-32768 < D < 0$. Hint: $h(-32767)$ is divisible by 13. (Runtime of about 30 minutes, is fine)

Solution: The reduced forms of discriminant $D = -32$ are given by the following table

a	b	c	Primitive?	Reduced?
1	0	8	✓	✓
2	0	4		✓
3	2	3	✓	✓
3	2	3	✓	

So there are 2 primitive reduced forms, confirming the number above.

Q5) The entries above for $D = -4, -8, -12$ correspond to Fermat's x^2+y^2, x^2+2y^2 and $x^2 + 3y^2$ theorems, which we now have powerful techniques to prove. Since $h(D) = 1$ for $D = -3, -7, -11, -16, -19, -27$ and -28, we obtain corresponding results for these cases.

i) State and prove congruence conditions on when a prime p can be represented by

- $x^2 + xy + y^2$, of discriminant -3,
- $x^2 + xy + 2y^2$, of discriminant -7,
- $x^2 + xy + 3y^2$, of discriminant -11,
- $x^2 + 4y^2$, of discriminant -16,
- $x^2 + xy + 5y^2$, of discriminant -19,
- $x^2 + xy + 7y^2$, of discriminant -27,

- $x^2 + 7y^2$, of discriminant -28.

Solution: We deal only with the case $x^2 + xy + 3y^2$ as the results are all very similar.
From our criterion/corollary, we have that for $p \neq 2, 11$

$$p = x^2 + xy + 3y^2$$

if and only if $\left(\frac{-11}{p}\right) = 1$. (Since this is the only form of discriminant -11.)
Using quadratic reciprocity, we have

$$\left(\frac{11}{p}\right)\left(\frac{p}{11}\right) = (-1)^{(p-1)/2\cdot(11-1)/2} = (-1)^{(p-1)/2} = \left(\frac{-1}{p}\right)$$

So

$$\left(\frac{-11}{p}\right) = \left(\frac{p}{11}\right) = 1$$

if and only if $p \equiv \Box \pmod{11}$, and this is if and only if $p \equiv (\pm 1)^2, \ldots (pm5)^2 = 1, 3, 4, 5, 9 \pmod{11}$.

ii) Show directly that the result $p = x^2 + 4y^2$ where $D = -16$ is (trivially) equivalent to result for $p = x^2 + y^2$ where $D = -4$.
Solution: The result we obtain is for $p \neq 2$, that $p = x^2 + 4y^2$ iff $p \equiv 1 \pmod 4$. But also the result that $p = x^2 + y^2$ iff $p \equiv 1 \pmod 4$.
If we can write $p = x^2 + 4y^2$, then certainly $p = x^2 + (2y)^2$. But if we have $p = x^2 + y^2$. Reducing modulo 2 shows that $1 = x^2 + y^2$, so one of x and y is even. Can't both be odd else the result is 0 modulo 2! Say $y = 2y'$ even, then

$$p = x^2 + 4(y')^2 .$$

So the $x^2 + 4y^2$ result follows directly from the $x^2 + y^2$ result.

iii) Similarly show the result for $p = x^2 + 7y^2$ with $D = -28$ is (trivially) equivalent to the result for $p = x^2 + xy + 2y^2$ with $D = -7$. Hint: reduce modulo 2 to show y is even in $x^2 + xy + 2y^2$, then write $x^2 + xy + 2y^2 = (x + y/2)^2 + 7(y/2)^2$.
Solution: The $p = x^2 + 7y^2$ result says that for $p \neq 2, 7$, we have

$$p = x^2 + 7y^2 \iff p \equiv 1, 2, 4 \pmod 7 ,$$

while the $p = x^2 + xy + y^2$ says that for $p \neq 2, 7$, we have

$$p = x^2 + xy + y^2 \iff p \equiv 1, 2, 4 \pmod 7 .$$

If we can write $p = x^2 + xy + 2y^2$, then reducing modulo 2 gives $1 = x^2 + xy = x(x + y)$. If y is odd, then x and $x + y$ have different parities, so one is even, giving 0 modulo 2. Hence $y = 2y'$ is even. Now we get

$$p = (x + y')^2 + 7(y')^2 .$$

But then, if

$$p = x^2 + 7y^2 ,$$

we may write

$$p = (x - y)^2 + (x - y)(2y) + 2(2y)^2 = x'^2 + x'y' + 2(y')^2 ,$$

where $x' = x - y$ and $y' = 2y$.

Q6) Suppose that the positive-definite form $f(x, y)$ represents the value 1. Show that $f(x, y)$ is equivalent to the principal form (recall this is: either $x^2 + ny^2$, for discriminant $D = -4n$, or $x^2 + xy + ny^2$,for discriminant $D = -4k + 1$).

What about if $f(x, y)$ is an indefinite form?

Solution: Since $f(x_0, y_0) = 1$ represents 1, it must represent 1 properly (as $d^2 \mid 1 \implies d = 1$, where $d = \gcd(x_0, y_0)$). Hence $f(x, y)$ is equivalent to $x^2 + bxy + cy^2$. For $D \equiv 0 \pmod 4$, we have $b \equiv 0 \pmod 2$. By changing $x \to x + ky$, we change $b \to b + 2k$. Thus, we can choose $b = 0$. This proves $f(x, y)$ equivalent to $x^2 - \frac{D}{4}y^2$.

If $D \equiv 1 \pmod 4$, we have $b \equiv 1 \pmod 2$. By so we can choose $b = 1$, which proves $f(x, y)$ is equivalent to $x^2 + xy + \frac{1-D}{4}y^2$. This holds for positive-definite, or indefinite forms.

Q7) Suppose p is a prime number, represented by two forms $f(x, y)$ and $g(x, y)$ of discriminant D (positive-definite, or indefinite). Show that $f(x, y)$ and $g(x, y)$ are equivalent (possibly improperly equivalent). Hint: use Lemma 4.19, and examine the middle coefficient modulo p.

Solution: Any representation of a prime is proper (otherwise $d^2 \mid p$!) Hence the form f is equivalent to $px^2 + m_1xy + c_1y^2$, and g to $px^2 + m_2xy + c_2y^2$.

We know that $m_1^2 - 4pc_1 = D = m_2^2 - 4pc_2$, so that modulo p, we have $m_1^2 \equiv m_2^2 \pmod p$, i.e. $m_1 = \pm m_2 \pmod p$. We can put m_i into the range $-p \le m_i \le p$, so we can assume $m_1 = \pm m_2$ with exact equality, not just congruence.

If $m_1 = m_2$, then the forms f and g are properly equivalent. If $m_1 = -m_2$, then the forms are improperly equivalent. (Because $m_1^2 = m_2^2$, so $c_1 = c_2$ follows.)

Q8) By considering reduced forms, of the form $ax^2 + cy^2$. Show that the class number of discriminant D can be arbitrarily high. Hint: consider $D = -4p_1p_2 \cdots p_k$, where p_i are distinct primes.

Solution: Choose n distinct primes $p_1, \ldots, p_n$, and wrie $D = -4p_1 \ldots p_n$. There are 2^n ways to write $p_1 \ldots p_n = ac$, by choosing which factors appear in a. Since the primes are distinct, $a \neq c$, so by swapping, we get 2^{n-1} ways of writing with $a < c$.

But the form $ax^2 + cy^2$ is reduced, so we have $h(D) \ge 2^{n-1} \to \infty$ as $n \to \infty$. Hence $h(D)$ can be arbitrarily large.

Indefinite

Q9) Imitate the proof of Theorem 5.5 to show that every indefinite quadratic form of some discriminant D is equivalent to one of the form $ax^2 + bxy + cy^2$ with $|b| \le |a| \le |c|$. Moreover, show that such a form has $ac < 0$ and $|a| \le \frac{1}{2}\sqrt{D}$.

Solution: Fix an equivalence class of indefinite forms, and look at the $|a|$ values. Find a form with minimal $|a|$. We must have $|a| \le |c|$, else we can get smaller $|a|$ by changing $(x, y) \to (y, -x)$ sending $ax^2 + bxy + cy^2 \to cx^2 - bxy + ay^2$.

Now we can put b into the range $-|a| \le b \le |a|$ by using the transformation $(x, y) \mapsto (x + ky, y)$. This does not change $|a|$, so we get $|b| \le |a| \le |c|$.

We now have $b^2 = |b|^2 \leq |ac|$, and $b^2 - 4ac > 0$ by definition. Thus $4ac < b^2 < |ac|$, and we must have $ac < 0$.

From here, we have $|ac| = -ac$, so $D = b^2 - 4ac = b^2 + 4|ac| > 0$, and $4|ac| = D - b^2 < D$. Then $a^2 = |a|^2 \leq |ac|$, so $4a^2 < D$, or equivalently $a < \frac{1}{2}\sqrt{D}$.

Q10) If $ax^2 + bxy + cy^2$ is a reduced indefinite binary quadratic form, show that

- $|a| + |c| < \sqrt{D}$,
- $|a|, b, |c| < \sqrt{D}$, and
- $ac < 0$.

Solution: For i), we have

$$|a| + |c| - \sqrt{D} = \frac{D - 4|D|\sqrt{D} + 4a^2 - b^2}{4|a|} = \frac{(\sqrt{D} - 2|a|)^2 - b^2}{4|a|},$$

so by the definition of reduced, this is < 0.

Then we get ii) automatically. (The condition on b is part of the definition.)

For iii) make use of $b < \sqrt{D}$, to get $ac = (b^2 - D)/4 < 0$.

Q11)

- Verify the following table of class numbers (in the indefinite case), by listing all reduced forms of the given discriminant and partitioning them into ρ-orbits.

D	$h^+(D)$	D	$h^+(D)$
5	1	8	1
12	2	13	1
17	1	20	1
21	2	24	2
28	2	29	1
32	2	33	2
37	1	40	2
41	1	44	2
45	2	48	2
52	1	53	1
56	2	57	2
60	4		

- Write a computer program to extend this to all non-square discriminants $0 < D < 32768$.

Solution: We only give the table for discriminant $D = 40$, since all cases are very similar.

The reduced forms are given by the following

a	b	c
-3	2	3
-3	4	2
-2	4	3
-1	6	1
1	6	-1
2	4	-3
3	2	-3
3	4	-2

Under ρ, we find

$$(-3,2,3) \mapsto (3,4,-2) \mapsto (-2,4,3) \mapsto (3,2,-3)$$
$$\mapsto (-3,4,2) \mapsto (2,4,-3) \mapsto (-3,2,3)$$

and

$$(-1,6,1) \mapsto (1,6,-1) \mapsto (-1,6,1)$$

So there are two equivalence classes, giving $h^{(+)}(40) = 2$.

Q12) The entry for $D = 8$ corresponds to the result for $p = x^2 - 2y^2$, as given in Problem Sheet 2. The entry for $D = 20$ corresponds to our result above for $p = x^2 - 5y^2$. Since $h^+(D) = 1$ for $D = 5, 13, 17, 20, 29, 7, 41, 52, 53$, we obtain corresponding results for these cases.

i) State and prove congruence conditions on when a prime p can be represented by
- $x^2 + xy - y^2$ of discriminant $D = 5$,
- $x^2 + xy - 3y^2$ of discriminant 13,
- $x^2 + xy - 4y^2$ of discriminant 17,
- $x^2 + xy - 7y^2$ of discriminant 29,
- $x^2 + xy - 9y^2$ of discriminant 37,
- $x^2 + xy - 10y^2$ of discriminant 41,
- $x^2 - 13y^2$ of discriminant 52,
- $x^2 + xy - 13y^2$ of discriminant 53.

Solution: We deal only with $D = 41$, since all cases are very similar. For $p \neq 2, 41$, we have $p = x^2 + xy - 10y^2$ iff $\left(\frac{41}{p}\right) = 1$. By QR

$$\left(\frac{41}{p}\right)\left(\frac{p}{41}\right) = (-1)^{(p-1)/2 \cdot (41-1)/2} = 1\,,$$

so

$$\left(\frac{41}{p}\right) = \left(\frac{p}{41}\right) = 1 \iff p \equiv \square \pmod{41}])\,.$$

And this is iff

$$p \equiv 1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39 \pmod{41}40$$

ii) Derive a result for $x^2 - 17y^2$ using the result for $x^2 + xy - 4y^2$. Hint: reduce $x^2 + xy - 4y^2$ modulo 2 to show y is even, and write $x^2 + xy - 4y^2 = (x + \frac{y}{2})^2 - 17(\frac{y}{2})^2$.
Solution: This is similar to the next question, see that solution.

iii) Derive a result for $x^2 - 41y^2$ using the result for $x^2 + xy - 10y^2$.
Solution: For $p \neq 2, 41$, I claim that the condition for $x^2 - 41y^2$ is the same as for $x^2 + xy - 10y^2$.
Since $p = x^2 + xy - 10y^2$ modulo 2, gives $1 = x^2 + xy = x(x + y)$, we sees y is even. (Else x and $x + y$ have the same parity.)

Then write $p = (x + y/2)^2 - 41(y/2)^2$.
Now given $p = x^2 - 41y^2$, we can write

$$p = x'^2 + x'y' - 10y'^2 \,,$$

where $x' = x - y$, and $y' = 2y$.

Q13) Suppose that $D = 8k+1$ is a discriminant, and that $h^+(D) = 1$. By considering the primes which $x^2 + xy - 2ky^2$ represents, show that every binary quadratic form of discriminant $4D$ is equivalent to x^2-2ky^2. Hence conclude $h^+(4D) = 1$. (You may assume that any primitive integral binary quadratic form attains a prime value - this follows from the Chebotarev density theorem.)

Solution: For odd primes $p \nmid D$, the primes represented by $x^2 + xy - 2ky^2$ are characterised by $\left(\frac{D}{p}\right) = 1$. But given

$$p = x^2 + xy - 2ky^2 \,,$$

reducing mod 2 shows that

$$1 \equiv x(x + y) \,.$$

Therefore we must have the y is even, otherwise x is even, or x is odd, and $x + y$ is even. Now we can write

$$p = (x + y/2)^2 - (8k + 1)(y/2)^2$$

so that p is represented by $x^2 - (8k + 1)y^2$. Now given $p = x^2 - (8k + 1)y^2$, we can write

$$p = (x - y)^2 + x(2y) - 2k(2y)^2 \,,$$

so that p is represented by $x^2 + xy - 2ky^2$. We now say

$$p = \text{some BQF of discriminant } 4D \iff \left(\frac{4D}{p}\right) = 1 \iff \left(\frac{D}{p}\right) = 1 \iff p = x^2-(8k+1)y^2 \,.$$

So any BQF of discriminant $4D$ (which represents a prime!) must be equivalent (or improperly equivalent) to $x^2-(8k+1)y^2$. Since $x^2-(8k+1)y^2$ is improperly equivalent to itself via $x \mapsto -x$, we have actually that such a form must be properly equivalent to $x^2 - (8k + 1)y^2$.

Finally, we need to see that any BQF attains a prime value! But we are allowed to assume this. (It follows from the Chebotarev Density Theorem. Is there another way to see this?)