# Primes - Problem Sheet 5

## 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:

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

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.)

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.

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)

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 $-28$.

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 $D = -4$.

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 $x^2 + xy + 2y^2 = (x + y/2)^2 + 7(y/2)^2$.

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?

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 $p$.

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.

## 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 $|a| \le \frac{1}{2}\sqrt{D}$.

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
- $ac < 0$.

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 $\rho$-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 $0 < D < 32768$.

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,
- $x^2 + xy - 1y^2$ of discriminant 53.

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 $x^2 + xy - 4y^2 = (x + \frac{y}{2})^2 - 17(\frac{y}{2})^2$.

iii) Derive a result for $x^2 - 41y^2$ using the result for $x^2 + xy - 10y^2$.

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.)