Introduction to number theory
Exercise sheet 5

https://www.maths.tcd.ie/~mascotn/teaching/2020/MAU22301/index.html

Version: December 2, 2020

Answers are due for Wednesday December 2nd, 2PM.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Reduction (15 pts)*

Find a reduced quadratic form equivalent to the form $22x^2 - 16xy + 3y^2$.

Solution 1

Since $A = 22 > C = 3$, we start by applying the transformation

$$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) : (x, y) \leftarrow (y, -x),$$

which gives us

$$3x^2 + 16xy + 22y^2.$$

Now we have $B = 16 > A = 3$, so we apply the transformation

$$\left(\begin{smallmatrix} 1 & -3 \\ 0 & 1 \end{smallmatrix}\right) : (x, y) \leftarrow (x - 3y, y)$$

(since $\lfloor B/2A \rceil = 3$, where $\lfloor \cdot \rceil$ denotes the nearest integer), and we get

$$3x^2 - 2xy + y^2.$$

This time $A = 3 > C = 1$, so we apply again the transformation

$$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) : (x, y) \leftarrow (y, -x),$$

and we get

$$x^2 + 2xy + 3y^2.$$

Since now $B = 2 > A = 1$, we apply

$$\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) : (x, y) \leftarrow (x - y, y)$$

(where $1 = \lfloor B/2A \rceil$) and this leads us to

$$x^2 + 2y^2,$$

which is reduced, so we're done.

Exercise 2 *Primes of the form... (85 pts)*

1. (5 pts) Let $p \neq 2, 11$ be prime. Prove that $\left(\frac{-11}{p}\right) = \left(\frac{p}{11}\right)$.

2. (50 pts) Let $p \in \mathbb{N}$ be an odd prime. Prove that p is of the form $x^2 + xy + 3y^2$ (with $x, y \in \mathbb{Z}$) if and only if $p = 11$ or $p \equiv 1, 3, 4, 5$ or $9 \pmod{11}$.

   *You are **not** allowed to use the theorem giving the list of D such that $h(D) = 1$.*

3. (30 pts) Let $p \in \mathbb{N}$ be an odd prime. Using only a minimum amount of computations, prove that p is of the form $15x^2 - 17xy + 5y^2$ (with $x, y \in \mathbb{Z}$) if and only if $p = 11$ or $p \equiv 1, 3, 4, 5$ or $9 \pmod{11}$.

   If you use the results of the previous question, there is a way to solve this question with almost no computations; this is what you must do in order to get all the marks for this question.

Solution 2

1. We compute that

$$\left(\frac{-11}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{11}{p}\right) = (-1)^{p'}(-1)^{11'p'}\left(\frac{p}{11}\right) = (-1)^{p'+5p'}\left(\frac{p}{11}\right) = \left(\frac{p}{11}\right)$$

   since $p' + 5p' = 6p'$ is always even.

2. The discriminant of $x^2 + xy + 3y^2$ is -11, so if $p \neq 2, 11$ then p is represented by one of the forms of discriminant -11 iff. -11 is a square mod p.

   When we compute $h(-11)$ we find $A < 2$ so $A = 1$ and B odd so $B = 1$, so the only possibility is $C = 3$ and so $x^2 + xy + 3y^2$ is the only reduced form of discriminant -11. Thus all forms of discriminant -11 are equivalent to it.

   So when $p \neq 2, 11$, we have that p is of the form $x^2 + xy + 3y^2$ iff. p is a (necessarily nonzero) square mod 11, and by trying all values we see that the nonzero squares mod 11 are $1, 3, 4, 5$ and 9 (note: we know that there are $11' = 5$ of them). Besides, 11 is represented by $x^2 + xy + 3y^2$ since $(-1)^2 - 1 \times 2 + 3 \times 2^2 = 11$.

3. The discriminant of $15x^2 - 17xy + 5y^2$ is $17^2 - 4 \times 15 \times 5 = 289 - 300 = -11$. Since $h(-11) = 1$, all forms of discriminant -11 are equivalent, and thus represent the same integers; so in particular $15x^2 - 17xy + 5y^2$ represents the same integers as $x^2 + xy + 3y^2$.

These were the only mandatory exercises, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercises.

Exercise 3 *Class numbers*

Compute the class number $h(D)$ for

1. $D = -116$,
2. $D = -47$.

Solution 3

For brevity, we write (A, B, C) for the form $Ax^2 + Bxy + Cy^2$.

1. If (A, B, C) is reduced of discriminant -116, we must have $A \leqslant \sqrt{116/3} < \sqrt{40} < 7$. Also, B must be even since -116 is.

   We apply the method seen in the lectures:

$$\begin{array}{lll} A = 1: & B = 0: & (1, 0, 29) \\ A = 2: & B = 0: & \text{✗} \\ & B = 2: & (2, 2, 15) \\ A = 3: & B = 0: & \text{✗} \\ & B = \pm 2: & (3, \pm 2, 10) \\ A = 4: & B = 0: & \text{✗} \\ & B = \pm 2: & \text{✗} \\ & B = 4: & \text{✗} \\ A = 5: & B = 0: & \text{✗} \\ & B = \pm 2 & (5, \pm 2, 6) \\ & B = \pm 4: & \text{✗} \\ A = 6: & B = 0: & \text{✗} \\ & B = \pm 2: & \xcancel{(6, \pm 2, 5)} \text{ (not reduced)} \\ & B = \pm 4: & \text{✗} \\ & B = 6: & \text{✗} \end{array}$$

   We find 6 reduced forms, so $h(-116) = 6$.

2. Same thing, except that this time $A \leqslant \sqrt{47/3} < \sqrt{16} = 4$ and B is odd.

$$\begin{array}{lll} A = 1: & B = 1: & (1, 1, 12) \\ A = 2: & B = \pm 1: & (2, \pm 1, 6) \\ A = 3: & B = \pm 1: & (3, \pm 1, 4) \\ & B = 3: & \text{✗} \end{array}$$

   so $h(-47) = 5$.

Exercise 4 *Easy cases of the class number 1 problem*

1. Let $n \in \mathbb{N}$ be congruent to 1 or 2 mod 4. Prove that $h(-4n) = 1$ if and only if $n < 3$.

   Hint: Imagine that you apply the method seen in class to compute $h(-4n)$. What happens when $n \geqslant 3$?

2. Let $n \in \mathbb{N}$. Prove that if $h(-4n+1) = 1$, then $n = 2$ or n is odd.

Solution 4

1. Let us treat the case $n < 3$ first. When we compute $h(-4n)$, we get $A \leqslant \sqrt{4n/3} < 2$, so $A = 1$, and $B = 0$ since B is even, so $C = n$; thus $h(-4n) = 1$ is this case.

   Now if $n \geqslant 3$, then we still have the reduced form $x^2 + ny^2$, but now we can also have $A = 2$, and so $B = 0$ or $B = 2$.

   $$\begin{array}{lll} A = 1: & B = 0: & (1, 0, n) \\ A = 2: & B = 0: & (2, 0, n/2) \text{ if } n \text{ even} \\ & B = 2: & (2, 2, \frac{n+1}{2}) \text{ if } n \text{ odd} \\ & \vdots & \end{array}$$

   So if $n \equiv 2 \pmod 4$, then $n/2$ is an odd integer, so the form $(2, 0, n/2)$ is primitive; thus $h(-4n) \geqslant 2$. And if $n \equiv 1 \pmod 4$, then $\frac{n+1}{2}$ is an odd integer, so again the form $(2, 2, \frac{n+1}{2})$ is primitive and $h(-4n) \geqslant 2$.

2. Suppose on the contrary that $n \geqslant 4$ is even. Then for $A = B = 1$ we have the form $(1, 1, n)$, whereas for $A = 2$, $B = 1$ we find the forms $(2, 1, n/2)$, which is primitive and reduced since $2 \leqslant n/2$. So we have $h(-4n+1) \geqslant 2$.