Elementary Number Theory - Exercise 9a

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Compute the reduced representative of the form $Q = [5, 6, 3]$.

Solution 1. We apply the reduction algorithm:

(1a) $[5, 6, 3] \circ T^n = [5, 6 + 10n, 5n^2 + 6n + 3] = [5, -4, 2]$, for $n = -1$.

(1b) $[5, -4, 2] \circ S = [2, 4, 5]$.

(2a) $[2, 4, 5] \circ T^n = [2, 4 + 4n, 2n^2 + 4n + 5] = [2, 0, 3]$, for $n = -1$.

(2b) Since $[2, 0, 3]$ is reduced, we are done.

Problem 2. Compute the class number $h(-8)$.

Solution 2. We need to find all reduced primitive positive definite form sof discriminant $D = -8$. They can be determined by going through all $a > 0$ with $a \leq \sqrt{|D|/3}$, and then all b with $|b| \leq a$ such that $c = \frac{b^2 - D}{4a}$ is a positive integer.

We have $\lfloor \sqrt{8/3} \rfloor = 2$, so we can only have $a = 1$ or $a = 2$. For $a = 1$ we can take $b \in \{0, \pm 1\}$. For $b = 0$ we obtain $c = 2$, so we get the reduced form

$$[1, 0, 2],$$

but for $b = \pm 1$ we see that c is not an integer. For $a = 2$ we can take $b \in \{0, \pm 1, \pm 2\}$. For $b = 0$ we obtain $c = 1$, but the form $[2, 0, 1]$ is not reduced. For $b = \pm 1, \pm 2$ we see that c is not an integer.

Hence there is precisely 1 reduced form of discriminant -8, namely $[1, 0, 2]$, so the class number is $h(-8) = 1$.

Problem 3. Let p be an odd prime. Show that

$$p = x^2 + 2y^2 \qquad \Leftrightarrow \qquad p \equiv 1 \pmod 8 \quad \text{or} \quad p \equiv 3 \pmod 8.$$

Hint: Rewrite the condition on the right in terms of the Legendre symbol $\left(\frac{-2}{p}\right)$.

Solution 3. By the first and second supplements to the quadratic reciprocity law, we have

$$p \equiv 1 \pmod 8 \quad \text{or} \quad p \equiv 3 \pmod 8 \qquad \Leftrightarrow \qquad \left(\frac{-2}{p}\right) = 1.$$

We have seen in an earlier exercise problem that $p = x^2 + 2y^2$ implies $\left(\frac{-2}{p}\right) = 1$.

Conversely, assume that $\left(\frac{-2}{p}\right) = 1$. Then -2 is a square modulo p, so there exists some $m \in \mathbb{Z}$ such that $-2 = m^2 + pk$ for some $k \in \mathbb{Z}$. Now the binary quadratic form

$$[p, 2m, -k]$$

has discriminant $4m^2 + 4pk = -8$ and is positive definite (since $D = -8 < 0$ and $p > 0$). Since $h(-8) = 1$, this form is equivalent to $[1, 0, 2] = x^2 + 2y^2$. Moreover, the form $[p, 2m, -k]$ represents p (plug in $(1, 0)$), so $[1, 0, 2]$ also represents p, so there are $x, y \in \mathbb{Z}$ with $x^2 + 2y^2 = p$.

Problem 4. Show that the class number $h(D)$ for $D < 0$ can become arbitrarily large.
Hint: Choose $D = -4p_1 \cdots p_n$ with different primes p_j, and consider the forms $[a, 0, c]$.

Solution 4. We let $D = -4p_1 \cdots p_n$ with different odd primes p_j. If we let a be the product of ℓ of these primes, and c the product of the remaining primes, we obtain 2^n different primitive quadratic forms $[a, 0, c]$ of discriminant D. Moreover, $[a, 0, c]$ is reduced if and only if $a < c$, so precisely half of these forms are reduced. This yields 2^{n-1} primitive reduced forms of discriminant D, so $h(D) \geq 2^{n-1}$, which becomes arbitrarily large as $n \to \infty$.

Problem 5. Let $Q = [a, b, c]$ be positive definite of discriminant $D < 0$. Show that, if $a < \sqrt{-D/4}$ and $-a < b \leq a$, then Q is already reduced.

Solution 5. Since we have $|b| \leq a$ by assumption, it remains to show that $a \leq c$, and that $b \geq 0$ if $|b| = a$ or $a = c$. We estimate

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

so we indeed have $a \leq c$. Since we even have $a < c$, the case $a = c$ does not occur. If $|b| = a$, then we have $b = a > 0$ since the case $b = -a$ is excluded by the assmption $-a < b \leq b$. This shows that Q is reduced.

Problem 6. Show that, if Q represents 1, then Q is equivalent to the principal form.
Hint: Use Problem 5 from exercise sheet 8b.

Solution 6. Suppose that Q represents 1. Then it represents 1 properly (since for any divisor d of both x and y we would have $d^2 \mid Q(x, y)$). We have seen in an earlier problem that then Q is equivalent to a form $[1, b, c]$ for some $b, c \in \mathbb{Z}$. Applying T^n, we get an equivalent form

$$[1, b, c] \circ T^n = [1, b + 2n, c'].$$

Now we use that b has the same parity as the discriminant D of Q (which is also the discriminant of $[1, b, c]$). If D is even, then b is even, and we can choose $b = -D/2$ to obtain the equivalent form $[1, 0, c'']$. Since the c-entry of a quadratic form is determined from D, b, a via $c = \frac{b^2 - D}{2a}$, we find $c'' = -D/4$, so Q is equivalent to the principal form $[1, 0, -D/4]$. The case of odd D is analogous.

Problem 7 (sage)**.** Write a program which, given a discriminant $D < 0$, computes the reduced forms of discriminant D and the class number $h(D)$. Use it to list the class number $h(D)$ for $0 > D \geq -100$.