ALGEBRAIC NUMBER THEORY

HOMEWORK 5

(1) Compute all reduced forms of discriminant $\Delta = -4 \cdot 17$.

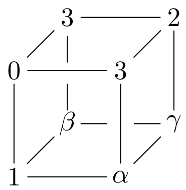
Since $A < \sqrt{4 \cdot 17/3} < 5$, we have to consider $A = 1, 2, 3, 4$. Oberve that $B \equiv \Delta \equiv 0 \bmod 2$. We find the principal form $Q_0 = (1, 0, 17)$, as well as $Q_2 = (2, 2, 9)$, $Q_1 = (3, 2, 6)$ and $Q_1 = (3, -2, 6)$. Note that $(2, -2, 9)$ is not reduced.

Also observe that we must have $\mathrm{Cl}(-4 \cdot 17) \simeq \mathbb{Z}/4\mathbb{Z}$: the class number is 4, and the classes of Q_1 and Q_3 are inverses of each other and distinct (distinct reduced forms give distinct classes). Thus the class $[(3, 2, 6)]$ must have order > 2.

(2) Use Shanks' method to compute the composition table for all reduced forms of discriminant $\Delta = -4 \cdot 17$.

The principal form Q_0 is the neutral element. Thus we need to deal with the classes of Q_1, Q_2 and Q_3. We have already seen that $[Q_1]$ generates the class group, and that $3[Q_1] = -[Q_1] = [Q_3]$; this implies $2[Q_1] = [Q_2]$, as well as $[Q_1] + [Q_2] = [Q_1] + 2[Q_1] = 3[Q_1] = [Q_3]$ etc. Let us now check via composition that we really have $2[Q_1] = [Q_2]$.

We find $A_1 = A_3 = 3$, $B = 2$, $d = \gcd(3, 3, 2) = 1$; the cube



gives the equations $2\alpha - 3\gamma = 6$, $2\beta - 3\gamma = 6$, and $3\alpha - 3\beta = 0$. Thus $\alpha = \beta = 0$ and $\gamma = -2$ gives a solution, and the resulting form is $(9, -2, 2) \sim (2, 2, 9)$. Note that we have proved $2[Q_1] + [(2, 2, 9)] = 0$, so strictly speaking we have $2[Q_1] = -[(2, 2, 9)] = [(2, -2, 9)]$; but since $(2, -2, 9) \sim (2, 2, 9)$, this does not matter here.

By the way: the fact that $2[Q_2] = Q_0$ can be checked immediately: here we have $A_1 = A_2 = B = 2$, hence $d = 2$ and $A_3 = A_1 A_2 / d^2 = 1$. Forms with leading coefficient 1 are equivalent to the principal form (reduction of B shows that the form is equivalent to $(1, 0, *)$ or $(1, 1, *)$).

You can check your calculations with `pari`. The commands

```
x = Qfb(3,2,6)
y=qfbcompraw(x,x)
qfbred(y)
```

give $y = (9, 2, 2)$, and $(2, 2, 9)$ as the final result.

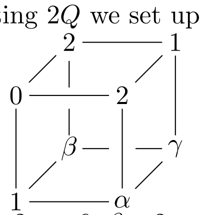
(3) Compute all reduced forms of discriminant $\Delta = -47$.

Here $A < 4$, and we easily find the reduced forms $(1, 1, 12)$, $(2, \pm 1, 6)$ and $(3, \pm 1, 4)$. (Side remark: with a little bit of experience you can predict the existence of the last pair like this: since $2 \cdot 6 = 3 \cdot 4$, the forms $(2, \pm 1, 6)$ and $(3, \pm 1, 4)$ have the same discriminant. For example, $(2, 1, 10)$ is a form of discriminant -89, and so is $(4, 1, 5)$). Thus the class number is 5, and the class group is cyclic, generated by any of the classes different from the principal class.

(4) Let $Q = (2, 1, 6)$ denote a form of discriminant -47. Show that $5[Q] = [Q_0]$ in the class group of forms. (Hint: compute $2[Q]$ and $4[Q]$ using composition.)

I claim that $2Q \sim (4, 1, 3) = (3, -1, 4)$ and $4Q \sim (9, 5, 2) \sim (2, -1, 6)$, hence $4[Q] = -[Q]$ and thus $5[Q] = 0$.

In fact, for computing $2Q$ we set up the cube



The equations are $\alpha - 2\gamma = 6$, $\beta - 2\gamma = 6$, (it is sufficient to work with the equations involving C_1 and C_2; they are easier to derive from the cube than the one involving $(B_2 - B_1)/2$) hence we can take $\alpha = \beta = 0$ and $\gamma = 3$. This gives $A_3 = A_1 A_2 = 4$, $B_2 = 1$ and $C_3 = 3$, hence $2[Q] + [(4, -1, 3)] = 0$, or $2[Q] = [(4, 1, 3)] = [(3, -1, 4)]$.

The computation of $2[(3, -1, 4)]$ gives $(9, 5, 2) \sim (2, -5, 9) \sim (2, -1, 6)$ as claimed.