ALGEBRAIC NUMBER THEORY

MIDTERM 2

(1) Let $\Delta \equiv 1 \bmod 4$ be a negative discriminant. Show that there is a quadratic form $Q = (2, B, C)$ with discriminant Δ if and only if $\Delta \equiv 1 \bmod 8$. For which values of Δ can you find a *reduced* form of type $Q = (2, B, C)$?

Assume that $\Delta \equiv 1 \bmod 8$; then we need a form $Q = (2, B, C)$ with $\Delta = B^2 - 8C$. We can simply take $B = 1$ and $C = \frac{1-\Delta}{8}$.

Conversely, if $Q = (2, B, C)$ has discriminant $\Delta = B^2 - 8C$, then $B \equiv \Delta \equiv 1 \bmod 2$, hence $\Delta \equiv B^2 \equiv 1 \bmod 8$.

The form $(2, 1, \frac{1-\Delta}{8})$ is reduced if $C = \frac{1-\Delta}{8} \geq 2 = A$, which happens if and only if $\Delta < -7$. If $\Delta = -7$, the form $(2, 1, 1)$ is not reduced, and in fact there is no reduced form with first coefficient 2 since reduced forms must satisfy $A \leq \sqrt{-\Delta/3} < 2$.

(2) Let $Q = (A, B, C)$ be a positive definite quadratic form with discriminant Δ, and consider the matrices $R = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$.
   (a) How does $M = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ act on quadratic forms?
   (b) Compute the coefficients of $Q|_R$ and $Q|_S$.
   (c) Describe how to use the action of R and S to find a quadratic form $Q' = (A, B, C) \sim Q$ whose coefficients satisfy $|B'| \leq A' \leq C'$.
   (d) Which additional condition must be satisfied for Q' to be reduced?

For a) and b) we do not need to assume that the forms are positive definite.

   (a) We have $Q|_M(X, Y) = Q(rX + sY, tX + uY)$.
   (b) $Q|_R$ and Q_S are given by

$$\begin{aligned} Q|_R(X, Y) &= Q(X + bY, Y) \\ &= A(X + bY)^2 + B(X + bY)Y + CY^2 \\ &= AX^2 + (B + 2bA)XY + (A^2b^2 + Bb + C)Y^2, \\ Q|_S(X, Y) &= Q(Y, -X) = AY^2 - BXY + CX^2, \end{aligned}$$

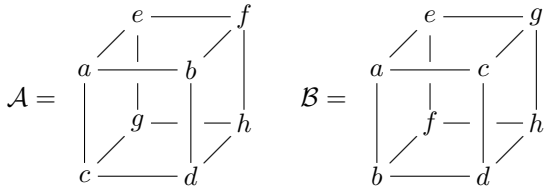
   hence $Q|_R = (A, A + 2bA, A^2b^2 + Bb + C)$ and $Q|_S = (C, -B, A)$.
   (c) Using R we can decrease the size of B until its absolute value is $\leq A$; if $C < A$, replace (A, B, C) by $(C, -B, A)$ and repeat.
   (d) The additional condition is that $B > 0$ if $|B| = A$ or $A = C$.

(3) Which are the three smallest integers that are represented properly by the form $Q = (13, 27, 17)$ of discriminant $\Delta = -155$?

Q represents the same integers as forms equivalent to Q. Reduction shows that $Q \sim (13, 1, 3) \sim (3, -1, 13)$, and the last form is reduced. The

three smallest integers represented by this reduced form are $A = 3$, $C = 13$, and $A - |B| + C = 15$.

(4) Consider the two cubes



and show that the associated quadratic forms satisfy $Q_1^{\mathcal{A}} = Q_1^{\mathcal{B}}$, $Q_2^{\mathcal{A}} = Q_3^{\mathcal{B}}$, and $Q_3^{\mathcal{A}} = Q_2^{\mathcal{B}}$. Explain how this implies that composition of forms is commutative.

The computations are straightforward (you don't have to compute the coefficients to see that the forms are equal!). The first cube shows that $[Q_1^{\mathcal{A}}] + [Q_2^{\mathcal{A}}] + [Q_3^{\mathcal{A}}] = 0$, the second that $0 = [Q_1^{\mathcal{B}}] + [Q_2^{\mathcal{B}}] + [Q_3^{\mathcal{B}}] = [Q_1^{\mathcal{A}}] + [Q_3^{\mathcal{A}}] + [Q_2^{\mathcal{A}}]$. This implies $[Q_2^{\mathcal{A}}] + [Q_3^{\mathcal{A}}] = [Q_3^{\mathcal{A}}] + [Q_2^{\mathcal{A}}]$.

(5) List all reduced forms of discriminant $\Delta = -4 \cdot 34$. Use the fact that the inverse of the class $[(A, B, C)]$ is $[(A, -B, C)]$ to deduce the structure of the class group.

We have $\sqrt{-\Delta/3} < 7$, so we have to consider integers A with $1 \le A \le 6$. Since $\Delta \equiv B^2 \bmod p$ for all odd primes $p \mid A$, and since $(\frac{\Delta}{3}) = -1$, we only need to check $A = 1, 2, 4, 5$. From $B^2 - 4AC = -4 \cdot 34 \equiv 8 \bmod 16$ we deduce that $A = 4$ is not possible (we would need $B \equiv 0 \bmod 4$, but then the left hand side is divisible by 16). Also note that $B \equiv \Delta \equiv 0 \bmod 2$. We find

A	B	Q
1	0	$(1, 0, -34)$
2	0	$(2, 0, -17)$
2	2	$- - -$
5	± 4	$- - -$
5	± 2	$(5, \pm 2, 7)$
5	0	$- - -$

Since $Q_1 = (5, 2, 7)$ and $Q_2 = (5, -2, 7)$ are reduced forms, and since their classes are inverses of each other, we must have $[Q_1] \ne [Q_2] = -[Q_1]$, that is, $2[Q_1] \ne 0$. Since the class number is 4, the class $[Q_1]$ must have order 4, hence $\mathrm{Cl}(\Delta) \simeq \mathbb{Z}/4\mathbb{Z}$.