Elementary Number Theory - Exercise 9b

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Show that the inverse of a primitive form $[a, b, c]$ in the class group is given by

$$[a, b, c]^{-1} = [a, -b, c].$$

Problem 2. Let $Q_1 = [a_1, b_1, c_1]$ and $Q_2 = [a_2, b_2, c_2]$ be united, and let $Q_1 \sim [a_1, B, a_2 C]$ and $Q_2 \sim [a_2, B, a_1 C]$. We defined the Gauss composion

$$Q_1 * Q_2 = [a_1 a_2, B, C].$$

Show that we have

$$(a_1 x^2 + Bxy + a_2 C y^2)(a_2 z^2 + Bzw + a_1 C w^2) = a_1 a_2 X^2 + BXY + CY^2,$$

where $X = xz - Cyw$ and $Y = a_1 xw + a_2 yz + Byw$. In particular, deduce that the Gauss composition $Q_1 * Q_2$ represents all products of numbers represented by Q_1 and Q_2.

Problem 3. Show that the Gauss composition of $[2, 1, 3]$ with itself is given by $[2, -1, 3]$.

Problem 4. Construct a group isomorphism from $\mathrm{Cl}(-23)$ to $\mathbb{Z}/3\mathbb{Z}$.

Problem 5. Show that a primitive, positive definite, reduced form $Q = [a, b, c]$ has order ≤ 2 in the class group $\mathrm{Cl}(D)$ if and only if $b = 0, a = b$, or $a = c$.

Problem 6 (Homework)**.** Show that $\mathrm{Cl}(-39)$ has order 4. Is it isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?

Problem 7 (sage)**.** Write a program which computes (the reduced representative of) the Gauss composition of two positive definite united forms.