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

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

Solution 1. Note that $[a, -b, c] \circ S = [c, b, a]$. Moreover, the forms $[a, b, c]$ and $[c, b, a]$ are united since $[a, b, c]$ is primitive, and the two forms are already of the shape $[a_1, B, a_2C]$ and $[a_2, B, a_1C]$, with $a_1 = a, a_2 = c, B = b$, and $C = 1$. Hence, the Gauss composition of $[a, b, c]$ and $[c, b, a]$ is defined by

$$[a, b, c] * [c, b, a] = [ac, b, 1].$$

Since the form on the right represents 1, it is equivalent to the principal form, which is the identity in the class group $\mathrm{CL}(D)$.

Problem 2. Let $Q_1 = [a_1, b_1, c_1]$ and $Q_2 = [a_2, b_2, c_2]$ be united, and let $Q_1 \sim [a_1, B, a_2C]$ and $Q_2 \sim [a_2, B, a_1C]$. We defined the Gauss composion

$$Q_1 * Q_2 = [a_1a_2, B, C].$$

Show that we have

$$(a_1x^2 + Bxy + a_2Cy^2)(a_2z^2 + Bzw + a_1Cw^2) = a_1a_2X^2 + BXY + CY^2,$$

where $X = xz - Cyw$ and $Y = a_1xw + a_2yz + Byw$. In particular, deduce that the Gauss composition $Q_1 * Q_2$ represents all products of numbers represented by Q_1 and Q_2.

Solution 2. This can be proved by multiplying out both sides. We omit the details of the computation.

Note that the identity can be rewritten as

$$[a_1, B, a_2C](x, y) \cdot [a_2, B, a_1C](z, w) = (Q_1 * Q_2)(X, Y),$$

so $Q_1 * Q_2$ represents all the products of numbers represented by $[a_1, B, a_2C]$ and $[a_2, B, a_1C]$. Since equivalent forms represent the same numbers, $Q_1 * Q_2$ represents all the 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 $[2, -1, 3]$.

Solution 3. Note that $[2, 1, 3]$ has discriminant $D = -23$ and is primitive. Since $\gcd(2, 2, \frac{1+1}{2}) = 1$, the "two" forms $[2, 1, 3]$ and $[2, 1, 3]$ are united. We need to find B such that $B \equiv b_1 \pmod{2a_1}, B \equiv b_2 \pmod{2a_2}$, and $B^2 \equiv D \pmod{4a_1a_2}$, which in our case means

$$B \equiv 1 \pmod 4,$$
$$B^2 \equiv -23 \equiv 9 \pmod{16}.$$

A suitable choice would be $B = -3$, hence $C = \frac{B^2-D}{4a_1a_2} = 2$ and indeed we have

$$[2,1,3] \sim [2,-3,4] = [2,B,2C],$$

via the matrix T^{-2}. The composition is now given by

$$[2,1,3] * [2,1,3] = [2,B,2C] * [2,B,2C] = [4,B,C] = [4,-3,2].$$

Applying S and then T^{-1} we see that

$$[4,-3,2] \sim [2,3,4] \sim [2,-1,3].$$

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

Solution 4. We first determine the reduced forms of discriminant -23. The possible integers $a > 0$ with $a \leq \sqrt{-D/3} = \sqrt{23/3} < 3$ are given by $a = 1$ and $a = 2$. For $a = 1$ the possible b with $|b| \leq a$ are $b = 0$ and $b = \pm 1$. Now $b = 0$ has the wrong parity, but $b = \pm 1$ leads to the forms $[1, \pm 1, 6]$, of which only

$$[1,1,6]$$

is reduced. For $a = 2$ we can take $b = 0, \pm 1, \pm 2$, which leads to the two reduced form $[2, \pm 1, 3]$. In total, we obtain the three reduced forms

$$[1,1,6], \quad [2,1,3], \quad [2,-1,3].$$

Hence, the class group $\mathrm{Cl}(-23)$ has order 3. It follows from a general result of basic group theory that $\mathrm{Cl}(-23)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, but in this case we can make this more explicit. We know that $[1,1,6]$ is the identity with respect to Gauss composition, and $[2,-1,3]$ is the inverse of $[2,1,3]$. Moreover, we have seen above that

$$[2,1,3] * [2,1,3] = [2,-1,3].$$

Hence we see that the map

$$\begin{aligned} [1,1,6] &\mapsto 0, \\ [2,1,3] &\mapsto 1, \\ [2,-1,3] &\mapsto 2, \end{aligned}$$

is an 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 $a = c$.

Solution 5. Let $Q' = [a,-b,c]$ be the inverse of Q with respect to Gauss composition. Then Q has order ≤ 2 in the class group if and only if Q is equivalent to Q'. We distinguish two cases:

- $|b| < a < c$. Then Q' is also reduced, so $Q' \sim Q$ is equivalent to $Q' = Q$, which means $b = 0$.

- $a = b$: In this case $Q' = [a, -b, c] = [a, -a, c]$ is equivalent to $Q = [a, b, c]$ via $Q = Q' \circ T$.
- $a = c$. In this case $Q' = [a, -b, c] = [a, -b, a]$ is equivalent to $Q = [a, b, c]$ via $Q = Q' \circ S$.

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

Solution 6. Going through the reduction algorithm, we obtain the four reduced forms

$$[1, 1, 10], \quad [2, 1, 5], \quad [2, -1, 5], \quad [3, 3, 4],$$

of discriminant -39, so we have class number $h(-39) = 4$. Every abelian group of order 4 is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. However, since $[2, 1, 5]$ is the inverse of $[2, -1, 5]$ (i.e. it is not its own inverse), $[2, 1, 5]$ must have order 4 (since the order of an element in a finite group divides the order of the group). Hence $\mathrm{Cl}(-39)$ is cyclic of order 4, and thus isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

Alternatively, we can use that in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ every element has order ≤ 2, but by the last problem, only $[1, 1, 10]$ and $[3, 3, 4]$ have order ≤ 2 in $\mathrm{Cl}(-39)$, so the two groups cannot be isomorphic.

One can also use Gauss composition to show directly that

$$[2, 1, 5]*[2, 1, 5] = [3, 3, 4], \quad [2, 1, 5]*[3, 3, 4] = [2, -1, 5], \quad [2, 1, 5]*[2, -1, 5] = [1, 1, 10] = 1_{\mathrm{Cl}(-39)},$$

so mapping $[2, 1, 5]$ to $1 \in \mathbb{Z}/4\mathbb{Z}$ gives an explicit isomorphism.

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