Elementary Number Theory - Exercise 8b

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Consider the quadratic forms

$$Q_1 = [1, 2, 3], \qquad Q_2 = [2, 4, 3], \qquad Q_3 = [1, 3, 1].$$

1. Write down the Gram matrices of Q_1, Q_2 and Q_3.
2. Compute the discriminants of Q_1, Q_2, and Q_3.
3. Which of these forms is positive definite or indefinite?
4. Show that Q_1 is equivalent to Q_2 via

$$Q_2 = Q_1 \circ \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}.$$

5. For each of the three forms, find three different integers that they represent.

Solution 1.

1. The Gram matrices are given by

$$Q_1 = \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}, \qquad Q_2 = \begin{pmatrix} 2 & 2 \\ 2 & 3 \end{pmatrix}, \qquad Q_3 = \begin{pmatrix} 1 & 3/2 \\ 3/2 & 1 \end{pmatrix}.$$

2. The discriminants of Q_1, Q_2, and Q_3 are given by $-8, -8$, and 5, respectively.
3. Q_1 and Q_2 have negative discriminants and positive a entry, so they are positive definite. Q_3 has positive discriminant, hence it is indefinite.
4. A direct computation gives

$$Q_1 \circ \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 2 & 3 \end{pmatrix} = Q_2,$$

so Q_1 and Q_2 are equivalent.

5. We can just plug in some values for x, y. For example, we have

$$Q_1(1, 0) = 1, \quad Q_1(0, 1) = 3, \quad Q_1(1, 1) = 1 + 2 + 3 = 6.$$

Analogously we can find numbers represented by Q_2 and Q_3.

Problem 2. Show that $Q = [a, b, c]$ properly represents a, c, and $a + b + c$.

Solution 2. We have $Q(1, 0) = a, Q(0, 1) = c$, and $Q(1, 1) = a + b + c$.

Problem 3. Let $Q = [a, b, c]$ be a quadratic form.

1. Let $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Show that $T^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ and compute

$$Q \circ T^n = [a, b + 2an, an^2 + bn + c], \qquad Q \circ S = [c, -b, a].$$

2. Let $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, and write

$$Q \circ M = M^t Q M = \begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix}.$$

Show that a', b', c' are explicitly given by

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \\ c' &= a\beta^2 + b\beta\delta + c\delta^2. \end{aligned}$$

Solution 3.

1. We compute

$$Q \circ T^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & (b+2an)/2 \\ (b+2an)/2 & an^2 + bn + c \end{pmatrix}$$

and

$$Q \circ S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}.$$

2. We compute

$$\begin{aligned} Q \circ M = M^t Q M &= \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \\ &= \begin{pmatrix} a\alpha^2 + b\alpha\gamma + c\gamma^2 & (2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta)/2 \\ (2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta)/2 & a\beta^2 + b\beta\delta + c\delta^2 \end{pmatrix}, \end{aligned}$$

so we obtain

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \\ c' &= a\beta^2 + b\beta\delta + c\delta^2. \end{aligned}$$

Problem 4. Let $Q = [a, b, c]$ and $Q' = [a', b', c']$ be equivalent. Show that

1. Q and Q' (properly) represent the same integers.
2. Q and Q' have the same discriminant.
3. Q is positive definite (resp. indefinite) if and only if Q' is positive definite (resp. indefinite).
4. Q is primitive if and only if Q' is primitive.

Solution 4. If Q and Q' are equivalent, there is some $M \in \mathrm{SL}_2(\mathbb{Z})$ with

$$Q' = Q \circ M = M^t Q M.$$

1. Let n be represented by Q, that is, there are $x, y \in \mathbb{Z}$ with

   $$n = \begin{pmatrix} x & y \end{pmatrix} Q \begin{pmatrix} x \\ y \end{pmatrix}.$$

   If we let

   $$\begin{pmatrix} x' \\ y' \end{pmatrix} = M^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$$

   then we have

   $$\begin{aligned} n &= \begin{pmatrix} x & y \end{pmatrix} Q \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} x & y \end{pmatrix} M^{-t} M^t Q M M^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} x' & y' \end{pmatrix} Q' \begin{pmatrix} x' \\ y' \end{pmatrix}. \end{aligned}$$

   Hence Q and Q' represent the same integers. Moreover, if $\gcd(x, y) = 1$, then $\gcd(x', y') = 1$ since M has determinant 1, so Q and Q' properly represent the same integers.

2. The discriminant of Q is given by $-4\det(Q)$, and since $\det(M) = \det(M^t) = 1$ we can compute

   $$\mathrm{disc}(Q') = -4\det(Q') = -4\det(M^t Q M) = -4\det(M^t)\det(Q)\det(M) = -4\det(Q) = \mathrm{disc}(Q).$$

3. We have seen above that $Q(x, y) = Q'(x', y')$, so Q represents only positive (resp. negative) values if and only if Q' represents only positive (resp. negative) values. This means that Q is positive (resp.) negative definite if and only if Q' is positive (resp.) negative definite.

   Alternatively, we can use the characterization of positive definite quadratic forms in terms of the discriminant, together with the fact that Q and Q' have the same discriminant.

4. From the equations

   $$Q' = M^t Q M, \quad Q = M^{-t} Q' M^{-1}$$

   it is clear that any common divisor of a, b, c would also be a common divisor of a', b', c', and vice versa. Hence Q is primitive if and only if Q' is primitive.

Problem 5. Show that a quadratic form properly represents an integer n if and only if it is equivalent to a form of the shape $[n, b', c']$ for some $b', c' \in \mathbb{Z}$.
Hint: Use the explicit formula for the coefficients of $Q \circ M$ derived above.

Solution 5. Let $Q = [a, b, c]$. Suppose that Q properly represents n. By definition, this means that there are coprime $x, y \in \mathbb{Z}$ with $Q(x, y) = ax^2 + bxy + cy^2 = n$. We are looking for a matrix $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $Q \circ M = [n, b', c']$. From the explicit formula for the action $Q \circ M$ derived in an earlier exercise, we see that the a' entry of $Q \circ M$ is given by $a\alpha^2 + b\alpha\gamma + c\gamma^2$, so it might be a good idea to choose $\alpha = x$ and $\gamma = y$. Indeed, since x, y are coprime, by Bézout's Lemma we can choose $\beta, \delta \in \mathbb{Z}$ with $x\delta - y\beta = 1$, so M lies in $\mathrm{SL}_2(\mathbb{Z})$. Then we have $Q \circ M = [n, b', c']$ as desired.

Conversely, suppose that Q is equivalent to $[n, b', c']$, that is, $Q \circ M = [n, b', c']$ for some $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. By the explicit formula for the action of M on Q, the a' entry of $Q \circ M$ is given by $a\alpha^2 + b\alpha\gamma + c\gamma^2$, so we have $n = a\alpha^2 + b\alpha\gamma + c\gamma^2$. In other words, Q represents n. Since $M \in \mathrm{SL}_2(\mathbb{Z})$ we have $\gcd(\alpha, \gamma) = 1$, so the representation is proper.

Problem 6 (sage)**.** A quadratic form can be represented in sage as an array $Q = [a, b, c]$. Write programs that

1. compute the discriminant of Q,
2. check whether Q is positive (resp. negative) definite or indefinite,
3. check whether Q is primitive,
4. compute $Q \circ M$ for $M \in \mathrm{SL}_2(\mathbb{Z})$.