PAWS 2025: ANALYSIS AND IMPLEMENTATION OF ALGORITHMS IN NUMBER THEORY
PROBLEM SET 4

THOMAS BOUCHET, KATE FINNERTY, ASIMINA S. HAMAKIOTES, YONGYUAN HUANG

Below are the exercises for Problem Set 4. The questions are loosely in ascending order of difficulty. Feel free to skip around and try whatever exercises would be the most helpful for you. Try as many as you can but don't feel like you need to complete them all!

1. Beginner Problems

Question 1: Apply the Gram-Schmidt orthogonalization process to the following sequence of vectors in $\mathbb{R}^3$:

$$\begin{bmatrix}1\\2\\0\end{bmatrix}, \begin{bmatrix}8\\1\\-6\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}.$$

Question 2: Find a 3×3 matrix representing the quadratic form

$$q(x_1, x_2, x_3) = x_1^2 + 5x_2^2 - 3x_3^2 + 6x_1x_2 - 4x_1x_3 + 8x_2x_3$$

for all $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{R}^3$. Is it positive definite, i.e. is $q(\mathbf{x}) \geq 0$ for all $\mathbf{x} \in \mathbb{R}^3$?

Question 3: Let L be a lattice with associated quadratic form $q\colon V \to K$ and $\mathbb{Z}$-basis $\{b_1, \ldots, b_n\}$. Then, we can recover q from the matrix

$$Q = [q_{i,j}]_{i,j}, \qquad \text{where } q_{i,j} = b(b_i, b_j), \tag{1}$$

with $b(b_i, b_j)$ denoting the bilinear form $b(x, y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$. Indeed, for all $x \in \mathbb{R}^n$, we have $q(x) = x^{\mathsf{t}}Qx$. Show that the determinant of the matrix Q is independent of the choice of $\mathbb{Z}$-basis for L.

Question 4: Let $A = \begin{bmatrix} a & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & a \end{bmatrix}$. For what range of values a is A positive definite?

Question 5: Implement the subalgorithm RED(k, l) (Algorithm 4.26 in the Lecture Notes) in Magma.

Question 6: Let $x = 0.30901699437494742410229341718 3 + 0.95105651629515357211643933338 0\, i$ be a numerical approximation of an algebraic integer. Can you find that algebraic integer?

2. Intermediate Problems

Question 7: In this question, we show that $K = \mathbb{Q}(\sqrt{-3})$ is a subfield of $L = \mathbb{Q}(\zeta_9)$, where ζ_9 is a primitive 9-th root of unity.

(1) First, choose an embedding of K and L into $\mathbb{C}$. You can use the command `Roots()` on each of the minimal polynomials of K and L (denoted by m_K and m_L respectively).
(2) Then, ask for an integral linear combination between the numerical approximations of $\sqrt{-3}$, and $1, \zeta_9, \ldots, \zeta_9^5$. You can use the command `IntegerRelation()` to do that.
(3) Using the previous item, find a polynomial P such that we have, at least heuristically, $\sqrt{-3} = P(\zeta_9)$. Check that $m_K(P(x))$ is divisible by m_L, and conclude that K is a subfield of L.

Question 8: Implement the subalgorithm SWAP(k) (Algorithm 4.27 in the Lecture Notes) in Magma.

Question 9: Show that the running time of the LLL algorithm is at most $O(n^6 \ln^3 B)$ field multiplications/divisions, if $|b_i|^2 \leq B$ for all i.

3. Advanced Problems

Question 10: Use the definitions at the start of Section 4.2 to prove the following theorem about LLL-reduced bases.

Theorem 1. *Let $\{b_1, \ldots, b_n\}$ be an LLL-reduced basis of a lattice L. Then*

$$d(L) \leq \prod_{i=1}^{n} |b_i| \leq 2^{n(n-1)/4} d(L); \tag{2}$$

$$|b_j| \leq 2^{(i-1)/2} |b_i^*|, \qquad \text{if } 1 \leq j \leq i \leq n; \tag{3}$$

$$|b_1| \leq 2^{(n-1)/4} d(L)^{1/n}; \tag{4}$$

for every $x \in L$ with $x \neq 0$, we have

$$|b_1| \leq 2^{(n-1)/2} |x|; \tag{5}$$

and for linearly independent vectors $x_1, \ldots, x_t \in L$, we have

$$|b_j| \leq 2^{(n-1)/2} \max(|x_1|, \ldots, |x_t|) \qquad \text{for } 1 \leq j \leq t. \tag{6}$$

Question 11: Try writing your own implementation of LLL and comparing running times for small examples. Use the subalgorithms from previous problems.