Exercises marked with a ★ can be handed in for bonus points. Due date is May 21.

**Exercise 1**
Recall that in class we defined, for \( k \in \mathbb{N} \)

\[
g_k = a_k g_{k-1} + g_{k-2}; \quad h_k = a_k h_{k-1} + h_{k-2} \quad \text{with} \quad g_{-1} = 1, g_{-2} = 0, h_{-1} = 0, h_{-2} = 1
\]

Show that for each \( k \in \mathbb{N} \):

- \( \frac{g_k}{h_k} = \langle a_0, \ldots, a_k \rangle \);
- \( g_{k+1} h_k - g_k h_{k+1} = (-1)^k \).

**Exercise 2**
Consider three points \( v_1, v_2, v_3 \in \mathbb{Z}^2 \) that do not lie on the same line.

- a) Show the following: the triangle with vertices \( v_1, v_2, v_3 \) does not contain an integer point other than its vertices if and only if the matrix \((v_2 - v_1, v_3 - v_2)\) is unimodular.

- b) Show that the previous statement cannot be extended to \( \mathbb{R}^3 \), providing linearly independent vectors \( v_1, v_2, v_3, v_4 \) such that \( \text{conv}\{v_1, v_2, v_3, v_4\} \) does not contain an integer different from its vertices but \( \det(v_2 - v_1, v_3 - v_1, v_4 - v_1) \neq \pm 1 \).

**Exercise 3 (★)**
Let \( v_1, \ldots, v_n \in \mathbb{Z}^2 \) and \( P = \text{conv}\{v_1, \ldots, v_n\} \). Let \( A, I, \) and \( B \) be respectively the area, the number of integer points in the interior, and the number of integer points on the boundary of \( P \). Prove that \( A = I + B/2 - 1 \).

**Exercise 4 (★)**
Implement the algorithm that computes the HNF of a given matrix.

**Exercise 5**
Let

\[
B = (b_1, \ldots, b_{i-1}, b_i, b_{i+1}, b_{i+2}, \ldots, b_n)
\]
and
\[C = (b_1, \ldots, b_{i-1}, b_{i+1}, b_i, b_{i+2}, \ldots, b_n)\]
be two lattice bases. Notice that \(C\) originates from \(B\) via swapping the \(i\)-th and \(i + 1\)-st column. Prove that \(B^*\) and \(C^*\) only differ in the \(i\)-th and \(i + 1\)-st column. Show further that
\[\|b_i^*\| \cdot \|b_{i+1}^*\| = \|c_i^*\| \cdot \|c_{i+1}^*\|\]
holds. What does this imply for \(\det(B)\) and \(\det(C)\)?
\((B^*\) and \(C^*\) are the output of the Gram-Schmidt process with input \(B\) and \(C\), respectively.\)

**Exercise 6**
Let \(p\) be an odd prime. Prove that \((p - 1)! \equiv -1 \pmod{p}\).