Exercise 5.1 (GCD revisited). (17 points)

Assume you are given two integers \(a, b \in \mathbb{N}\) and consider the lattice \(L = \mathcal{L}(B)\) spanned by the basis (in row notation)

\[
B = \begin{bmatrix}
1 & 0 & \gamma a \\
0 & 1 & \gamma b
\end{bmatrix},
\]

where \(\gamma \in \mathbb{R}_{>1}\) is some large constant.

(i) Do some experiments with the lattice \(L\): Select, say, 100 pairs \((a, b)\) randomly, where \(a\) and \(b\) are at most \(C = 100\) and check for which values of \(\gamma\) the basis reduction algorithm yields always a basis of the form

\[
B = \begin{bmatrix}
x_1 & x_2 & 0 \\
s & t & \pm \gamma \gcd(a, b)
\end{bmatrix},
\]

with \(sa + tb = \pm \gcd(a, b)\).

(ii) Try also the values \(C = 500\), \(C = 1000\) and \(C = 5000\). Hand in a table of 3 values of \(\gamma\) for which your experiment succeeded.

(iii) We are now going to prove that for \(\gamma > 2C\), the above basis reductions will always compute the correct solution.

(a) Show that every vector \(v \in L\) is of the form \((v_1, v_2, \gamma(v_1a + v_2b))\).

(b) Take any such vector with \(v_1a + v_2b \neq 0\). Show that then \(\|v\|^2 \geq \gamma^2\).

(c) Now consider a reduced basis \(\bar{B}\). We know from the lecture that we have \(\|\bar{b}_1\| \leq \sqrt{2}\lambda_1(L)\), where \(\lambda_1(L)\) is the length of a nonzero shortest vector in \(L\). In particular it follows that \(\|\bar{b}_1\| \leq \sqrt{2}\|v\|\) for any nonzero vector \(v \in L\). Show that from that it follows that \(\|\bar{b}_1\| \leq 2C\). Hint: Consider the vector \((-b, a, 0)\).

(d) Conclude that for \(\gamma > 2C\) the vector \(\bar{b}_1\) is of the form \((x_1, x_2, 0)\).

We now know that we have a reduced basis \(\bar{B} = \begin{bmatrix} x_1 & x_2 & 0 \\ s & t & \pm \gamma g \end{bmatrix}\). Further we know from the lecture that there is a unimodular transformation \(U\) with \(\bar{B} = UB\) with \(U = \begin{bmatrix} x_1 & x_2 \\ s & t \end{bmatrix}\) such that \(x_1t - x_2s = \pm 1\). The inverse is given as \(U^{-1} = \begin{bmatrix} t & x_2 \\ s & x_1 \end{bmatrix}\).

(e) Argue that we have \(U[\gamma a, \gamma b]^T = [0, \gamma g]^T\) and conclude from it that \(g = \pm \gcd(a, b)\).

(iv) Compare your result to the experiments you were doing in the beginning.
Exercise 5.2 (Linear congruential generators). (7+5 points)

We consider the linear congruential generators with $x_i = (ax_{i-1} + b) \text{rem} \ m$.

(i) Compute the pseudorandom sequence of numbers resulting from

(a) $m = 10, a = 3, b = 2, x_0 = 1$ and
(b) $m = 10, a = 8, b = 7, x_0 = 1$.

What do you observe?

(ii) You observe the sequence of numbers

$13, 223, 793, 483, 213, 623, 593, \ldots$

generated by a linear congruential generator. Find matching values of $m, a$ and $b$.

How do you do this?

(iii) Consider $m = 100, a = 3, b = 2, x_0 = 1$. Compute the result of the truncated linear congruential generator, which outputs the top half of the bits.

(iv) Implement the truncated linear congruential generator in a programming language of your choice. Also implement the non-truncated generator together with the algorithm breaking it.