7.14.1 Congruential Cryptosystems

Recall the congruential cipher described in Sect. 7.1. Alice chooses a modulus q and two small secret integers f and g, and her public key is the integer $h \equiv f^{-1}g \pmod{q}$. Eve knows the public values of q and h, and she wants to recover the private key f. One way for Eve to find the private key is to look for small vectors in the lattice L generated by

$$\boldsymbol{v}_1 = (1, h) \quad \text{and} \quad \boldsymbol{v}_2 = (0, q),$$

since as we saw, the vector (f, g) is in L, and given the size constraints on f and g, it is likely to be the shortest nonzero vector in L.

We illustrate by breaking Example 7.1. In that example,

$$q = 122430513841 \quad \text{and} \quad h = 39245579300.$$

We apply Gaussian lattice reduction (Proposition 7.66) to the lattice generated by

$$(1, 39245579300) \quad \text{and} \quad (0, 122430513841).$$

The algorithm takes 11 iterations to find the short basis

$$(-231231, -195698) \quad \text{and} \quad (-368222, 217835).$$

Up to an irrelevant change of sign, this gives Alice's private key $f = 231231$ and $g = 195698$.

7.14.2 Applying LLL to Knapsacks

In Sect. 7.2 we described how to reformulate a knapsack (subset-sum) problem described by $\boldsymbol{M} = (m_1, \ldots, m_n)$ and S as a lattice problem using the lattice $L_{\boldsymbol{M},S}$ with basis given by the rows of the matrix (7.4) on page 383. We further explained in Example 7.33 why the target vector $\boldsymbol{t} \in L_{\boldsymbol{M},S}$, which has length $\|\boldsymbol{t}\| = \sqrt{n}$, is probably about half the size of all other nonzero vectors in $L_{\boldsymbol{M},S}$.

We illustrate the use of the LLL algorithm to solve the knapsack problem

$$\boldsymbol{M} = (89, 243, 212, 150, 245) \quad \text{and} \quad S = 546$$

considered in Example 7.7. We apply LLL to the lattice generated by the rows of the matrix

$$A_{\boldsymbol{M},S} = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 89 \\ 0 & 2 & 0 & 0 & 0 & 243 \\ 0 & 0 & 2 & 0 & 0 & 212 \\ 0 & 0 & 0 & 2 & 0 & 150 \\ 0 & 0 & 0 & 0 & 2 & 245 \\ 1 & 1 & 1 & 1 & 1 & 546 \end{pmatrix}.$$