This basis has Hadamard ratio $\mathcal{H} = 0.956083$, which is even better than Alice's good basis. Eve next applies Babai's algorithm (Theorem 7.34) to find a lattice vector

$$\boldsymbol{v} = (-79081423, -35617459, 11035471)$$

that is very close to $\boldsymbol{e}$. Finally she writes $\boldsymbol{v}$ in terms of the original lattice vectors,

$$\boldsymbol{v} = 86\boldsymbol{w}_1 - 35\boldsymbol{w}_2 - 32\boldsymbol{w}_3,$$

which retrieves Bob's plaintext $\boldsymbol{m} = (86, -35, -32)$.

7.14.4 Applying LLL to NTRU

We apply LLL to the NTRU cryptosystem described in Example 7.53. Thus $N = 7$, $q = 41$, and the public key is the polynomial

$$\boldsymbol{h}(x) = 30 + 26x + 8x^2 + 38x^3 + 2x^4 + 40x^5 + 20x^6.$$

As explained in Sect. 7.11, the associated NTRU lattice is generated by the rows of the matrix

$$M_{\boldsymbol{h}}^{\mathrm{NTRU}} = \begin{pmatrix}
1&0&0&0&0&0&0&30&26&8&38&2&40&20\\
0&1&0&0&0&0&0&20&30&26&8&38&2&40\\
0&0&1&0&0&0&0&40&20&30&26&8&38&2\\
0&0&0&1&0&0&0&2&40&20&30&26&8&38\\
0&0&0&0&1&0&0&38&2&40&20&30&26&8\\
0&0&0&0&0&1&0&8&38&2&40&20&30&26\\
0&0&0&0&0&0&1&26&8&38&2&40&20&30\\
0&0&0&0&0&0&0&41&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&41&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&41&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&41&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&41&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&41&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&41
\end{pmatrix}.$$

Eve applies LLL reduction to $M_{\boldsymbol{h}}^{\mathrm{NTRU}}$. The algorithm performs 96 swap steps and returns the LLL reduced matrix

$$M_{\mathrm{red}}^{\mathrm{NTRU}} = \begin{pmatrix}
1&0&-1&1&0&-1&-1&-1&0&-1&0&1&1&0\\
0&1&1&-1&0&1&-1&-1&-1&0&1&0&1&0\\
-1&1&0&-1&-1&1&0&-1&0&1&1&0&-1&0\\
-1&-1&1&0&-1&1&0&1&0&-1&0&-1&0&1\\
-1&1&0&-1&1&0&-1&0&-1&0&-1&0&1&1\\
-1&-1&-1&-1&-1&-1&-1&0&0&0&0&0&0&0\\
0&1&0&1&0&-1&1&-1&-1&0&0&2&0&0\\
-8&-1&0&9&0&-1&0&-4&2&6&0&-4&7&-7\\
8&1&0&0&-8&-1&2&0&-5&8&-7&-3&1&6\\
0&-9&-2&1&9&-1&0&-6&-3&2&5&0&-5&7\\
0&8&0&-9&-1&-8&8&2&7&-11&3&-5&2&2\\
1&0&0&9&2&-1&-9&5&-7&6&3&-2&-5&0\\
-2&1&9&-1&0&0&-9&2&5&0&-5&7&-6&-3\\
3&2&3&3&-6&2&-6&11&6&8&0&9&5&2
\end{pmatrix}.$$

We can compare the relative quasi-orthogonality of the original and the reduced bases by computing the Hadamard ratios,

$$\mathcal{H}(M_{\boldsymbol{h}}^{\text{NTRU}}) = 0.1184 \quad \text{and} \quad \mathcal{H}(M_{\text{red}}^{\text{NTRU}}) = 0.8574.$$

The smallest vector in the reduced basis is the top row of the reduced matrix,

$$(1, 0, -1, 1, 0, -1, -1, -1, 0, -1, 0, 1, 1, 0).$$

Splitting this vector into two pieces gives polynomials

$$\boldsymbol{f}'(x) = 1 - x^2 + x^3 - x^5 - x^6 \quad \text{and} \quad \boldsymbol{g}'(x) = -1 - x^2 + x^4 + x^5.$$

Note that $\boldsymbol{f}'(x)$ and $\boldsymbol{g}'(x)$ are not the same as Alice's original private key polynomials $\boldsymbol{f}(x)$ and $\boldsymbol{g}(x)$ from Example 7.53. However, they are simple rotations of Alice's key,

$$\boldsymbol{f}'(x) = -x^3 \star \boldsymbol{f}(x) \quad \text{and} \quad \boldsymbol{g}'(x) = -x^3 \star \boldsymbol{g}(x),$$

so Eve can use $\boldsymbol{f}'(x)$ and $\boldsymbol{g}'(x)$ to decrypt messages.

Exercises

Section 7.1. A Congruential Public Key Cryptosystem

7.1. Alice uses the congruential cryptosystem with $q = 918293817$ and private key $(f, g) = (19928, 18643)$.

(a) What is Alice's public key h?

(b) Alice receives the ciphertext $e = 619168806$ from Bob. What is the plaintext?

(c) Bob sends Alice a second message by encrypting the plaintext $m = 10220$ using the random element $r = 19564$. What is the ciphertext that Bob sends to Alice?

Section 7.2. Subset-Sum Problems and Knapsack Cryptosystems

7.2. Use the algorithm described in Proposition 7.5 to solve each of the following subset-sum problems. If the "solution" that you get is not correct, explain what went wrong.

(a) $\boldsymbol{M} = (3, 7, 19, 43, 89, 195), \quad S = 260.$

(b) $\boldsymbol{M} = (5, 11, 25, 61, 125, 261), \quad S = 408.$

(c) $\boldsymbol{M} = (2, 5, 12, 28, 60, 131, 257), \quad S = 334.$

(d) $\boldsymbol{M} = (4, 12, 15, 36, 75, 162), \quad S = 214.$

7.3. Alice's public key for a knapsack cryptosystem is

$$\boldsymbol{M} = (5186, 2779, 5955, 2307, 6599, 6771, 6296, 7306, 4115, 637).$$

Eve intercepts the encrypted message $S = 4398$. She also breaks into Alice's computer and steals Alice's secret multiplier $A = 4392$ and secret modulus $B = 8387$. Use this information to find Alice's superincreasing private sequence $\boldsymbol{r}$ and then decrypt the message.