$A = \frac{7.3}{\ln(3+2\sqrt{2})}$, $B = (2+\sqrt{3})^2$. The continued fraction expansion of κ is

$$[0, 1, 2, 1, 20, 1, 5, 3, 8, 5, 1, 2, 1, 1, 1, 1, 4, 3, 3, 3, 1, 6, 3, 1, 2, 22,$$
$$1, 2, 8, 2, 1, 2, 6, 3, 20, 2, 10, 3, \ldots],$$

so the first convergent of κ which satisfies the condition $q > 6N$ is

$$\frac{p}{q} = \frac{742265900639684191}{993522360732597120}.$$

We will see that for μ_1 it will be needed to take the next convergent, so let us first consider what is obtained for μ_2. We have $\|\mu_2 q\| \approx 0.24492$, $\|\kappa q\| \cdot N \approx 0.01878$, so $\varepsilon \approx 0.22614 > 0$. By applying Lemma 14.8, we obtain $n \leq 16$. Now, we can repeat the reduction with $N = 16$. The corresponding convergent is now $\frac{p'}{q'} = \frac{387}{518}$, and the reduction gives $n \leq 3$.

As we already mentioned, by applying Lemma 14.8 for μ_1 and the above p, q, we obtain negative ε ($\|\mu_1 q\| \approx 0.007626$, $\|\kappa q\| \cdot N \approx 0.01878$). Therefore, we take the next convergent

$$\frac{P}{Q} = \frac{2297570640187354392}{3075296607888933649}.$$

We obtain $\|\mu_1 Q\| \approx 0.2989$, $\|\kappa Q\| \cdot N \approx 0.002254$, so the corresponding $\varepsilon \approx 0.29665 > 0$ and we can apply the reduction, which gives $n \leq 17$. If we repeat the reduction for $N = 17$, we again obtain that the corresponding convergent is $\frac{p'}{q'} = \frac{387}{518}$, and the reduction gives $n \leq 4$.

It is easily checked that the equations $v_n = w_m^{+,-}$ do not have solutions for $n = 3$ and $n = 4$. Hence, we finished the proof of the theorem. □

14.5 LLL reduction

We will now show how the LLL algorithm, described in Chapter 8.9, can be applied to Diophantine problems which can be transformed into inequalities for linear forms. Among books dealing with this topic, that we used in this section, we recommend [378] and [416].

Let us consider an inequality of the form

$$|\alpha_0 + x_1\alpha_1 + \cdots + x_n\alpha_n| < c_2 e^{-c_3 X}, \tag{14.32}$$

where α_i are given real or complex numbers, c_2 and c_3 positive real constants, and $X = \max(|x_1|, \ldots, |x_n|)$. We look for solutions of the inequality

in integers $x_1, \ldots, x_n$. Let us assume that it is known that $X \leq X_0$, where X_0 is a (large) constant. Similarly to the Baker-Davenport reduction, we want to obtain a new upper bound of the form $X \leq c \ln X_0$. We will consider the case when all α_i's are real.

Let us choose the constant $C \approx X_0^n$. We assign to the linear form $\alpha_0 + \sum_{i=1}^n x_i\alpha_i$, a lattice L (see Definition 8.11) generated by the columns of the matrix

$$A = \begin{bmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & 0 & 0 \\ 0 & \cdots & 1 & 0 \\ \lfloor C\alpha_1 \rceil & \cdots & \lfloor C\alpha_{n-1} \rceil & \lfloor C\alpha_n \rceil \end{bmatrix}.$$

Here $\lfloor \alpha \rceil$ denotes the nearest integer to the real number α. The constant C was chosen to be approximately equal to X_0^n, because then, according to Lemma 8.57.3), we can expect that the shortest vector of an LLL-reduced basis has the norm approximately equal to X_0. By applying the LLL algorithm, we can also find the lower bound c_4 for the quantity

$$l(L, y) = \begin{cases} \min\{\|x - y\| \,:\, x \in L,\ y \notin L \\ \min\{\|x\| \,:\, x \in L,\ x \neq 0\},\ y \in L, \end{cases}$$

where $y = [0, \ldots, 0, -\lfloor C\alpha_0 \rceil]^\tau$.

Lemma 14.10. *Let $S = (n-1)X_0^2$ and $T = \frac{1+nX_0}{2}$. If $c_4^2 \geq T^2 + S$, then either*

$$X \leq \frac{1}{c_3}\left(\ln(Cc_2) - \ln(\sqrt{c_4^2 - S} - T)\right)$$

or $x_1 = \cdots = x_{n-1} = 0$, $x_n = -\frac{\lfloor C\alpha_0 \rceil}{\lfloor C\alpha_n \rceil}$.

Proof: Let $\varphi = \lfloor C\alpha_0 \rceil + \sum_{i=1}^n x_i \lfloor C\alpha_i \rceil$. Then

$$\left|\varphi - C(\alpha_0 + \sum_{i=1}^n x_i\alpha_i)\right| \leq \frac{1}{2} + \sum_{i=1}^n \frac{X_0}{2} = T.$$

Therefore, $|\varphi| \leq T + C \cdot c_2 e^{-c_3 X}$. Let $x = [x_1, \ldots, x_n]^\tau$ and $z = Ax$. Then $z - y = [x_1, \ldots, x_{n-1}, \varphi]^\tau$. Since $z \in L$, we conclude that either $z = y$ (so $x_1 = \cdots = x_{n-1} = 0$ and $x_n = -\frac{\lfloor C\alpha_0 \rceil}{\lfloor C\alpha_n \rceil}$) or

$$c_4^2 \leq l(L, y)^2 \leq \sum_{i=1}^{n-1} x_i^2 + \varphi^2 \leq S + \left(T + Cc_2 e^{-c_3 X}\right)^2.$$

By the assumption, $c_4^2 \geq S$, so we obtain

$$e^{-c_3 X} \geq \frac{1}{Cc_2}\Big(\sqrt{c_4^2 - S} - T\Big). \tag{14.33}$$

By using the assumption that $c_4^2 \geq T^2 + S$, from (14.33), by taking logarithms, we obtain

$$X \leq \frac{1}{c_3}\Big(\ln(Cc_2) - \ln\Big(\sqrt{c_4^2 - S} - T\Big)\Big). \qquad \square$$

Remark 14.4. If α_i's are complex numbers, then instead of the above matrix A, we consider the matrix

$$\begin{bmatrix} 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & 0 & 0 & 0 \\ 0 & \cdots & 1 & 0 & 0 \\ \lfloor C\,\mathrm{Re}(\alpha_1)\rceil & \cdots & \cdots & \lfloor C\,\mathrm{Re}(\alpha_{n-1})\rceil & \lfloor C\,\mathrm{Re}(\alpha_n)\rceil \\ \lfloor C\,\mathrm{Im}(\alpha_1)\rceil & \cdots & \cdots & \lfloor C\,\mathrm{Im}(\alpha_{n-1})\rceil & \lfloor C\,\mathrm{Im}(\alpha_n)\rceil \end{bmatrix}.$$

Example 14.2. *Find a cubic polynomial with integer coefficients (small in absolute value) which has one root near $\pi = 3.14159\ldots$, and the other near $e = 2.71828\ldots$*

Solution: The problem can be understood as the problem of finding coefficients $x_1, \ldots, x_4$ such that the linear forms $|x_1\pi^3 + x_2\pi^2 + x_3\pi + x_4|$ and $|x_1e^3 + x_2e^2 + x_3e + x_4|$ are (simultaneously) small, while at the same time $|x_i|$ are not too large (say of magnitude 10^2). Therefore, let us consider the lattice generated by the columns of the matrix

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 3101 & 987 & 314 & 100 \\ 2009 & 739 & 272 & 100 \end{pmatrix}$$

(elements in the third row are $\lfloor 100 \cdot \pi^{4-i} \rceil$ and in the fourth $\lfloor 100 \cdot e^{4-i} \rceil$). We want to obtain an LLL-reduced basis for this lattice. In fact, here we are interested in the transformation matrix U such that the columns of the matrix AU form the LLL-reduced basis. It can be obtained by using the command `qflll`$(A, 1)$ in the program package PARI. We obtain

$$U = \begin{pmatrix} -3 & 0 & -8 & 1 \\ 2 & 1 & -1 & -9 \\ 66 & -6 & 214 & 27 \\ -134 & 9 & -414 & -27 \end{pmatrix}.$$

Now, the first column of U gives us the coefficients of the required polynomial

$$f(x) = 3x^3 - 2x^2 - 66x + 134.$$

Its roots are approximately 3.147875, 2.725321 and -5.20653. $\diamondsuit$

Example 14.3. *Find all solutions of the inequality*

$$|x_1 \ln 2 + x_2 \ln 3 + x_3 \ln 5| \le 2e^{-X}, \tag{14.34}$$

where $X = \max(|x_1|, |x_2|, |x_3|) \le X_0 = 10^{30}$.

Solution: The inequality is of the form $|\Lambda| \le c_2 e^{-c_3 X}$, where $c_2 = 2$, $c_3 = 1$. As we already described, we assign to the linear form Λ the lattice generated by the columns of the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \lfloor C \ln 2 \rceil & \lfloor C \ln 3 \rceil & \lfloor C \ln 5 \rceil \end{pmatrix}.$$

The advice was to take C of magnitude X_0^3. Usually, C should be taken somewhat larger for the conditions of Lemma 14.10 to be satisfied. Therefore, let us take $C = 10^{100}$. The quantities S and T from Lemma 14.10 are $S = 2 \cdot 10^{60}$, $T = \frac{1}{2}(1 + 3 \cdot 10^{30})$. For the first vector of the LLL-reduced basis, we obtain

$$\begin{pmatrix} -151524626390368016373546862561679 9 \\ -502897304507254890263203391695738 \\ 116593725586775716630432905636640 3 \end{pmatrix}.$$

We have $\|b_1\|^2 \approx 3.9083 \cdot 10^{66}$, and we obtain $c_1 = 1$ in Lemma 8.57. From Lemma 8.57, we get

$$l(L,0)^2 \ge c_1^{-1} \|b_1\|^2 = c_4^2 \approx 3.9083 \cdot 10^{66}.$$

We see that the condition $c_4^2 \ge T^2 + S$ from Lemma 14.10 is satisfied. By inserting all known values in Lemma 14.10, we obtain a new bound

$$X \le 154.$$

This new bound is significantly smaller than the initial bound $X \le 10^{30}$. However, it can be further reduced. Hence, let us take that $X_0 = 154$, and let $C = 10^9$. Consider the lattice generated by the columns of the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 693147181 & 1098612289 & 1609437912 \end{pmatrix}.$$

The corresponding LLL-reduced basis consists of the columns of the matrix

$$\begin{pmatrix} 573 & 747 & 713 \\ -237 & 938 & -611 \\ -300 & -55 & 1794 \end{pmatrix}.$$

Furthermore, $c_1 = 1$, $c_4 = 474498$, $S = 47432$, $T = 231.5$, so Lemma 14.10 can be applied, which gives a new upper bound

$$X \leq 15.$$

The process can be continued further, however, the bound is now sufficiently small for all remaining possibilities to be directly checked. We find that the solutions are

$$\begin{aligned}(x_1, x_2, x_3) = {} & (-6,-5,6), (-4,4,-1), (-3,-4,4), (-3,-1,2), (-2,0,1), \\ & (-1,-1,1), (-1,0,0,), (-1,1,0), (-1,2,-1), (0,-3,2), \\ & (0,-1,1), (0,0,0), (0,1,-1), (0,3,-2), (1,-2,1), (1,-1,0), \\ & (1,0,0), (1,1,-1), (2,0,-1), (3,1,-2), (3,4,-4), (4,-4,1), \\ & (6,5,-6).\end{aligned}$$

Let us observe that these 23 solutions are in fact all solutions of inequality (14.34) because, from the Baker-Wüstholz theorem, it follows that (14.34) does not have solutions with $X > 10^{15}$. ♢

14.6 Diophantine m-tuples

Definition 14.1. *A* Diophantine m-tuple *is a set of m distinct positive integers with the property that the product of any two of its distinct elements plus* 1 *is a perfect square.*

The first example of a Diophantine quadruple was found by Fermat and it was the set $\{1, 3, 8, 120\}$, which we already discussed in Theorem 14.9. Indeed, we have

$$1 \cdot 3 + 1 = 2^2, \quad 1 \cdot 8 + 1 = 3^2, \quad 1 \cdot 120 + 1 = 11^2,$$

$$3 \cdot 8 + 1 = 5^2, \quad 3 \cdot 120 + 1 = 19^2, \quad 8 \cdot 120 + 1 = 31^2.$$

Definition 14.2. *A* rational Diophantine m-tuple *is a set of m distinct nonzero rational numbers with the property that the product of any two of its distinct elements plus* 1 *is the square of a rational number.*