		k								

Name (deutlich lesbar!) Matrikelnummer

Aufgabe 1. Seien $v = \begin{pmatrix} 3 \\ 6 \\ -71 \end{pmatrix} \in \mathbb{Z}^3$ und $L = \langle \begin{pmatrix} 3 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 8 \end{pmatrix}, \begin{pmatrix} 2 \\ 8 \\ 0 \end{pmatrix} \rangle \subseteq \mathbb{Z}^3$. Wie könnten Sie mithilfe von LLL nachweisen, dass v in L liegt? (Es genügt anzugeben, auf welche Basis Sie den LLL-Algorithmus anwenden würden; Sie brauchen die Rechnung natürlich nicht durchzuführen.)

Lösung. Wende LLL auf die Basis

$$\{ \begin{pmatrix} 3w \\ 6w \\ -71w \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 3w \\ 0 \\ -w \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2w \\ 8w \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2w \\ 8w \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \}$$

an, z.B. mit $w = 10^{10}$. Die reduzierte Basis enthält den Vektor $(0, 0, 0, 1, 1, 9, -3)$. Daraus folgt

$$\begin{pmatrix} 3 \\ 6 \\ -71 \end{pmatrix} = - \begin{pmatrix} 3 \\ 0 \\ -1 \end{pmatrix} - 9 \begin{pmatrix} 0 \\ 2 \\ 8 \end{pmatrix} + 3 \begin{pmatrix} 2 \\ 8 \\ 0 \end{pmatrix},$$

d.h. der Vektor liegt tatsächlich im gegebenen Gitter. Hätte die reduzierte Basis keinen Vektor der Form $(0, 0, 0, \pm 1, *, *, *)$ enthalten, wäre das kein Beweis, dass der Vektor nicht im Gitter liegt.

Aufgabe 2. Schätzen Sie die Komplexität des folgenden Algorithmus ab (in Abhängigkeit von n):

Eingabe: $a \in \mathbb{K}$, $n \in \mathbb{N}$
Ausgabe: a^n

1 $b = 1$
2 solange $n \geq 1$ gilt:
3 wenn n ungerade ist, setze $b = ab$
4 setze $a = a^2$ und $n = \lfloor n/2 \rfloor$
5 return b

Lösung. Wegen $\lfloor n/2 \rfloor \leq n/2$ ist die Schleife spätestens nach $k = \lceil \log_2 n \rceil$ Durchläufen fertig, denn für dieses k gilt sicher $n/2^k < 1$. Jeder einzelne Schleifendurchlauf kostet eine konstante Anzahl von Operationen. Der Algorithmus hat also insgesamt eine Komplexität von $\mathrm{O}(k) = \mathrm{O}(\log(n))$.