Prof. Dr. H.-G. Gräbe, Uni Leipzig; Prof. Dr. J. Waldmann, HTWK Leipzig
Vorlesung Symbolisches Rechnen, Wintersemester 2014

Aufgabenblatt 8 vom 8. 12.

Zur Besprechung in der Übung am 11. 12.

Ü8-1 Gesucht ist eine LLL-reduzierte Basis $[b_1, b_2]$ in $\mathbb{Z}^2$ mit $|b_1| > |b_2|$ und $[b_2, b_1]$ ist nicht LLL-reduziert.

Ü8-2 Gitter Γ, Basis B, GSO von B ist B^*. Zeige: wenn $\forall i : |b_1| \leq |b_i^*|$, dann ist b_1 ein kürzester Vektor in Γ.

Ü8-3 Bestimme eine Lagrange-Gauß-reduzierte Basis für das von { [12,3], [56,7]} erzeugte Gitter.

Überprüfe daran die Behauptung aus S8-4.

Bestimme eine LLL-reduzierte Basis für dieses Gitter.

Ü8-4 Bestimme die ersten zwei Austausch-Schritte des LLL-Algorithums für `A7-3highscore`

Ü8-5 Gib Beispiele für die Ungleichung in S8-3 an. Kann man den Faktor 1/4 verbessern?

Besprechung weiterer Autotool-Aufgaben?

Besprechung der Aufgaben (S6-1) bis (S6-4).

autotool-Aufgaben

(werden evtl. noch gestellt)

nicht autotool, aber ähnlich: `http://www.latticechallenge.org/`

Löse die *toy challenge* (dim 200).

Löse wenigsten eine der echten challenges.

Vergleiche mit Einträge aus Highscore-Liste.

Dabei heißt *Lösen:* einen Vektor finden, der kürzer ist als alle aus der angegebenen Basis. (Bsp: für Dimension 200: kürzer als 30).

Zur schriftlichen Korrektur, Abgabe bis 5. 1., Besprechung am 8. 1.

S8-1 Die meisten CAS kennen exakte Werte von Winkelfunktionen mit dem Argument $\frac{m}{n}\,\pi$ und $n \leq 6$.
Bestimmen Sie exakte Werte von $\sin(15°)$ sowie von $\sin(6°)$ und erläutern Sie Ihr Vorgehen.
Hinweis: Wegen $6° = \frac{\pi}{30}$ gilt $\sin(6°) = \sin\left(\frac{\pi}{5} - \frac{\pi}{6}\right)$.

S8-2 Gegeben ist die Funktionenschar $f_k, k \in \mathbb{R}$, welche durch $f_k(x) = e^{-x/2} + \frac{k}{x}$ für $x \neq 0$ definiert ist.

a) Zeigen Sie, dass sich die Graphen zweier beliebiger Funktionen der Funktionenschar f_k nicht schneiden.

b) Geben Sie für die Funktionen f_{-2} und f_2 jeweils Nullstellen, Koordinaten der lokalen Extrempunkte und die Art der Extrema an.

c) Leiten Sie aus b) eine Vermutung über die Existenz von lokalen Extrempunkten der Funktionen f_k für allgemeines k (in Abhängigkeit von k) ab und beweisen Sie Ihre Vermutung.

   Analysieren Sie insbesondere den Fall $k < 0$ genau.

(Quelle: Sächsisches Abitur 2001, Leistungskurs Mathematik)

S8-3 Seien $g_1, \ldots, g_n \in \mathbb{R}^n$ linear unabhängig und $\Gamma = \mathbb{Z}g_1 + \cdots + \mathbb{Z}g_n$ das dadurch erzeugte Gitter. Beweise: $\forall x \in \mathbb{R}^n \exists y \in \Gamma : |x - y|^2 \leq 1/4 \sum_i |g_i|^2$.

S8-4 Beweise: wenn $[b_1, b_2]$ eine Lagrange-Gauß-reduzierte Basis für Gitter Γ ist,

- dann ist b_1 ein kürzester Vektor in Γ
- und b_2 ein kürzester Vektor in Γ, der von b_1 linear unabhängig ist.