Zahlentheorie und Kryptologie, Wintersemester 2012/13
M. Hortmann

Blatt 11

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen					Gruppe	Tutor
1	2a	b	c	d	**Summe**	**bearbeitet**
1	1	1	1	1	2 Pkte=100%	

Aufgabe 1

Sei $b_1, \ldots, b_n$ eine Basis des $\mathbb{R}^n$.
Im Gram-Schmidt-Prozeß wird daraus eine Orthogonalbasis[1]:

$$b_1^* := b_1$$
$$b_{i+1}^* := b_{i+1} - \sum_{j=1}^{i} \mu_{ij} b_j^* \text{ mit } \mu_{ij} := \frac{<b_i, b_j^*>}{<b_j^*, b_j^*>} .$$

Wählt man ein festes δ mit $1/4 < \delta \leq 1$, so nennt man die Basis $b_1, \ldots, b_n$ LLL-reduziert mit Reduktionskoeffizient δ, wenn $1 \leq j < i \leq n \rightarrow \mu_{ij} < 1/2$ und $1 \leq i < n \rightarrow (\delta - \mu_{i+1\,i}^2)\|b_i^*\|^2 \leq \|b_{i+1}^*\|^2$.

Rechnen Sie mit Pari oder Sage nach: die Spaltenvektoren der Matrix $\begin{pmatrix} -16 & -29 & 7 & -6 \\ 20 & 2 & 19 & 43 \\ -5 & 8 & 28 & -17 \\ 16 & -9 & 13 & 18 \end{pmatrix}$ bilden eine LLL-reduzierte Basis; bestimmen Sie den zugehörigen maximalen Reduktionskoeffizienten. Was ist die geometrische Interpretation der μ_{ij} ?

1 bei dieser Konstruktion keine Orthonormalbasis!

Aufgabe 2

a) Zeigen Sie $\prod_{n=2}^{\infty}\left(1-\frac{1}{n^2}\right)=\frac{1}{2}$.

b) Zeigen Sie, daß für $z\in\mathbb{C}$, $|z|<1$ gilt: $\prod_{n=0}^{\infty}\left(1+z^{2^n}\right)=\frac{1}{1-z}$.

c) Für welche $z\in\mathbb{C}$ konvergiert das Produkt $\prod_{n=1}^{\infty}\left(1+\frac{z}{n}\right)$?

d) Man zeige, daß das Produkt $\prod_{n=1}^{\infty}\left(1+\frac{z}{n}\right)\exp\left(-\frac{z}{n}\right)$ in ganz $\mathbb{C}$ absolut und lokal gleichmäßig konvergiert.

(Man nennt im obigen Produkt $\exp\left(-\frac{z}{n}\right)$ einen "konvergenzerzeugenden Faktor".
Eine Folge von Funktionen $f_n:\mathbb{C}\rightarrow\mathbb{C}$ konvergiert lokal gleichmäßig, wenn es zu jedem $z_0\in\mathbb{C}$ ein $\delta>0$ gibt, so daß $\forall\epsilon>0\,\exists n_0\in\mathbb{N}\,\forall m,n\geq n_0\,\forall z\in\mathbb{C}:\ |z-z_0|<\delta\ \rightarrow\ |f_n(z)-f_m(z)|<\epsilon$. Eine lokal gleichmäßig konvergente Folge stetiger Funktionen ist stetig und eine lokal gleichmäßig konvergente Folge komplex analytischer Funktionen ist komplex analytisch. Also wird durch obiges Produkt eine komplex analytische Funktion gegeben. Diese Funktion besitzt offenbar Nullstellen genau in den negativen ganzen Zahlen.)