Algoritmy na mřížích

Pavel Příhoda

24. října 2021

Obsah

1 Úvod

Definice 1.1. Mříž v n-dimenzionálním prostoru je množina $L \subseteq \mathbb{R}^n$ taková, že $\exists b_1, b_2, \dots, b_d \in \mathbb{R}^n$, LN (nad $\mathbb{R}$) tak, že $L = \mathbb{Z} b_1 + Z b_2 + \dots + \mathbb{Z} b_d = \{z_1 b_1 + z_2 b_2 + \dots + z_d b_d | z_1, \dots z_d \in \mathbb{Z}\}$.

Poznámka 1.2. $\{b_1, b_2, \dots, b_d\}$ se nazývá *báze* L. Není určená jednoznačně. $d = \dim < L >$, d je hodnost (rank) určená množinou L, $0 \le d \le n$.

1.1 Algebraická struktura mříží

- L je komutativní grupa (podgrupa grupy $(R^n, +)$)
- L je konečně generovaná (báze je množina generátorů)
- L je beztorzní ($\forall z \in \mathbb{Z}\ \forall \underline{l} \in L : z \cdot \underline{l} = 0 \implies z = 0 \vee \underline{l} = 0$)

Věta 1.3. *Každá beztorzní konečně generovaná komutativní grupa je volná.*

Důsledek 1.4. $(L, +) \simeq (\mathbb{Z}^d, +)$

Definice 1.5 (Euklidovská norma v $\mathbb{R}^n$). Nechť $u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$, $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$. Potom standradní skalární součin $\cdot$ definujeme jako $u \cdot v = \sum_{i=1}^n u_i v_i = u^T v$. *Euklidovskou normu* definujeme jako $\|u\| := \sqrt{u \cdot u} = \left(\sum_{i=1}^n u_i v_i\right)^{\frac{1}{2}}$.

1.2 Rozložení mříže v $\mathbb{R}^n$

Definice 1.6 (Diskrétní podgrupy $(\mathbb{R}^n, +)$). Podgrupa $G \subseteq (\mathbb{R}^n, +)$ je *diskrétní*, pokud

$$\forall g \in G\ \exists \varepsilon > 0 : G \cap \{v \in \mathbb{R}^n \,|\, \|v - g\| < \varepsilon\} = \{0\}.$$

Pozorování 1.7. $G \subseteq (\mathbb{R}^n, +)$ je diskrétní $\iff \exists \varepsilon > 0 : G \cap \{v \in \mathbb{R}^n \,|\, \|v\| < \varepsilon\} = \{0\}$

Důkaz. $\Rightarrow \checkmark$
$\Leftarrow$ vezmi $\varepsilon > 0$ tak, aby platila pravá strana tvrzení. Zvol $g \in G$ libovolné. Potom pro každé $v \in G$ splňující $\|v - g\| < \varepsilon$ platí $v = g$, neboť $v - g \in G$ a tedy z předpokladu $v - g = 0$.
Celkem tedy $G \cap \{v \in \mathbb{R}^n \,|\, \|v - g\| < \varepsilon\} = \{g\}$. □

Důsledek 1.8. *Je-li* $G \subseteq (\mathbb{R}^n, +)$ *diskrétní, pak* $\forall M \in \mathbb{R}^+\ |\{g \in G | \|g\| < M\}| < \infty$.

Důkaz. $B_M := \{v \in \mathbb{R}^n \,|\, \|v\| < M\}$, $B_\varepsilon := \{v \in \mathbb{R}^n \,|\, \|v\| < \varepsilon\}$, kde $\varepsilon > 0$ splňuje $B_\varepsilon \cap G = \{0\}$. $X := G \cap B_M$, $B_{\frac{\varepsilon}{2}} := \{v \in \mathbb{R}^n \,|\, \|v\| < \frac{\varepsilon}{2}\}$. Potom $\forall g_1, g_2 \in G : g_1 \neq g_2 \implies (g_1 + B_{\frac{\varepsilon}{2}}) \cap (g_2 + B_{\frac{\varepsilon}{2}}) = \emptyset$, neboť $\|g_1 - g_2\| \ge \varepsilon$.

$$\begin{aligned} \dot{\bigcup_{x \in X}} x + B_{\frac{\varepsilon}{2}} &\subseteq B_{M+\varepsilon} \\ |X| \cdot \mathrm{vol}(B_{\frac{\varepsilon}{2}}) &\le \mathrm{vol}(B_{M+\varepsilon}) \\ |X| &\le \frac{\mathrm{vol}(B_{M+\varepsilon})}{\mathrm{vol}(B_{\frac{\varepsilon}{2}})} < \infty \end{aligned}$$

□

Tvrzení 1.9. *Každá n-dimenzionální mříž je diskrétní podgrupa* $(\mathbb{R}^n, +)$.

Důkaz. Indukcí dle hodnosti mříže $L(d)$. (Případ $d = 0$ platí, ale vynecháme jej.)
$\boxed{d = 1}$ tj. $\exists_1 \in \mathbb{R}^n$, $b_1 \neq 0$, $L = \mathbb{Z}b_1$ $0 \neq b \in L \iff l = zb_1,\ z \in \mathbb{Z}\setminus\{0\}$.
$\|l\| = |z| \cdot \|b_1\| \geq \|b_1\| \implies \varepsilon = \|b_1\|$ projde.
$\boxed{d > 1}$ $\{b_1, \ldots, b_d\}$ báze L. Definujme $L_0 = \mathbb{Z}b_1 + \mathbb{Z}b_2 + \cdots + \mathbb{Z}b_{d-1}$. To odpovídá bázi $\{b_1, \ldots, b_{d-1}\}$, potom z indukčního předpokladu $\exists \varepsilon_0 > 0$ takové, že $\forall l \in L_0 \setminus \{0\}$ $\|l\| \geq \varepsilon_0$. Platí, že $\mathbb{R}^n = \langle L_0 \rangle \oplus \langle L_0 \rangle^\perp$. Z toho plyne $\forall v \in \mathbb{R}^n$ $\exists v_0, v^\perp \in \mathbb{R}^n$ $v = v_0 + v^\perp,\ v_0 \in \langle L_0 \rangle,\ v^\perp \in \langle L_0 \rangle^\perp$.

$$0 \neq l = z_1 b_1 + z_2 b_2 + \cdots + z_d b_d,\ z_1, \ldots, z_d \in \mathbb{Z}$$

1. $z_d = 0 \implies l \in L_0 \setminus \{0\} \overset{\text{I.P.}}{\implies} \|l\| \geq \varepsilon_0$ a důkaz je hotov, nebo
2. $z_d \neq 0\ \ldots\ l = l_0 + l^\perp \implies \|l\| \geq \|l^\perp\| = \|z_d b_d^\perp\|$
   $b_d \notin L_0$, neboť $b_1, \ldots, b_d$ jsou LN $\implies b_d = \underset{\in L_0}{b_{d_0}} + \underset{\neq \emptyset}{b_d^\perp} \implies \|l\| \geq |z_d| \cdot \|b_d^\perp\| \geq \|b_d^\perp\| > 0.$

   Tedy platí, že $\|l\| \geq \min\{\varepsilon_0, \|b_d^\perp\|\}$

□

2 Výpočetní problémy na mřížích

SVP - shortest vector problem

Definice 2.1 (První postupné minimum). Nechť $0 \neq L \subseteq (\mathbb{R}^n, +)$ je n-dimenzionální mříž. Definujeme *první postupné minimum* $\lambda_1(L) := \min\{\|v\| : 0 \neq v \in L\}$. Toto minimum existuje, neboť $\forall l : 0 \neq l \in L$, $\{v \in L \setminus \{0\} : \|v\| \leq \|l\|\}$ je konečná.

Definice 2.2 (Nejkratší vektor L). Nechť $0 \neq L \subseteq (\mathbb{R}^n, +)$ je n-dimenzionální mříž. v je *nejkratší vektor* L, pokud $\|v\| = \lambda_1(L)$

Poznámka 2.3. v je nejkratší vektor $L \iff -v$ je nejkratší vektor L.

Poznámka 2.4. $L = \mathbb{Z}^2 \subseteq (\mathbb{R}^2, +)$ má tyto nejkratší vektory: $\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\-1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}-1\\0\end{pmatrix}$.

Definice 2.5 (Formulace SVP).
Vstup: Mříž zadaná bází.
Výstup: Nejkratší vektor L (stačí jeden libovolný).

Věta 2.6 (M. Ajtai, 1998). SVP *je* NP-*hard (*NP-*těžký).*

Definice 2.7 (SVP_γ). (aproximační verze SVP)
Definujeme aproximační faktor $\gamma : \mathbb{N} \to \mathbb{R}^+$.
Vstup SVP_γ: n-dimenzionální mříž zadaná bází.
Výstup: $0 \neq v \in L$ takový, že $\forall 0 \neq v \in L : \gamma(n) \cdot \|u\| \geq \|v\|$.

Věta 2.8 (A. K. Lenstra, H. W. Lenstra, L. G. Lowász, 1982).

$$\mathrm{SVP}_{2^{\frac{n-1}{2}}}$$

je řešitelný v polynomiálním čase.

Definice 2.9 (Gap SVP_γ). (rozhodovací verze SVP_γ)
$L \subseteq (\mathbb{R}^n, +)$ mříž, úplná (hodnost $= n$), víme, že $\lambda_1(L) \leq 1$ nebo $\lambda_1(L) \geq \gamma(n)$. Máme rozhodnout, který případ nastává.

Learning with errors: Odvozuje se od BDD$_\gamma$ (bounded distance decoding)

Definice 2.10 (BDD$_\gamma$ - bounded distance decoding). $L \subseteq (\mathbb{R}^n,+), v \in \mathbb{R}^n$. Víme: $dist(v,L) < \frac{\lambda_1(L)}{2\gamma(n)}$. Chceme najít vektor $l \in L$, který tuto nerovnost dokazuje, tedy splňuje

$$\|v-l\| < \frac{\lambda_1(L)}{2\gamma(n)}$$

.

Poznámka 2.11. $l_1 \neq l_2 \in L$, $\|l_1 - l_2\| \geq \lambda_1(L)$
Pak $|\{u \in \mathbb{R}^n : \|u-v\| < \frac{\lambda_1(L)}{2} \cap L\}| \leq 1$

Definice 2.12 (i-té postupné minimum). $L \subseteq (\mathbb{R}^n,+)$ mříž hodnosti d. Pro $i \in \{1,\ldots,d\}$ definujeme *i-té postupné minimum* $\lambda_i(L) = \min\{r \in \mathbb{R} : L$obsahuje i LN vektorů normy $\leq r\}$

Definice 2.13 (SIVP$_\gamma$ - short independent vectors problem). Dána $L \subseteq (\mathbb{R}^n,+)$ úplná. Chceme nalézt $S = \{s_1,\ldots,s_n\} \subseteq L$ lineárně nezávislé tak, aby $\|s_i\| \leq \gamma(n) \cdot \lambda_n(L)$.

Definice 2.14 (SIS$_{n,q,s,m}$ - short integer soultion). Nechť $q \in \mathbb{N}$. Volíme náhodně $a_1, a_2, \ldots, a_m \in \mathbb{Z}_q^n$. $A := (a_1|a_2|\cdots|a_m)$, $n \times m$ nad $\mathbb{Z}_q$. Chceme najít $0 \neq t \in \mathbb{Z}^m$ $\|z\| \leq \beta, Az \equiv 0 \pmod q$

Poznámka 2.15. $L = \{n \in \mathbb{Z}^m : An \equiv 0 \pmod q\}$ je celočíselná mříž obsahující $q : \mathbb{Z}^m$ (q-ární mříž)

Příklad 2.16. $2^m > q^n (m > n \cdot \log(q))$. Vezmeme $f_A : \{0,1\}^m \to \mathbb{Z}_q^n$ $f_A(n) := An \mod q$
$\exists u_1 \neq u_2 \in \{0,1\}^m : f_A(u_1) = f_A(u_2)$
$z = u_1 - u_2 \in \{0,1\}^m, O < \|z\| \leq \sqrt{m},\ Az \equiv 0 \pmod q$.
Potom z řeší SIS$_{n,q,\sqrt{m},n}$.

Věta 2.17 (M. Ajatai, 1996). *Nechť $m = \mathrm{poly}(n), q \geq \beta\,\mathrm{poly}(n)$. Pokud existuje algoritmus řešící SIS$_{n,q,\beta,n}$ s nezanedbatelnou pravděpodobností, pak existuje srovnatelně efektivní algoritmus, který řeší SIVP$_\gamma$ s nezanedbatelnou pravděpodobností pro všechny instance $n-$dimenzionálních mříží, kde $\gamma = \mathrm{poly}(n) \cdot \beta$.*

Příklad 2.18. Nechť $2^m > q^n$, $\beta \geq \sqrt{m}$. Díváme se na $\{f_A : A \in M_{n,m}(t_q)\}$ jako na množinu hashovacích funkcí, která má q^n prvků. Hledáme v ní náhodnou kolizi (speciální případ SIS$_{n,q,\beta,m}$). Důkaz obtížnosti SIVP$_\gamma$ pro odpovídající γ povede k důkazu obtížností problému hledání kolizí.

3 Lineární algebra nad $\mathbb{Z}$

Definice 3.1 (volná grupa). konečně generovaná komutativní grupa G je *volná*, pokud $\exists b_1, b_2, \ldots, b_d \in G$ takové, že $\forall g \in G \quad \exists! z_1, z_2, \ldots, z_d \in \mathbb{Z}$ tak, aby $g = z_1 b_1 + z_2 b_2 + \cdots + z_d b_d$. Množina $\{b_1, b_2, \ldots, b_d\}$ se nazývá *volná báze G*.

Poznámka 3.2. $G = O$ volná grupa s volnou bází $\emptyset$
$L \subseteq (\mathbb{R}^n,+)$ mříž. Potom báze mříže je volná báze grupy $(L,+)$
$(\mathbb{Z}^n,+)$ Potom volná báze např. $\{e_1, e_2, \ldots, e_n\}, e_1 = \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, \ldots, e_n = \begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix}$

Tvrzení 3.3. *Konečně generovaná volná grupa je izomorfní $(\mathbb{Z}^n,+)$ pro nějaké $n \in \mathbb{N}$.*

Důkaz. G s volnou bází is $\{b_1, + \dots, b_d\}$ $\varphi : \mathbb{Z}^d \to G$ $\begin{pmatrix} z_1 \\ \vdots \\ z_d \end{pmatrix} \to \sum_{i=1}^d z_i b_i$ je izomorfizmus grup. $\square$

Tvrzení 3.4. $(\mathbb{Z}^{d_1}, +) \simeq (\mathbb{Z}^{d_2}, +) \Rightarrow d_1 = d_2$

Důkaz. $\varphi : \mathbb{Z}^{d_1} \to \mathbb{Z}^{d_2}$
$\varphi/2\mathbb{Z}^{d_i} : 2\mathbb{Z}^{d_1} \to \mathbb{Z}^{d_2}$
tyto dvě věci implikují: $\mathbb{Z}^{d_1}/2\mathbb{Z}^{d_2} \simeq \mathbb{Z}^{d_2}/2\mathbb{Z}^{d_2} \implies 2^{d_1} = 2^{d_2} \implies d_1 = d_2$. $\square$

Důsledek 3.5. *$\{b_1, \dots, b_d\}, \{b'_1, \dots, b'_d\}$ volné báze komutativní volné grupy $G \Rightarrow d = d'$. ($G \simeq (\mathbb{Z}^d, +) \simeq (\mathbb{Z}^{d'}, +)$)*

Definice 3.6 (rank grupy). Rankem volné komutativní grupy G rozumíme počet prvků nějaké její volné báze.

Tvrzení 3.7. *$\forall \varphi : (\mathbb{Z}^n, +) \to (\mathbb{Z}^m, +)$ hom. $\exists! A \in M_{m,n}(\mathbb{Z})$ tak, že $\varphi(u) = A \cdot u \forall u \in \mathbb{Z}^n$.*

Důkaz. Pro $i = 1, \dots, n$: $\varphi(e_i) =: a_i \in \mathbb{Z}^m$. Dále $A := (a_1|a_2|\dots|a_n)$. Potom $Au = A \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} =$
$\sum_{i=1}^n u_i a_i = \sum_{i=1}^n u_i \varphi(e_i) = \varphi(\sum_{i=1}^n u_i e_i) = \varphi(\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}) = \varphi(n)$.
Jednoznačnost: $\varphi(u) = A \cdot u \implies \varphi(e_i) = Ae_i \implies \varphi(e_i)$ musí být i-tý sloupec matice A. $\square$

3.1 Souřadnice

Nechť G je konečně generovaná volná komutativní grupa a $B = \{b_1, \dots, b_d\}$ je volná báze G.
Pro $g \in G$ je $[g]_B = \begin{pmatrix} z_1 \\ \vdots \\ z_d \end{pmatrix} \in \mathbb{Z}^d$, kde $g = \sum_{i=1}^d z_i b_i$, souřadnice g vzhledem k bázi B.

Definice 3.8 (Matice homomorfismu). Nechť $0 \neq G, H$ jsou konečně generované volné komutativní grupy, B_G volná báze G, B_H volná báze H.
$\varphi : G \to H$ homomorfismus $[\varphi]_{B_H}^{B_G}$ je matice $|B_H| \times |B_G|$ nad $\mathbb{Z}$ splňující $[\varphi]_{B_H}^{B_G} \cdot [g]_{B_G} = [\varphi(g)]_{B_H}$ pro každé $g \in G$

Sestrojí se tak, že $[\varphi]_{B_H}^{B_G} = ([\varphi(b_1)]_{B_H} | [\varphi(b_2)]_{B_H} | \dots | [\varphi(b_d)]_{B_H})$, $B_G = \{b_1, \dots, b_d\}$

Tvrzení 3.9. *$\varphi : G \to H, \psi : H \to K$, G, H, K volné komutativní grupy,
B_G, B_H, B_K jejich volné báze*
$[\psi \circ \varphi]_{B_K}^{B_G} = [\psi]_{B_K}^{B_H} \cdot [\psi]_{B_H}^{B_G}$

Důkaz. Stejný důkaz jako v lineární algebře $\square$

opakování

- Každá konečně generovaná volná komutativní grupa G je isomorfní $(\mathbb{Z}^n, +)$, kde $n \in \mathbb{N}_0$ je *rank grupy G.*
- $\varphi : \mathbb{Z}^n \to \mathbb{Z}^m$ maticová násobení: $\exists! A \in M_{m,n}(\mathbb{Z}) : \varphi(u) = Au \forall u \in \mathbb{Z}$. Potom tedy A je matice φ vzhledem ke kanonickým bazím.

- $M_n(\mathbb{Z})$ značí množinu všech čtvercových matic $n \times n$ nad $\mathbb{Z}$. E značí jednotkovou matici.
- $\mathrm{adj}(A)$ značí adjungovanou matici (TODO: přidat odkaz :D)
- K značí kanonickou bázi.

3.2 Unimodulární matice

Definice 3.10. $A \in M_n(\mathbb{Z})$ je *unimodulární*, pokud $\det(A) = \pm 1$. $GL(n,\mathbb{Z})$ je *množina všech unimodulárních matic* stupně n.

Lemma 3.11. *$A \in M_n(\mathbb{Z})$ je unimodulární $\Leftrightarrow$ A je regulární a $A^{-1} \in M_n(\mathbb{Z})$.*

Důkaz. $\Rightarrow$:
Mějme regulární $A \in M_n(\mathbb{Z})$. Potom $A \cdot A^{-1} = E \Rightarrow \det(A) \cdot \det(A^{-1}) = 1$. Ale jelikož $A, A^{-1} \in M_n(\mathbb{Z})$, tak $\det(A), \det(A^{-1}) \in \mathbb{Z}$ a tedy $\det(A) = \pm 1 = \det(A^{-1})$.
$\Leftarrow$:
$A^{-1} = \frac{1}{\det(A)} \cdot \mathrm{adj}(A)$. $\det(A)$ je ± 1 z definici unimodulární matice. $\mathrm{adj}(A) \in M_n(\mathbb{Z})$, protože všechny subdeterminanty (?) A jsou celočíselné. Nakonec A je regulární, protože je unimodulární. $\square$

Tvrzení 3.12. *Homomorfismus $\varphi : \mathbb{Z}^n \leftarrow \mathbb{Z}^n$ je isomorfismus $\Leftrightarrow$ $A = [\varphi]^K_K$ je unimodulární.*

Důkaz. $\Leftarrow$:
Mějme $\psi = \varphi^{-1}$. Označme $B = [\psi]^K_K$. Potom $A \cdot B = [\varphi]^K_K \cdot [\psi]^K_K = [\varphi \circ \psi]^K_K = [id]^K_K = E \Rightarrow B = A^{-1}$. Tedy A je regulární. Dále $B = [\psi]^K_K = (\psi(e_1)|\psi(e_2)|\dots|\psi(e_n)) \in M_n(\mathbb{Z})$, protože $\psi : \mathbb{Z}^n \leftarrow \mathbb{Z}^n$.
$\Rightarrow$:
$A = [\varphi]^K_K$ je unimodulární. Označme tedy $B = A{-}1 \in M_n(\mathbb{Z})$. Mějme zobrazení $\psi : \mathbb{Z}^n \leftarrow \mathbb{Z}^n$ definované vztahem $\psi(u) = B \cdot u$ pro $u \in \mathbb{Z}^n$. Potom $\varphi \circ \psi(u) = A \cdot B \cdot u = A \cdot A^{-1} \cdot u = u = B \cdot A \cdot u = \psi \circ \varphi(u)$. Tedy $\psi = \varphi^{-1}$. $\square$

Poznámka 3.13. Vezmene mříž s hezkou bází a tu potom schováme $\Rightarrow$ dostaneme kryptosystém.

3.3 Hermitův tvar regulární celočíselné matice

Definice 3.14. $A \in M_n(\mathbb{Z})$ regulární je v *Hermitově normálním tvaru (HNF)*, pokud:

- A je horní trojúhelníková
- na diagonále A jsou kladná čísla
- $\forall i \in \{1, \dots, n\} \forall j \in \{i+1, \dots, n\} : a_{i,j} \in \{0, \dots, a_{i,i} - 1\}$

Poznámka 3.15. Tedy matice A je v HNF, pokud je horní trojúhelníková, má na diagonále kladná čísla a všechny prvky vpravo od diagonály jsou menší než prvek na diagonále na stejném řádku.

Věta 3.16. *$\forall A \in M_n(\mathbb{Z})$ regulární $\exists! B, U \in M_n(\mathbb{Z}) : B$ je HNF, $U \in GL(n,\mathbb{Z})$, $B = A \cdot U$*

Důkaz. existence:
(algoritmem)
Na sloupce A opakovaně aplikujeme úpravy, které nemění absolutní hodnotu determinantu:

- permutace sloupců
- přenásobení sloupce -1

- přičtení celočíselné lineární kombinace ostatních sloupců k jinému sloupci

Potom tedy $A \cdot U_1 \cdot U_2 \cdot \dots \cdot U_t = B$ je HNF a $U = U_1 \cdot U_2 \cdot \dots \cdot U_t \in GL(n, \mathbb{Z})$.
Algoritmus:

1. $B := A$
2. $i := n$ *//na rozdíl od Gaussovy eliminace postupujeme od pravého dolního rohu doleva nahoru*
3. dokud $b_{i,1}, b_{i,2}, \dots, b_{i,i-1}$ nejsou 0:
   - permutujeme prvních i sloupců B tak, aby platilo: $\|b_{i,i}\| = \min\{\|b_{i,j}\| : 1 \leq j \leq i, b_{i,j} \neq 0\}$
   - pokud $b_{i,i} < 0$, tak vynásobíve $i-$tý sloupec -1
   - pro $j \in \{1, \dots, i-1\}$ označíme $q = \lfloor \frac{b_{i,j}}{b_{i,i}} \rfloor$ a od $j-$tého sloupce odečteme $q-$násobek $i-$tého sloupce. *//dělení se zbytkem*
4. pokud $b_{i,i} < 0$, tak vynásobíve $i-$tý sloupec -1
5. *//čísla vpravo od $b_{i,i}$ taky vydělíme se zbytkem*
   pro $j \in \{i+1, \dots, n\}$ označíme $q = \lfloor \frac{b_{i,j}}{b_{i,i}} \rfloor$ a od $j-$tého sloupce odečteme $q-$násobek $i-$tého sloupce.
6. pokud $i > 1$, tak od i odečteme 1 a pokračujeme znovu od kroku 2.
7. **return** B

Poznámka 3.17. Při výpočtu B může dojít k velké expanzi koeficientů.

jednoznačnost:
Mějme $B = A \cdot U$ a $C = A \cdot V$ takové, že $B, C, U, V \in M_n(\mathbb{Z})$, B, C jsou v HNF a $U, V \in GL(n, \mathbb{Z})$. Jelikož $B = A \cdot U$ a $C = A \cdot V$, tak $C = B \cdot U^{-1} \cdot V$. Označme $W = U^{-1} \cdot V \in GL(n, \mathbb{Z})$. Víme, že $W = B^{-1} \cdot C$ a tedy je W horní trojúhelníková a na diagonále má $\frac{c_{i,i}}{b_{i,i}}$. Jelikož $W = U^{-1} \cdot V$, tak $\det(W) = 1$ a tedy i $w_{1,1} = w_{2,2} = \dots = w_{n,n} = 1$. Tedy $b_{i,i} = c_{i,i} \forall i$.
Chceme dokázat $W = E$. Označme z prvek v $i-$tém sloupci nad diagonálou, který je nenulový. Označme j řádek, ve kterém leží z. Dále označme $C = (c_1 \| c_2 \| \dots \| c_n) = (b_1 \| b_2 \| \dots \| b_n) \cdot W = B \cdot W$. Potom $c_i = b_i + z b_j +$ nějaká celočíselná LK $b_1, \dots, b_{j-1}$. Tedy $c_{j,i} = b_{j,i} + z b_{j,j}$. Ale $c_{j,i} \in \{0, \dots, c_{j,j} - 1\}$ a $b_{j,i} \in \{0, \dots, b_{j,j} - 1\}$ a tedy $z = 0$, protože jinak by $c_{j,i}$ bylo moc velké. $\square$

3.4 HNF obecné matice

Definice 3.18. $A \in M_n(\mathbb{Z})$ je v *HNF*, pokud $\exists r \in \{0, \dots, n\}$ a $f : \{r+1, \dots, n\} \leftarrow \{1, \dots, m\}$ ostře rostoucí takové, že:

- prvních r sloupců A je nulových
- $\forall j \in \{r+1, \dots, n\} : a_{f(j),j} \geq 1$ *//"pivot"*
- $\forall j \in \{r+1, \dots, n\} \forall f(j) < i \leq m : a_{i,j} = 0$ *//pod pivotem jsou nuly*
- $\forall k < j \in \{r+1, \dots, n\} : 0 \leq a_{f(k),j} < a_{f(k),k}$

Věta 3.19. *$\forall A \in M_{m,n}(\mathbb{Z}) \exists B \in M_{m,n}(\mathbb{Z}), U \in GL(n, \mathbb{Z})$, kde B je HNF a $B = A \cdot U$. Navíc matice B je jednoznačně určená.*

Důkaz. není $\square$

Tvrzení 3.20. *$A, B \in M_{m,n}(\mathbb{Z})$. Nechť $\exists U \in GL(n,\mathbb{Z}) : A = B \cdot U$. Pak sloupce matice A generují v $\mathbb{Z}^n$ stejnou podgrupu jako sloupce matice B.*

Důkaz. $A = (a_1 \| a_2 \| \dots \| a_n) = (b_1 \| b_2 \| \dots \| b_n) \cdot U$. Každé a_i je tedy celočíselná LK $b_1, \dots, b_n$. Tedy $\langle a_1, a_2, \dots, a_n \rangle_{\mathbb{Z}^n} \subseteq \langle b_1, b_2, \dots, b_n \rangle_{\mathbb{Z}^n}$. Jelikož ale také $B = A \cdot U^{-1}$, tak i $\langle b_1, b_2, \dots, b_n \rangle_{\mathbb{Z}^n} \subseteq \langle a_1, a_2, \dots, a_n \rangle_{\mathbb{Z}^n}$ $\square$

Důsledek 3.21. *$\forall$ konečně generovaná podgrupa $(\mathbb{Z}^n, +)$ je volná komutativní grupa*

Důkaz. Mějme $G \subseteq (\mathbb{Z}^n, +)$ podgrupu. Označme generátory $G = \langle g_1, g_2, \dots, g_n \rangle$. Mějme $A := (g_1 \| g_2 \| \dots \| g_n) \in M_{m,n}(\mathbb{Z})$. Poslední věta nám implikuje, že $\exists B$ HNF, $V \in GL(n,\mathbb{Z}) : B = A \cdot U$. Nenulové sloupce B generují G a jsou lineárně nezávislé $\Rightarrow$ tvoří volnou bázi G.
//a taky jsme tím dokázali, že je to mříž $\square$

opakování

Minule: AB $\in M_{m,n}(\mathbb{Z})$ AU=B U in GL, sloupce matic A,B generují stejnou podgrupu $(\mathbb{Z}^m, +)$

Poznámka 3.22. Každá podgrupa konečně generované komutativní grupy je konečně generovaná.

Příklad 3.23. $A = \begin{pmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 & 1 & 1 \end{pmatrix}$. Určete volnou bázi grupy $G = \{u \in \mathbb{Z}^4 \,|\, A \cdot u \equiv 0 (\mathrm{mod}\, 5)\}$:
Vyřeším soustavu $A \cdot u = 0$ nad $\mathbb{Z}_5$

$$\begin{pmatrix} 1 & 1 & 2 & 3 \\ 0 & 1 & -1 & -2 \end{pmatrix}, \; u_1 = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \; u_2 = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$\forall u \in G, (u \bmod 5) \in \mathbb{Z} u_1 + \mathbb{Z} u_2$

$$\begin{pmatrix} 5 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 5 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 5 \end{pmatrix}, \; u_1, \; u_2 \text{ generují G.}$$

$\exists z_1, z_2 : z_1 u_+ + z_2 u_2 \equiv u \mod 5$

$$z_1 u_1 + z_2 u_2 - u = \begin{pmatrix} 5a_1 \\ 5a_2 \\ 5a_3 \\ 5a_4 \end{pmatrix} \implies u = z_1 u_1 + z_2 u_2 + a_1 \cdot \begin{pmatrix} 5 \\ 0 \\ 0 \\ 0 \end{pmatrix} + a_2 \cdot \begin{pmatrix} 0 \\ 5 \\ 0 \\ 0 \end{pmatrix} + a_3 \cdot \begin{pmatrix} 0 \\ 0 \\ 5 \\ 0 \end{pmatrix} + a_4 \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 5 \end{pmatrix}$$

HNF

$$\begin{pmatrix} 5 & 0 & 0 & 0 & 2 & 0 \\ 0 & 5 & 0 & 0 & 1 & 2 \\ 0 & 0 & 5 & 0 & 1 & 0 \\ 0 & 0 & 0 & 5 & 0 & 1 \end{pmatrix} \sim \dots \sim \begin{pmatrix} 0 & 0 & 5 & 0 & 2 & 0 \\ 0 & 0 & 0 & 5 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Označíme nenulové sloupce $z_1 = \begin{pmatrix} 5 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $z_2 = \begin{pmatrix} 0 \\ 5 \\ 0 \\ 0 \end{pmatrix}$, $z_3 = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \end{pmatrix}$, $z_4 = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 1 \end{pmatrix}$. Poté $\{z_1, z_2, z_3, z_4\}$ tvoří volnou bázi G.

3.5 Soustavy lineárních diofantických rovnic

$A \in M_{m,n}(\mathbb{Z})$, hledáme $R = \{u \in \mathbb{Z} | A \cdot u = 0\}$... podgrupa $\mathbb{Z}^n$. Hledáme volnou bázi R. $\exists U \in GL(n,\mathbb{Z})$, AU je v HNF, $A \cdot (u_1|u_2|\dots|u_n) =$ (obrazek s nulami - viz Martin Pastyrik). $u_1, u_2, \dots, u_r \in R$, $u_1, u_2, \dots, u_r$ LN (nad $\mathbb{Q}$), U je regulární, $u \in R$, $Au = 0 \implies (AU)(U^{-1}u) = 0 \implies U^{-1}u \in \begin{pmatrix} * \\ \vdots \\ * \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

(r hvězdiček, pak nuly) $\implies \exists \begin{pmatrix} z_1 \\ \vdots \\ z_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{Z}^n$, $u = U \begin{pmatrix} z_1 \\ \vdots \\ z_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} = z_1u_1 + z_2u_2 + \dots + z_ru_r$

Příklad 3.24. Určete celočíselné řešení rovnice $2x + 3y + 5z = 0$

$$\left(\begin{array}{ccc} 2 & 3 & 5 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc} 2 & 3 & 5 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc} 5 & 3 & 2 \\ \hline 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc} 1 & 1 & 2 \\ \hline -2 & -1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc} 1 & 2 & 1 \\ \hline -2 & 1 & -1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc} 0 & 0 & 1 \\ \hline -1 & 3 & -1 \\ -1 & -2 & 1 \\ 1 & 0 & 0 \end{array}\right) =: U$$

3.6 Jednozančnost HNF

$A \in M_{m,n}(\mathbb{Z})$, $U, U' \in \mathrm{GL}(n,\mathbb{Z})$, $AU = B, AU' = B'$ obě v HNF. Pak $B = B'$. G... podgrupa $\mathbb{Z}^m$ generovaná sloupci A. Sloupce B, sloupce B' rovněž generují G.

definice B a B'pomocí obrázků,. viz Martin P.

$r = n - \text{rank } G$, $r' = n - \text{rank } G \implies r = r'$

$L_1 = \left\{ \begin{pmatrix} z_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \middle| z_1 \in \mathbb{Z} \right\}$, $L_2 = \left\{ \begin{pmatrix} z_1 \\ z_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \middle| z_1, z_2 \in \mathbb{Z} \right\}$ atp., tj. L_i má na prvních i souřadnicích z_1 až z_i, dále samé nuly.

$G_i = G \cap L_i$, $f(r+i) = \min\{j \in \{1,\dots,m\} \mid \text{rank } G_j = i\} = f'(r+i)$

$b_{f(r+i),r+i} = b'_{f(r+i),i}$ (z definice jsou oba kladné)

$b_{f(n),n}$: podívám se na poslední nenulový řádek matice A... vidím, že $b_{f(n),n}$ je NSD prvků v posledním řádku A.

Vidíme, že $b_{f(n),n} | b'_{f(n),n}$ a zároveň $b'_{f(n),n} | b_{f(n),n}$.

$B = B' \cdot W$, $W = U^{-1} \cdot U$

např. b'_i je (r+i)-tý sloupec B', $b'_i \in G$

$b'_i \dots$ celočíselná lineární kombinace sloupců B (ale kterých??)

$b'_i = b_i +$ LK sloupců vlevo od b_i

$\vdots$

$b_{f(r+i),r+i} = b'_{f(r+i),r+i}$

$r < j < k \leq n$, $b_{f(j),k} \in \{0,\dots,b_{f(j),k}-1\}$ vynutí, že LK sloupců vlevo od b_i je triviální.

3.7 Smithova normální forma

Definice 3.25 (Smithův normální tvar). $A \in M_n(\mathbb{Z})$ je ve *Smithově normálním tvaru* (SNF), pokud je diagonální $A = diag(a_1,a_2,\dots,a_n), a_1,\dots,a_n \in \mathbb{N}_0$, $\forall i \in \{1,\dots,n-1\} a_{i+1}|a_i$

Věta 3.26. *Pro všechny matice $A \in M_n(\mathbb{Z})$ $\exists U,V \in \mathrm{GL}(n,\mathbb{Z})$ takové, že UAV je ve Smithově normálním tvaru.*

Definice 3.27. Součin UAV je určený jednoznačně a nazývá se Smithova normální forma A.

K důkazu existence: Na řádky/sloupce aplikujeme tyto úpravy

- permutace řádků, permutace sloupců
- řádek/sloupec přenásobíme (-1)
- k sloupci přičíst celočíselnou LK ostatních sloupců
- k řádku přičíst celočíselnou LK ostatních řádků

...snažíme se A převést do SNF

Věta 3.28. *Nechť G je konečně generovaná volná komutativní grupa, H podgrupa G. Pak $\{b_1,\dots,b_d\}$ volné báze G, $z_1,z_2,\dots,z_d \in \mathbb{Z}$ tak, že $\{z_1b_1,z_2b_2,\dots,z_db_d\} \setminus \{0\}$ je volná báze H.*

Idea důkazu:
$G \simeq (\mathbb{Z}^d,+)$, BÚNO $G = \mathbb{Z}^d$, H je konečně generovaná volná komutativní grupa ranku $\leq d$, $\{h_1,h_2,\dots,h_l\}$ volná báze H.

$$A = (h_1|h_2|\dots|h_l|0|\dots|0)\ \exists U,V \in \mathrm{GL}(d,\mathbb{Z})\ UAV = \mathrm{diag}(z_1,\dots,z_d)$$

H... podgrupa $\mathbb{Z}^d$ generovaná sloupci A = podgrupa generovaná sloupci AV
$\phi_U : \mathbb{Z}^d \to \mathbb{Z}^d$, $\phi_U(v) := U \cdot v$... automorfismus $\phi_U(H)$ je volná kom. grupa s volnou bází $\{z_1e_1,z_2e_2,\dots,z_de_d\} \setminus \{0\}$, kde e_i je i-tý vektor kanonické báze.
$b_i := \phi_U^{-1}(e_i) = U^{-1} \cdot e_i$
$\{b_1,\dots,b_d\}$ volná báze $(\mathbb{Z}^d,+)$
$\{z_1b_1,\dots,z_db_d\} \setminus \{0\}$ je volná báze $\varphi_U^{-1}(\varphi_U(H)) = H$

3.8 Opakování

L úplná mříž v $\mathbb{R}^n$. Pak $\exists x_1,x_2,\dots,x_n \in L$ lineárně nezávislé, $\|x_i\| = \lambda_i(L)$ $\forall 1 \leq i \leq n$ x_i nenulový vektro L s nejmenší normou ... $\|x_1\| = \lambda_1(L)$
x_1,x_i máme, x_{i+1} vektor z $L \setminus <x_1,\dots,x_i>_\mathbb{R}$ s nejmenší normou
$\|x_i\| \geq \lambda_i(L)$. Pokud $\|x_i\| > \lambda_i(L)$, $M = \{v \in L | \|v\| < \|x_i\|\}$ obsahuje i LN vektorů. Proto $M \setminus <x_1,\dots,x_{i-1}>_\mathbb{R} \neq \emptyset$, i-tý vektor by měl mít normu $< \|x_i\|$

Máme $x_1,\dots,x_n \in L$ LN $\|x_i\| = \lambda_i(L)$, $v \in L \setminus \{0\}$. Nechť $k \in \mathbb{N}$ je největší takové, že $\|v\| \geq \lambda_k(L)$. Pak $v \in <x_1,x_2,\dots,x_k>_\mathbb{R}$

- Pokud $k = n \to x_1,\dots,x_n$ je báze $\mathbb{R}^n$
- $k < n \to$ Nechť $v \notin <x_1,\dots,x_k>_\mathbb{R}$, $M = \{u \in L | \|u\| \leq \|v\|\}$ obsahuje $x_1,x_2,\dots,x_k,v \to \lambda_{kM}(L) \leq \|v\|\dots$ spor s volbou k

3.9 Gram-Schmidtova ortogonalizace

$b_1, b_2, \dots, b_k$ LN vektory v $\mathbb{R}^n$. G-S ortogonalizace nalezne $b_1^*, b_2^*, \dots, b_k^* \in \mathbb{R}^n$ splňující

1. $b_i^* \cdot b_j^* = 0 \ \forall 1 \leq i \neq j \leq k$
2. $b_i^* = b_i - x_i, \ x_i \in < b_1, \dots, b_{i-1} >_{\mathbb{R}}$ pro $i = 1, \dots, k$ $(i = 1 \implies b_1 = b_1^*)$

Poznámka 3.29. $< b_1, \dots, b_i >_{\mathbb{R}} = < b_1^*, \dots, b_i^* >_{\mathbb{R}} \ \forall 1 \leq i \leq k, \ b_i^* + x_i = b_i, x_i \in < b_1^*, \dots, b_{i_1}^* >_{\mathbb{R}}$
$b_i^* \perp x_i, \ b_i^*$ je kolmá projekce b_i do $< b_1, \dots, b_{i-1} >^{\perp}$
$\|b_i^*\|^2 + \|x_i\|^2 = \|b_i\|^2 \implies \|b_i^*\|^2 \leq \|b_i\|^2$

Lemma 3.30. *$L \subseteq (\mathbb{R}^n, +)$ mříž s bází $b_1, b_2, \dots, b_k$. Pak $\lambda_1(L) \geq \min\{\|b_1^*\|, \dots, \|b_k^*\|\}$*

Důkaz. Chceme $\forall 0 \neq v \in L \ \|v\| \geq \{\|b_1^*\|, \dots, \|b_k^*\|\}$.
$v = \sum_{i=1}^{k} z_i b_i, \ z_1, \dots, z_k \in \mathbb{Z}, \ l \in \{1, \dots, k\}, \ z_l \neq 0, z_{l+1} = \dots = z_k = 0$
$v = z_l b_l^* + \sum_{i=1}^{l-1} r_i b_i^*$ pro $r_1, \dots, r_{l-1} \in \mathbb{R}$, TADY KOUSEK CHYBÍ!!! ☐

Značení 3.31. $b_i^* = b_i - \sum_{j=1}^{i-1} u_{i,j} b_j^*, \ u_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*}$

Chceme vyjádření $x_i = \sum_{j=1}^{i-1} r_j b_j, \ r_1, \dots, r_{i-1} \in \mathbb{R}, \ (b_i - x_i) \cdot b_t = O \ \forall t = 1, 2, \dots, i-1$
$\forall t = 1, \dots, i-1 \ 0 = (b_i - \sum_{j=1}^{i-1} r_j b_j) \cdot b_t \iff \sum_{j=1}^{i-1} (b_t \cdot b_j) r_j = b_i b_t \ \forall t = 1, \dots, i-1 \iff (matice s prvkem\, b_t \cdot b_j) \cdot \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{i-1} \end{pmatrix} = \begin{pmatrix} b_i \cdot b_1 \\ b_i \cdot b_2 \\ \vdots \\ b_i \cdot b_{i-1} \end{pmatrix}$. Tato matice se nazývá *Grammova matice* vektorů $b_1, \dots, b_{i-1}$. Značíme ji $G_{b_1, \dots, b_{i-1}}$.
Koeficienty $r_1, \dots, r_{i-1}$ získám řešením soustavy lineárních rovnic s maticí $G_{b_1, \dots, b_{i-1}}$.

Tvrzení 3.32. *$b_1, b_2, \dots, b_k \in \mathbb{R}^n$ LN, $\det G_{b_1, \dots, b_{i-1}} = \|b_1^*\|^2 \|b_2^*\|^2 \cdots \|b_k^*\|^2 \leq \|b_1\|^2 \|b_2\|^2 \cdots \|b_k\|^2$ - Hadamardova nerovnost.*

Důkaz.
$A = (b_1 | b_2 | \cdots | b_k) \in M_{n,k}(\mathbb{R})$
$B = (b_1^* | b_2^* | \cdots | b_k^*) \in M_{n,k}(\mathbb{R})$
$A^T \cdot A = G_{b_1, \dots, b_{i-1}}$ - na pozici (t, j) je prvek $b_t \cdot b_j$
$B^T \cdot B = G_{b_1^*, \dots, b_{i-1}^*} = \mathrm{diag}(\|b_1^*\|^2 \|b_2^*\|^2 \cdots \|b_k^*\|^2)$
$b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^* = b_i$
$A = B.$(matice která tady není!!!!! - doplnit)
$A = BU$
$\det G_{b_1, \dots, b_{i-1}} = \det A^T A = \det U^T (B^T B) U = \det(U^T) \cdot \det(B^T B) \cdot \det(U) = \|b_1^*\|^2 \|b_2^*\|^2 \cdots \|b_k^*\|^2$
$\|b_1^*\|^2 \|b_2^*\|^2 \cdots \|b_k^*\|^2 \leq \|b_1\|^2 \|b_2\|^2 \cdots \|b_k\|^2$ plyne z $\|b_i^*\| \leq \|b_i\|$ ☐

Připomenutí 3.33. $L = \mathbb{Z} b_1 + \cdots \mathbb{Z} b_k \subseteq \mathbb{R}^n \ d(L) = \sqrt{\det A^T A}$, kde $A = (b_1 | b_2 | \cdots | b_k)$
$d(L) = \sqrt{\det A^T A} = \|b_1^*\|^2 \|b_2^*\|^2 \cdots \|b_k^*\|^2 \dots$ lze chápat jako k-rozměrný objem množiny $F = \{\sum_{i=1}^{k} r_i b_i | r_i \in < 0, 1)\}$ v $\mathbb{R}^n$

3.10 Gaussova redukce úplné dvourozměrné mříže

Definice 3.34. $L \subseteq (\mathbb{R}^2, +)$ úplná mříž, (b_1, b_2) báze L se nazývá *nejkratší báze* L, pokud

1. b_1, b_2 je báze L

2. $\forall v \in L \setminus \{0\}: \ \|v\| \geq \|b_1\|$

3. $\forall v \in L \setminus < b_1 >_{\mathbb{R}}$: $\|v\| \geq \|b_2\|$

Příklad 3.35. $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ldots, e_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, f = \begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{pmatrix}$
$L = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_5 + \mathbb{Z}f$
báze e_1, e_2, e_3, e_4, f $e_5 = 2f - e_1 = e_2 - e_3 - e_4$
L nemá nejkratší bázi, tedy bázi $b_1, b_2, \ldots, b_5$
$b_1 \ldots$ nejkratší vektor $L \setminus \{0\}$, $b_2 \ldots$ nejkratší vektor $L \setminus < b_1 >_{\mathbb{R}}, \ldots b_i \ldots$ nejkratší vektor $L \setminus < b_1, \ldots, b_{i-1} >_{\mathbb{R}}$
$v \in L \setminus \{0\} \begin{cases} v \in \mathbb{Z}^5 & \|v\| \geq 1 \\ v \in f + \mathbb{Z}^5 & \|v\| \geq \sqrt{5 \cdot 1/4} > 1 \end{cases}$
TADY CHYBÍ SEZNAM, čemu náleží které b i a že f nenáleží tomu, co generují

Definice 3.36 (Algoritmus - Gaussova redukce mříže).
VSTUP:(b_1, b_2) báze $L \subseteq \mathbb{Z}^2$
VÝSTUP: nejkratší báze L

1. Repeat

   - if $\|b_2\| \leq \|b_1\|$ then vyměň hodnoty proměnných b_1 a b_2
     $x := \lfloor \mu_{2,1} \rceil = \lfloor \frac{b_2 \cdot b_1}{b_1 \cdot b_1} \rceil$ (celočíselné zaokrouhlení $\mu_{2,1}$)
     $b_2 := b_2 - xb_1$

   until $x = 0$

2. return (b_1, b_2)

TADY NECO CHYBÍ

Poznámka 3.37 (Zaokrouhlení). Pokud $\mu_{2,1} \in 1/2 \pm \mathbb{Z}$, lze $\mu_{2,1}$ zaokrouhlit nahoru i dolů. Ale pokud $\mu_{2,1} = \pm 1/2$, zaokrouhlíme vždy na nulu!