Lecturer: Thomas Rothvoss Due date: Friday, Feb 3, 2023, 11pm, on GradeScope

Problem Set 4
CSE 599S - Lattices
Winter 2023

Exercise 1.9 (10pts)
Let $\boldsymbol{A} \in \mathbb{Z}^{m \times n}$ and $\boldsymbol{b} \in \mathbb{Z}^m$ with $m \leq n$ where $\boldsymbol{A}$ has full row rank. Show that in polynomial time one can compute a vector $\boldsymbol{x} \in \mathbb{Z}^n$ with $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$ (or decide that no such vector exists).
Remark: Use the HNF.

Exercise 1.11 (10pts)
We want to consider a relaxed version of a KZ-reduced basis. We say that a basis $\boldsymbol{B} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) \in \mathbb{R}^{n \times n}$ for a lattice Λ is *α-KZ-reduced* for $\alpha \geq 1$ if $\boldsymbol{B}$ is coefficient reduced and $\|\boldsymbol{b}_i^*\|_2 \leq \alpha \cdot \lambda_1(\pi_{U_i}(\Lambda))$ for all $i = 1, \ldots, n$. Here π_{U_i} is again the projection into $U_i := \text{span}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{i-1}\}^{\perp}$. Show that the orthogonality defect of such a basis is $\gamma(\boldsymbol{B}) \leq (\alpha n)^n$.