Problem Set 4
CSE 599S - Lattices
Winter 2023

Exercise 1.9 (10pts)
Let \( A \in \mathbb{Z}^{m \times n} \) and \( b \in \mathbb{Z}^m \) with \( m \leq n \) where \( A \) has full row rank. Show that in polynomial time one can compute a vector \( x \in \mathbb{Z}^n \) with \( Ax = b \) (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 \( B = (b_1, \ldots, b_n) \in \mathbb{R}^{n \times n} \) for a lattice \( \Lambda \) is \( \alpha \)-KZ-reduced for \( \alpha \geq 1 \) if \( B \) is coefficient reduced and \( \|b_i^*\|_2 \leq \alpha \cdot \lambda_1(\pi_{U_i}(\Lambda)) \) for all \( i = 1, \ldots, n \). Here \( \pi_{U_i} \) is again the projection into \( U_i := \text{span}\{b_1, \ldots, b_{i-1}\}^\perp \). Show that the orthogonality defect of such a basis is \( \gamma(B) \leq (\alpha n)^n \).