

CO 789, Homework 1

Ganyu (Bruce) Xu (g66xu)

Fall 2023

1 First section

Definition 1.1 (Lattice). *A lattice is a discrete subgroup of \mathbb{R}^n*

Theorem 1.1 (Minkowski's bound). *let $\mathcal{L}(B)$ be a full-rank lattice with basis $B \in \mathbb{R}^{n \times n}$, and $B^* = [\mathbf{b}_1^*, \mathbf{b}_2^*, \dots, \mathbf{b}_n^*]$ be the Gram-Schmidt orthogonalization of B , then*

$$\lambda_1(\mathcal{L}(B)) \geq \min_{1 \leq i \leq n} |\mathbf{b}_i^*| \quad (1)$$

Algorithm 1: Euclid's algorithm

Data: Two positive integers a and b

Result: The greatest common divisor of a and b

```
1 while  $b \neq 0$  do  
2    $r \leftarrow a \bmod b$ ;  
3    $a \leftarrow b$ ;  
4    $b \leftarrow r$ ;  
5 end  
6 return  $a$ ;
```
