Scribe Notes for *Algorithmic Number Theory*
Class 21—June 16, 1998
Scribes: Cara Struble and Craig Struble

Abstract

Today students present their solutions to Homework 4 and we give a brief introduction to lattices.

1 Lattices

Let $b_1, b_2, \ldots, b_m \in \mathbb{R}^n$ be linearly independent vectors. They span an n-dimensional subspace. A piece of that subspace is a lattice.

The set

$$L = \left\{ \sum_{i=1}^{m} c_i b_i | c_i \in \mathbb{Z} \right\}$$

is a **lattice** with **basis** $\{b_1, b_2, \ldots, b_m\}$.

Example 1.1. The integer lattice has basis $\{(1,0),(0,1)\}$. This is the first handout.

Example 1.2. A lattice may have basis $\{(3,1),(1,2)\}$. See the class handout for a picture of this lattice.

If $m = n$, define $d(L) = |\det B|$. The basis can be written as an $m \times n$ matrix:

$$B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

We may perform the following elementary row operations on this matrix:

1. Swap b_i and b_j.
2. Replace b_j with $b_j + kb_i$ where $k \in \mathbb{Z}$, if $i \neq j$.

This gives B' where the rows of B' are also a basis.

Example 1.3. Given the basis $\{(3,1),(1,2)\}$, we start with the matrix

$$B = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}.$$

After adding 3 times the first row to the second row, we obtain

$$B' = \begin{pmatrix} 3 & 1 \\ 10 & 5 \end{pmatrix}.$$

So $\{(3,1),(10,5)\}$ is also a basis.

Proposition 1.4. *The rows of B' are also a basis of L. Moreover, there is an $m \times m$ integer matrix U such that $B' = UB$. The determinant of U is ± 1.*