

# INTRODUCTION TO LATTICES AND THE LLL ALGORITHM

Hendrik Lenstra

Mathematisch Instituut  
Universiteit Leiden



## *Literature*

A. K. Lenstra, H. W. Lenstra jr., L. Lovász,  
*Factoring polynomials with rational coefficients*,  
Math. Ann. **261** (1982), 515–534.

H. W. Lenstra jr., *Lattices*, pp. 127–181 in:  
J. P. Buhler, P. Stevenhagen (eds), *Algorithmic  
number theory*, Cambridge University Press, 2008.

P. Q. Nguyen, B. Vallée (eds), *The LLL  
algorithm*, Springer-Verlag, 2010.

### *Definition of lattice*

A lattice is an abelian group  $L$  together with a map  $q: L \rightarrow \mathbf{R}$  satisfying certain conditions.

### *Definition of lattice*

A lattice is an abelian group  $L$  together with a map  $q: L \rightarrow \mathbf{R}$  satisfying certain conditions.

### *Algebraically*

- $L$  is finitely generated,
- $q(x + y) + q(x - y) = 2 \cdot q(x) + 2 \cdot q(y)$   
for all  $x, y \in L$ ,
- $q(x) \neq 0$  for all  $x \in L, x \neq 0$ ,
- $\#\{x \in L : q(x) \leq r\} < \infty$  for all  $r \in \mathbf{R}$ .

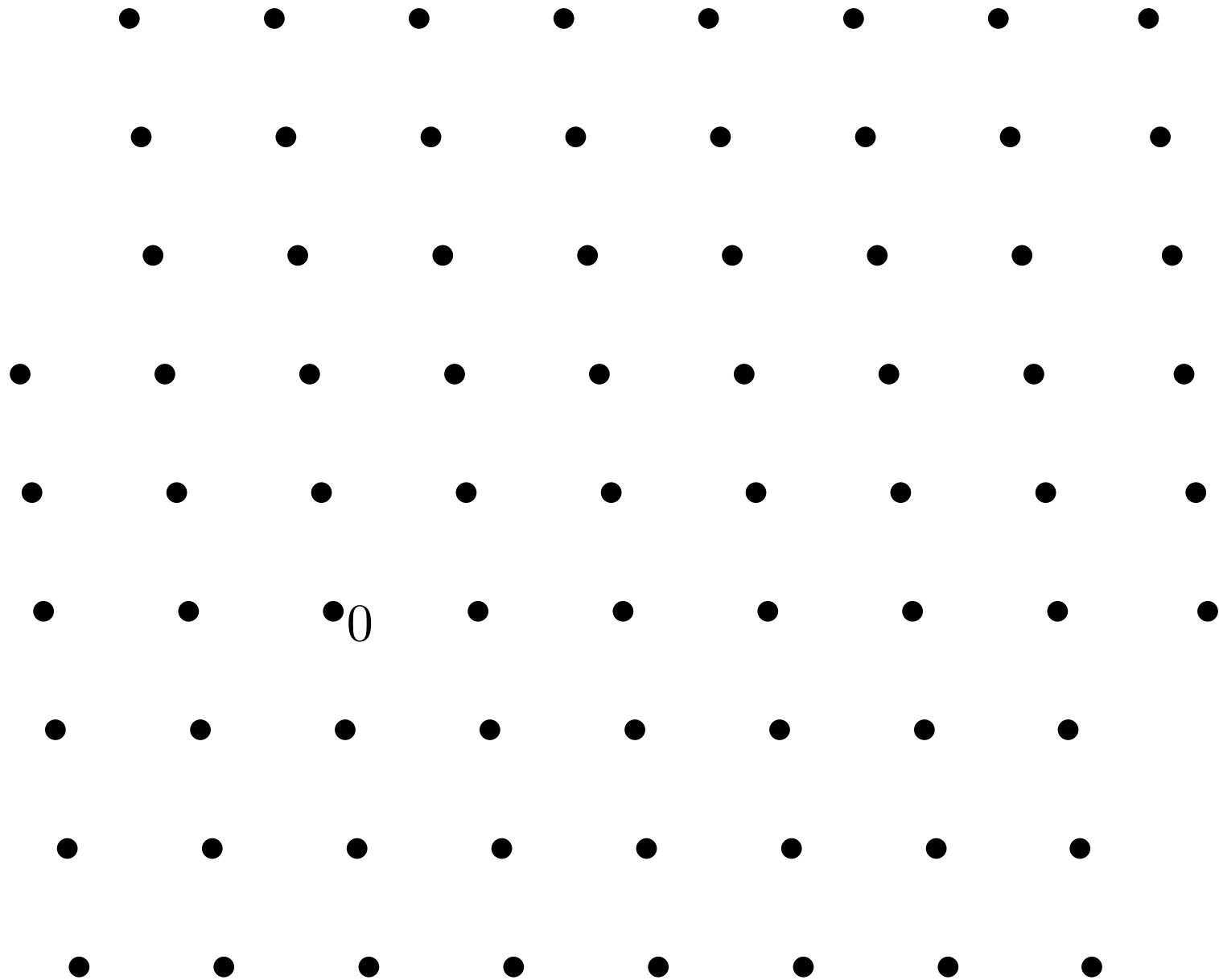
### *Definition of lattice*

A lattice is an abelian group  $L$  together with a map  $q: L \rightarrow \mathbf{R}$  satisfying certain conditions.

### *Geometrically*

There exist  $n \in \mathbf{Z}_{\geq 0}$ , a basis  $b_1, \dots, b_n$  of  $\mathbf{R}^n$ , and an identification  $L = \sum_{i=1}^n \mathbf{Z} \cdot b_i$ , such that  $q(x) = \|x\|^2 (= \langle x, x \rangle)$  for all  $x \in L$ .

One calls  $b_1, \dots, b_n$  a *basis* for  $L$ .



### *Definition of lattice*

A lattice is an abelian group  $L$  together with a map  $q: L \rightarrow \mathbf{R}$  satisfying certain conditions.

### *Algorithmically*

There exist  $n \in \mathbf{Z}_{\geq 0}$ , an identification  $L = \mathbf{Z}^n$ , and a positive definite symmetric  $n \times n$ -matrix  $\mathbf{A}$  over  $\mathbf{R}$ , such that  $q(x) = x^T \cdot \mathbf{A} \cdot x$  for all  $x \in L$ .

One calls  $\mathbf{A}$  a *Gram matrix* for  $L$

(Jorgen Gram, 1850–1916).

## *Gram-Schmidt orthogonalization*

(Pierre-Simon Laplace, 1749–1827)

Let  $b_1, \dots, b_n$  be a basis of  $\mathbf{R}^n$ , and let  $b_i^*$  be the unique shortest vector in  $b_i + \sum_{j < i} \mathbf{R} \cdot b_j$ .

- $\sum_{j \leq i} \mathbf{R} \cdot b_j^* = \sum_{j \leq i} \mathbf{R} \cdot b_j$ ,
- $b_1^*, \dots, b_n^*$  form a basis of  $\mathbf{R}^n$ ,
- $\langle b_i^*, b_j^* \rangle = 0$  for  $i \neq j$ ,
- the  $b_i^*$  are easy to compute from the  $b_i$ .

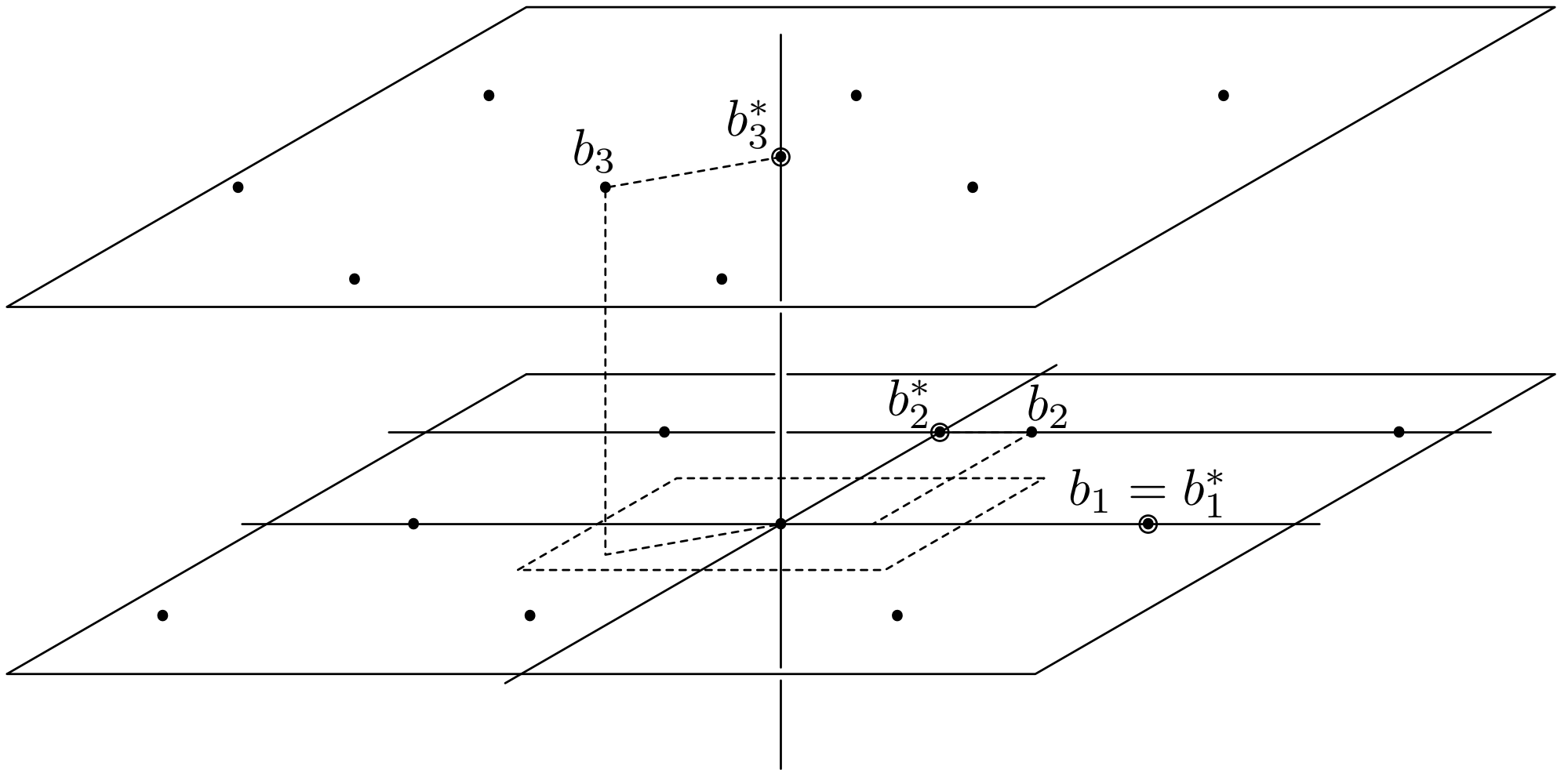
They form the *Gram-Schmidt orthogonalization* of  $b_1, \dots, b_n$  (Erhard Schmidt, 1876–1959).

## *Reduced bases*

$$b_i = b_i^* + \sum_{j < i} \mu_{ij} \cdot b_j^*, \quad \mu_{ij} \in \mathbf{R}.$$

$b_1, \dots, b_n$  is *reduced* if

- $|\mu_{ij}| \leq \frac{1}{2}$  for  $j < i$ ,
- $\|b_i^*\|^2 \leq 2 \cdot \|b_{i+1}^*\|^2$  for  $i < n$ .



*What a reduced basis is good for*

Let  $b_1, \dots, b_n$  be a reduced basis for a lattice  $L$ .

*Short vectors:*

$$\|b_1\|^2 \leq 2^{n-1} \cdot \min\{\|x\|^2 : x \in L, x \neq 0\}.$$

*Close vectors:*

$$\mathbf{R}^n = L + \sum_{i=1}^n \left[-\frac{1}{2}, \frac{1}{2}\right] \cdot b_i^*.$$

If  $z = x + y \in \mathbf{R}^n$ , with  $x \in L$ ,  $y \in \sum_i \left[-\frac{1}{2}, \frac{1}{2}\right] \cdot b_i^*$ ,

then

$$\|y\|^2 \leq (2^n - 1) \cdot \text{distance}(z, L)^2.$$

## *Reduction steps*

- if  $|\mu_{ij}| > \frac{1}{2}$ , replace  $b_i$  by  $b_i - m \cdot b_j$ ,  
where  $m \in \mathbf{Z}$ ,  $|m - \mu_{ij}| \leq \frac{1}{2}$ ;
- if  $\|b_i^*\|^2 > 2 \cdot \|b_{i+1}^*\|^2$  and  $|\mu_{i+1 i}| \leq \frac{1}{2}$ ,  
interchange  $b_i$  and  $b_{i+1}$ .

The *LLL-algorithm* (1982) finds a reduced basis for a given lattice, in polynomial time.

*The use of short vectors*

Put  $L = \mathbf{Z}^2$  and define  $q: L \rightarrow \mathbf{R}$  by

$$q(x, y) = y^2 + N \cdot (x - \alpha y)^2,$$

with  $\alpha \in [0, 1]$  and  $N$  large.

A ‘small’ non-zero vector in  $L$  gives a  
‘good’ rational approximation  $x/y$  to  $\alpha$ .

## *Simultaneous diophantine approximation*

Similarly, finding good simultaneous approximations  $x_1/y, x_2/y, \dots, x_k/y$  to  $k$  given real numbers  $\alpha_1, \alpha_2, \dots, \alpha_k$  amounts to finding a short non-zero vector in a lattice of rank  $k + 1$ .

## *Approximate linear dependencies*

Let  $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbf{R}$ .

Define  $q: L = \mathbf{Z}^n \rightarrow \mathbf{R}$  by

$$q(x) = \sum_i x_i^2 + N \cdot \left(\sum_i x_i \alpha_i\right)^2$$

for  $x = (x_i)_{i=1}^n$ , with  $N$  large.

A ‘small’ non-zero vector in  $L$  corresponds to an approximate linear dependency of the  $\alpha_i$  with small integer coefficients.

## *Factoring polynomials*

With  $\alpha_i = \alpha^{i-1}$ , this yields a test whether  $\alpha$  is very close to an algebraic number  $\beta$  of degree  $< n$  and small height, and if so determines the irreducible polynomial of  $\beta$ .

*Linear algebra over  $\mathbf{Z}$*

Given an  $m \times n$ -matrix  $\mathbf{F}$  over  $\mathbf{Z}$ ,  
and  $a \in \mathbf{Z}^m$ , one wishes to solve

$$\mathbf{F} \cdot x = a, \quad x \in \mathbf{Z}^n.$$

## *Constructing the lattice*

Take  $L = \mathbf{Z}^n \times \mathbf{Z}$ , and define  $q: L \rightarrow \mathbf{R}$  by

$$q(x, z) = \|x\|^2 + M \cdot z^2 + N \cdot \|\mathbf{F} \cdot x - a \cdot z\|^2,$$

where  $x \in \mathbf{Z}^n$ ,  $z \in \mathbf{Z}$ ,  $N \gg M \gg 1$ .

## *Constructing the lattice*

Take  $L = \mathbf{Z}^n \times \mathbf{Z}$ , and define  $q: L \rightarrow \mathbf{R}$  by

$$q(x, z) = \|x\|^2 + M \cdot z^2 + N \cdot \|\mathbf{F} \cdot x - a \cdot z\|^2,$$

where  $x \in \mathbf{Z}^n$ ,  $z \in \mathbf{Z}$ ,  $N \gg M \gg 1$ .

It will suffice to assume

$$M > 2^n \cdot (r + 1) \cdot r^r \cdot F^{2r},$$

$$N > 2^n \cdot (r + M) \cdot r^r \cdot F^{2r},$$

where  $r = \text{rank } \mathbf{F}$  and

$$F = \max |\text{entries of } \mathbf{F} \text{ and } a|.$$

## *Linear algebra over $\mathbf{Z}$*

Let  $\mathbf{F}$  be a  $m \times n$ -matrix over  $\mathbf{Z}$ , let  $a \in \mathbf{Z}^m$ , and let  $b_1, \dots, b_{n+1}$  be a reduced basis for  $L$ .

**Theorem.** *There exists  $x \in \mathbf{Z}^n$  with  $\mathbf{F} \cdot x = a$  if and only if  $M \leq q(b_i) < 4 \cdot M$  for some  $i$ .*

*If  $i$  exists, then it is unique, and one has*

$$b_j = (b'_j, 0) \quad (j < i), \quad \pm b_i = (b'_i, 1)$$

*for certain  $b'_j \in \mathbf{Z}^n$ ; moreover the solution set  $\{x \in \mathbf{Z}^n : \mathbf{F} \cdot x = a\}$  equals  $b'_i + \sum_{j < i} \mathbf{Z} \cdot b'_j$ .*

*Idea*

Do not use numerical values for  $M$  and  $N$ ,  
but view them as “indefinitely large symbols”  
that satisfy  $N \gg M \gg 1$ .

Write all values assumed by  $q$  and  $\langle \cdot, \cdot \rangle$  as  
expressions  $r + s \cdot M + t \cdot N$  with  $r, s, t \in \mathbf{R}$ ,  
ordered anti-lexicographically.

## *Ordered vector spaces*

An ordered vector space over  $\mathbf{R}$  is an  $\mathbf{R}$ -vector space  $V$  together with a total ordering on  $V$  such that for all  $x \in V$  with  $x > 0$  one has:

- $x + y > y$  for all  $y \in V$ ,
- $r \cdot x > 0$  for all  $r \in \mathbf{R}$ ,  $r > 0$ .

## *Example*

$V = \mathbf{R}^m$ , ordered anti-lexicographically.

## *Layered lattices*

A layered lattice is an abelian group  $L$  together with a map  $q$  from  $L$  to an ordered vector space  $V$  over  $\mathbf{R}$ , satisfying certain conditions.

*Algebraically*

- $L$  is finitely generated,
- $q(x + y) + q(x - y) = 2 \cdot q(x) + 2 \cdot q(y)$   
for all  $x, y \in L$ ,
- $q(x) \neq 0$  for all  $x \in L, x \neq 0$ ,
- $q(L)$  is a well-ordered subset of  $V$ .

*Theory and algorithms*

The theoretical and algorithmic aspects of layered lattices are worked out by *Erwin Dassen* in his Leiden Ph. D. thesis.

For more information, come to his lecture *Using layered lattices* tomorrow.