The Lattice Base Reduction Algorithm

This is a method which was developed in 1982 by Arjen Lenstra, Hendrik Lenstra and László Lovász to prove that factoring polynomials in $\mathbb{Z}[x]$ can be done in polynomial time. It is sometimes called the LLL-algorithm or the L^3-algorithm.

Definitions and Notations. Let $\mathbb{Q}^n$ denote the set of vectors $\langle a_1, a_2, \dots, a_n \rangle$ with $a_j \in \mathbb{Q}$. For

$$\vec{b} = \langle a_1, a_2, \dots, a_n \rangle \in \mathbb{Q}^n \quad \text{and} \quad \vec{b}' = \langle a_1', a_2', \dots, a_n' \rangle \in \mathbb{Q}^n,$$

define the usual dot product $\vec{b} \cdot \vec{b}'$ by

$$\vec{b} \cdot \vec{b}' = a_1 a_1' + a_2 a_2' + \cdots + a_n a_n',$$

and set

$$\|\vec{b}\| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.$$

Definitions and Notations. Let $\mathbb{Q}^n$ denote the set of vectors $\langle a_1, a_2, \ldots, a_n \rangle$ with $a_j \in \mathbb{Q}$. For

$$\vec{b} = \langle a_1, a_2, \ldots, a_n \rangle \in \mathbb{Q}^n \quad \text{and} \quad \vec{b}' = \langle a'_1, a'_2, \ldots, a'_n \rangle \in \mathbb{Q}^n,$$

define the usual dot product $\vec{b} \cdot \vec{b}'$ by

$$\vec{b} \cdot \vec{b}' = a_1 a'_1 + a_2 a'_2 + \cdots + a_n a'_n,$$

and set

$$\|\vec{b}\| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.$$

Further, we use A^T to denote the transpose of a matrix A, so the rows and columns of A are the same as the columns and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1 \mathbb{Z} + \cdots + \vec{b}_n \mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1\mathbb{Z} + \cdots + \vec{b}_n\mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

Comment: Different A can determine the same $\mathcal{L}$. But given $\mathcal{L}$, the value of $|\det A|$ is the same for all such A. To see this, observe that if $\vec{b}_1, \ldots, \vec{b}_n$ and $\vec{b}'_1, \ldots, \vec{b}'_n$ are two bases for $\mathcal{L}$, there are matrices U and V with integer entries such that

$$(\vec{b}_1, \ldots, \vec{b}_n)UV = (\vec{b}'_1, \ldots, \vec{b}'_n)V = (\vec{b}_1, \ldots, \vec{b}_n).$$

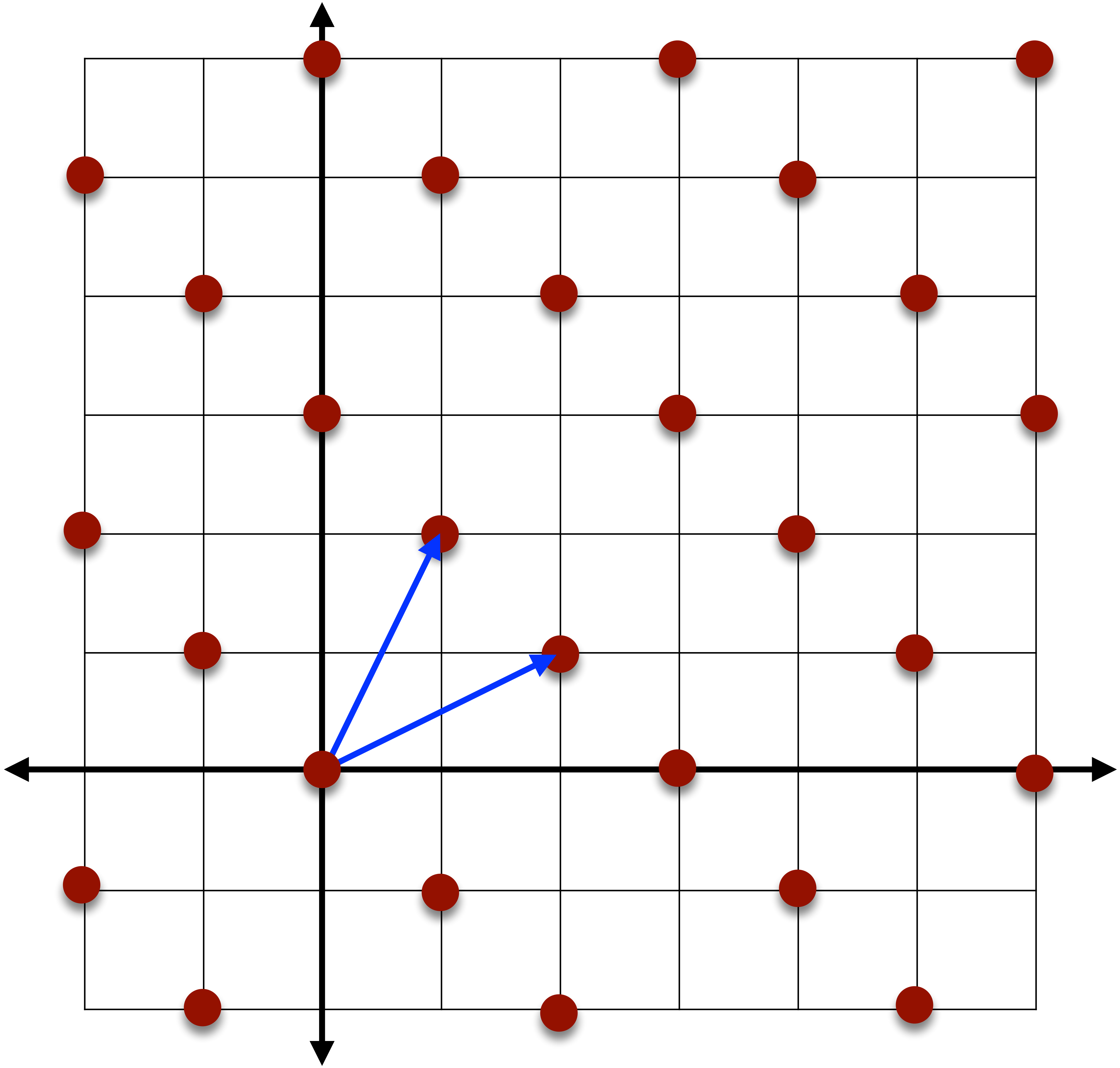
Given that $\vec{b}_1, \ldots, \vec{b}_n$ is a basis for $\mathbb{R}^n$, it follows that UV is the identity matrix and $\det V = \pm 1$. The second equation above then implies

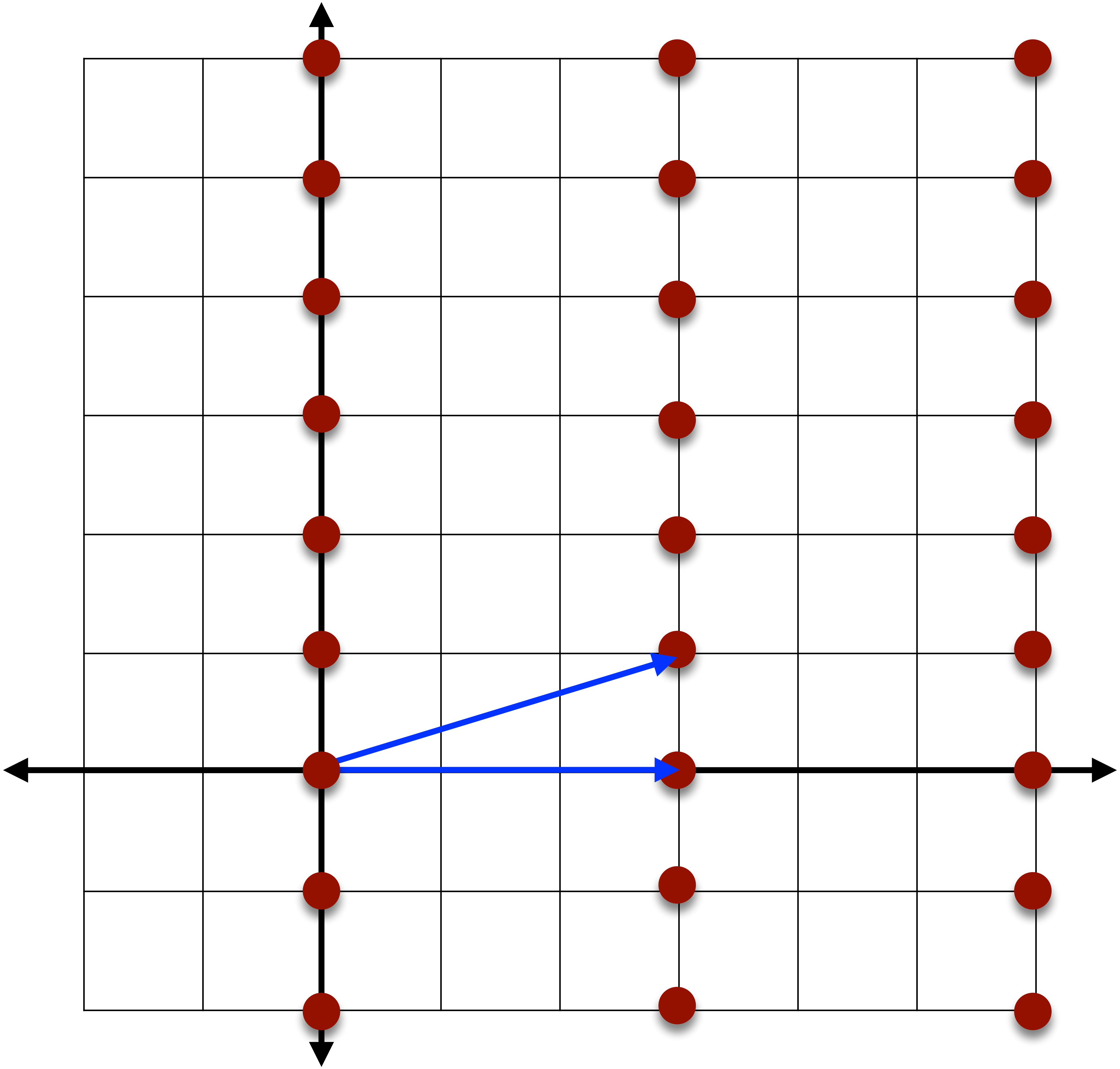
$$|\det(\vec{b}'_1, \ldots, \vec{b}'_n)| = |\det(\vec{b}_1, \ldots, \vec{b}_n)|.$$

We set $\det \mathcal{L}$ to be this common value.

Example. In $\mathbb{R}^2$, the lattice formed from the basis $\langle 1, 0\rangle$ and $\langle 0, 1\rangle$ is the same as the lattice formed from the basis $\langle 1, 0\rangle$ and $\langle 1, 1\rangle$. This can be seen geometrically and algebraically.

Example 2. The lattice $\mathcal{L}_1$ with basis $\langle 2, 1\rangle$ and $\langle 1, 2\rangle$ and the lattice $\mathcal{L}_2$ with basis $\langle 3, 0\rangle$ and $\langle 3, 1\rangle$ are such that $\det \mathcal{L}_1 = \det \mathcal{L}_2$. But the lattices are quite different.





The Gram-Schmidt orthogonalization process

Define recursively

$$\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*, \qquad \text{for } 1 \leq i \leq n,$$

where

$$\mu_{ij} = \mu_{i,j} = \frac{\vec{b}_i \cdot \vec{b}_j^*}{\vec{b}_j^* \cdot \vec{b}_j^*}, \qquad \text{for } 1 \leq j < i \leq n.$$

Then for each $i \in \{1, \ldots, n\}$, the vectors $\vec{b}_1^*, \ldots, \vec{b}_i^*$ span the same subspace of $\mathbb{R}^n$ as $\vec{b}_1, \ldots, \vec{b}_i$. In other words,

$$\{a_1 \vec{b}_1^* + \cdots + a_i \vec{b}_i^* : a_j \in \mathbb{R} \text{ for } 1 \leq j \leq i\}$$
$$= \{a_1 \vec{b}_1 + \cdots + a_i \vec{b}_i : a_j \in \mathbb{R} \text{ for } 1 \leq j \leq i\}.$$

Furthermore, the vectors $\vec{b}_1^*, \ldots, \vec{b}_n^*$ are linearly independent (hence, non-zero) and pairwise orthogonal (i.e., for distinct i and j, we have $\vec{b}_i^* \cdot \vec{b}_j^* = 0$).

Hadamard's Inequality

The value of $\det \mathcal{L}$ can be viewed as the volume of the polyhedron with edges parallel to and the same length as $\vec{b}_1, \ldots, \vec{b}_n$. This volume is independent of the basis that is used for $\mathcal{L}$. Geometrically (in low dimensions),

$$\det \mathcal{L} \leq \|\vec{b}_1\| \, \|\vec{b}_2\| \cdots \|\vec{b}_n\|.$$

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \implies \|\vec{b}\| \geq \min\{\|\vec{b}_1^*\|, \|\vec{b}_2^*\|, \ldots, \|\vec{b}_n^*\|\}$$

$$\vec{b}_i = \vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^* \qquad \mu_{i,j} = \frac{\vec{b}_i \cdot \vec{b}_j^*}{\vec{b}_j^* \cdot \vec{b}_j^*}$$

$$\vec{b} = u_1 \vec{b}_1 + \cdots + u_k \vec{b}_k, \qquad \text{where each } u_j \in \mathbb{Z} \text{ and } u_k \neq 0$$

$$\vec{b} = v_1 \vec{b}_1^* + \cdots + v_k \vec{b}_k^*, \qquad \text{where each } v_j \in \mathbb{Q} \text{ and } v_k = u_k$$

$$\|\vec{b}\|^2 = \left(v_1 \vec{b}_1^* + \cdots + v_k \vec{b}_k^*\right) \cdot \left(v_1 \vec{b}_1^* + \cdots + v_k \vec{b}_k^*\right)$$
$$= v_1^2 \|\vec{b}_1^*\|^2 + \cdots + v_k^2 \|\vec{b}_k^*\|^2 \geq \|\vec{b}_k^*\|^2$$

$$(*) \qquad \vec{b} \in \mathcal{L},\ k \text{ as above} \implies \|\vec{b}\|^2 \geq \|\vec{b}_k^*\|^2$$

Definition. Let $\vec{b}_1, \ldots, \vec{b}_n$ be a basis for a lattice $\mathcal{L}$, and let $\vec{b}_1^*, \ldots, \vec{b}_n^*$ be the corresponding basis in $\mathbb{R}^n$ obtained from the Gram-Schmidt orthogonalization process, with μ_{ij} as defined before. Then we say that $\vec{b}_1, \ldots, \vec{b}_n$ is *reduced* if both of the following hold

(i) $|\mu_{ij}| \leq \frac{1}{2} \quad$ for $1 \leq j < i \leq n$

(ii) $\|\vec{b}_i^* + \mu_{i,i-1}\vec{b}_{i-1}^*\|^2 \geq \frac{3}{4}\|\vec{b}_{i-1}^*\|^2 \quad$ for $1 < i \leq n$.

Comment: The main part of the work of Lenstra, Lenstra and Lovász establishes an algorithm that runs in polynomial time that constructs a reduced basis of $\mathcal{L}$ from an arbitrary basis $\vec{b}_1, \ldots, \vec{b}_n$ of $\mathcal{L}$.

Definition. Let $\vec{b}_1, \ldots, \vec{b}_n$ be a basis for a lattice $\mathcal{L}$, and let $\vec{b}_1^*, \ldots, \vec{b}_n^*$ be the corresponding basis in $\mathbb{R}^n$ obtained from the Gram-Schmidt orthogonalization process, with μ_{ij} as defined before. Then we say that $\vec{b}_1, \ldots, \vec{b}_n$ is *reduced* if both of the following hold

(i) $|\mu_{ij}| \leq \dfrac{1}{2} \quad \text{for } 1 \leq j < i \leq n$

(ii) $\|\vec{b}_i^* + \mu_{i,i-1}\vec{b}_{i-1}^*\|^2 \geq \dfrac{3}{4}\|\vec{b}_{i-1}^*\|^2 \quad \text{for } 1 < i \leq n.$

Comment: The main part of the work of Lenstra, Lenstra and Lovász establishes an algorithm that runs in polynomial time that constructs a reduced basis of $\mathcal{L}$ from an arbitrary basis $\vec{b}_1, \ldots, \vec{b}_n$ of $\mathcal{L}$. We do not give this algorithm, but instead give a little more background and then explain how a reduced basis can be used to factor a polynomial $f(x)$.

In the notation of the definition,

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \implies \|\vec{b}_1\| \leq 2^{(n-1)/2}\|\vec{b}\|.$$

Thus, $\vec{b}_1$ is not far from being the shortest vector in $\mathcal{L}$.

$$\|\vec{b}_i^*\|^2 + \frac{1}{4}\|\vec{b}_{i-1}^*\|^2 \geq \|\vec{b}_i^* + \mu_{i,i-1}\vec{b}_{i-1}^*\|^2 \geq \frac{3}{4}\|\vec{b}_{i-1}^*\|^2$$

Definition. Let $\vec{b}_1, \ldots, \vec{b}_n$ be a basis for a lattice $\mathcal{L}$, and let $\vec{b}_1^*, \ldots, \vec{b}_n^*$ be the corresponding basis in $\mathbb{R}^n$ obtained from the Gram-Schmidt orthogonalization process, with μ_{ij} as defined before. Then we say that $\vec{b}_1, \ldots, \vec{b}_n$ is *reduced* if both of the following hold

(i) $|\mu_{ij}| \leq \dfrac{1}{2} \quad$ for $1 \leq j < i \leq n$

(ii) $\|\vec{b}_i^* + \mu_{i,i-1}\vec{b}_{i-1}^*\|^2 \geq \dfrac{3}{4}\|\vec{b}_{i-1}^*\|^2 \quad$ for $1 < i \leq n$.

In the notation of the definition,

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \implies \|\vec{b}_1\| \leq 2^{(n-1)/2}\|\vec{b}\|.$$

Thus, $\vec{b}_1$ is not far from being the shortest vector in $\mathcal{L}$.

$$\|\vec{b}_i^*\|^2 + \frac{1}{4}\|\vec{b}_{i-1}^*\|^2 \geq \|\vec{b}_i^* + \mu_{i,i-1}\vec{b}_{i-1}^*\|^2 \geq \frac{3}{4}\|\vec{b}_{i-1}^*\|^2$$

$$\implies \|\vec{b}_i^*\|^2 \geq (1/2)\|\vec{b}_{i-1}^*\|^2$$

$$\|\vec{b}_i^*\|^2 \geq \frac{1}{2^{i-j}}\|\vec{b}_j^*\|^2 \quad \text{for } 1 \leq j < i \leq n$$

$$\|\vec{b}\|^2 \geq \|\vec{b}_k^*\|^2 \geq \frac{1}{2^{k-1}}\|\vec{b}_1^*\|^2 \geq \frac{1}{2^{n-1}}\|\vec{b}_1^*\|^2 = \frac{1}{2^{n-1}}\|\vec{b}_1\|^2$$

$$(*) \qquad \vec{b} \in \mathcal{L},\ k \text{ as above} \implies \|\vec{b}\|^2 \geq \|\vec{b}_k^*\|^2$$

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \implies \|\vec{b}_1\| \leq 2^{(n-1)/2} \|\vec{b}\|$$

$$\|\vec{b}_i^*\|^2 \geq \frac{1}{2^{i-j}} \|\vec{b}_j^*\|^2 \quad \text{for } 1 \leq j < i \leq n$$

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \implies \|\vec{b}_1\| \leq 2^{(n-1)/2}\|\vec{b}\|$$

Let $\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_t$ be t linearly independent vectors in $\mathcal{L}$. Then

$$\|\vec{b}_j\| \leq 2^{(n-1)/2} \max\{\|\vec{x}_1\|, \|\vec{x}_2\|, \ldots, \|\vec{x}_t\|\} \quad \text{for } 1 \leq j \leq t.$$

$$\|\vec{b}_i^*\|^2 \geq \frac{1}{2^{i-j}}\|\vec{b}_j^*\|^2 \quad \text{for } 1 \leq j < i \leq n$$

$$\|\vec{b}_i\|^2 = \left\|\vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij}\vec{b}_j^*\right\|^2 = \|\vec{b}_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 \|\vec{b}_j^*\|^2$$

$$\|\vec{b}_i\|^2 \leq \|\vec{b}_i^*\|^2 + \frac{1}{4}\sum_{j=1}^{i-1} \|\vec{b}_j^*\|^2 \leq \|\vec{b}_i^*\|^2 + \frac{1}{4}\sum_{j=1}^{i-1} 2^{i-j}\|\vec{b}_i^*\|^2$$
$$= \left(1 + \frac{1}{4}(2^i - 2)\right)\|\vec{b}_i^*\|^2 \leq 2^{i-1}\|\vec{b}_i^*\|^2$$

$$\|\vec{b}_j\|^2 \leq 2^{j-1}\|\vec{b}_j^*\|^2 \leq 2^{i-1}\|\vec{b}_i^*\|^2 \quad \text{for } 1 \leq j \leq i \leq n$$

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \quad \Longrightarrow \quad \|\vec{b}_1\| \leq 2^{(n-1)/2}\|\vec{b}\|$$

Let $\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_t$ be t linearly independent vectors in $\mathcal{L}$. Then

$$\|\vec{b}_j\| \leq 2^{(n-1)/2} \max\{\|\vec{x}_1\|, \|\vec{x}_2\|, \ldots, \|\vec{x}_t\|\} \quad \text{for } 1 \leq j \leq t.$$

$$\|\vec{b}_j\|^2 \leq 2^{j-1}\|\vec{b}_j^*\|^2 \leq 2^{i-1}\|\vec{b}_i^*\|^2 \quad \text{for } 1 \leq j \leq i \leq n$$

$$(*) \qquad \vec{b} \in \mathcal{L},\ k \text{ as above} \quad \Longrightarrow \quad \|\vec{b}\|^2 \geq \|\vec{b}_k^*\|^2$$

$$\vec{x}_j = \sum_{i=1}^{m(j)} u_{ji}\vec{b}_i, \quad u_{jm(j)} \neq 0, \quad m(1) \leq m(2) \leq \cdots \leq m(t)$$

$$m(j) \geq j \text{ for } 1 \leq j \leq t$$

$$\|\vec{x}_j\|^2 \geq \|\vec{b}_{m(j)}^*\|^2 \quad \text{for } 1 \leq j \leq t$$

$$\|\vec{b}_j\|^2 \leq 2^{m(j)-1}\|\vec{b}_{m(j)}^*\|^2 \leq 2^{n-1}\|\vec{x}_j\|^2 \quad \text{for } 1 \leq j \leq t$$

$$\|\vec{b}_j\|^2 \le 2^{j-1}\|\vec{b}_j^*\|^2 \le 2^{i-1}\|\vec{b}_i^*\|^2 \quad \text{for } 1 \le j \le i \le n$$

Recall $\det \mathcal{L} = \prod_{i=1}^{n} \|\vec{b}_i^*\|$.

$$\|\vec{b}_j\|^2 \le 2^{j-1}\|\vec{b}_j^*\|^2 \le 2^{i-1}\|\vec{b}_i^*\|^2 \quad \text{for } 1 \le j \le i \le n$$

Recall $\det \mathcal{L} = \prod_{i=1}^{n} \|\vec{b}_i^*\|$. We obtain

$$\prod_{i=1}^{n} \|\vec{b}_i\|^2 \le \prod_{i=1}^{n} 2^{i-1}\|\vec{b}_i^*\|^2 = 2^{n(n-1)/2}(\det \mathcal{L})^2.$$

$$\|\vec{b}_j\|^2 \le 2^{j-1}\|\vec{b}_j^*\|^2 \le 2^{i-1}\|\vec{b}_i^*\|^2 \quad \text{for } 1 \le j \le i \le n$$

Recall $\det \mathcal{L} = \prod_{i=1}^n \|\vec{b}_i^*\|$. We obtain

$$\prod_{i=1}^n \|\vec{b}_i\|^2 \le \prod_{i=1}^n 2^{i-1}\|\vec{b}_i^*\|^2 = 2^{n(n-1)/2}(\det \mathcal{L})^2.$$

Thus, from Hadamard's inequality, we obtain

$$2^{-n(n-1)/4}\|\vec{b}_1\|\,\|\vec{b}_2\|\cdots\|\vec{b}_n\| \;\le\; \det \mathcal{L} \;\le\; \|\vec{b}'_1\|\,\|\vec{b}'_2\|\cdots\|\vec{b}'_n\|$$

for any basis $\vec{b}'_1, \ldots, \vec{b}'_n$ of $\mathcal{L}$.

$$\|\vec{b}_j\|^2 \le 2^{j-1}\|\vec{b}_j^*\|^2 \le 2^{i-1}\|\vec{b}_i^*\|^2 \quad \text{for } 1 \le j \le i \le n$$

Recall $\det \mathcal{L} = \prod_{i=1}^{n} \|\vec{b}_i^*\|$. We obtain

$$\prod_{i=1}^{n} \|\vec{b}_i\|^2 \le \prod_{i=1}^{n} 2^{i-1}\|\vec{b}_i^*\|^2 = 2^{n(n-1)/2}(\det \mathcal{L})^2.$$

Thus, from Hadamard's inequality, we obtain

$$2^{-n(n-1)/4}\|\vec{b}_1\|\,\|\vec{b}_2\|\cdots\|\vec{b}_n\| \;\le\; \det \mathcal{L} \;\le\; \|\vec{b}'_1\|\,\|\vec{b}'_2\|\cdots\|\vec{b}'_n\|$$

for any basis $\vec{b}'_1, \ldots, \vec{b}'_n$ of $\mathcal{L}$.

Comment: Recall that finding a basis $\vec{b}'_1, \ldots, \vec{b}'_n$ for which the product on the right is minimal is NP-hard. The above implies that a reduced basis is close to being such a basis.

Goal: Find a non-trivial factorization of a given $f(x) \in \mathbb{Z}[x]$ or show no such factorization exists.

Initial Idea: Begin as in the Zassenhaus algorithm. Factor $f(x)$ into irreducibles modulo p^k where p is a prime and $k \in \mathbb{Z}^+$ is large (using Berlekamp's algorithm and Hensel lifting).

Goal: **Find a non-trivial factorization of a given $f(x) \in \mathbb{Z}[x]$ or show no such factorization exists.**

Initial Idea: **Begin as in the Zassenhaus algorithm. Factor $f(x)$ into irreducibles modulo p^k where p is a prime and $k \in \mathbb{Z}^+$ is large (using Berlekamp's algorithm and Hensel lifting). Suppose $h(x)$ is a monic irreducible factor of $f(x)$ mod p^k.**

Goal: Find a non-trivial factorization of a given $f(x) \in \mathbb{Z}[x]$ or show no such factorization exists.

Initial Idea: Begin as in the Zassenhaus algorithm. Factor $f(x)$ into irreducibles modulo p^k where p is a prime and $k \in \mathbb{Z}^+$ is large (using Berlekamp's algorithm and Hensel lifting). Suppose $h(x)$ is a monic irreducible factor of $f(x)$ mod p^k. Let $h_0(x)$ denote an irreducible factor of $f(x)$ in $\mathbb{Z}[x]$ such that $h_0(x)$ is divisible by $h(x)$ modulo p^k.

Goal: Find a non-trivial factorization of a given $f(x) \in \mathbb{Z}[x]$ or show no such factorization exists.

Initial Idea: Begin as in the Zassenhaus algorithm. Factor $f(x)$ into irreducibles modulo p^k where p is a prime and $k \in \mathbb{Z}^+$ is large (using Berlekamp's algorithm and Hensel lifting). Suppose $h(x)$ is a monic irreducible factor of $f(x)$ mod p^k. Let $h_0(x)$ denote an irreducible factor of $f(x)$ in $\mathbb{Z}[x]$ such that $h_0(x)$ is divisible by $h(x)$ modulo p^k. (Note that the greatest common divisor of the coefficients of $h_0(x)$ is 1.)

New Goal: Show how one can determine $h_0(x)$ using $h(x)$ and without worrying about other factors of $f(x)$ modulo p^k.

Why would this improve on the Zassenhaus approach?

What is the lattice we want to use?

What is the lattice we want to use?

$h(x)$ monic irreducible factor of $f(x)$ modulo p^k

$h_0(x)|f(x)$ in $\mathbb{Z}[x]$, $h(x)|h_0(x)$ modulo p^k

$\ell = \deg h$, $m \in \{\ell, \ell+1, \dots, n-1\}$

m is the possible degree of $h_0(x)$

$$w(x) = a_m x^m + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

$$\longleftrightarrow \quad \vec{b} = \langle a_0, a_1, \dots, a_m \rangle \in \mathbb{Z}^{m+1}$$

Define $\mathcal{L}$ to be the lattice in $\mathbb{Z}^{m+1}$ spanned by the vectors associated with

$$w_j(x) = \begin{cases} p^k x^{j-1} & \text{for } 1 \le j \le \ell \\ h(x) x^{j-\ell-1} & \text{for } \ell+1 \le j \le m+1. \end{cases}$$

Define $\mathcal{L}$ to be the lattice in $\mathbb{Z}^{m+1}$ spanned by the vectors associated with

$$w_j(x) = \begin{cases} p^k x^{j-1} & \text{for } 1 \le j \le \ell \\ h(x)x^{j-\ell-1} & \text{for } \ell+1 \le j \le m+1. \end{cases}$$

Example

```
> f := x^14-4*x^3+2*x^2+x-3;
```

$$f := x^{14} - 4\,x^3 + 2\,x^2 + x - 3$$

```
> Factor(f) mod 151;
```

$$(x^2 + 129\,x + 44)\,(x^2 + 147\,x + 92)\,(x^2 + 127\,x + 31)\,(x^7 + 24\,x^6 + 91\,x^5 + 81\,x^4 + 30\,x^3 + 20\,x^2 + 2\,x + 34)\,(x + 26)$$

$$m = 5$$

Define $\mathcal{L}$ to be the lattice in $\mathbb{Z}^{m+1}$ spanned by the vectors associated with

$$w_j(x) = \begin{cases} p^k x^{j-1} & \text{for } 1 \le j \le \ell \\ h(x) x^{j-\ell-1} & \text{for } \ell + 1 \le j \le m+1. \end{cases}$$

```
> factor(f) mod 151;
```

$$(x^2 + 129\,x + 44)\,(x^2 + 147\,x + 92)\,(x^2 + 127\,x + 31)\,(x^7 + 24\,x^6 + 91\,x^5 + 81\,x^4 + 30\,x^3 + 20\,x^2 + 2\,x + 34)\,(x + 26)$$

$$\langle 151, 0, 0, 0, 0, 0 \rangle$$

$$\langle 0, 151, 0, 0, 0, 0 \rangle$$

$$\langle 44, 129, 1, 0, 0, 0 \rangle$$

$$\langle 0, 44, 129, 1, 0, 0 \rangle$$

$$\langle 0, 0, 44, 129, 1, 0 \rangle$$

$$\langle 0, 0, 0, 44, 129, 1 \rangle$$

Example

```
> f := x^14-4*x^3+2*x^2+x-3;
```

$$f := x^{14} - 4\,x^3 + 2\,x^2 + x - 3$$

```
> Factor(f) mod 151;
```

$$(x^2 + 129\,x + 44)\,(x^2 + 147\,x + 92)\,(x^2 + 127\,x + 31)\,(x^7 + 24\,x^6 + 91\,x^5 + 81\,x^4 + 30\,x^3 + 20\,x^2 + 2\,x + 34)\,(x + 26)$$

Claim: The lattice $\mathcal{L}$ is exactly the vectors corresponding to $w(x) \in \mathbb{Z}[x]$ that are divisible by $h(x)$ modulo p^k.

$$\langle 151, 0, 0, 0, 0, 0 \rangle$$

$$\langle 0, 151, 0, 0, 0, 0 \rangle$$

$$\langle 44, 129, 1, 0, 0, 0 \rangle$$

$$\langle 0, 44, 129, 1, 0, 0 \rangle$$

$$\langle 0, 0, 44, 129, 1, 0 \rangle$$

$$\langle 0, 0, 0, 44, 129, 1 \rangle$$

Example

```
> f := x^14-4*x^3+2*x^2+x-3;
```

$$f := x^{14} - 4x^3 + 2x^2 + x - 3$$

```
> Factor(f) mod 151;
```

$$(x^2 + 129x + 44)(x^2 + 147x + 92)(x^2 + 127x + 31)(x^7 + 24x^6 + 91x^5 + 81x^4 + 30x^3 + 20x^2 + 2x + 34)(x + 26)$$

Claim: The lattice $\mathcal{L}$ is exactly the vectors corresponding to $w(x) \in \mathbb{Z}[x]$ that are divisible by $h(x)$ modulo p^k. Hence, the vector $\vec{b}_0$ corresponding to $h_0(x)$ is in $\mathcal{L}$.

$$\langle 151, 0, 0, 0, 0, 0 \rangle$$
$$\langle 0, 151, 0, 0, 0, 0 \rangle$$
$$\langle 44, 129, 1, 0, 0, 0 \rangle$$
$$\langle 0, 44, 129, 1, 0, 0 \rangle$$
$$\langle 0, 0, 44, 129, 1, 0 \rangle$$
$$\langle 0, 0, 0, 44, 129, 1 \rangle$$

```
> f := x^14-4*x^3+2*x^2+x-3;
```

$$f := x^{14} - 4\,x^3 + 2\,x^2 + x - 3$$

```
> Factor(f) mod 151;
```

$$(x^2 + 129\,x + 44)\,(x^2 + 147\,x + 92)\,(x^2 + 127\,x + 31)\,(x^7 + 24\,x^6 + 91\,x^5 + 81\,x^4 + 30\,x^3 + 20\,x^2 + 2\,x + 34)\,(x + 26)$$

Claim: The lattice $\mathcal{L}$ is exactly the vectors corresponding to $w(x) \in \mathbb{Z}[x]$ that are divisible by $h(x)$ modulo p^k. Hence, the vector $\vec{b}_0$ corresponding to $h_0(x)$ is in $\mathcal{L}$.

We will show that in fact if p^k is large and $\vec{b}_1, \ldots, \vec{b}_{m+1}$ is a reduced basis for $\mathcal{L}$ with

$$b_1 = \langle a_0, a_1, \ldots, a_m \rangle,$$

then

$$\vec{b}_0 = \langle a_0/d, a_1/d, \ldots, a_m/d \rangle,$$

where $d = \gcd(a_0, \ldots, a_m)$.

$\langle 151, 0, 0, 0, 0, 0 \rangle$

$\langle 0, 151, 0, 0, 0, 0 \rangle$

$\langle 44, 129, 1, 0, 0, 0 \rangle$

$\langle 0, 44, 129, 1, 0, 0 \rangle$

$\langle 0, 0, 44, 129, 1, 0 \rangle$

$\langle 0, 0, 0, 44, 129, 1 \rangle$

```
> f := x^14-4*x^3+2*x^2+x-3;
```

$$f := x^{14} - 4x^3 + 2x^2 + x - 3$$

```
> Factor(f) mod 151;
```

$$(x^2 + 129x + 44)(x^2 + 147x + 92)(x^2 + 127x + 31)(x^7 + 24x^6 + 91x^5 + 81x^4 + 30x^3 + 20x^2 + 2x + 34)(x + 26)$$

Claim: The lattice $\mathcal{L}$ is exactly the vectors corresponding to $w(x) \in \mathbb{Z}[x]$ that are divisible by $h(x)$ modulo p^k. Hence, the vector $\vec{b}_0$ corresponding to $h_0(x)$ is in $\mathcal{L}$.

(Go to Maple.)

We will show that in fact if p^k is large and $\vec{b}_1, \ldots, \vec{b}_{m+1}$ is a reduced basis for $\mathcal{L}$ with

$$b_1 = \langle a_0, a_1, \ldots, a_m \rangle,$$

then

$$\vec{b}_0 = \langle a_0/d, a_1/d, \ldots, a_m/d \rangle,$$

where $d = \gcd(a_0, \ldots, a_m)$.