- This can be rephrased as an integral system:

$$\sum_{i=0}^{n-1} c_i x^i = \sum_{i=0}^{n-1-n'} \alpha_i \cdot (x^i g_k) + \sum_{i=0}^{n-1} \beta_i \cdot (p^{\ell k} x^i), \quad \text{----- (ii)}$$

where the unknown c's, α's & β's are in $\mathbb{Z}$.

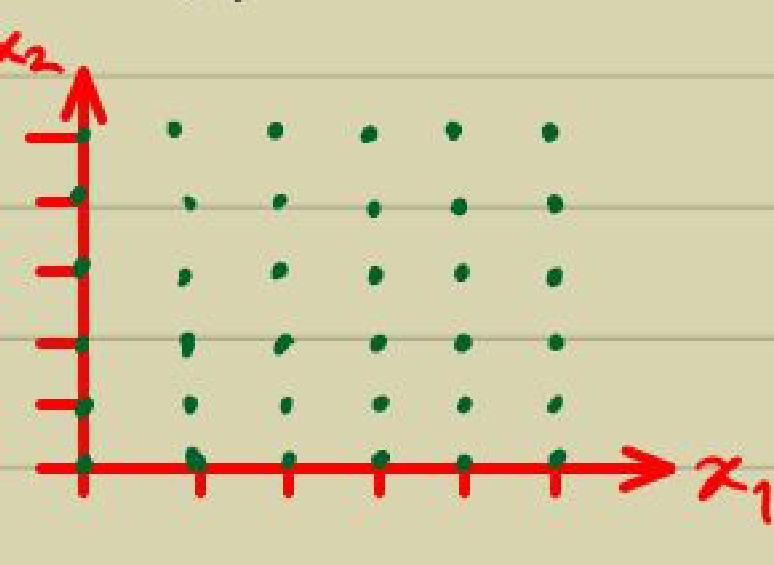
- We want a solution to (ii) s.t. $\|\bar{c}\| := \left(\sum_{i=0}^{n-1} c_i^2\right)^{1/2}$ is "small" $(< 2^{(\ell+\lg n)\cdot n})$.
  [assuming the existence of length $< 2^{(\ell+\lg n-1)n}$.]

- So the related fundamental problem to be solved is:

  Given $b_1, \ldots, b_m \in \mathbb{Z}^n$, find $\gamma_1, \ldots, \gamma_m \in \mathbb{Z}$ s.t. $\|\sum \gamma_i b_i\|$ is "small".

<u>Defn</u>: The $\mathbb{Z}$-linear-combinations of $\{b_i\}$ form a <u>lattice</u> $\underline{\mathcal{L}(b_1, \ldots, b_m)} := \left\{\sum_{i=1}^{m} \gamma_i b_i \mid \gamma_i \in \mathbb{Z}\right\}$.

- Eg. $\mathcal{L}\left(\binom{1}{0}, \binom{1}{1}\right)$ is:



$\triangleright$ $\mathcal{L}\left(\binom{1}{0}, \binom{1}{1}\right) = \mathcal{L}\left(\binom{1}{0}, \binom{0}{1}\right)$.

- Computing a <u>shortest</u> vector in $\mathcal{L}(b_1,..,b_m)$ is an NP-hard problem (<u>SVP</u>).

  But, we need merely a 2^n-approximation.

- First, we do a preprocessing step:

<u>Lemma 1:</u> We could assume, wlog, that $\{b_1,..,b_m\} =: B$ are linearly independent.

<u>Proof:</u>

- Consider the matrix $B := \begin{pmatrix} b_{11} & b_{21} & \cdots & b_{m1} \\ b_{12} & b_{22} & \cdots & b_{m2} \\ \vdots & \vdots & & \vdots \\ b_{1n} & b_{2n} & \cdots & b_{mn} \end{pmatrix}$
- Let $\sum_{i=1}^{m} a_i b_{i1} = g := \gcd(b_{11}, b_{21}, \ldots, b_{m1})$.
- Apply the extended-Euclid-algo. transformations on the columns.
- Say, the new columns are $b_1', b_2', \ldots, b_m'$.
- Next, transform the cols. $2 \leq j \leq m$, $b_j' \leftarrow b_j' - \frac{b_{j1}'}{g} \cdot b_1'$.
- This gives us a $B' = \begin{pmatrix} g & 0 \cdots 0 \\ * & \\ \vdots & * \\ * & \end{pmatrix}_{n \times m}$.

• The transformation is $B' = B \cdot \mathcal{U}$, where

$$\mathcal{U} := \mathcal{E} \cdot \begin{pmatrix} 1 & -b_{21}/g & \cdots & -b_{m1}/g \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

& $\mathcal{E}$ is the product of matrices following the Euclid's algorithm on the numbers $\{b_{11}, b_{21}, \ldots, b_{m1}\}$.

• Note that each step in the Euclid's algo. is <u>unimodular</u>, i.e. $|\mathcal{E}| = \pm 1$

$\Rightarrow |\mathcal{U}| = 1$.

$\Rightarrow \mathcal{L}(B') = \mathcal{L}(B)$. [$\mathcal{E}^{-1}$ is integral.]

• On repeatedly applying this Gauss-Euclid trick, we get a matrix

$$\tilde{B} := \left(\begin{array}{c|c} A_{m' \times m'} & \\ C_{(n-m') \times m'} & O_{n \times (m-m')} \end{array} \right)$$

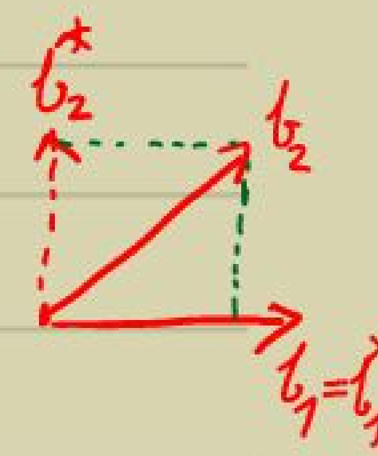
where A is <u>lower-triangular</u> and $\mathcal{L}(\tilde{B}) = \mathcal{L}(B)$.

$\Rightarrow$ The first m' columns of $\tilde{B}$ form a basis of size $m' \leq \min(n,m)$ spanning our lattice. $\square$

- So, we work with l.i. $b_1,\dots,b_m \in \mathbb{Z}^n$.
- In the vector space $\mathrm{span}_{\mathbb{R}}(b_1,\dots,b_m) =: V(B)$ there is an <u>orthogonal</u> basis:

- <u>Idea:</u> • Orthogonalize $\{b_1, b_2\}$ to

$$\left\{ b_1^* = b_1 ,\ b_2^* := b_2 - \frac{\langle b_2, b_1^* \rangle}{\|b_1^*\|^2} \cdot b_1^* \right\}.$$



▷ It is easily seen that the shorter of b_1^*, b_2^* is the shortest vector in $\mathcal{L}(b_1^*, b_2^*)$.

<u>Gram-Schmidt Orthogonalization</u>:

1) Let $b_1^* := b_1$.
2) For all $2 \leq i \leq m$, do

$$b_i^* := b_i - \sum_{j=1}^{i-1} \underbrace{\frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2}}_{\mu_{ij}} \cdot b_j^* .$$

<u>Lemma 2</u>: Any shortest vector $b \in \mathcal{L}(b_1,\dots,b_m)$ satisfies $\|b\| \geq \min_i \|b_i^*\|$.

<u>Proof</u>:

• Let $b = \lambda_1 b_1 + \dots + \lambda_m b_m$ for λ's in $\mathbb{Z}$ s.t. $\lambda_m \neq 0$.

• $\Rightarrow b = \lambda_1 b_1^* + \lambda_2(b_2^* + \mu_{21} b_1^*) + \ldots + \lambda_m(b_m^* + \mu_{m,m-1} b_{m-1}^* + \ldots$
$+ \mu_{m1} b_1^*)$.

$\Rightarrow \|b\|^2 = (\ldots)^2 \cdot \|b_1^*\|^2 + (\ldots)^2 \cdot \|b_2^*\|^2 + \ldots + \lambda_m^2 \cdot \|b_m^*\|^2$

$\Rightarrow \|b\| \geq |\lambda_m| \cdot \|b_m^*\| \geq \|b_m^*\|$. $\square$

– Using $\mathbb{Z}$-coefficients it may not be possible to orthogonalize $\mathcal{L}(B)$. So, L^3 tries to make the "angles" around $60°$! [$\cos 60° = 1/2$]

<u>Defn</u>: • L^3 will find a <u>reduced basis</u> of $\mathcal{L}(b_1, \ldots, b_m)$. These are lattice elements $c_1, \ldots, c_m$ s.t.

(i) $\forall i$, $\|c_i^*\|^2 \leq \frac{4}{3} \cdot \|c_{i+1}^* + \mu_{i+1,i} c_i^*\|^2$

(ii) $\forall i \geq j$, $|\mu_{ij}| \leq 1/2$

where $\mu_{ij} := \dfrac{\langle c_i, c_j^* \rangle}{\|c_j^*\|^2}$

$\triangleright \Rightarrow \|c_i^*\|^2 \leq \frac{4}{3} \|c_{i+1}^*\|^2 + \frac{1}{3} \cdot \|c_i^*\|^2$

$\Rightarrow \|c_i^*\| \leq \sqrt{2} \cdot \|c_{i+1}^*\| \Rightarrow \|c_1^*\| \leq \min_i \{2^{\frac{i-1}{2}} \cdot \|c_i^*\|\}$.

$\Rightarrow \|c_1^*\| \leq 2^{\frac{n-1}{2}} \cdot \lambda(\mathcal{L})$.

where $\lambda(\mathcal{L})$ is the shortest length in $\mathcal{L}(B)$.