LLL e applicazioni.

L'algoritmo LLL (Lenstra-Lenstra-Lovasz) fornisce una soluzione al problema A-SVP.

Abbiamo visto l'algoritmo di Gauss che risolve SVP per $n=2$ - LLL generalizza questo algoritmo per $n>2$.

Applicazioni:

1. Fattorizzazione di polinomi $f(x) \in \mathbb{Z}[x]$
2. Costruzione del polinomio minimo di un numero algebrico α noto con buona approssimazione (es. $\alpha = 1.414213 \rightarrow x^2-2$)
3. Trovare relazioni intere i.e. dati $x_1, \dots, x_n \in \mathbb{R}$ trovare $a_i \in \mathbb{Z}$ t.c. $\sum a_i x_i = 0$
4. Approssimazione di CVP
5. Attacchi a sistemi crittografici. Es. attacchi a RSA

=

∴ Descriviamo LLL per il caso di reticoli di rango massimo $m=n$.

∴ Consideriamo $\| \ \|_2$, anche se esistono estensioni ad altre norme.

Algoritmo LLL.

1. Definizioni
2. Descrizione e correttezza
3. Analisi del tempo di esecuzione

---

1. Ricordiamo G.S. dati $b_1, \dots, b_n \in \mathbb{R}^n$, l. ind.

$$\begin{cases} b_1^* = b_1 \\ b_i^* = b_i - \sum_{j<i} \mu_{ij} b_j^* \end{cases} \qquad \mu_{ij} = \frac{(b_i, b_j^*)}{\|b_j^*\|^2} \quad i>1$$

nota $\langle \mathcal{B}^* \rangle = \langle \mathcal{B} \rangle$ ma $\mathcal{B}^*$ non è base di $\mathcal{L}(\mathcal{B})$!

Definizione* una base $\{b_1, \dots, b_n\} \subseteq \mathbb{R}^n$ si dice δ-LLL ridotta se:

1. $\forall j<i \qquad |\mu_{ij}| \leq \frac{1}{2}$
2. $\forall i \qquad \delta \| b_i^* \|^2 \leq \| b_{i+1}^* + \mu_{i,i+1} b_i^* \|^2$

∴ ~~Esiste~~ È sempre possibile trasformare una base in una δ-LLL-ridotta.

∴ Consideriamo $\delta = \frac{3}{4}$

∴ l'algoritmo funziona $\forall \ \frac{1}{4} < \delta < 1$

Oss. Se riscriviamo la condizione 2:

$$\delta \| b_i^* \|^2 \leq \| b_{i+1}^* + \mu_{i+1,i}\, b_i^* \|^2 = \mu_{i+1,i}^2 \|b_i^*\|^2 + \| b_{i+1}^* \|^2$$

$\Downarrow$

$$\| b_{i+1}^* \|^2 \geq \left(\delta - \cancel{\tfrac{}{4}} \mu_{i+1,i}^2 \right) \| b_i^* \|^2 \geq \left(\delta - \tfrac{1}{4} \right) \| b_i^* \|^2$$

in questo modo dice che b_{i+1}^* non è troppo più corto di b_i^*.

Oss Se normalizziamo la base $b_1^*, \dots, b_n^*$ e mettiamo ~~colle~~ colonne in una matrice le coordinate di $b_1, \dots, b_n$ rispetto a questa nuova base otteniamo

$$\begin{pmatrix} \|b_1^*\| & \mu_{21} \|b_1^*\| & \mu_{31} \|b_1^*\| & * \; * \; * \; * \; * \\ 0 & \|b_2^*\| & \mu_{32} \|b_2^*\| & * \; * \; * \; \cdots \\ \vdots & 0 & \|b_3^*\| & * \; * \; * \; * \; \cdots \\ \vdots & \vdots & 0 & \ddots \\ 0 & 0 & \vdots & \|b_n^*\| \end{pmatrix}$$

Se $b_1, \dots, b_n$ è LLL-ridotta che proprietà ha questa matrice?

Condizione 1 Il valore assoluto di ogni elemento fuori diagonale è al più $\frac{1}{2}$ del valore sulla diagonale (della stessa riga)

$$\begin{pmatrix} \|b_1^*\| & \leq \frac{1}{2}\|b_1^*\| & \cdots & \leq \frac{1}{2}\|b_1^*\| \\ 0 & \|b_2^*\| & \leq \frac{1}{2}\|b_2^*\| \cdots & \leq \frac{1}{2}\|b_2^*\| \\ \vdots & & \ddots & \\ 0 & & & \|b_n^*\| \end{pmatrix}$$

Condizione 2 Se consideriamo la sottomatrice 2x2

$$\begin{pmatrix} \|b_i^*\| & \mu_{i+1,i}\|b_{i+1}^*\| \\ 0 & \|b_{i+1}^*\| \end{pmatrix}$$

allora la seconda colonna è al più lunga come la prima colonna.

Come per il caso di Gauss anche il primo vettore di una base LLL ha un'importante proprietà: è relativamente corto!

<u>Proposizione</u> Siano $\mathcal{B}=\{b_1,\dots,b_n\}$ una base LLL-ridotta. Allora

$$\|b_1\| \leq \left(\frac{2}{\sqrt{4\delta-1}}\right)^{n-1} \lambda_1(\mathcal{L}(\mathcal{B}))$$

<u>Nota</u> se $\delta = \frac{3}{4}$ $\quad \|b_1\| \leq 2^{\frac{n-1}{2}} \lambda_1(\mathcal{L}(\mathcal{B}))$

<u>Dim.</u> Per ogni base di $\mathcal{L}$, $\mathcal{B}=\{b_1,\dots,b_n\}$ vale che $\lambda_1(\mathcal{L}) \geq \min \|b_i^*\|$.

Quindi

$$\|b_n^*\|^2 \geq \left(\delta-\frac{1}{4}\right)\|b_{n-1}^*\|^2 \geq \dots \geq \left(\delta-\frac{1}{4}\right)^{n-1}\underbrace{\|b_1^*\|}_{=\|b_1\|}$$

e $\forall i$

$$\|b_1\| \leq \left(\delta-\frac{1}{4}\right)^{-\frac{(i-1)}{2}} \|b_i^*\| \leq \left(\delta-\frac{1}{4}\right)^{-\left(\frac{n-1}{2}\right)} \|b_i^*\|$$

Da cui

$$\|b_1\| \leq \left(\delta-\frac{1}{4}\right)^{\frac{-(n-1)}{2}} \cdot \min_i \|b_i^*\| \leq \left(\frac{2}{\sqrt{4\delta-1}}\right)^{n-1} \cdot \lambda_1(\mathcal{L})$$

$\delta = 3/4$ $\quad b_1$ soluzione ASVP $\gamma = 2^{\frac{n-1}{2}}$

Algoritmo LLL

Input: $b_1, .., b_n \in \mathbb{Z}^n$ base di $\mathcal{L}$

Output: δ-LLL base ridotta di $\mathcal{L}$

1. $b_1^*, .., b_n^* := GS \cdot (b_1, .., b_n)$ base ortogonale

2. Passo di Riduzione

   for i in $2..n$ repeat

   for j in $(i-1)..1$ repeat

   ** $b_i := b_i - c_{ij} b_j$ $\qquad c_{ij} := \left\lceil \frac{(b_i, b_j^*)}{\|b_j^*\|^2} \right\rfloor \in \mathbb{Z}$

   sommiamo alla colonna i multipli interi delle colonne precedenti

3. Passo di scambio

   if $\exists i$ $\delta \|b_i^*\|^2 > \|\mu_{i+1,i} b_i^* + b_{i+1}^*\|^2$ then

   $b_i \leftrightarrow b_{i+1}$

   Torna a 1

4. output $b_1, .., b_n$.

<u>oss</u> il Passo di scambio garantisce che la cond. 2 sia soddisfatta.

<u>Se</u> l'algoritmo termina (lo dimostreremo) l'output soddisfa 2.

Inoltre dal momento che le operazioni su $B = [b_1, .., b_n]$ sono op. el. di colonna ** con coeff. interi il risultato è una base di $\mathcal{L}$

Vediamo ora la condizione 1. Di questa si occupa il passo di riduzione.

Innanzitutto $b_1^*, \dots, b_n^*$ non cambiano dato che

$$b_i := b_i + c_{ij}\, b_j \quad \text{e} \quad \underline{\underline{j < i}}\ , \ c_{ij} \in \mathbb{Z}$$

Nel passo $\underline{\underline{i}}$ aggiustiamo la condizione

$$|(b_i, b_j^*)| \leq \frac{1}{2} \|b_j^*\| \quad \forall\ j < i$$

sottraendo alla colonna i ~~essa~~ multipli opportuni delle colonne precedenti.

Es. Scriviamo come prima $b_1, \dots, b_n$ rispetto alla base GS normalizzata e supponiamo di essere al passo $\underline{i}$ e $j = 2$. allora la matrice

$$\begin{array}{c}
\begin{array}{ccccccc} & & & & \downarrow i & & \end{array} \\
\begin{pmatrix}
\|b_1^*\| & \leq \frac{1}{2}\|b_1^*\| & \leq \frac{1}{2}\|b_1^*\| & \dots & * & * \ * \ \dots & \\
0 & \|b_2^*\| & \leq \frac{1}{2}\|b_2^*\| & & * & & \\
\vdots & 0 & \|b_3^*\| & \dots & \leq \frac{1}{2}\|b_3^*\| & & * \\
0 & \vdots & & & \vdots & & * \\
\vdots & 0 & & & \leq \frac{1}{2}\|b_{i-1}^*\| & & * \\
0 & 0 & & \ddots & \|b_i^*\| & & * \\
 & \dots & \dots & \dots & \dots & \dots & \|b_n^*\|
\end{pmatrix}
\end{array}$$

A questo passo ci occupiamo di ⊛ (el. $(2, i)$)
~~d~~ sottraendo alla colonna i $c_{i2} \cdot$ la colonna 2 il valore ⊛ sarà tale che in valore assoluto $\leq \frac{1}{2} \|b_2^*\|$. ~~[illegible]~~
(Iterando per $j = 1$ "sistemiamo" l'elemento $(1, i)$.)

infatti in $(2,1) \rightarrow \left| \mu_{i2} \|b_2^*\| - c_{i2} \|b_2^*\| \right| \leq \frac{1}{2} \|b_2^*\|$

In generale se $i > j$ avremo che il nuovo μ_{ij} al passo j nel loop i è:

$$|\mu_{ij}| = \left| \frac{(b_i - c_{ij} b_j, b_j^*)}{\|b_j^*\|^2} \right| =$$

$$= \left| \frac{(b_i, b_j^*)}{\|b_j^*\|^2} - \left\lceil \frac{(b_i, b_j^*)}{\|b_j^*\|^2} \right\rfloor \cdot \frac{(b_j, b_j^*)}{\|b_j^*\|^2} \right| \leq \frac{1}{2}$$

e quindi la condizione 1 è soddisfatta

Proviamo che l'algoritmo termina trovando un bound per il numero di iterazioni.

Definizione: Dato una base $\{b_1, \dots, b_n\} = \mathcal{B}$ di un reticolo $\mathcal{L}$, siano $\mathcal{L}_i = \{ \sum a_{ij} b_j \mid j = 1, \dots, i\}$ i sottoreticoli generati da $\{b_1, \dots, b_i\}$ $i \leq n$ definiamo "potenziale" di $\mathcal{B}$:

$$\mathcal{D}_{\mathcal{B}} = \prod_{i=1}^{n} \|b_i^*\|^{n-i+1} = \prod_{i=1}^{n} \|b_1^*\| \cdots \|b_i^*\| =$$

$$= \prod_{i=1}^{n} \mathcal{D}_{\mathcal{B}_i} = \prod \det(\mathcal{L}_i)$$

Usiamo $\mathcal{D}_{\mathcal{B}}$ per limitare il # di passi di LLL.

1. Dal momento che $\forall i$ $\|b_i^*\| \leq \|b_i\|$ il valore iniziale di $\mathcal{D}_{\mathcal{B}}$ soddisfa

$$\mathcal{D}_{\mathcal{B}} = \prod_{1}^{n} \|b_i^*\|^{n-i+1} \leq (\max \|b_i\|)^{\frac{n(n+1)}{2}}$$

2. Vediamo cosa succede durante l'algoritmo:

   a. Passo di riduzione: $b_1^*, \dots, b_n^*$ <u>non cambiano</u> quindi $\mathcal{D}_{\mathcal{B}}$ <u>non cambia</u>

b. Passo di scambio.

Supponiamo che b_i e b_{i+1} si scambino

Dato che $\det \mathcal{L}_k = \sqrt{B_k^T \cdot B_k}$ $\quad B_k = [b_1 \dots b_k]$

se $k \neq i$ D_{B_k} non cambia

se $k = i$ consideriamo D_{B_i} e siano

$\mathcal{L}_i' = \{b_1, \dots, b_{i-1}, b_{i+1}\}$ e $D_{B_i'}' = \det \mathcal{L}_i'$

i nuovi valori. Allora

nuovo vett. base ortogonale $GS\{b_1 \dots b_{i-1}, b_{i+1}\}$

$$\frac{D_{B_i'}'}{D_{B_i}} = \frac{\det \mathcal{L}_i'}{\det \mathcal{L}_i} = \frac{\prod_{j=1}^{i-1} \|b_j^*\| \cdot \|\tilde{b}_i^*\|}{\prod_{1}^{i} \|b_j^*\|} = \frac{\|\tilde{b}_i^*\|}{\|b_i^*\|}$$

dal momento che i nuovi $b_j^* = b_j^*$ $j<i$ si ha

e $\mu_{i,j}' = \mu_{i+1,j}$

$$\tilde{b}_i^* = b_{i+1} - \sum_{j<i} \mu_{i+1,j}\, b_j^*$$

$$= \left(b_{i+1}^* + \sum_{j<i+1} \mu_{i+1,j}\, b_j^*\right) - \sum_{j<i} \mu_{i+1,j}\, b_j^*$$

$$= b_{i+1}^* + \mu_{i+1,i}\, b_i^*$$

condizione di scambio

$$\frac{D_{B_i'}'}{D_B} = \frac{\|\tilde{b}_i^*\|}{\|b_i^*\|} = \frac{\|b_{i+1}^* + \mu_{i+1,i}\, b_i^*\|}{\|b_i^*\|} < \sqrt{\delta}$$

Quindi in ogni iterazione D_B <u>decresce</u> di un fattore $\sqrt{\delta}$ $\Rightarrow$ se $D_{B,0}$ valore iniziale il # di iterazioni può essere limitato da:

$$\log_{\frac{1}{\sqrt{\delta}}} D_{B,0} = \frac{\log D_{B_0}}{\log\left(\frac{1}{\delta}\right)} \leq \frac{1}{\log\left(\frac{1}{\sqrt{\delta}}\right)} \cdot \frac{n(n+1)}{2} \log(\max \|b_i\|$$

e $\forall \delta$ questo è polinomiale in

$$M = \max\{n, \log(\max \|b_i\|)\}$$

Per finire dobbiamo limitare il tempo per ogni iterazione: vale

<u>Lemma</u> il tempo di ogni iterazione è polinomiale in M. Si prova:

1). ogni iterazione richiede solo un numero polinomiale di operazioni aritmetiche.
2) gli interi che appaiono in ogni iterazione sono rappresentabili con un numero polinomiale di bits.

....

Prima di passare alle applicazioni ricapitoliamo dei risultati che usiamo;

Se $b_1, \dots, b_n$ è la base LLL ridotta, $\delta = \frac{3}{4}$ di un reticolo $\mathcal{L}$ allora

1. $\|b_1\| \le 2^{\frac{n-1}{2}} \lambda_1(\mathcal{L})$

2. $\|b_j^*\|^2 \le 2^{n-i} \|b_i^*\|^2 \qquad 1 \le i \le j \le n$

(segue dalla condizione 2. $\|b_i^*\|^2 \geq \left(\frac{3}{4} - \frac{1}{4}\right) \|b_{i-1}^*\|^2 \dots$)

3. Teorema (di Minkowski). $\lambda_1(\mathcal{L}) < \sqrt{n} \det(\mathcal{L})^{1/n}$.

Esempio sia $\mathcal{L}$ con base $B = \begin{array}{c} \begin{pmatrix} 1 & 4 & 0 \\ 0 & 2 & 0 \\ 0 & 15 & 3 \end{pmatrix} \\ b_1 \; b_2 \; b_3 \end{array}$

1. Calcoliamo b_1^*, b_2^*, b_3^*

$b_1^* = b_1 = (1,0,0)$

$b_2^* = b_2 - \mu_{21} b_1^* = (0,2,15)$ $\qquad \mu_{21} = 4$

$b_3^* = b_3 - \mu_{31} b_1^* - \mu_{32} b_2^*$ $\qquad \mu_{31} = 0 \quad \mu_{32} = \frac{45}{229}$

$= b_3 - \frac{45}{229} b_2^* = \left(0, \frac{-90}{229}, \frac{12}{229}\right)$

1. passo

$b_1 = (1,0,0)$

$b_2 = b_2 - 4 b_1 = (0,2,15)$ $\qquad \lceil \mu_{21} \rfloor = 4$

$b_3 = b_3$ $\qquad \lceil \mu_{31} \rfloor = 0$

2. Scambio

$B_1 = \|b_1^*\|^2 = 1$

$B_2 = \|b_2^*\|^2 = 229$

$B_2 > \left(\frac{3}{4} - \mu_{21}^2\right) B_1$ no scambio

$B_3 = \|b_3^*\|^2 = \frac{8244}{52441}$ e $B_3 < \left(\frac{3}{4} - \mu_{32}^2\right) B_2$

$\Rightarrow$ Scambiamo b_2 e b_3

abbiamo $b_1 = (1,0,0)$ $\quad b_2 = (0,0,3)$ $\quad b_3 = (0,2,15)$

ES $B = \begin{pmatrix} 0 & -1 & 5 \\ 3 & 3 & 4 \\ 4 & 3 & -7 \end{pmatrix}$

$b_1^* = b_1 \quad = (1,0,0)$

$b_2^* = b_2 = (0,0,3) \qquad \mu_{21} = 0$

$B_1 := \|b_1^*\|^2 = 1$

$B_2 := \|b_2^*\|^2 = 9$

$B_2 > \left(\frac{3}{4} - \mu_{21}^2\right) B_1$ ok

$b_3^* = b_3 - \mu_{31} b_1^* - \mu_{32} b_2^* \qquad \mu_{31} = 0$

$= (0,2,0) \qquad \mu_{32} = \frac{45}{9} = 5$

$b_3 = b_3 - \lceil \mu_{31} \rfloor b_1^* - \lceil \mu_{32} \rfloor b_2 = (0,2,0) \qquad \lceil \mu_{32} \rfloor = 5$

$B_3 = \|b_3^*\|^2 = 4$ e $B_3 < \left(\frac{3}{4} - \mu_{32}^2\right) B_2$

$\Rightarrow$ scambiamo b_2 e b_3

Così $b_1 = (1,0,0)$, $b_2 = (0,2,0)$ e $b_3 = (0,0,3)$

niente cambia

ma ora $B_3 = 9 > \left(3/4 - \mu_{32}^2\right) B_2 = 3$ ok

$\Rightarrow$ output $(1,0,0)$, $(0,2,0)$ $(0,0,3)$.

Attacco a RSA (con ~~esponente~~ chiave pubblica piccola)

$$N = p \cdot q\ ,\quad r \cdot s \equiv 1\ (\varphi(N))$$

N - modulo $\quad (N, r)$ = chiave pubblica

$\qquad\qquad\quad (N, S)$ = chiave privata

$M \in \mathbb{Z}_N^*$ messaggio $\xrightarrow{\text{crypt}} C \equiv M^r (N)$

$C^S \equiv M^{rs} \equiv M \xleftarrow[\text{decrypt}]{}$

In molte applicazioni per semplificare e per efficienza es. $r = 3$ (o piccolo comunque)

$(r^3 = r^2 \cdot r \Rightarrow 2$ molt.) - Ma:

Se

$$A \to \begin{cases} B & N_B \\ C & N_C \\ D & N_D \end{cases}$$

manda lo <u>stesso</u> messaggio e lo crypta

$$C_B \equiv M^3 (N_B) \quad C_C \equiv M^3 (N_C) \quad C_D \equiv M^3 (N_D)$$

e si conoscono C_B, C_C, C_D si può recuperare M con il <u>CRA</u>

Se si suppone $(N_B, N_C) = (N_C, N_D) = (N_D, D_B) = 1$ (altrimenti col gcd si fattorizza!) il sistema:

$$\begin{cases} X \equiv C_B & (N_B) \\ X \equiv C_C & (N_C) \\ X \equiv C_D & (N_D) \end{cases} \overset{\text{Soluzione}}{\rightsquigarrow} \quad X \equiv M^3 \ (N_B N_C N_D)$$

$(C_B \equiv M^3 \dots)$ ma $M < N_B, N_C, N_D \Rightarrow$
$M^3 < (N_B \cdot N_C \cdot N_D)$

da cui $X = M^3$ (su $\mathbb{Z}$) e $\underline{M = \sqrt[3]{X}}$!!!

1. <u>Soluzione</u>: non mandare a più persone lo stesso messaggio.

<u>Es.</u> modificarlo "aggiungendo" un'informazione

Se si assegna a ogni ricevente un ID e cifriamo $M \underset{\text{trasformo}}{\rightsquigarrow} M + 2^k \cdot ID$ $(k = \log_2 M$

o più in generale $M \rightsquigarrow \underline{g(M)}$ g polinomi

$\left(M + 2^k ID \quad g(x) = (x + 2^k ID)^3 \right)$

Nuova chiave $\underline{(N, g)}$.

ma non basta!

Oss. Ancora si considera sicuro RSA con esp. piccolo

Oss. Esistono attacchi migliori del successivo.

ATTACCO: Si basa su CRA e sul seguente

Teorema (Coppersmith) se $N \in \mathbb{Z}$, $f(x) \in \mathbb{Z}/_N[x]$ monico, $\deg f = d$, e $B = N^{\frac{1}{d}}$ allora possiamo trovare le radici $\alpha \in \mathbb{Z}$ di f mod N (i.e. $f(\alpha) \equiv 0$ (N)). t.c. $|\alpha| \leq B$.

Vediamo l'attacco: Siano $N_1, \dots, N_k \in \mathbb{Z}$ $(N_i, N_j) = 1$ $i \neq$ e sia $\tilde{N} = \min N_i$. Siano $g_1, \dots, g_k$, $g_i \in \mathbb{Z}/_{N_i}[x]$ e $c_1 \dots c_k$, $c_i = g_i(M)$ (N_i) con $M < \tilde{N}$ (unico)

Allora se $k \geq d$ si recupera in modo efficient M (noti (N_i, g_i, c_i)).

monici o si fanno

Dim. Risolviamo:
$$\begin{cases} g_1(M) - c_1 = h_1 \equiv h & (N_1) \\ \vdots \\ g_k(M) - c_k = h_k \equiv h & (N_k) \end{cases}$$

$\deg h_i = \deg h_j = d$
(o si moltiplica per x°)

La sol $h(x)$ è t.c.
$$\begin{cases} h(M) \equiv 0 \quad (N_1 \cdots N_k) \\ \text{monico} \\ \deg h = d. \end{cases}$$

$\Rightarrow$ per il teorema $\exists\, M$ t.c. $M < \tilde{N} \leq (N_1 \cdots N_k)^{1/k} \leq (N_1 \cdots N_k)^{1/d}$
e quindi M messaggio (su $\mathbb{Z}$).

Traccia dim. teorema

RS

Sia $f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0$ cerchiamo $\alpha \in \mathbb{Z}$ t.c. $f(\alpha) \equiv 0 \ (N)$ e $|\alpha| \le B$

* Se $\forall i \ |a_i B^i| < \frac{N}{d+1}$ allora $|f(\alpha)| \le \sum_0^d |a_i B^i| < N$

e quindi da $-N < f(\alpha) < N$ e $f(\alpha) \equiv 0 \ (N) \Rightarrow f(\alpha) =$ su $\mathbb{Z}$

Oss. i coefficienti devono essere "piccoli"

IDEA Costruire un polinomio con la stessa radice ma con coefficienti piccoli (mod N)

ES $f(x) = x^2 + 33x + 215$ $\quad N = 323$

Vogliamo trovare α soluzione mod N piccola
($\alpha = 3$ $\quad f(\alpha) \equiv 0 \ (N)$ ma $f(\alpha) \not\equiv 0$ su $\mathbb{Z}$)

Cerchiamo un polinomio con coefficienti "piccoli"

$$g(x) \equiv 9 \cdot f(x) \mod (N)$$
$$= 9x^2 - 26x - 3$$

$g(3) = 0$ e 3 si può trovare es Newton

Per costruire $g(x)$ consideriamo il reticolo $\mathcal{L}$ in $\mathbb{R}^{d+1}$ generato dalle coordinate (coefficienti) dei polinomi

$$N, xN, \dots, x^{d-1}N, f(x)$$

È chiaro che se $v \in \mathcal{L} \to v(\alpha) \equiv 0 \ (N)$ $\Leftarrow f(\alpha) \equiv 0 \ (N)$.

Sia

$$\mathcal{L}' \longleftrightarrow \begin{pmatrix} N & 0 & \cdots & & a_0 \\ 0 & NB & & & a_1 B \\ & & NB^2 & & \vdots \\ & 0 & & \ddots & \vdots \\ & & & & B^d \end{pmatrix}$$

Vale: $\det(\mathcal{L}') = N^d \cdot B^{\frac{d(d+1)}{2}}$

se applichiamo LLL il primo vettore è t.c.

$$\|v_1\| \leq O(\lambda_1(\mathcal{L}_1)) \underset{\uparrow \text{minkowski}}{\leq} O(\det \mathcal{L}_1)^{\frac{1}{d+1}} = O(N^{\frac{d}{d+1}} B^{\frac{d}{2}})$$

Se scegliamo

$B \leq c_1(d) \cdot N^{\frac{2}{(d+1)d}}$ per $c_1(d)$ che dip solo da d

$\Rightarrow$ ogni coordinata di v_1 è $\leq \frac{N}{d+1}$

e quindi $v_1 \longleftrightarrow g(x)$ soddisfa $*$

e $g(\alpha) = 0 \Leftrightarrow f(\alpha) = 0$.

__Esempio__ Sia $f(x) = x^3 + 10x^2 + 5000x - 222$

e $N = 10001$ $(= 73 \cdot 137)$.

$f(x)$ è irriducibile su $\mathbb{Z}$, ma $f(4) \equiv 0 \ (N)$

Poniamo $B = 10$ e consideriamo

$$\begin{pmatrix} N & 0 & 0 & -222 \\ 0 & NB & 0 & 5000B \\ 0 & 0 & NB^2 & 10B^2 \\ 0 & 0 & 0 & B^3 \end{pmatrix}$$

applicando LLL - il primo vettore della base è $(444, 10, -2000, -2000)$ e il polinomio corrispondente $g(x) = 444 + x - 20x^2 - 2x^3$ è tale che $g(4) = 0$ (si trova la radice es. con Newton).

$f \in \mathbb{Z}[x]$, primitivo, libero da quadrati, deg f
monico $\left(f(x) \leftarrow a_n^{n-1} f\left(\frac{x}{a_n}\right)\right)$

1. Si sceglie p primo t.c. $f \bmod (p)$ square free
   $(p \nmid \mathrm{Ris}(f, f'))$

2. Si fattorizza $f \bmod p$. (Berlekamp)
   polinomiale

3. Bound (Mignotte): Se $f, g \in \mathbb{C}[x]$ $g \mid f$
   f, g monici. Se $\deg g = m \Rightarrow \|g(x)\| \leq 2^m \|f\|$ $*$

4. Lemma di Hensel: Dati $g_1^{(1)}, \ldots, g_k^{(1)} \in \mathbb{Z}_p[x]$ t.c.
   $g_1^{(1)} \cdots g_k^{(1)} \equiv f \ (p)$ (fattorizzazione mod p)
   monici, irriducibili, $g_i \neq g_j$

   $$\Downarrow$$

   $g_1 \cdots g_k \equiv f \ (p^N)$ e $g_i \equiv g_i^{(1)} \ (p)$

5. Se $p^N > 2 B_m = 2 \cdot 2^{m-1} \|f\|$ $*$

   e $g_i \mid f$ su $\mathbb{Z}$ $\Rightarrow$ g_i fattore irriducibile

6. Se no $I = \{ i_1, \ldots, i_s \mid i_i \in \{1, \ldots, k\}\ g_{i_1} \cdots g_{i_s} \mid f \}$.
   $\Rightarrow$ al peggio 2^{k-1} volte.

Invece di ⑥ — LLL. Si sostituisce "ricombinare" i fattori con ~~la~~ riduzione di un reticolo!

Useremo:

<u>Lemma</u> se $f(x) \equiv g_0 \cdot v \ (p^N)$, g_0, v monici $\in \mathbb{Z}[x]$

Se $g \in \mathbb{Z}[x]$, $\deg g = m < n$, è t.c. $g(x) \equiv g_0 \cdot u \ (p^N)$

($\deg u = \deg g - \deg g_0$) e $\|g(x)\|^n \cdot \|f(x)\|^m < p^N$

allora $\gcd(f(x), g(x)) \neq 1$ in $\mathbb{Q}[x]$.

Sia $N = \left\lceil \log_p 2^{2n^2} \|f(x)\|^{2n} \right\rceil = O(n^2 + n\log\|f(x)\|)$

e sia $g_0 \mid f(x) \ (p^N)$ irriducibile, $\deg g_0 = d < n$

Se consideriamo $S = \{ g(x) \overset{\in \mathbb{Z}[x]}{} \mid \deg g \leq n-1, \exists h \in \mathbb{Z}[x] \ g \equiv hg$

S è un reticolo (considerando le coordinate date dai coefficienti) in $\mathbb{R}^n$ con base

$$\left(\underbrace{\begin{matrix} p^N & & \\ & p^N & \\ & & \ddots \ p^N \end{matrix}}_{d} \ \underbrace{[g_0] \ [xg_0] \cdots [x^{n-d-1} g_0]}_{n-d} \right)$$

e si ha:

<u>Th</u> se $g_1 \in \mathbb{Z}[x]$ è t.c. $[g_1]$ il vettore dei coefficienti è il primo elemento ~~del~~ di $\tilde{\mathcal{B}}$ base LLL ridotta di $\mathcal{L}$ allora $f(x)$ irriducibile $\Longleftrightarrow \gcd(f, g_1) = 1$.

Dim. se f_1 irriducibile $\Rightarrow$ ok

viceversa se f è riducibile e $g(x) \mid f(x)$ con $g_0 \mid g \ (p)$ in $\mathbb{Z}_p[x]$.
usando Hensel $g_0 \mid g \ (p^N)$ e quindi $g \in S$. Allora

$$\|g(x)\| \le 2^{n-1} \|f(x)\| \quad \text{(Mignotte)}$$

per LLL

$$\|g_1(x)\| \le 2^{\frac{(n-1)}{2}} \|g(x)\| < 2^n \|g(x)\| \le 2^{2n} \|f(x)\|$$

e quindi

$$\|g_1(x)\|^n \cdot \|f(x)\|^{\deg g_1} \le \|g_1(x)\|^n \|f(x)\|^n$$

$$\le 2^{2n^2} \|f(x)\|^{2n} \le p^N$$

$\Rightarrow$ per il lemma

$$\gcd(f, g_1) \ne 1.$$