Reticulados e Fatoração Implícita

José Laudelino de M. Neto

professor do Departamento de Ciências Exatas da UFPB

Sumário

Este texto é um estudo do artigo intitulado *Implicit Factoring: On Polynomial Time Factoring Given Only an Implicit Hint* [1], o qual trata de uma aplicação da Teoria de Reticulados na fatoração de números na forma $N_1 = p_1 q_1$ com p_1 e q_1 primos ímpares (*RSA moduli*), onde sabemos apenas algumas informações implícitas do número N_1; no caso, temos um outro número N_2 com algumas características em comum.

Lembrando que neste estudo não estamos interessados em analisar o custo do algoritmo, o qual sabemos que é de tempo polinomial.

Para melhor compreensão deste texto, aconselhamos a leitura de [2] e [3].

Rio Tinto, outubro de 2017.

1 Notações e Lema de Hadamard

Um *reticulado inteiro* L é um subgrupo discreto e adititivo de $\mathbb{Z}^n$. Equivalentemente, sejam $d, n \in \mathbb{N}$ e $\mathbf{b}_1, \ldots, \mathbf{b}_d \in \mathbb{Z}^n$ vetores LI, um reticulado inteiro L é o conjunto de todas as combinações lineares inteiras dos vetores $\mathbf{b}_i$, ou seja,

$$L = \{a_1\mathbf{b}_1 + \ldots + a_d\mathbf{b}_d; a_i \in \mathbb{Z}\}.$$

Dizemos que

$$B = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_d \end{pmatrix} \text{ ou } B = [\mathbf{b}_1, \ldots, \mathbf{b}_d]$$

é uma *base* do reticulado e d seu *posto*. Um reticulado tem *posto cheio* quando $d = n$. O *determinante* de um reticulado é definido como

$$\det(L) = \sqrt{\det(B \cdot B^t)} = \text{vol}(\mathcal{P}(B)),$$

onde $\mathcal{P}(B)$ denota o *paralelepípedo fundamental* do reticulado L. Quando L tem posto cheio, $\det(L) = |\det(B)|$. O $\det(L)$ não depende da escolha da base; o $\det(L)$ é invariante sobre mudança de base do reticulado L, através de matrizes mudança de base *unimodulares*. Uma matriz U é unimodular quando suas entradas são inteiros e $\det(U) = \pm 1$.

Seja $\mathbf{v} = (x_1, \ldots, x_n)$, definimos $\|\mathbf{v}\| = \sqrt{x_1^2 + \ldots + x_n^2}$, ou seja, $\|\mathbf{v}\|$ denota a norma euclidiana do vetor $\mathbf{v}$; ℓ_2-norma.

Lema 1 (Hadamard) *Sejam* $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$ *vetores LI e* $B = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_n \end{pmatrix}$. *Então,*

$$\det(B) \leq \prod_{i=1}^{n} \|\mathbf{b}_i\|.$$

Demonstração: Pelo processo de *Ortogonalização de Gram-Schimdt*, existe uma base ortonormal $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ de $\mathbb{R}^n$ tal que o espaço vetorial gerado por $\mathbf{b}_1, \ldots, \mathbf{b}_j$ é o mesmo espaço vetorial gerado por $\mathbf{b}_1^*, \ldots, \mathbf{b}_j^*$, para $j = 1, \ldots, n$. Definimos

$$B^* = \begin{pmatrix} \mathbf{b}_1^* \\ \vdots \\ \mathbf{b}_n^* \end{pmatrix}.$$

Cada vetor $\mathbf{v} \in \mathbb{R}^n$ pode ser escrito na forma

$$\mathbf{v} = \sum_{i=1}^{n} \langle \mathbf{v}, \mathbf{b}_i^* \rangle \mathbf{b}_i^*,$$

e, consequentemente,

$$\|\mathbf{v}\|^2 = \sum_{i=1}^{n} |\langle \mathbf{v}, \mathbf{b}_i^* \rangle|^2.$$

Em particular, cada vetor $\mathbf{b}_j$ é escrito na forma

$$\mathbf{b}_j = \sum_{i=1}^{j} \langle \mathbf{b}_j, \mathbf{b}_i^* \rangle \mathbf{b}_i^*.$$

Seja $C = (c_{kl})$ uma matriz triangular inferior definida por

$$c_{kl} := \begin{cases} \langle \mathbf{b}_k, \mathbf{b}_l^* \rangle, & 1 \leq l \leq k \\ 0 & k < l \leq n. \end{cases}$$

Assim, temos $B = C \cdot B^*$. Logo,

$$\begin{aligned} \det(B)^2 &= \det(B \cdot B^t) \\ &= \det[C \cdot B^* \cdot (B^*)^t C^t] \\ &= \det(C)^2 = \prod_{i=1}^{n} |\langle \mathbf{b}_i, \mathbf{b}_i^* \rangle|^2 \leq \prod_{i=1}^{n} \left\{ \sum_{j=1}^{i} |\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle|^2 \right\} = \prod_{i=1}^{n} \|\mathbf{b}_i\|. \quad \blacksquare \end{aligned}$$

2 Mínimos sucessivos e Teorema de Minkowski

Os mínimos sucessivos $\lambda_i(L)$ de um reticulado L são definidos como o menor raio da bola centrada na origem contendo i vetores LI pertencentes ao reticulado L. Em um reticulado bidimensional L é possível determinar uma base $\mathbf{b}'_1, \mathbf{b}'_2$ tal que $\|\mathbf{b}'_1\| = \lambda_1(L)$ e $\|\mathbf{b}'_2\| = \lambda_2(L)$, basta utilizar *redução de Gauss*. O vetor $\mathbf{b}'_1$ satisfazendo $\|\mathbf{b}'_1\| = \lambda_1(L)$ é o menor vetor do reticulado.

Teorema 1 (Minkowski) *Seja L um reticulado de posto n. Então L contém um vetor não-nulo $\mathbf{v}$ com*

$$\|\mathbf{v}\| = \lambda_1(L) \leq \sqrt{n}\,\sqrt[n]{\det(L)}.$$

3 Redução de Gauss

Descreveremos um algoritmo para resolver o *Problema do Menor Vetor* (ou *problema do vetor curto*, em inglês *shortest vector problem*) para reticulados de dimensão 2. O algoritmo é genérico com respeito a norma, isto é, calcula corretamente um menor vetor em um reticulado de dimensão 2 com respeito a qualquer norma $\|\cdot\|$, desde que $\|\cdot\|$ possa ser calculada de modo efetivo.

$\|\cdot\|$ é uma norma arbitrária, porém fixa.

A entrada do algoritmo é um par de vetores inteiros linearmente independente, $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$. Estamos interessados em determinar uma nova base $\mathbf{a}', \mathbf{b}'$ do reticulado $L(\mathbf{a}, \mathbf{b})$ tal que $\|\mathbf{a}'\| = \lambda_1(L)$ e $\|\mathbf{b}'\| = \lambda_2(L)$.

3.1 Base reduzida em dimensão 2

Dizemos que uma base $[\mathbf{a}, \mathbf{b}]$ de um reticulado L é reduzida (com respeito a norma $\|\cdot\|$) quando

$$\|\mathbf{a}\|, \|\mathbf{b}\| \leq \|\mathbf{a} + \mathbf{b}\|, \|\mathbf{a} - \mathbf{b}\|.$$

Geometricamente, esta definição nos diz que as diagonais do paralelepípedo fundamental associado a base do reticulado são, pelo menos, tão grandes quanto as arestas.

Além disso, esta definição é motivada pelo fato de que uma base é reduzida em um reticulado de dimensão 2 se, e só se, $\|\mathbf{a}\| = \lambda_1(L)$ e $\|\mathbf{b}\| = \lambda_2(L)$.

O Lema a seguir garante que se a distância de algum ponto aumenta ao nos deslocarmos em linha reta, então esta mesma distância aumenta se continuarmos nos deslocando na mesma direção.

Lema 2 *Consideremos os vetores* $\mathbf{x}, \mathbf{x} + \mathbf{y}, \mathbf{x} + \alpha\mathbf{y}, \alpha \geq 1$. *Para qualquer vetor* $\|\cdot\|$, *se* $\|\mathbf{x}\| \leq \|\mathbf{x} + \mathbf{y}\|$, *então* $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x} + \alpha\mathbf{y}\|$. *Além disso,* $\|\mathbf{x}\| < \|\mathbf{x} + \mathbf{y}\| \Rightarrow \|\mathbf{x} + \mathbf{y}\| < \|\mathbf{x} + \alpha\mathbf{y}\|$.

Demonstração: Provaremos para o caso "$<$", para "$\leq$" basta substituir "$<$" por "$\leq$".

Seja $\delta = \frac{1}{\alpha}$, então

$$\mathbf{x} + \mathbf{y} = (1 - \delta)\mathbf{x} + \delta(\mathbf{x} + \alpha\mathbf{y}).$$

Pela desigualdade triangular,

$$\|\mathbf{x} + \mathbf{y}\| \leq (1 - \delta)\|\mathbf{x}\| + \delta\|\mathbf{x} + \alpha\mathbf{y}\|.$$

Por hipótese, $\|\mathbf{x}\| < \|\mathbf{x} + \mathbf{y}\|$, assim,

$$\|\mathbf{x} + \mathbf{y}\| < (1 - \delta)\|\mathbf{x} + \mathbf{y}\| + \delta\|\mathbf{x} + \alpha\mathbf{y}\| \Rightarrow$$

$$\Rightarrow \delta\|\mathbf{x}+\mathbf{y}\| < \delta\|\mathbf{x}+\alpha\mathbf{y}\|.$$

Como $\delta > 0$ temos $\|\mathbf{x}+\mathbf{y}\| < \|\mathbf{x}+\alpha\mathbf{y}\|$. ■

Teorema 2 *Seja* $[\mathbf{a},\mathbf{b}]$ *a base de um reticulado* L. *Então,* $[\mathbf{a},\mathbf{b}]$ *é base reduzida se, e somente se,* $\|a\| = \lambda_1(L)$ *e* $\|b\| = \lambda_2(L)$.

Demonstração: ($\Leftarrow$) Suponhamos $\|\mathbf{a}\| = \lambda_1(L) \leq \lambda_2(L) = \|\mathbf{b}\|$. Por definição de $\lambda_1(L)$, temos

$$\|\mathbf{a}\| = \lambda_1(L) \leq \|\mathbf{a}-\mathbf{b}\|, \|\mathbf{a}+\mathbf{b}\|.$$

Como $[\mathbf{a},\mathbf{b}]$ é uma base, $\mathbf{a},\mathbf{b}$ é LI e, consequentemente, $\mathbf{a}-\mathbf{b},\mathbf{a}$ e $\mathbf{a}+\mathbf{b},\mathbf{a}$ também são LI.

Pela definição de $\lambda_2(L)$,

$$\begin{aligned} \lambda_2(L) &\leq \max\{\|\mathbf{a}\|, \|\mathbf{a}+\mathbf{b}\|\} = \|\mathbf{a}+\mathbf{b}\| \text{ e} \\ \lambda_2(L) &\leq \max\{\|\mathbf{a}\|, \|\mathbf{a}-\mathbf{b}\|\} = \|\mathbf{a}-\mathbf{b}\|. \end{aligned}$$

Portanto, $\|\mathbf{a}\|, \|\mathbf{b}\| \leq \lambda_2(L) \leq \|\mathbf{a}+\mathbf{b}\|, \|\mathbf{a}-\mathbf{b}\|$.

($\Rightarrow$) Seja $[\mathbf{a},\mathbf{b}]$ uma base reduzida. Sem perda de generalidade, assumimos que $\|\mathbf{a}\| \leq \|\mathbf{b}\|$. Sejam $r,s \in \mathbb{Z}$ e consideremos um vetor genérico $r\mathbf{a}+s\mathbf{b}$ pertencente ao reticulado L.

Provaremos que

$$\|\mathbf{a}\| \leq \|r\mathbf{a}+s\mathbf{b}\|, \forall (r,s) \neq (0,0) \text{ e} \quad (1)$$

$$\|\mathbf{b}\| \leq \|r\mathbf{a}+s\mathbf{b}\|, \forall s \neq 0. \quad (2)$$

Observamos que a Equação (1) nos diz que $\mathbf{a}$ é o menor vetor do que qualquer outro vetor não nulo pertencente a L, ou seja, $\|\mathbf{a}\| = \lambda_1(L)$. Simirlarmente, a Equação (2) garante que $\mathbf{b}$ é o menor vetor dentre todos os vetores que são LI com $\mathbf{a}$. Como $\mathbf{a}$ é o menor vetor do reticulado, temos $\|\mathbf{b}\| = \lambda_2(L)$.

Para provar as Equações (1) e (2) temos três casos para analisar:

1. $s = 0 \Rightarrow r \neq 0$ e $\|\mathbf{a}\| \leq \|r\mathbf{a}\| = \|r\mathbf{a}+s\mathbf{b}\|$;
2. $r = 0 \Rightarrow s \neq 0$ e $\|\mathbf{a}\| \leq \|\mathbf{b}\| \leq \|s\mathbf{b}\| = \|r\mathbf{a}+s\mathbf{b}\|$; e
3. $(r,s) \neq (0,0)$ e assumindo $s \leq 0 \leq r$ (os outros casos são similares). Suponhamos $r \geq |s| \geq 0 \Rightarrow \frac{r}{|s|} \geq 1$, assim

$$\left\|\frac{r\mathbf{a}}{|s|} - \mathbf{b}\right\| = \left\|\frac{r\mathbf{a}-|s|\mathbf{b}}{|s|}\right\| \leq \|r\mathbf{a}-|s|\mathbf{b}\| = \|r\mathbf{a}+s\mathbf{b}\|.$$

Pelo Lema 2,

$$\|\mathbf{a}\| \leq \|\mathbf{b}\| \leq \|\mathbf{a}-\mathbf{b}\| \leq \left\|\frac{r\mathbf{a}}{|s|} - \mathbf{b}\right\| \leq \|r\mathbf{a}+s\mathbf{b}\|. \quad ■$$

Observação 1 *Para o caso em que* $r \geq s \geq 0$ *utilizamos o fato que* $\|\mathbf{a}\| \leq \|\mathbf{b}\| \leq \|\mathbf{a}+\mathbf{b}\| \leq \|\mathbf{b}+\frac{r\mathbf{a}}{s}\|$.

3.2 O algoritmo da Redução de Gauss

Enunciaremos um algoritmo, conhecido como Redução de Gauss, para determinar uma base reduzida para qualquer reticulado de dimensão 2.

O algoritmo trabalha calculando uma sequência de bases bem ordenadas.

Uma base de um reticulado de dimensão 2, $[\mathbf{a}, \mathbf{b}]$, é *bem ordenada* quando

$$\|\mathbf{a}\| \leq \|\mathbf{a}-\mathbf{b}\| \leq \|\mathbf{b}\|.$$

Seja $[\mathbf{a}, \mathbf{b}]$ uma base do reticulado L. Como a base de entrada do algoritmo não é necessariamente bem ordenada, a primeira etapa a fazer é calcular uma base bem ordenada para o reticulado L, a qual é facilmente obtida através de uma simples análise.

Algoritmo da Redução de Gauss

Entrada: Base de um reticulado L, $[\mathbf{a}, \mathbf{b}]$.

Saída: Base reduzida do reticulado L.

1. Se $\|\mathbf{a}\| > \|\mathbf{b}\|$, então troque $\mathbf{a}$ por $\mathbf{b}$ e vá para 2. Caso contrário, vá para 2.
2. Se $\|\mathbf{a}-\mathbf{b}\| > \|\mathbf{a}+\mathbf{b}\|$, então $\mathbf{b} := -\mathbf{b}$ e vá para 3. Caso contrário, vá para 3.
3. Se $\|\mathbf{b}\| \leq \|\mathbf{a}-\mathbf{b}\|$, então pare e retorne $[\mathbf{a}, \mathbf{b}]$. Caso contrário, vá para 4.
4. Se $\|\mathbf{a}\| \leq \|\mathbf{a}-\mathbf{b}\|$, então vá para 7. Caso contrário, vá para 5.
5. Se $\|\mathbf{a}\| = \|\mathbf{b}\|$, então pare e retorne $[\mathbf{a}, \mathbf{a}-\mathbf{b}]$. Caso contrário, vá para 6.
6. Faça $[\mathbf{a}, \mathbf{b}] := [\mathbf{b}-\mathbf{a}, -\mathbf{a}]$ e vá para 7.
7. Determine $\mu \in \mathbb{Z}$ tal que $\|\mathbf{b}-\mu\mathbf{a}\|$ é o menor possível, faça $\mathbf{a} := \pm(\mathbf{b}-\mu\mathbf{a})$, $\mathbf{b} := \mathbf{a}$ e retorne para 2.

O problema para determinar μ é contornado ao considerarmos o seguinte

Lema 3 *Sejam* $\|\cdot\|$ *uma norma que é calculada de forma eficiente e* $\mathbf{a}, \mathbf{b}$ *vetores tais que* $\|\mathbf{b}\| > \|\mathbf{b}-\mathbf{a}\|$. *Então, podemos calcular de modo eficiente um inteiro* μ *tal que* $\|\mathbf{b}-\mu\mathbf{a}\|$ *é o menor possível. Além disso,* $1 \leq \mu \leq 2\dfrac{\|\mathbf{b}\|}{\|\mathbf{a}\|}$.

Demonstração: Seja $c = \left\lceil 2\dfrac{\|\mathbf{b}\|}{\|\mathbf{a}\|} \right\rceil$, assim

$$\|\mathbf{b}-c\mathbf{a}\| \geq \|\mathbf{a}\| - \|\mathbf{b}\| \geq 2\frac{\|\mathbf{b}\|}{\|\mathbf{a}\|}\|\mathbf{a}\| - \|\mathbf{b}\| = \|\mathbf{b}\|$$

e, usando o Lema 2, $\|\mathbf{b} - c\mathbf{a}\| \leq \|\mathbf{b} - (c+1)\mathbf{a}\|$. Logo,

$$\|\mathbf{b}\| \leq \|\mathbf{b} - k\mathbf{a} \leq \|\mathbf{b} - (k+1)\mathbf{a}\| \text{ vale } \forall k \in \{c, c+1, \ldots\},$$

mas, por hipótese, é falso para $k = 0 \Rightarrow 1 \leq k \leq c$.

Utilizando busca em binário (*binary search*), podemos determinar $1 \leq \mu \leq c$ tal que $\|\mathbf{b} - k\mathbf{a}\| \leq \|\mathbf{b} - (k+1)\mathbf{a}\|$ é verdade para $k = \mu + 1$ e falso para $k = \mu$, ou seja,

$$\|\mathbf{b} - (\mu - 1)\mathbf{a}\| > \|\mathbf{b} - \mu\mathbf{a}\| \leq \|\mathbf{b} - (\mu + 1)\mathbf{a}\|.$$

Afirmamos que este valor μ minimiza $\|\mathbf{b} - k\mathbf{a}\|$ (dentre todos os valores possíveis de k). De fato, pelo Lema 2, $\forall k \geq \mu + 1$ temos

$$\|\mathbf{b} - \mu\mathbf{a}\| \leq \|\mathbf{b} - (\mu + 1)\mathbf{a}\| \leq \|\mathbf{b} - k\mathbf{a}\|.$$

De modo análogo,

$$\|\mathbf{b} - \mu\mathbf{a}\| < \|\mathbf{b} - (\mu - 1)\mathbf{a}\| \leq \|\mathbf{b} - k\mathbf{a}\|. \quad \blacksquare$$

Lema 4 *Em qualquer execução da redução de Gauss, no início da etapa 7 a base* $[\mathbf{a}, \mathbf{b}]$ *é bem ordenada.*

Demonstração: No início da etapa 7 $[\mathbf{a}, \mathbf{b}]$ é bem ordenada. Devemos provar que ao final dessa etapa, a base de saída $[\mathbf{a}', \mathbf{b}']$ é reduzida (neste caso o algoritmo termina), ou bem ordenada (neste caso voltamos pra etapa 2).

Consideremos $\mathbf{a}' = \pm(\mathbf{b} - \mu\mathbf{a})$ e $\mathbf{b}' = \mathbf{a}$. Assim, $\|\mathbf{a}' - \mathbf{b}'\| \leq \|\mathbf{a}' + \mathbf{b}'\|$ e

$$\|\mathbf{a}' - \mathbf{b}'\| = \| \pm (\mathbf{b} - \mu\mathbf{a}) - \mathbf{a}\| = \|\mathbf{b} - (\mu \pm 1)\mathbf{a}\| \geq \|\mathbf{a}'\| = \|\mathbf{b} - \mu\mathbf{a}\|.$$

Se $\|\mathbf{b}'\| \leq \|\mathbf{a}' - \mathbf{b}'\|$, então encontramos uma base reduzida.

Se $\|\mathbf{b}'\| > \|\mathbf{a}' - \mathbf{b}'\| \geq \|\mathbf{a}'\|$, então encontramos uma base bem ordenada. $\blacksquare$

Teorema 3 *Seja* L *o reticulado gerado pelos vetores LI* $[\mathbf{a}, \mathbf{b}]$*. Ao entrarmos com os vetores* $[\mathbf{a}, \mathbf{b}]$*, o algoritmo da redução de Gauss sempre termina e retorna uma base reduzida para o reticulado* L*.*

Demonstração: O algoritmo executa operações com os vetores $\mathbf{a}$ e $\mathbf{b}$ de tal forma que os vetores resultantes sempre pertencem a L. Além disso, se o algoritmo termina, então a base $[\mathbf{a}, \mathbf{b}]$ é reduzida. Resta provarmos que o algoritmo não entra em um *loop* eterno. Sabemos, do Lema 4, que no início da etapa 7 a base $[\mathbf{a}, \mathbf{b}]$ é bem ordenada. Em particular, $\|\mathbf{b} - \mathbf{a}\| < \|\mathbf{b}\|$ e $\|\mathbf{b} - \mu\mathbf{a}\| < \|\mathbf{b}\| \Rightarrow$ em cada iteração $\|\mathbf{b}\|$ diminui e como existe uma quantidade finita de vetores de L menores que $\|\mathbf{a}\| + \|\mathbf{b}\| \Rightarrow$ o algoritmo terá de parar após um número finito de iterações. $\blacksquare$

4 Resultado Principal

Um *RSA moduli* é um número inteiro $N = pq$, onde p e q são números primos ímpares e diferentes. O termo RSA é oriundo do criptossistema RSA.

Teorema 4 *Sejam $N_1 = p_1q_1$ e $N_2 = p_2q_2$ dois RSA moduli distintos, onde q_i tem α bits. Suponhamos que p_i possuem $t > 2(\alpha + 1)$ bits finais em comum. Então, N_1 e N_2 podem ser fatorados simultaneamente.*

Demonstração: Como p_1, p_2 possuem t bits finais em comum, temos

$$p_1 = 2^t\widetilde{p_1} + p \quad \text{e} \quad p_2 = 2^t\widetilde{p_2} + p.$$

Assim, $N_i = (p + 2^t\widetilde{p_i})q_i \Rightarrow pq_i \equiv N_i(\text{mod } 2^t), i = 1, 2$. Sendo q_i primos ímpares, possuem inversos multiplicativos em $\mathbb{Z}_{2^t}$,

$$\frac{N_1}{q_1} \equiv \frac{N_2}{q_2}(\text{mod } 2^t) \Rightarrow (N_1^{-1}N_2)q_1 - q_2 \equiv 0(\text{mod } 2^t). \tag{3}$$

O conjunto de soluções

$$L = \left\{(x_1, x_2) \in \mathbb{Z}^2; (N_1^{-1}N_2)x_1 - x_2 \equiv 0(\text{mod } 2^t)\right\}$$

forma um grupo aditivo e discreto de $\mathbb{Z}^2$. Assim, L é um reticulado bidimensional. Afirmamos que L possui os vetores $\mathbf{b}_1 = (1, N_1^{-1}N_2)$ e $\mathbf{b}_2 = (0, 2^t)$ como base. De fato, $\mathbf{b}_1, \mathbf{b}_2 \in L$; por outro lado, seja $(x_1, x_2) \in L$, então $x_2 = (N_1^{-1}N_2)x_1 - k2^t$, para algum $k \in \mathbb{Z}$, assim $(x_1, x_2) = x_1\mathbf{b}_1 - k\mathbf{b}_2$.

Pela Equação (3), $\mathbf{q} = (q_1, q_2) \in L$. Mostraremos que $\mathbf{q}$ é o menor vetor de $L \Rightarrow \|\mathbf{q}\| = \lambda_1(L)$.

Utilizando a redução de Gauss em $\mathbf{b}_1, \mathbf{b}_2$, obtemos uma base reduzida $\mathbf{b}'_1, \mathbf{b}'_2$ de L tal que $\|\mathbf{b}'_1\| = \lambda_1(L)$ e $\|\mathbf{b}'_2\| = \lambda_2(L)$. Nosso objetivo é mostrar que $\mathbf{b}'_1 = \pm\mathbf{q} = \pm(q_1, q_2)$, o que é suficiente para fatorar N_1 e N_2 simultaneamente.

Pela desigualdade de Hadamard,

$$\det(L) \leq \|\mathbf{b}'_1\| \cdot \|\mathbf{b}'_2\|$$

e

$$\|\mathbf{b}'_2\| \geq \frac{\det(L)}{\|\mathbf{b}'_1\|} = \frac{\det(L)}{\lambda_1(L)} = \frac{2^t}{\lambda_1(L)}.$$

Por Minkowski,

$$\lambda_1(L) \leq \sqrt{2}\sqrt{\det(L)} = 2^{\frac{t+1}{2}}.$$

Logo,

$$\|\mathbf{b}_2'\| \geq \frac{2^t}{2^{\frac{t+1}{2}}} = 2^{\frac{t-1}{2}}.$$

Assim, $\mathbf{v} = a_1\mathbf{b}_1' + a_2\mathbf{b}_2', a_i \in \mathbb{Z}$ com $\|\mathbf{v}\| < 2^{\frac{t-1}{2}} \Rightarrow a_2 = 0$, pois, caso contrário, $\lambda_2(L) \leq \|\mathbf{v}\| < 2^{\frac{t-1}{2}} \leq \|\mathbf{b}_2'\|$, o que é absurdo.

Desta forma, todo $\mathbf{v}$ com $\|\mathbf{v}\| < 2^{\frac{t-1}{2}}$ é múltiplo de b_1'. Observamos que

$$\|\mathbf{q}\| = \sqrt{q_1^2 + q_2^2} \leq \sqrt{2} \cdot 2^{\alpha} = 2^{\frac{2\alpha+1}{2}}$$

e

$$\|\mathbf{q}\| < b_2 \Leftrightarrow 2^{\frac{2\alpha+1}{2}} < 2^{\frac{t-1}{2}} \Leftrightarrow t > 2(\alpha+1).$$

Logo, $\mathbf{q} = ab_1'$, para algum $a \in \mathbb{Z}$.

Consideremos $b_1' = (b_{11}', b_{12}') \Rightarrow \text{mdc}(q_1, q_2) = \text{mdc}(ab_{11}', ab_{12}') \geq a$, mas q_1 e q_2 são primos e, sem perda de generalidade, $q_1 \neq q_2$; caso $q_1 = q_2$ poderiamos fatorar N_1 e N_2 calculando $\text{mdc}(N_1, N_2)$. Portanto, $|a| = 1 \Rightarrow \mathbf{q} = \pm\mathbf{b}_1'$. ■

4.1 Algoritmo para fatorar implicitamente dois RSA moduli

Apresentamos o algoritmo garantido pelo Teorema 4.

Entrada: dois RSA moduli N_1 e N_2 satisfazendo as hipóteses do Teorema 4.

Saída: q_1 e q_2, onde $N_1 = p_1q_1$ e $N_2 = p_2q_2$.

1. Calcular $N_1^{-1}N_2 \in \mathbb{Z}_{2^t}$.
2. Consideremos L o reticulado gerado por $\mathbf{a} = (1, N_1^{-1}N_2)$ e $\mathbf{b} = (0, 2^t)$.
3. Utilizando redução de Gauss, determinar o menor vetor $\mathbf{q} = (q_1, q_2)$ do reticulado L.

4.2 Exemplo

Sejam $N_1 = p_1q_1 = 372581$ e $N_2 = p_2q_2 = 493571$ dois RSA moduli tais que q_1 e q_2 possuem 4 bits e p_1 e p_2 possuem 12 bits em comum, ou seja, N_1 e N_2 satisfazem as condições do Teorema 4. Sendo assim, estamos aptos para utilizar o algoritmo apresentado na seção anterior. Primeiro, calculemos $N_1^{-1}N_2$ módulo $2^{12} = 4096$,

$$N_1^{-1}N_2 \equiv 1863 (\text{mod } 4096).$$

Consideremos o reticulado L gerado pelos vetores $(1, 1863)$ e $(0, 4096)$. Utilizando redução de Gauss encontramos os vetores $\mathbf{q} = (11, 13)$ e $(-189, 149)$. Portanto, $q_1 = 11$ e $q_2 = 13$, consequentemente, $p_1 = 33871$ e $p_2 = 37967$.

Referências

[1] May & Ritzenhofen, *Implicit Factoring: On Polynomial Time Factoring Given Only an Implicit Hint*, In Stanislaw Jarecki and Gene Tsudik, editores, Public Key Cryptography, volume 5443 of Lecture Notes in Computer Science, p. 1-14. Springer, 2009.

[2] Coelho, *O Algoritmo LLL e Aplicações*. Departamento de Matemática, Faculdade de Ciências e Tecnologia - Universidade de Coimbra - Dissertação de Mestrado, 2007. `http://www.mat.uc.pt/~jsoares/research/mest_Fernando_Coelho.pdf`.

[3] Souza, *Uma Introdução à Teoria dos Reticulados*. Instituto de Matemática e Estatística, IME, UFG, 2009. `http://www.catalao.ufg.br/mat/simmi/simmi2009/arquivos/MC3.pdf`.

[4] Dwork, *Lecture Notes: Lattices and Their Application to Cryptography*, Stanford University, 1998. `http://www.dim.uchile.cl/~mkiwi/topicos/00/dwork-lattice-lectures.ps`

[5] Nguyen & Vallée, editores, *The LLL algorithm Survey and Applications*, Springer, 2010.

[6] Micciancio & Goldwasser, *Complexity of lattice problems: a cryptographic perspective*, Kluwer Academic Publishers, 2002.