



**HAL**  
open science

## CRYPTANALYSE DE RSA

Abderrahmane Nitaj

► **To cite this version:**

Abderrahmane Nitaj. CRYPTANALYSE DE RSA. 3rd cycle. Oujda (Maroc), 2009, pp.56. cel-00420490v2

**HAL Id: cel-00420490**

**<https://cel.hal.science/cel-00420490v2>**

Submitted on 12 Jan 2010

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# CRYPTANALYSE DE RSA

Abderrahmane Nitaj

Laboratoire de Mathématiques Nicolas Oresme  
Université de Caen, France

<http://www.math.unicaen.fr/~nitaj>

[nitaj@math.unicaen.fr](mailto:nitaj@math.unicaen.fr)

© *Version du 28 juin 2009*

# Table des matières

Contenu	i
Préface	1
<b>1 Introduction au cryptosystème RSA</b>	<b>3</b>
1.1 Principe de RSA . . . . .	3
1.1.1 Le module RSA . . . . .	3
1.1.2 Les clés publiques et privées . . . . .	5
1.1.3 Envoi d'un message . . . . .	7
1.1.4 Déchiffrement d'un message . . . . .	8
1.1.5 Signature d'un message . . . . .	9
1.1.6 Preuve de RSA . . . . .	11
1.2 Un exemple d'utilisation de RSA . . . . .	12
1.2.1 Transformation d'un texte en nombres . . . . .	12
1.2.2 L'exemple . . . . .	13
1.3 Cryptanalyses élémentaires de RSA . . . . .	15
1.3.1 Cryptanalyse de RSA connaissant $\varphi(N)$ . . . . .	15
1.3.2 Utilisation du même module et deux exposants différents . . . . .	16
1.3.3 Utilisation de modules différents pour le même message. . . . .	18
1.3.4 Cryptanalyse de RSA si $ p - q  < cN^{1/4}$ : Méthode de Fermat . . . . .	21
<b>2 Cryptanalyse de RSA par les fractions continues</b>	<b>25</b>
2.1 Les fractions continues . . . . .	25

2.1.1	Introduction . . . . .	25
2.1.2	Définitions et propriétés . . . . .	26
2.2	Cryptanalyse de RSA par les fractions continues . . . . .	37
2.2.1	L'attaque de Wiener . . . . .	38
<b>3</b>	<b>Cryptanalyse de RSA par l'algorithme LLL</b>	<b>43</b>
3.1	L'algorithme LLL . . . . .	43
3.1.1	Introduction aux réseaux . . . . .	43
3.1.2	L'algorithme LLL . . . . .	50
3.2	Cryptanalyse de RSA par la réduction des réseaux . . . . .	59
3.2.1	La méthode de Coppersmith : polynômes à une variable . . . . .	59
3.2.2	Factorisation de $N$ . . . . .	69
	<b>Bibliographie</b>	<b>73</b>

# Préface

*Si vous enseignez à un homme, vous n'enseignez qu'à une personne. Si vous enseignez à une femme, vous enseignez à toute une famille.*

إِذَا عَلَّمْتَ رَجُلًا فَقَدْ عَلَّمْتَ فَرْدًا، أَمَّا إِذَا عَلَّمْتَ إِمْرَأَةً فَقَدْ عَلَّمْتَ عَائِلَةً.

La cryptographie moderne est basée sur les mathématiques pour sécuriser l'information. On distingue deux types de protocoles cryptographiques : la cryptographie à clé privée et la cryptographie à clé publique. La cryptographie à clé publique a été introduite par Whitfield Diffie et Martin Hellman en 1976, marquant ainsi la naissance de la cryptographie moderne. Le principe de la cryptographie à clé publique repose sur deux types de clés : une clé publique et une clé privée. Pour chiffrer un message, on utilise la clé publique de son destinataire. Alors, seul le destinataire peut déchiffrer le message reçu avec sa propre clé privée. En 1978, Ronald Rivest, Adi Shamir et Leonard Adleman ont proposé le premier cryptosystème à clé publique, appelé **RSA**. Ce cryptosystème est devenu le plus répandu dans le monde car il est facile à réaliser mais très difficile à casser. En effet, sa sécurité repose sur l'un des problèmes les plus difficiles en mathématiques : la factorisation des grands nombres.

Dans ce travail, nous introduisons les principes généraux du cryptosystème RSA ainsi que certaines attaques permettant de le casser, si les paramètres de sécurité sont mal choisis ou s'il vérifient des relations permettant à un attaquant d'en tirer profit. Dans le chapitre 1, nous donnons les principes généraux du cryptosystème RSA et nous présentons quelques attaques élémentaires permettant de le casser. Dans le chapitre 2, nous présentons une introduction à la théorie des fractions continues et leur utilisation pour attaquer le cryptosystème RSA dans certains cas. Dans le chapitre 3, nous présentons quelques aspects de la réduction des réseaux, plus précisément l'algorithme **LLL** et son utilisation pour attaquer le cryptosystème RSA grâce à la méthode de Coppersmith.

Dans ce travail, la plupart des résultats sont illustrés par des algorithmes programmés à l'aide des systèmes de calcul **Maple 12** et **Magama** dont un calculateur

en ligne est à l'adresse <http://magma.maths.usyd.edu.au/calc/>.

# Chapitre 1

## Introduction au cryptosystème RSA

*Celui qui n'aime pas gravir les montagnes, vivra toute sa vie dans les trous.*

Abou Al Qasim Achabi

وَمَنْ لَا يُحِبُّ صُعُودَ الْجِبَالِ  
أَبُو الْقَاسِمِ الشَّابِّي  
يَعِشُ أَبَدَ الدَّهْرِ بَيْنَ الْحُقُورِ.

### 1.1 Principe de RSA

Toutes les opérations du cryptosystème RSA se passent dans un ensemble de nombres entiers. Soient  $p$  et  $q$  deux nombres premiers assez grands. On note  $N = pq$ . Le nombre  $N$  est appelé *module RSA*. Supposons que deux personnes  $A$  et  $B$  veulent communiquer de façon sûre en utilisant le cryptosystème RSA. Pour cela, ils doivent, chacun de son côté préparer un module RSA, deux clés  $e$  et  $d$ , exécuter une procédure de chiffrement et de signature et une procédure de déchiffrement et de vérification de la signature.

#### 1.1.1 Le module RSA

Avant tout, pour utiliser le cryptosystème RSA, chacun des intervenants  $A$  et  $B$  doit fabriquer son propre module RSA. L'algorithme 1 peut être alors utilisé.

---

**Algorithme 1** : Fabrication du module

---

**Entrée** : Une taille  $t$  pour le module du cryptosystème RSA.

**Sortie** : Un module RSA  $N$  de taille  $t$ .

- 1: Prendre un nombre premier aléatoire  $p$  dans l'intervalle  $\left[2^{\frac{t}{2}}, 2^{\frac{t+1}{2}}\right]$ .
  - 2: Prendre un nombre premier aléatoire  $q$  dans l'intervalle  $\left[2^{\frac{t}{2}}, 2^{\frac{t+1}{2}}\right]$ .
  - 3: **Si**  $p = q$  **alors**
  - 4:   Aller à l'étape 2.
  - 5: **Sinon**
  - 6:    $N = pq$ .
  - 7: **Fin Si**
- 

Comme  $p$  et  $q$  sont dans l'intervalle  $\left[2^{\frac{t}{2}}, 2^{\frac{t+1}{2}}\right]$ , alors on a

$$2^t < pq < 2^{t+1},$$

ce qui montre que  $N = pq$  est de taille  $t$ .

### Maple 1.1.1.

Avec Maple 12, l'algorithme 1 peut être réalisé comme ceci.

Programme	Commentaires
<code>t:=1024:</code>	<----- la taille du module RSA
<code>x1:=round(2.0^(t/2)):</code>	<----- la borne inférieure $2^{(t/2)}$
<code>x2:=round(2.0^((t+1)/2)):</code>	<----- la borne supérieure $2^{((t+1)/2)}$
<code>m1:=(rand(x1 .. x2))():</code>	<----- une valeur aléatoire
<code>p:=nextprime(m1);</code>	<----- le nombre premier $p$
<code>m2:=rand(x1 .. x2)():</code>	<----- une valeur aléatoire
<code>q:=nextprime(m2);</code>	<----- le nombre premier $q$
<code>N:=p*q</code>	<----- le module RSA

### Magma 1.1.2.

Avec Magma, l'algorithme 1 peut être réalisé comme ceci.



Programme	Commentaire
t:=1024;	<----- la taille du module RSA
x1:=Round(2.0^(t/2));	<----- la borne inférieure $2^{(t/2)}$
x2:=Round(2.0^((t+1)/2));	<----- la borne supérieure $2^{((t+1)/2)}$
m1:=Random(x1,x2);	<----- une valeur aléatoire
p:=NextPrime(m1);	<----- le nombre premier p
m2:=Random(x1,x2);	<----- une valeur aléatoire
q:=NextPrime(m2);	<----- le nombre premier q
N:=p*q;	<----- le module RSA
N;	<----- affichage du module RSA

Dans Magma, la fonction **RSAModulus(t,e)** permet de créer un module RSA  $N$  à  $t$ -bits tel que  $\text{pgcd}(e, \phi(N)) = 1$ . Voici un exemple et sa vérification.

Programme	Commentaire
t:=100;	<--- Taille du module
e:=3;	<--- L'exposant public
N:=RSAModulus(t,e);	<--- Création du module
N;	<--- Affichage de N
f:=Factorization(N);	<--- Sa factorisation
f;	<--- Affichage de la factorisation
Log(N)/Log(2);	<--- Taille du module
p:=f[1,1];	<--- Premier nombre premier
q:=f[2,1];	<--- Deuxième nombre premier
p;	<--- Affichage de p
q;	<--- Affichage de p

### 1.1.2 Les clés publiques et privées

Après avoir fabriqué un module RSA, chacun des intervenants doit préparer une clé secrète  $d$  et une clé publique  $e$  :

Dans certains cas, on peut prendre pour la clé publique des valeurs spécifiques, par exemple  $e = 3$  ou  $e = 2^{16} + 1$ . Dans ce cas, les étapes 2 à 5 de l'algorithme 2 ne sont pas exécutées.

La fonction  $\phi$  joue un rôle central dans le cryptosystème RSA et s'appelle la fonction d'Euler.

**Définition 1.1.3.** Soit  $n$  un nombre entier. La fonction indicatrice d'Euler est

$$\phi(n) = \# \{a \mid 0 \leq a \leq n - 1, \text{pgcd}(a, n) = 1\}.$$

---

**Algorithme 2** : Fabrication des clés
 

---

**Entrée** : Deux nombres premiers  $p$  et  $q$ .

**Sortie** : Une clé privée  $d$  et une clé publique  $e$ .

- 1: Calculer  $\phi(N) = (p - 1)(q - 1)$ .
  - 2: Prendre un nombre aléatoire  $e$  dans l'intervalle  $[1, \phi(N)]$ .
  - 3: **Si**  $\text{pgcd}(e, \phi(N)) \neq 1$  **alors**
  - 4: Aller à l'étape 2.
  - 5: **Sinon**
  - 6: Calculer  $d \equiv e^{-1} \pmod{\phi(N)}$ .
  - 7: **Fin Si**
- 

Cette fonction est définie pour tout entier  $n \geq 2$ . Si la décomposition en facteurs premiers est

$$n = \prod_{i=1}^s p_i^{x_i},$$

alors on a :

$$\phi(n) = \prod_{i=1}^s p_i^{x_i-1} (p_i - 1).$$

#### Maple 1.1.4.

Dans Maple 12, la fonction  $\phi$  est tout simplement **phi**. Attention, pour calculer  $\phi(N)$ , Maple est obligé de factoriser  $N$ , ce qui peut être très difficile si  $N$  est du type module de RSA.

Programme	Commentaires
<code>with(numtheory):</code>	<code>&lt;--- Package numtheory "Théorie des Nombres"</code>
<code>N:=5*8*61:</code>	<code>&lt;--- un exemple simple</code>
<code>phi(N);</code>	<code>&lt;--- Calcul de phi(n)</code>

La réponse est immédiate : 960.

#### Magma 1.1.5.

Dans Magma, la fonction  $\phi$  est tout simplement **EulerPhi**. Attention, pour calculer  $\phi(N)$ , Magma aussi est obligé de factoriser  $N$ , ce qui peut être très difficile si  $N$  est du type module de RSA.

Programme	Commentaires
<code>N:=5*8*61:</code>	<code>&lt;--- un exemple simple</code>
<code>EulerPhi(N);</code>	<code>&lt;--- Calcul de phi(N)</code>

#### Maple 1.1.6.

Avec Maple 12, l'algorithme 2 peut être écrit comme ceci où on suppose que la procédure 1.1.1 a été exécutée.

Programme	Commentaires
<code>phi:=(p-1)*(q-1):</code>	<code>&lt;---</code> L'indicateur d'Euler
<code>e:=rand(3..phi/2):</code>	<code>&lt;---</code> On choisit un exposant e aléatoire
<code>while(gcd(e,phi) &lt;&gt; 1) do</code>	<code>&lt;---</code> il faut que pgcd(e,phi)=1
<code>e:=rand(3..phi):</code>	<code>&lt;---</code> On reprend un autre exposant e
<code>od;</code>	
<code>d := modp(1/e, phi);</code>	<code>&lt;---</code> d est l'inverse de d modulo phi

### Magma 1.1.7.

Avec Magma, l'algorithme 2 peut être écrit comme ceci.

Programme	Programme
<code>t:=102;</code>	<code>&lt;--</code> Taille du module
<code>x1:=Round(2.0^(t/2));</code>	<code>&lt;--</code> Valeur aléatoire
<code>x2:=Round(2.0^((t+1)/2));</code>	<code>&lt;--</code> Valeur aléatoire
<code>m1:=Random(x1,x2);</code>	<code>&lt;--</code> Valeur aléatoire
<code>p:=NextPrime(m1);</code>	<code>&lt;--</code> Premier nombre premier
<code>m2:=Random(x1,x2);</code>	<code>&lt;--</code> Valeur aléatoire
<code>q:=NextPrime(m2);</code>	<code>&lt;--</code> deuxième nombre premier
<code>N:=p*q;</code>	<code>&lt;--</code> Module RSA
<code>N;</code>	<code>&lt;--</code> Valeur de N
<code>phi:=(p-1)*(q-1);</code>	<code>&lt;--</code> phi
<code>e:=Random(3,Round(phi/2));</code>	<code>&lt;--</code> Un exposant public aléatoire
<code>while(GCD(e,phi) gt 1) do</code>	<code>&lt;--</code> procédure de recherche
<code>e:=Random(3,Round(phi/2));</code>	<code>&lt;--</code> GCD(e,phi)=1
<code>end while;</code>	<code>&lt;--</code>
<code>d:= InverseMod(e,phi);</code>	<code>&lt;--</code> Inverse de e modulo phi
<code>d;</code>	<code>&lt;--</code> Valeur de l'exposant privé

### 1.1.3 Envoi d'un message

Supposons maintenant que les intervenants A et B possèdent chacun son module RSA et ses clés,  $N_A, e_A, d_A$  pour A et  $N_B, e_B, d_B$  pour B.

Si A veut envoyer un message à B, il peut procéder comme dans l'algorithme 3.

### Maple 1.1.8.

---

**Algorithme 3** : Chiffrement d'un message

---

**Entrée** : Un message clair et la clé publique  $(N_B, e_B)$ .

**Sortie** : Un message chiffré  $C$ .

- 1: Transformer le message en un nombre entier  $M$  de l'intervalle  $[2, N_B]$ .
  - 2: Calculer  $C \equiv M^{e_B} \pmod{N_B}$ .
  - 3: Envoyer le message  $C$ .
- 

Avec Maple 12, l'algorithme 3 peut être programmé de la façon suivante.

Programme	Commentaires
M:=12345:	<--- un exemple simple de message
C:=modp(M^e,N):	<--- e permet de calculer M^e modulo N

**Magma 1.1.9.**

Avec Magma, l'algorithme 3 peut être programmé de la façon suivante.

Programme	Commentaires
M:=12345;	<--- un exemple simple de message
C:=Modexp(M,e,N);	<--- Fonction pour calculer M^e modulo N

### 1.1.4 Déchiffrement d'un message

Supposons enfin que  $B$  a reçu un message chiffré  $C$  de la part de  $A$ . Alors  $B$  peut le déchiffrer en utilisant sa clé secrète  $d_B$  comme dans l'algorithme 4.

---

**Algorithme 4** : Déchiffrement d'un message

---

**Entrée** : Un message chiffré  $C$  et la clé privée  $(N_B, d_B)$ .

**Sortie** : Un message clair  $M$ .

- 1: Calculer  $M \equiv C^{d_B} \pmod{N_B}$ .
  - 2: Transformer le nombre  $M$  en un message clair.
- 

**Maple 1.1.10.**

Avec Maple 12, l'algorithme 4 qui permet de déchiffrer un message  $C$  peut être le suivant.

Programme	Commentaires
M2:=modp(C^d,N):	<--- Calcul de C^d modulo N
M-M2	<--- Permet de vérifier que M2=M

**Magma 1.1.11.**

Avec Magma, l'algorithme 4 qui permet de déchiffrer un message  $C$  peut être le suivant.

Programme	Commentaires
M2:=Modexp(C,d,N);	<--- Calcul de $C^d$ modulo N
M-M2;	<--- Permet de vérifier que M2=M

**1.1.5 Signature d'un message**

Supposons que A veut envoyer un message  $M$  à B. Comment B peut-il être sûr que le message reçu a bien été envoyé par A. Pour résoudre ce problème, RSA peut être utilisé aussi bien pour transmettre un message que pour le signer.

Pour cela, A et B doivent avoir chacun ses clés publiques et privées,  $N_A, e_A, d_A$  pour A et  $N_B, e_B, d_B$  pour B.

Tout d'abord, A utilise la clé publique  $(N_B, e_B)$  de B pour transmettre le message  $C$  et produire une signature  $S$  du message à l'aide de sa propre clé privée  $(N_A, e_A)$ . En effet, A doit produire et transmettre  $C$  et  $S$  comme ceci (voir algorithme 5).

$$C \equiv M^{e_B} \pmod{N_B}, \quad S = C^{d_A} \pmod{N_A}.$$

En possession du message chiffré  $C$  et de la signature  $S$ , B peut alors vérifier si c'est bien A qui a transmit ce message en utilisant la clé publique  $(N_A, e_A)$  de A, du fait de la relation (voir algorithme 6).

$$S^{e_A} \equiv (C^{d_A})^{e_A} \equiv C^{d_A e_A} \equiv C \pmod{N_A}.$$

En effet, seul A peut produire la signature  $S$  et donc B peut aisément vérifier si la signature  $S$  donne une deuxième fois le message chiffré  $C$ .

**Algorithme 5 : Signature d'un message**

**Entrée :** Un message clair  $M$ , deux clés publiques  $(N_B, e_B)$  et  $(N_A, e_A)$  et une clé privée  $(N_A, d_A)$ .

**Sortie :** Un message chiffré  $C$  et sa signature  $S$ .

- 1: A transforme le message en un nombre entier  $M$  de l'intervalle  $[2, N_B]$ .
- 2: A calcule  $C \equiv M^{e_B} \pmod{N_B}$ .
- 3: A calcule  $S \equiv C^{d_A} \pmod{N_A}$ .
- 4: A transmet le message  $C$  et la signature  $S$ .

**Maple 1.1.12.**

Avec Maple 12, l'algorithme 5 qui permet de chiffrer et signer un message  $C$  peut être le suivant.

Programme	Commentaires
NA:=1577801413:	<--- Module RSA de A
eA:=147944791:	<--- Clé publique de A
dA:=295049071:	<--- Clé privée de A
NB:=1303570001:	<--- Module RSA de B
eB:=902841103:	<--- Clé publique de B
dB:=1208086831:	<--- Clé privée de B
M:=12345:	<--- Un exemple simple de message clair
C:=modp(M&^eB,NB):	<--- Le message chiffré
S:=modp(C&^dA,NA):	<--- La signature du message

**Magma 1.1.13.**

Avec Magma, l'algorithme 5 qui permet de chiffrer et signer un message  $C$  peut être le suivant.

Programme	Commentaires
NA:=1577801413;	<--- Module RSA de A
eA:=147944791;	<--- Clé publique de A
dA:=295049071;	<--- Clé privée de A
NB:=1303570001;	<--- Module RSA de B
eB:=902841103;	<--- Clé publique de B
dB:=1208086831;	<--- Clé privée de B
M:=12345;	<--- Un exemple simple de message clair
C:=Modexp(M,eB,NB);	<--- Le message chiffré
S:=Modexp(C,dA,NA);	<--- La signature du message

L'algorithme de la vérification de la signature est alors l'algorithme 6.

---

**Algorithme 6** : Vérification d'une signature

**Entrée** : Un message chiffré  $C$ , une signature  $S$ , la clé publique  $(N_A, e_A)$ .

**Sortie** : Vérification d'une signature.

- 1: B calcule  $C' \equiv S^{e_A} \pmod{N_A}$ .
  - 2: Si  $C' = C$  la signature est authentifiée.
- 

**Maple 1.1.14.**

Avec maple 12, on peut alors vérifier la signature avec un programme simple.

Programme	Commentaires
<pre>C2:=modp(S&amp;^eA,NA): dif:=C2-C: if dif=0 then   print('Signature valide') else   print('Signature non valide') end if</pre>	<pre>&lt;--- calcul de S^eA modulo NA &lt;--- Difference des messages &lt;--- vérification de la signature</pre>

### Magma 1.1.15.

Avec Magma, on peut alors vérifier la signature avec un programme simple.

Programme	Commentaires
<pre>C2:=Modexp(S,eA,NA); dif:=C2-C; if dif eq 0 then   print("Signature valide"); else   print("Signature non valide"); end if</pre>	<pre>&lt;--- Calcul de S^eA modulo NA &lt;--- Difference des messages &lt;--- Vérification de la signature</pre>

## 1.1.6 Preuve de RSA

La justesse du cryptosystème RSA qu'un message chiffré  $C$  à partir d'un message clair  $M$  redonne bien le message original  $M$  est basée sur le théorème suivant, dû à Euler.

**Théorème 1.1.16** (Euler). *Soit  $N$  un nombre entier et  $\phi(N)$  l'indicateur d'Euler. Si  $a$  est un entier premier avec  $N$ , alors*

$$a^{\phi(N)} \equiv 1 \pmod{N}.$$

*Démonstration.* Par définition, on a  $\phi(N) = \#\{a \mid 0 \leq a \leq N-1, \text{pgcd}(a, N) = 1\}$ , ce qui montre qu'on peut écrire

$$\{a \mid 0 \leq a < N, \text{pgcd}(a, N) = 1\} = \{a_1, a_2, \dots, a_{\phi(N)}, a_1 < a_2 < \dots < a_{\phi(N)} < N\}.$$

Soit  $a$  un entier tel que  $\text{pgcd}(a, N) = 1$ . On considère maintenant l'ensemble

$$\{\overline{aa_1}, \overline{aa_2}, \dots, \overline{aa_{\phi(N)}}\},$$

où  $\bar{x}$  désigne la réduction de  $x$  modulo  $N$ . Si  $\overline{aa_i} = \overline{aa_j}$ , alors  $\bar{a}(\bar{a}_i - \bar{a}_j) \equiv 0 \pmod{N}$ , et donc  $a_i = a_j$  puisque  $\text{pgcd}(a, N) = 1$  et  $|a_i - a_j| < N$ . Ainsi, on a

$$\{a_1, a_2, \dots, a_{\phi(N)}\} = \{\overline{aa_1}, \overline{aa_2}, \dots, \overline{aa_{\phi(N)}}\}.$$

En formant les produits des éléments de ces deux ensembles, on obtient :

$$\prod_{i=1}^{\phi(N)} a_i = \prod_{i=1}^{\phi(N)} \overline{aa_i} \equiv a^{\phi(N)} \prod_{i=1}^{\phi(N)} a_i \pmod{N}.$$

De plus, pour chaque  $i$ , on a  $\text{pgcd}(a_i, N) = 1$ . Donc le produit  $\prod_{i=1}^{\phi(N)} a_i$  est inversible modulo  $N$ , ce qui donne

$$a^{\phi(N)} \equiv 1 \pmod{N}.$$

□

## 1.2 Un exemple d'utilisation de RSA

Dans cette section, on donne le détail de l'utilisation du cryptosystème RSA sur un exemple concret. En effet, on montre comment chiffrer, transmettre et déchiffrer le message suivant :

*Cette semaine, je suis à Oujda. Je pars le 22 mai à 13h*

### 1.2.1 Transformation d'un texte en nombres

Il y a plusieurs façon de réaliser une correspondance entre les lettres de l'alphabet et des valeurs numériques. On peut par exemple faire correspondre la valeur 1 à la lettre **a**, la valeur 2 à la lettre **b**,..., et la valeur 26 à la lettre **z** et travailler ainsi en mode 27. Cette correspondance peut ne pas être pratique sur des textes très longs.

Une autre façon, plus efficace est d'utiliser la correspondance ASCII (American Standard Code for Information Interchange). ASCII est la norme d'encodage informatique des caractères alphanumériques de l'alphabet latin. Dans la table ci-dessous, on a représenté quelques correspondances.

Caractère	a	A	b	z	0	1	2	"espace"	à	+
Code	097	065	098	122	048	049	050	32	224	43

**Maple 1.2.1.**



Dans Maple 12, la fonction qui transforme un caractère en valeur numérique est `convert("texte en caractères", bytes)`. Inversement, la fonction qui transforme une liste de valeurs numériques en texte est `convert([v1,v2,...,vn],bytes)`.

Programme	Commentaires
<code>liste:=convert("123 abc...z", bytes)</code>	<code>&lt;--- liste = [49, 50, 51, 32,</code> <code>                  97, 98, 99, 46,</code> <code>                  46, 46, 122]</code>
<code>convert(liste, bytes)</code>	<code>&lt;--- "123 abc...z"</code>

### Magma 1.2.2.

Dans Magma, la fonction qui transforme un caractère en valeur numérique est `BinaryString("texte en caractères")` ou `BString("texte en caractères")`. Inversement, la fonction qui transforme un code ASCII  $n$  en caractère est `CodeToString(n)`. Voici un exemple

Programme	Programme
<code>s:="Je suis à côté" ;</code>	<code>&lt;--- Le texte</code>
<code>s;</code>	<code>&lt;--- Son affichage</code>
<code>t:=BString(s);</code>	<code>&lt;--- Transformation en code ASCII</code>
<code>t;</code>	<code>&lt;--- On obtient [74, 101, ..., 169]</code>
<code>l:=#t;</code>	<code>&lt;--- Longueur de la liste</code>
<code>u:=CodeToString(t[1]);</code>	<code>&lt;--- Transformation en texte</code>
<code>for i:=2 to l do</code>	<code>&lt;--- Formation du texte</code>
<code>  u:=u*CodeToString(t[i]);</code>	
<code>end for;</code>	
<code>u;</code>	<code>&lt;--- Affichage du texte Je suis à côté</code>

## 1.2.2 L'exemple

Dans cette partie, on exécute en détail un exemple de l'utilisation du cryptosystème RSA. On va chiffrer, puis déchiffrer le message suivant

**Cette semaine, je suis à Oujda. Je pars le 22 mai à 13h**

On commence écrire le programme qui sera exécuté par Maple. La fonction `seq` permet de créer une liste de valeurs et la fonction `nops(liste)` donne le nombre de termes dans son argument (liste).

### Maple 1.2.3.

```

Programme

retart:
t := 100:
x1 := round(2.0^((1/2)*t)):
x2 := round(2.0^((t+1)*(1/2))):
m1 := (rand(x1 .. x2))():
p := nextprime(m1):
m2 := (rand(x1 .. x2))():
q := nextprime(m2):
N := p*q:
phi := (p-1)*(q-1):
e := (rand(3 .. phi))():
while gcd(e, phi) <> 1 do e := (rand(3 .. phi))() end do:
d := modp(1/e, phi):
message:="Cette semaine, je suis à Oujda. Je pars le 22 mai à 13h":
listeclaire:= convert(message, bytes):
listecrypte:=[seq(modp(listeclaire[k]&^e,N),k=1..nops(listeclaire))]:
listedecrypte:=[seq(modp(listecrypte[k]&^d,N),k=1..nops(listecrypte))]:
messageoriginale:=convert(listedecrypte, bytes):
listeclaire-listedecrypte;

```

La dernière ligne permet de vérifier que le message de départ et le message décrypté sont identiques. La différence listeclaire-listedecrypte doit donner une liste de zéros.

#### Magma 1.2.4.

```

Programme

t:=100;
x1:=Round(2.0^(t/2));
x2:=Round(2.0^((t+1)/2));
m1:=Random(x1,x2);
p:=NextPrime(m1);
m2:=Random(x1,x2);
q:=NextPrime(m2);
N:=p*q;
phi:=(p-1)*(q-1);
e:=Random(3,Round(phi/2));
while(GCD(e,phi) gt 1) do
e:=Random(3,Round(phi/2));
end while;

```

```

d:= InverseMod(e,phi);
message:="Cette semaine, je suis à Oujda. Je pars le 22 mai à 13h";
listeclaire:= BString(message);
l:=#listeclaire;
listecrypte:= AssociativeArray();
for k:=1 to l do
listecrypte[k]:=Modexp(listeclaire[k],e,N);
end for;
listedecrypte:= AssociativeArray();
for k:=1 to l do
listedecrypte[k]:=Modexp(listecrypte[k],d,N);
end for;
u:=CodeToString(listedecrypte[1]);
for i:=2 to l do
u:=u*CodeToString(listedecrypte[i]);
end for;
u;

```

## 1.3 Cryptanalyses élémentaires de RSA

Dans cette partie, on présente quelques attaques élémentaires sur le cryptosystème RSA, qui consistent à factoriser le module.

### 1.3.1 Cryptanalyse de RSA connaissant $\varphi(N)$

**Proposition 1.3.1.** *Soit  $N$  un module RSA. Si on connaît  $\varphi(N)$ , alors on peut factoriser  $N$ .*

*Démonstration.* Supposons que  $\varphi(N)$  est connu. Ainsi, on dispose d'un système de deux équations en  $p$  et  $q$  :

$$\begin{cases} pq = N, \\ p + q = N + 1 - \varphi(N), \end{cases}$$

qui donnent l'équation en  $p$  :

$$p^2 - (N + 1 - \varphi(N))p + N = 0.$$

On obtient ainsi

$$p = \frac{N + 1 - \varphi(N) + \sqrt{(N + 1 - \varphi(N))^2 - 4N}}{2},$$

$$q = \frac{N + 1 - \varphi(N) - \sqrt{(N + 1 - \varphi(N))^2 - 4N}}{2}.$$

□

### Maple 1.3.2.

Avec Maple 12, cette attaque peut être programmée comme dans l'exemple suivant où on utilise la fonction **solve** qui permet de résoudre une équation.

Programme	Commentaires
<code>p := 67676767676789:</code>	<code>&lt;--- Le premier nombre premier</code>
<code>q := 33838383838463:</code>	<code>&lt;--- Le deuxième nombre premier</code>
<code>N := p*q:</code>	<code>&lt;--- Le module RSA</code>
<code>ph := (p-1)*(q-1):</code>	<code>&lt;--- L'indicateur d'Euler</code>
<code>eq:=x^2-(N+1-ph)*x+N:</code>	<code>&lt;--- L'équation</code>
<code>solve(eq);</code>	<code>&lt;--- Résolution de l'équation</code>
<code>67676767676789, 33838383838463</code>	<code>&lt;--- Les deux solutions</code>

### Magma 1.3.3.

Avec Magma, cette attaque peut être programmée comme dans l'exemple suivant où on utilise la fonction **Roots** qui permet de résoudre une équation.

Programme	Commentaires
<code>P&lt;x&gt; := PolynomialRing(IntegerRing());</code>	
<code>p := 67676767676789;</code>	<code>&lt;--- Le premier nombre premier</code>
<code>q := 33838383838463;</code>	<code>&lt;--- Le deuxième nombre premier</code>
<code>N := p*q;</code>	<code>&lt;--- Le module RSA</code>
<code>ph := (p-1)*(q-1);</code>	<code>&lt;--- L'indicateur d'Euler</code>
<code>A:=x^2-(N+1-ph)*x+N;</code>	<code>&lt;--- L'équation</code>
<code>Roots(A);</code>	<code>&lt;--- Résolution de l'équation</code>
<code>[ &lt;33838383838463, 1&gt;, &lt;67676767676789, 1&gt; ]</code>	<code>&lt;--- Les deux solutions</code>

## 1.3.2 Utilisation du même module et deux exposants différents

**Proposition 1.3.4.** *Soit  $N$  un module RSA. Soient  $e_1$  et  $e_2$  deux exposants premiers entre eux. Si un message clair  $M$  est chiffré avec  $e_1$  et  $e_2$ , alors on peut calculer  $M$ .*

*Démonstration.* Soient  $C_1$  et  $C_2$  deux messages chiffrés par

$$\begin{aligned} C_1 &\equiv M^{e_1} \pmod{N}, \\ C_2 &\equiv M^{e_2} \pmod{N}, \end{aligned}$$

et supposons que  $C_1$  et  $C_2$  sont rendus publiques. Si  $\text{pgcd}(e_1, e_2) = 1$ , alors il existe deux entiers  $x_1$  et  $x_2$  tels que  $x_i < \frac{1}{2}e_i$  et vérifiant  $e_1x_1 - e_2x_2 = \pm 1$ . Ces deux entiers peuvent être déterminés par l'algorithme d'Euclide. D'autre part, ils vérifient

$$\left| \frac{e_1}{e_2} - \frac{x_2}{x_1} \right| = \frac{|e_1x_1 - e_2x_2|}{x_1e_1} = \frac{1}{x_1e_1} < \frac{1}{2x_1^2}.$$

Ainsi  $x_1$  et  $x_2$  peuvent être déterminés comme dénominateur et numérateur de l'une des convergentes de  $\frac{e_1}{e_2}$ . Si  $e_1x_1 - e_2x_2 = 1$ , on obtient alors

$$C_1^{x_1} C_2^{-x_2} \equiv M^{e_1x_1} M^{-e_2x_2} \equiv M^{e_1x_1 - e_2x_2} \equiv M \pmod{N},$$

ce qui donne le message  $M$ . Si  $e_1x_1 - e_2x_2 = -1$ , on calcule  $C_1^{-x_1} C_2^{x_2}$  et on obtient le même résultat.  $\square$

### Maple 1.3.5.

Avec Maple 12, cette attaque peut être programmée comme dans l'exemple suivant.

Programme	Commentaires
N:=2290072441593672048770535307:	<--- Le module RSA
e1:=4543322112211:	<--- Le premier exposant public
e2:=787654321187:	<--- Le deuxième exposant public
igcdex(e1,e2,'x1','x2'):	<--- L'algorithme d'Euclide
x1;x2;	<--- Affichage de x1 et x2
M:=98776655441:	<--- Le message clair
C1:=modp(M&^e1,N):	<--- Le premier message chiffré
C2:=modp(M&^e2,N):	<--- Le deuxième message chiffré
M2:=modp(C1&^x1,N)	<--- Produit des deux messages
*modp(C2&^x2,N) mod N:	
M2-M:	<--- Vérification des messages

### Magma 1.3.6.

Avec Maple 12, cette attaque peut être programmée comme dans l'exemple suivant. La fonction **XGCD(a,b)** retourne trois nombres entiers,  $g, x$  et  $y$  vérifiant  $g = \text{pgcd}(a, b) = ax + by$ .

Programme	Commentaires
N:=2290072441593672048770535307;	<--- Le module RSA
e1:=4543322112211;	<--- Le premier exposant public
e2:=787654321187;	<--- Le deuxième exposant public
g,x1,x2:=XGCD(e1,e2);	<--- L'algorithme d'Euclide
g;x1;x2;	<--- Affichage de g, x1 et x2
M:=98776655441;	<--- Le message clair
C1:=Modexp(M,e1,N);	<--- Le premier message chiffré
C2:=Modexp(M,e2,N);	<--- Le deuxième message chiffré
M2:=Modexp(C1,x1,N)	<--- Produit des deux messages
*Modexp(C2,x2,N) mod N;	
M2-M;	<--- Vérification des messages

### 1.3.3 Utilisation de modules différents pour le même message.

Dans cette attaque, on considère qu'un message  $M$  est envoyé un certain nombre de fois en utilisant plusieurs clés publiques  $(N_i, e_i)$ . Ce scénario peut se produire si le même message doit être diffusé à plusieurs destinataires. Cette attaque, due à Hastad, est basée sur le théorème des restes chinois.

**Théorème 1.3.7.** *Si les entiers  $N_1, N_1, \dots, N_k$  sont deux à deux premiers entre eux, alors le système*

$$\begin{cases} x = a_1 \pmod{N_1}, \\ x = a_1 \pmod{N_1}, \\ \vdots = \quad \quad \quad \vdots \\ x = a_k \pmod{N_k}, \end{cases}$$

admet une solution unique modulo  $N = \prod_{i=1}^k N_i$ . Cette solution est

$$x \equiv \sum_{i=1}^k a_i p_i M_i \pmod{N},$$

avec  $p_i = \frac{N}{N_i}$  et  $M_i \equiv p_i^{-1} \pmod{N_i}$ .

*Démonstration.* Soit  $N = \prod_{i=1}^k N_i$ ,  $p_i = \frac{N}{N_i}$  et  $M_i \equiv p_i^{-1} \pmod{N_i}$ . Alors, pour chaque  $i$ ,  $1 \leq i \leq k$ , on a  $p_i M_i \equiv 1 \pmod{N_i}$  et  $N_i | p_j$  si  $i \neq j$ . Ainsi, avec  $x \equiv \sum_{i=1}^k a_i p_i M_i \pmod{N}$ , on a pour  $1 \leq i \leq k$ , en considérant  $x$  modulo  $N_i$  :

$$x \equiv a_i p_i M_i + \sum_{j \neq i} a_j p_j M_j \equiv a_i + \sum_{j \neq i} a_j M_j N_i \times \frac{p_j}{N_i} \equiv a_i \pmod{N_i}.$$

Ceci montre que  $x$  est solution du système. Si  $x'$  est une autre solution du système avec  $0 \leq x' < N$ , alors pour chaque  $i$ ,  $1 \leq i \leq k$ , on a

$$x' - x \equiv 0 \pmod{N_i}.$$

Puisque les entiers  $N_i$ ,  $1 \leq i \leq k$ , sont premiers entre deux à deux, alors

$$x' - x \equiv 0 \pmod{N}$$

Ainsi, puisque  $|x' - x| < N$ , on a  $x' = x$ , ce qui montre l'unicité de la solution.  $\square$

### Maple 1.3.8.

Dans Maple, le théorème des restes chinois est la fonction

$$\mathbf{chrem}([a_1, a_2, \dots, a_k], [N_1, N_2, \dots, N_k]).$$

Voici un exemple pour résoudre le système

$$\begin{cases} x = 1 \pmod{101}, \\ x = 2 \pmod{103}, \\ x = 3 \pmod{201}. \end{cases}$$

Programme	Commentaires
<code>x:=chrem([1,2,3],[101,103,201]); x;</code>	<code>&lt;--- Le théorème des restes chinois &lt;--- On obtient x=1482378.</code>

### Magma 1.3.9.

Dans Magma, le théorème des restes chinois est la fonction

$$\mathbf{CRT}([a_1, a_2, \dots, a_k], [N_1, N_2, \dots, N_k]).$$

Voici un exemple pour résoudre le système

$$\begin{cases} x = 1 \pmod{101}, \\ x = 2 \pmod{103}, \\ x = 3 \pmod{201}. \end{cases}$$

Programme	Commentaires
<code>x:=CRT([1,2,3],[101,103,201]); x;</code>	<code>&lt;--- Le théorème des restes chinois &lt;--- On obtient x=1482378</code>

**Proposition 1.3.10.** Soient  $k \geq 2$  et  $k$  modules RSA  $N_i$  avec  $1 \leq i \leq k$ . Soient  $C_i$ ,  $1 \leq i \leq k$ , des messages chiffrés du même message clair  $M$  à l'aide du même exposant  $e$ . Si  $m^e < \prod_{i=1}^k N_i$  alors on peut déterminer le message clair  $M$  sans factoriser les modules.

*Démonstration.* Supposons que le même message clair  $M$  est chiffré  $k$  fois par

$$C_i \equiv M^e \pmod{N_i},$$

pour  $i = 1, \dots, k$ . Soit  $N = \prod_{i=1}^k N_i$ . On peut appliquer le Théorème des Restes Chinois pour résoudre le système formé des  $k$  équations

$$x \equiv C_i \pmod{N_i},$$

avec  $x < N$ . Si on suppose que  $M^e < N$ , alors  $x = M^e$  en tant que nombres entiers. Ainsi

$$M = x^{\frac{1}{e}},$$

ce qui donne le message clair  $M$ . □

### Maple 1.3.11.

Pour illustrer cette attaque, on teste un exemple avec  $e = 3$  et  $k = 4$  dans Maple.

Programme	Commentaires
<pre> for i from 1 to 4 do   N[i]:=nextprime(rand()*nextprime(rand())): end do: e:=3: M:=5454321115654321: for i from 1 to 4 do   C[i]:=modp(M&amp;^e,N[i]): end do: x:=chrem([C[1],C[2],C[3],C[4]],           [N[1],N[2],N[3],N[4]]): M2:=round((x^(1/e))): M2-M; </pre>	<pre> &lt;--- 4 module RSA       aléatoires &lt;--- e=3 &lt;--- un message claire &lt;--- 4 messages chiffré &lt;--- Le théorème       des restes chinois &lt;--- racine e-ème de x &lt;--- Comparaison de M2 et M </pre>

### Magma 1.3.12.

Pour illustrer la même attaque avec Magma, on teste le même exemple avec  $e = 3$  et  $k = 4$ . La fonction **Random(b)** retourne un nombre entier aléatoire de l'intervalle  $[0, b]$ .



Programme	Programme
<pre> b:=2^30; N := AssociativeArray(); for i:=1 to 4 do N[i]:=NextPrime(Random(b))   *NextPrime(Random(b)); end for; e:=3; M:=5454321115654321; C := AssociativeArray(); for i:=1 to 4 do   C[i]:=Modexp(M,e,N[i]); end for; x:=CRT([C[1],C[2],C[3],C[4]],   [N[1],N[2],N[3],N[4]]); M2:=Round((x^(1/e))); M2-M; </pre>	<pre> &lt;--- Borne pour les nombres premiers &lt;--- Création du tableau N &lt;--- Création de 4 module RSA  &lt;--- e=3 &lt;--- Le message claire &lt;--- Création d'un tableau C &lt;--- Création des 4 messages chiffrés  &lt;--- Théorème Chinois  &lt;--- Calcule de x^(1/e) &lt;--- Vérification des messages </pre>

### 1.3.4 Cryptanalyse de RSA si $|p - q| < cN^{1/4}$ : Méthode de Fermat

Dans cette partie, on suppose que les nombres premiers  $p$  et  $q$  qui forment le module RSA  $N = pq$  sont très proches, plus précisément  $|p - q| < cN^{1/4}$  où  $c$  est une constante fixe, assez petite.

**Théorème 1.3.13.** *Soit  $N = pq$  un modules RSA où les nombres premiers  $p$  et  $q$  vérifient  $|p - q| < cN^{1/4}$  où  $c$  est une constante assez petite. Alors on peut factoriser  $N$  en temps polynômial dépendant de  $c$ .*

*Démonstration.* La méthode de Fermat consiste en la recherche de deux nombres entiers  $x$  et  $y$  tels que

$$4N = x^2 - y^2 = (x + y)(x - y).$$

Si en plus  $x - y \neq 2$ , alors on obtient la factorisation de  $N$  en posant

$$p = \frac{x + y}{2}, \quad q = \frac{x - y}{2}.$$

Pour déterminer  $x$  et  $y$ , on prend pour  $x$  les valeurs  $x_0 = \lceil 2\sqrt{N} \rceil$ ,  $x_1 = \lceil 2\sqrt{N} \rceil + 1$ ,  $x_2 = \lceil 2\sqrt{N} \rceil + 2, \dots$  et on teste si  $4N - x^2$  est un carré parfait. On désigne alors

par  $k$  le nombre entier pour lequel  $x_k = \lfloor 2\sqrt{N} \rfloor + k$  donne la factorisation de  $N$ . Alors  $x_k = p + q$  et on a, en supposant que  $|p - q| < cN^{1/4}$  :

$$\begin{aligned}
 k &= x_k - \lfloor 2\sqrt{N} \rfloor \\
 &= p + q - \lfloor 2\sqrt{N} \rfloor \\
 &< p + q - 2\sqrt{N} + 1 \\
 &= \frac{(p + q)^2 - 4N}{p + q + 2\sqrt{N}} + 1 \\
 &= \frac{(p - q)^2}{p + q + 2\sqrt{N}} + 1 \\
 &< \frac{c^2\sqrt{N}}{2\sqrt{N}} + 1 \\
 &< \frac{c^2}{2} + 1.
 \end{aligned}$$

Il en résulte que le nombre de tests est assez petits si  $c$  est une constante qui ne dépend pas de  $N$ .  $\square$

### Maple 1.3.14.

On teste maintenant la méthode de Fermat avec Maple 12 sur des modules RSA  $N = pq$  de taille  $t = 100$ , avec  $|p - q| < cN^{1/4}$ . Pour cela, on utilise le programme suivant qui fabrique deux nombres premiers  $p$  et  $q$  avec

$$|p - q| < 10N^{1/4}.$$

Ensuite, on exécute la méthode de Fermat pour retrouver un des nombres premiers de  $N$ .

Programme	Commentaires
Digits := 100:	<--- Précision des calculs
t := 100:	<--- Taille du module
x1 := round(2.0^((1/2)*t)):	<--- Borne inférieur pour p
x2 := round(2.0^((t+1)*(1/2))):	<--- Borne supérieur pour p

<code>m1 := (rand(x1 .. x2))():</code>	<code>&lt;--- Valeur aléatoire</code>
<code>p := nextprime(m1):</code>	<code>&lt;--- Nombre premier suivant</code>
<code>m2 := round(p+10*2^(t/4)):</code>	<code>&lt;--- Borne inférieur pour q</code>
<code>q := nextprime(m2):</code>	
<code>N := p*q:</code>	<code>&lt;--- Module RSA</code>
<code>c := trunc(abs(p-q)/N^0.25)+1:</code>	<code>&lt;--- Rapport</code>
<code>n := round(2*sqrt(N)):</code>	<code>&lt;--- Entier le plus proche</code>
<code>k := 0:</code>	<code>&lt;--- Compteur</code>
<code>while k &lt; (1/2)*c^2+1 do</code>	<code>&lt;--- Boucle de Fermat</code>
<code>x := n+k:</code>	<code>&lt;--- Une valeur pour x</code>
<code>y := round(sqrt(x^2-4*N)):</code>	<code>&lt;--- La valeur de y</code>
<code>s := round((x+y)/2):</code>	<code>&lt;--- Un candidat pour q</code>
<code>if gcd(s, N) &gt; 1 then</code>	<code>&lt;--- pgcd</code>
<code>print('Un facteur est', s):</code>	
<code>break:</code>	
<code>end if:</code>	
<code>k := k+1:</code>	
<code>end do:</code>	

En exécutant ce programme, on a obtenu les résultats suivants.

<code>p=1184367162931181</code>	<code>&lt;--- Un facteur premier</code>
<code>q=1184367498475709</code>	<code>&lt;--- L'autre facteur premier</code>
<code>N=1402725974037575305865967182329</code>	<code>&lt;--- Le module RSA</code>
<code>c=10</code>	<code>&lt;--- c vérifie <math>abs(p-q) &lt; cN^{1/4}</math></code>
<code>k=24</code>	<code>&lt;--- Le nombre d'itérations</code>
<code>Un facteur est 1184367498475709</code>	<code>&lt;--- Sortie de la procédure</code>

### Magma 1.3.15.

On teste aussi la méthode de Fermat avec Magma sur des modules RSA  $N = pq$  de taille  $t = 100$ , avec  $|p - q| < cN^{1/4}$ . Pour cela, on utilise le programme suivant qui fabrique deux nombres premiers  $p$  et  $q$  avec

$$|p - q| < 10N^{1/4}.$$

Ensuite, on exécute la méthode de Fermat pour retrouver un des nombres premiers de  $N$ .

Programme	Programme
t := 100;	<--- Taille du module
x1 := Round(2^((1/2)*t));	<--- Valeur minimale du nombre premier
x2 := Round(2^((t+1)*(1/2)));	<--- Valeur maximale du nombre premier
m1 := Random(x1,x2);	<--- Valeur aléatoire
p := NextPrime(m1);	<--- Premier nombre premier
m2 := Round(p+10*2^(t/4));	<--- Valeur aléatoire
q := NextPrime(m2);	<--- Deuxième nombre premier
N := p*q;	<--- Module RSA
c := Truncate(Abs(p-q)/N^0.25)+1;	<--- Le rapport Abs(p-q)/N^0.25)+1;
n := Round(2*Sqrt(N))+1;	<--- Valeur de départ
k := 0;	<--- Initiation
while k lt (1/2)*c^2+1 do	<--- Boucle de Fermat
x := n+k;	<--- Valeur de x
y := Round(Sqrt(x^2-4*N));	<--- Valeur de y
s := Round((x+y)/2);	<--- Valeur candidate pour p
if GCD(s, N) gt 1 then	
printf("Un facteur est ");s;	
break;	<--- Arrêt de la boucle
end if;	
k := k+1;	
end while;	<--- Fin de la boucle

En exécutant ce programme, on a obtenu les résultats suivants.

p=1320614251431253	<--- Un facteur premier
q=1320614586975679	<--- L'autre facteur premier
N=1744022444208079680278451495787	<--- Le module RSA
c=10	<--- c vérifie abs(p-q)<cN^(1/4)
k=20	<--- Le nombre d'itérations
Un facteur est 1320614586975679	<--- Sortie de la procédure

# Chapitre 2

## Cryptanalyse de RSA par les fractions continues

*Le coléreux ne peut pas atteindre la gloire et le glorieux ne ressent pas la colère.*

Antara Ibno Shaddad Al Absy

لَا يَنَالُ الْعَلَا مَنْ طَبَعَهُ الْعَضْبُ      وَ لَا يَحْمِلُ الْحِقْدَ مَنْ تَعَلَّوْا بِهِ الرُّتْبُ  
عَنْتَرَةَ ابْنِ شَدَّادِ الْعَبْسِيِّ

### 2.1 Les fractions continues

#### 2.1.1 Introduction

On considère le nombre  $x = 3 + \sqrt{10} \approx 6.162277\dots$ , solution de l'équation  $x^2 - 6x - 1$ . On peut alors écrire  $x^2 = 6x + 1$  et donc  $x = 6 + \frac{1}{x}$ . En recommençant le processus, on obtient

$$x = 6 + \frac{1}{6 + \frac{1}{6 + \frac{1}{6 + \frac{1}{\dots}}}}$$

Une telle fraction, qui peut être finie, s'appelle une fraction continue, ici, c'est la fraction continue de  $x = 3 + \sqrt{10}$ . On note plus simplement  $3 + \sqrt{10} = [6, 6, 6, \dots]$ . On peut aussi prendre un nombre fini d'éléments 6. On obtient ainsi

$$[6] = 6, \quad [6, 6] = 6 + \frac{1}{6} = \frac{37}{6} \approx 6,166666\dots,$$

$$[6, 6, 6] = 6 + \frac{1}{6 + \frac{1}{6}} = \frac{228}{37} \approx 6.162162\dots,$$

$$[6, 6, 6, 6] = 6 + \frac{1}{6 + \frac{1}{6 + \frac{1}{6}}} = \frac{1405}{228} \approx 6.162280\dots,$$

Chacune des fractions  $6, \frac{37}{6}, \frac{228}{37}, \frac{1405}{228}, \dots$  s'appelle une *réduite* ou *convergentes*. On observe que ces fractions vérifient

$$|6 - x| > \left| \frac{37}{6} - x \right| > \left| \frac{228}{37} - x \right| > \left| \frac{1405}{228} - x \right|.$$

Ceci est une des nombreuses propriétés des fractions continues.

## 2.1.2 Définitions et propriétés

**Théorème 2.1.1.** *Tout nombre réel positif  $x$  a une écriture unique comme fraction continue :*

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots}}}}$$

où les  $a_i$  sont des entiers positifs. De plus, la fraction continue est finie si et seulement si le nombre  $x$  est rationnel.

*Démonstration.* Soit  $x$  un nombre réel positif. On pose  $x_0 = x$ . On considère la partie entière  $a_0 = [x_0]$ . Si  $x_0$  est un entier,  $a_0 = x_0$  et la fraction continue de  $x$  est  $x = [a_0]$ .

Supposons que  $x$  n'est pas un entier. Dans ce cas, on a  $0 < x_0 - a_0 < 1$  et  $\frac{1}{x_0 - a_0} > 1$ . Puisque  $x_0 = a_0 + (x_0 - a_0)$ , on définit  $x_1$  par

$$x_1 = \frac{1}{x_0 - a_0} > 1,$$

ce qui donne

$$x_0 = a_0 + \frac{1}{x_1}.$$

On recommence le processus pour  $x_1$ . On a  $a_1 = [x_1]$ . Si  $x_1$  est un nombre entier, alors  $a_1 = x_1$ , et la fraction continue de  $x$  est

$$x = a_0 + \frac{1}{a_1} = \frac{a_0 + a_1}{a_1},$$

qui représente un nombre rationnelle. Si  $x_1$ , n'est pas un entier, en recommence le processus en définissant  $x_2$  par

$$x_2 = \frac{1}{x_1 - a_1} > 1,$$

ce qui donne

$$x_0 = a_0 + \frac{1}{a_1 + \frac{1}{x_2}}.$$

Ce processus s'arrête au rang  $n$  si et seulement si  $a_n = [x_n]$ , avec  $a_n \geq 1$ , et dans ce cas, la fraction continue de  $x$  est

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots + \frac{1}{a_n}}}}}} = [a_0, a_1, a_2, a_3, \dots, a_n],$$

qui représente un nombre rationnel. Si  $x$  est un nombre irrationnelle, le processus continue indéfiniment et on obtient pour  $x$  une fraction continue infinie :

$$x = [a_0, a_1, a_2, a_3, \dots].$$

□

**Définition 2.1.2.** Soit  $[a_1, a_2, a_3, \dots]$  une fraction continue d'un nombre  $x$ .

1. Les nombres entiers  $a_i$  s'appellent les quotients partiels.

2. Les nombres rationnels  $[a_1, a_2, a_3, \dots, a_k]$  s'appellent les réduites de  $x$ .

### Maple 2.1.3.

Avec le logiciel Maple, la fonction qui calcule la fraction continue d'un nombre  $x$  est **cfrac(x,n,'quotients')** :  $n$  est le nombre de quotients partiels et 'quotients' pour afficher la fraction continue sous la forme  $[a_0, a_1, a_2, \dots, a_n]$ , ce qui correspond à la notation standard. Voici un exemple pour calculer la fraction continue de  $x = 1 + 7^{\frac{1}{3}}$ .

Programme	Commentaire
restart:	<--- Remise à zéro
with(numtheory):	<--- Fonctionnalités "Théorie des Nombres"
Digits:=100:	<--- Précision
x:=1+7^(1/3):	<--- Un nombre réel
n:=30:	<--- nombre de quotients partiels
s:=cfrac(x,n,'quotients'):	<--- Calcul de la fraction continue
s;	<--- s=[2,1,10,2,16,...]

**Magma 2.1.4.**

Avec le logiciel Magma, la fonction qui calcule la fraction continue de  $x = 1 + 7^{\frac{1}{3}}$  est **ContinuedFraction(x)**. Magma donne alors la forme  $x = [a_1, a_2, \dots]$ , est commence donc avec  $a_1$ .

Programme	Commentaire
x:=1+7^(1/3);	<--- Déclaration de x=1+7^(1/3)
print(x);	<--- Valeur décimal de x
s:=ContinuedFraction(x);	<--- Liste des quotients partiels
s;	<--- Affichage de la liste

Pour un nombre  $x$  dont la fraction continue est  $[a_0, a_1, a_2, \dots]$ , on peut facilement calculer les premières convergentes :

$$[a_0] = a_0 = \frac{p_0}{q_0}.$$

$$[a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}.$$

$$[a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1} = \frac{p_2}{q_2}.$$

On observe facilement que

$$p_2 = a_2(a_0 a_1 + 1) + a_0 = a_2 p_1 + p_0,$$

$$q_2 = a_2 a_1 + 1 = a_2 q_1 + q_0.$$

Ceci est une propriété générale des convergentes d'un nombre réel.

**Théorème 2.1.5.** Soit  $[a_0, a_1, a_2, \dots]$  la fraction continue de  $x$ . Pour tout  $n \geq 0$ , on définit les nombres  $p_n$  et  $q_n$  par,

$$p_n = a_n p_{n-1} + p_{n-2},$$

$$q_n = a_n q_{n-1} + q_{n-2},$$



avec la convention

$$p_{-2} = 0, \quad q_{-2} = 1, \quad p_{-1} = 1, \quad q_{-1} = 0.$$

Alors tout  $n \geq 0$ , on a  $\frac{p_n}{q_n} = [a_0, a_1, a_2, \dots, a_n]$ .

*Démonstration.* La preuve se fait par récurrence sur  $n$ . On a déjà vu que  $[a_0] = \frac{p_0}{q_0}$ . Supposons que

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n q_{n-1} + q_{n-2}, \end{aligned}$$

et que  $[a_1, a_2, a_3, \dots, a_n] = \frac{p_n}{q_n}$ . Alors, on a aussi, en utilisant la récurrence.

$$\begin{aligned} [a_1, a_2, a_3, \dots, a_n, a_{n+1}] &= [a_1, a_2, a_3, \dots, a_n + \frac{1}{a_{n+1}}] \\ &= \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}} \\ &= \frac{(a_n a_{n+1} + 1) p_{n-1} + a_{n+1} p_{n-2}}{(a_n a_{n+1} + 1) q_{n-1} + a_{n+1} q_{n-2}} \\ &= \frac{a_{n+1} (a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1} (a_n q_{n-1} + q_{n-2}) + q_{n-1}} \\ &= \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_n + q_{n-1}} \\ &= \frac{p_{n+1}}{q_{n+1}}, \end{aligned}$$

et la récurrence est démontrée. Ceci termine la preuve.  $\square$

### Maple 2.1.6.

Avec Maple, la fonction qui détermine les convergentes est **nthconver** : la  $n + 1$ -ème convergente d'une liste  $s$  de convergente est **nthconver(s,n)**. Le numérateur et le dénominateur sont alors **nthnumer(s,n)** et **nthdenom(s,n)**. Voici un exemple dans lequel on cherche la convergente  $\frac{p_7}{q_7}$  de  $x = 1 + 7^{\frac{1}{3}}$ .

Programme	Commentaires
restart:	<--- Remise à zéro
with(numtheory):	<--- Fonctionnalités "Théorie des Nombres"
Digits:=100:	<--- Précision
x:=1+7^(1/3):	<--- Un nombre réel
s:=cfraction(x,100,'quotients'):	<--- s=[2,1,10,2,...]
n:=7:	<--- On considère la 8-ème convergentes
nthconver(s,n);	<--- La convergente d'indice 7
nthnumer(s,n);	<--- Son numérateur est 15791
nthdenom(s,n);	<--- Son dénominateur 5421

### Magma 2.1.7.

Avec Magma, pour calculer la convergente  $\frac{p_n}{q_n}$ , il faut utiliser la fonction **Convergents(s)** où  $s = [a_1, a_2, \dots, a_n]$ . La réponse est alors une matrice de la forme

$$\begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}.$$

Programme	Commentaires
x:=1+7^(1/3);	<--- La valeur x=1+7^(1/3)
c:=ContinuedFraction(x);	<--- La liste des quotients partiels
c;	<--- Affichage de la liste
s:=[];	<--- Initialisation
n:=7;	<--- Convergente p7/q7
for i in [1..n] do s:=Append(s,c[i]);end for;	<--- Formation de [a1,...,a7]
s;	<--- Affichage de [a1,...,a7]
t:=Convergents(s);	<--- Matrice ([p7,p6],[q7,q6])
t[1,1];	<--- p7
t[2,1];	<--- q7

La réponse est  $p_7 = 3379$  et  $q_7 = 1160$ .

Dans magma, on peut aussi écrire un programme afin de déterminer la liste des numérateurs et dénominateurs des convergentes.

Programme	Commentaires
<code>x:=1+7^(1/3);</code>	<--- La valeur x
<code>x;</code>	<--- Sa valeur décimale
<code>s:=ContinuedFraction(x);</code>	<--- Liste des quotients partiels
<code>s;</code>	<--- Affichage de la liste
<code>p0:=0;q0:=1;p1:=1;q1:=0;</code>	<--- Initialisations
<code>N:=[];D:=[];</code>	<--- Initialisations
<code>l:=15;</code>	<--- Longueur de la liste
<code>for i in [1..l] do</code>	<--- Boucle
<code>  p2:=s[i]*p1+p0;</code>	<--- Calcul de p2
<code>  q2:=s[i]*q1+q0;</code>	<--- Calcul de q2
<code>  N:=Append(N,p2);</code>	<--- Formation de la liste N
<code>  D:=Append(D,q2);</code>	<--- Formation de la liste D
<code>  p0:=p1;q0:=q1;</code>	<--- Echange
<code>  p1:=p2;q1:=q2;</code>	<--- Echange
<code>end for;</code>	<--- Fin de la boucle
<code>N;</code>	<--- Affichage de N
<code>D;</code>	<--- Affichage de D
<code>n:=7;</code>	<--- 7ème convergente
<code>N[n];</code>	<--- Numérateur
<code>D[n];</code>	<--- Dénominateur

La septième convergente est alors  $p_7 = 3379$  et  $q_7 = 1160$ .

**Théorème 2.1.8.** Soit  $[a_0, a_1, a_2, \dots]$  la fraction continue d'un nombre  $x$ . Alors les convergentes  $\frac{p_n}{q_n}$  de  $x$  vérifient pour tout  $n \geq -2$

$$\begin{aligned} p_n q_{n+1} - q_n p_{n+1} &= (-1)^{n+1}, \\ p_n q_{n+2} - q_n p_{n+2} &= (-1)^{n+1} a_{n+2}. \end{aligned}$$

*Démonstration.* Les preuves se font aisément par récurrence. Considérons la première égalité. Pour  $n = -2$ , on a bien

$$p_{-2} q_{-1} - q_{-2} p_{-1} = -1 = (-1)^{-2+1}.$$

Supposons donc que  $p_{n-1} q_n - q_{n-1} p_n = (-1)^n$ . On a, en utilisant le théorème 2.1.5,

$$\begin{aligned} p_n q_{n+1} - q_n p_{n+1} &= p_n (a_{n+1} q_n + q_{n-1}) - q_n (a_{n+1} p_n + p_{n-1}) \\ &= p_n q_{n-1} - q_n p_{n-1} \\ &= -(-1)^n \\ &= (-1)^{n+1}, \end{aligned}$$

ce qui démontre la récurrence.

La deuxième égalité s'obtient directement en combinant l'égalité  $p_n q_{n+1} - q_n p_{n+1} = (-1)^{n+1}$  et le théorème 2.1.5.

$$\begin{aligned} p_n q_{n+2} - q_n p_{n+2} &= p_n (a_{n+2} q_{n+1} + q_n) - q_n (a_{n+2} p_{n+1} + p_n) \\ &= a_{n+2} (p_n q_{n+1} - q_n p_{n+1}) \\ &= a_{n+2} (-1)^{n+1}. \end{aligned}$$

Ceci prouve donc la deuxième égalité. □

### Maple 2.1.9.

Vérifions ce théorème avec les convergentes de  $x = 1 + 7^{\frac{1}{3}}$ .

Programme	Commentaires
restart:	
with(numtheory):	
Digits:=100:	
x:=1+7^(1/3):	
s:=cfrac(x,100,'quotients');	<--- liste des quotients partiels
nu:=i->nthnumer(s,i):	<--- Numérateurs des convergentes
de:=i->nthdenom(s,i):	<--- Dénominateurs des convergentes
n:=7;	<--- Un indice quelconque
r:=nu(n)*de(n+1)-nu(n+1)*de(n):	<--- Première égalité
(-1)^(n+1)-r;	<--- Différence (nulle)
n:=10;	<--- Un indice quelconque
r:=nu(n)*de(n+2)-nu(n+2)*de(n):	<--- Deuxième égalité
(-1)^(n+1)*s[n+3]-r;	<--- Différence (nulle)

### Magma 2.1.10.

On vérifie maintenant le théorème 2.1.8 avec les convergentes de  $x = 1 + 7^{\frac{1}{3}}$  pour  $n = 7$  avec magma. Attention au décalage de l'exposant de  $-1$  puisque Magma commence les quotients partiels par  $a_1$  et non par  $a_0$ .

Programme	Programme
<code>x:=1+7^(1/3);</code>	<code>&lt;--- Valeur de x</code>
<code>c:=ContinuedFraction(x);</code>	<code>&lt;--- Liste des quotients partiels</code>
<code>s:=[];</code>	<code>&lt;--- Initiation</code>
<code>t:=[];</code>	<code>&lt;--- Initiation</code>
<code>l:=20;</code>	<code>&lt;--- Nombre de convergentes</code>
<code>for i in [1..l] do</code>	<code>&lt;--- Boucle</code>
<code>s:=Append(s,c[i]);</code>	<code>&lt;--- Liste s</code>
<code>t:=Append(t,Convergents(s));</code>	<code>&lt;--- Liste des convergentes</code>
<code>end for;</code>	
<code>n:=7;</code>	<code>&lt;--- n=7</code>
<code>p1:=t[n][1,1];p2:=t[n+1][1,1];</code>	<code>&lt;--- p7 et p8</code>
<code>q1:=t[n][2,1];q2:=t[n+1][2,1];</code>	<code>&lt;--- q7 et q8</code>
<code>p1*q2-p2*q1-(-1)^(n);</code>	<code>&lt;--- Vérification, réponse nulle</code>
<code>n:=7;</code>	
<code>p1:=t[n][1,1];p3:=t[n+2][1,1];</code>	<code>&lt;--- p7 et p9</code>
<code>q1:=t[n][2,1];q3:=t[n+2][2,1];</code>	<code>&lt;--- q7 et q9</code>
<code>p1*q3-p3*q1-(-1)^(n+2)*c[n+2];</code>	<code>&lt;--- Vérification, réponse nulle</code>

**Corollaire 2.1.11.** Les convergentes  $\frac{p_n}{q_n}$  d'un nombre réel  $x$  vérifient  $\text{pgcd}(p_n, q_n) = 1$  pour tout  $n \geq 0$ .

*Démonstration.* Supposons que  $\frac{p_{n+1}}{q_{n+1}}$  existe. Alors, d'après Théorème 2.1.8, on a  $p_n q_{n+1} - q_n p_{n+1} = (-1)^{n+1}$  et donc  $\text{pgcd}(p_n, q_n) = 1$ .  $\square$

**Théorème 2.1.12.** La suite des convergentes d'indices pairs  $\frac{p_{2n}}{q_{2n}}$  et d'indices impairs  $\frac{p_{2n+1}}{q_{2n+1}}$  d'un nombre irrationnel positif  $x$  vérifient :

$$\frac{p_{2n-2}}{q_{2n-2}} < \frac{p_{2n}}{q_{2n}} < x < \frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}}.$$

*Démonstration.* Démontrons d'abord que pour tout  $n \geq 0$ , on a  $\frac{p_{2n}}{q_{2n}} < \frac{p_{2n+1}}{q_{2n+1}}$ . En effet, en utilisant le théorème 2.1.8

$$\frac{p_{2n}}{q_{2n}} - \frac{p_{2n+1}}{q_{2n+1}} = \frac{p_{2n}q_{2n+1} - q_{2n}p_{2n+1}}{q_{2n}q_{2n+1}} = \frac{(-1)^{2n+1}}{q_{2n}q_{2n+1}} < 0.$$

Démontrons maintenant que pour tout  $n \geq 0$ , on a  $\frac{p_{2n-2}}{q_{2n-2}} < \frac{p_{2n}}{q_{2n}}$ . On a, en utilisant le théorème 2.1.8 :

$$\frac{p_{2n-2}}{q_{2n-2}} - \frac{p_{2n}}{q_{2n}} = \frac{p_{2n-2}q_{2n} - p_{2n}q_{2n-2}}{q_{2n-2}q_{2n}} = \frac{(-1)^{2n-1}a_{2n}}{q_{2n-2}q_{2n}} < 0.$$

On a de même

$$\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n-1}}{q_{2n-1}} = \frac{p_{2n+1}q_{2n-1} - p_{2n-1}q_{2n+1}}{q_{2n+1}q_{2n-1}} = \frac{-(-1)^{2n}a_{2n+1}}{q_{2n+1}q_{2n-1}} < 0,$$

ce qui donne  $\frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}}$ .

Il reste à démontrer que les deux inégalités  $\frac{p_{2n}}{q_{2n}} < x$  et  $x < \frac{p_{2n+1}}{q_{2n+1}}$ . En écrivant  $x = [a_0, a_1, a_2, \dots, a_n, x_{n+1}]$  avec  $x_{n+1} = [a_{n+1}, \dots]$ , on obtient, en utilisant Théorème 2.1.8, pour tout  $n \geq 0$  :

$$x - \frac{p_n}{q_n} = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - p_nq_{n-1}}{q_n(x_{n+1}q_n + q_{n-1})} = \frac{(-1)^n}{q_n(x_{n+1}q_n + q_{n-1})}.$$

Ainsi, on obtient  $x - \frac{p_{2n}}{q_{2n}} > 0$  et  $x - \frac{p_{2n+1}}{q_{2n+1}} < 0$ .  $\square$

Le corollaire suivant est une conséquence de Théorème 2.1.12

**Corollaire 2.1.13.** *Si  $[a_0, a_1, a_2, \dots]$  est la fraction continue d'un nombre  $x$ , alors les convergentes  $\frac{p_n}{q_n}$  de  $x$  vérifient :*

1. Pour tout  $n \geq 0$ ,  $(q_n x - p_n)(q_{n+1} x - p_{n+1}) < 0$ .
2. Pour tout  $n \geq 0$ ,  $|q_{n+1} x - p_{n+1}| < |q_n x - p_n|$ .

*Démonstration.* En écrivant  $x = [a_1, a_2, a_3, \dots, a_n, x_{n+1}] = [a_0, a_1, a_2, \dots, a_{n+1}, x_{n+2}]$  avec  $x_{n+1} = [a_{n+1}, \dots]$  et  $x_{n+2} = [a_{n+2}, \dots]$ , on obtient, comme dans la preuve du théorème 2.1.12, pour  $n \geq 0$ ,

$$q_n x - p_n = \frac{(-1)^n}{x_{n+1}q_n + q_{n-1}}, \quad q_{n+1} x - p_{n+1} = \frac{(-1)^{n+1}}{x_{n+2}q_{n+1} + q_n}.$$

ceci montre que  $q_n x - p_n$  et  $q_{n+1} x - p_{n+1}$  sont de signes contraires et donc la propriété 2.

En écrivant  $x_{n+1} = a_{n+1} + \frac{1}{x_{n+2}}$  avec  $x_{n+2} > 1$ , on a

$$a_{n+1} < x_{n+1} < a_{n+1} + 1.$$

Ainsi

$$x_{n+1}q_n + q_{n-1} < (a_{n+1} + 1)q_n + q_{n-1} = q_{n+1} + q_n < x_{n+2}q_{n+1} + q_n.$$

Donc

$$\frac{1}{x_{n+1}q_n + q_{n-1}} > \frac{1}{x_{n+2}q_{n+1} + q_n},$$

et par conséquent

$$|q_n x - p_n| > |q_{n+1} x - p_{n+1}|,$$

ce qui montre la propriété 2.  $\square$

**Proposition 2.1.14.** Si  $x = [a_1, a_2, a_3, \dots]$ , alors les convergentes  $\frac{p_n}{q_n}$  de  $x$  vérifient pour tout  $n \geq 0$ ,

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

*Démonstration.* Puisque  $x = [a_0, a_1, a_2, \dots, a_n, x_{n+1}]$  avec  $x_{n+1} = [a_{n+1}, \dots]$ , alors  $x_{n+1} > a_{n+1}$ . Comme dans la preuve de Théorème 2.1.12, pour  $n \geq 0$ , on obtient

$$\left| x - \frac{p_n}{q_n} \right| = \frac{1}{q_n(x_{n+1}q_n + q_{n-1})} < \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} = \frac{1}{q_n q_{n+1}},$$

ce qui termine la preuve. □

On obtient alors la propriété suivante pour un nombre irrationnel.

**Proposition 2.1.15.** Si  $[a_0, a_1, a_3, \dots]$  est la fraction continue d'un nombre irrationnel  $x$ , alors il existe une infinité de nombres rationnels  $\frac{p}{q}$  tels que

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}.$$

*Démonstration.* Puisque  $q_n < q_{n+1}$ , alors, en utilisant la proposition 2.1.14, on obtient pour toutes les convergentes  $\frac{p_n}{q_n}$  de  $x$  on a

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

Donc, comme il y a une infinité de convergentes si  $x$  est irrationnel, il y a une infinité de nombres rationnels  $\frac{p}{q}$  qui vérifient

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}.$$

□

Nous avons aussi un théorème concernant les *meilleures* approximations.

**Théorème 2.1.16** (Meilleures approximations). Si  $[a_1, a_2, a_3, \dots]$  est la fraction continue d'un nombre irrationnel  $x$ . Soit  $\frac{p_n}{q_n}$  une convergente de  $x$  avec  $n \geq 0$  et  $\frac{p}{q}$  un nombre rationnel.

1. Si  $q < q_{n+1}$ , alors  $|q_n x - p_n| \leq |q x - p|$ .
2. Si  $q \leq q_n$ , alors  $\left| x - \frac{p_n}{q_n} \right| \leq \left| x - \frac{p}{q} \right|$ .

*Démonstration.* On suppose que  $0 < q < q_{n+1}$ . Montrons que  $|q_n x - p_n| \leq |qx - p|$ . Soit  $a$  et  $b$  deux entiers tels que

$$\begin{aligned} p &= ap_n + bp_{n+1}, \\ q &= aq_n + bq_{n+1}. \end{aligned}$$

L'existence de  $a$  et  $b$  est garantie par le théorème 2.1.8. En effet, on a  $p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$  et donc

$$a = (-1)^{n+1}(pq_{n+1} - qp_{n+1}), \quad b = (-1)^{n+1}(qp_n - pq_n).$$

On peut discuter les valeurs de  $p$  et  $q$  suivant les valeurs de  $a$  et  $b$ .

- Si  $a = 0$ , alors  $q = bq_{n+1}$ , donc  $b \geq 1$ , ce qui contredit  $0 < q < q_{n+1}$ .

- Si  $b = 0$ , alors  $p = ap_n$  et  $q = aq_n$ , ce qui donne  $\left|x - \frac{p_n}{q_n}\right| = \left|x - \frac{p}{q}\right|$ .

- Supposons donc que  $ab \neq 0$ . Puisque  $q < q_{n+1}$ , alors  $aq_n + bq_{n+1} < q_{n+1}$  et donc  $aq_n < (1-b)q_{n+1}$ , ce qui montre que  $b \geq 1$  et  $a < 0$  ou  $b \leq -1$  et dans ce cas, on doit avoir  $q = aq_n + bq_{n+1} > 0$ , donc  $a > 0$ . Dans les deux cas,  $ab < 0$ . On a alors

$$qx - p = (aq_n + bq_{n+1})x - (ap_n + bp_{n+1}) = a(q_n x - p_n) + b(q_{n+1} x - p_{n+1}),$$

où les termes  $a(q_n x - p_n)$  et  $b(q_{n+1} x - p_{n+1})$  sont de même signe. Alors

$$|qx - p| = |a(q_n x - p_n)| + |b(q_{n+1} x - p_{n+1})| \geq |q_n x - p_n|.$$

Ceci termine la preuve de 1.

De plus, si on a  $q \leq q_n$ , alors

$$\left|x - \frac{p}{q}\right| = \frac{|qx - p|}{q} \geq \frac{|q_n x - p_n|}{q_n} = \left|x - \frac{p_n}{q_n}\right|,$$

et termine la preuve de 2. □

On a déjà vu dans la proposition 2.1.15 que pour  $n \geq 0$ , les convergentes d'un nombre réel  $x$  vérifient

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}.$$

En fait, le résultat suivant est encore plus précis.

**Proposition 2.1.17.** *Si  $[a_0, a_1, a_2, \dots]$  est la fraction continue d'un nombre  $x$ , alors pour  $n \geq 0$ , on a*

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \quad \text{ou} \quad \left|x - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{2q_{n+1}^2}.$$



*Démonstration.* On sait par le corollaire 2.1.13 que  $x - \frac{p_n}{q_n}$  et  $x - \frac{p_{n+1}}{q_{n+1}}$  sont de signes contraires. Alors

$$\left| \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} \right| = \left| x - \frac{p_n}{q_n} \right| + \left| x - \frac{p_{n+1}}{q_{n+1}} \right|$$

Or, en utilisant le théorème 2.1.8 et l'inégalité  $2q_n q_{n+1} < q_n^2 + q_{n+1}^2$ , on obtient :

$$\left| \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} \right| = \frac{1}{q_n q_{n+1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}.$$

Ainsi

$$\left| x - \frac{p_n}{q_n} \right| + \left| x - \frac{p_{n+1}}{q_{n+1}} \right| < \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}.$$

Ceci montre alors que  $\left| x - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2}$  ou  $\left| x - \frac{p_{n+1}}{q_{n+1}} \right| < \frac{1}{2q_{n+1}^2}$ .  $\square$

On termine avec le théorème suivant, très utile pour reconnaître les convergentes d'un nombre réel.

**Proposition 2.1.18.** *Si  $x$  est un nombre réel. Si  $\frac{p}{q}$  est un nombre rationnel qui vérifie*

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2},$$

*alors  $\frac{p}{q}$  est une convergente de  $x$ .*

*Démonstration.* Soit  $\frac{p}{q}$  est un nombre rationnel. Puisque la suite des dénominateurs ( $q_n$ ) des convergentes  $\frac{p_n}{q_n}$  de  $x$  est strictement croissantes, alors  $q_n \leq q < q_{n+1}$  pour un entier  $n \geq 0$ . On a alors, en utilisant le théorème 2.1.16 et l'hypothèse  $\left| x - \frac{p}{q} \right| < \frac{1}{2q^2}$ ,

$$\left| \frac{p}{q} - \frac{p_n}{q_n} \right| \leq \left| \frac{p}{q} - x \right| + \left| x - \frac{p_n}{q_n} \right| \leq 2 \left| x - \frac{p}{q} \right| < \frac{1}{q^2}$$

Il en résulte que

$$|pq_n - p_nq| < \frac{q_n}{q} \leq 1.$$

Ainsi,  $pq_n - p_nq = 0$  et donc  $\frac{p}{q} = \frac{p_n}{q_n}$ .  $\square$

## 2.2 Cryptanalyse de RSA par les fractions continues

Dans cette partie, nous considérons deux attaques basées sur l'utilisation des fractions continues. La première est due à Wiener (1990).

### 2.2.1 L'attaque de Wiener

**Théorème 2.2.1.** Soit  $N = pq$  un module RSA où les nombres premiers  $p$  et  $q$  sont de même taille ( $q < p < 2q$ ). Soit  $e < \phi(N)$  un exposant public pour lequel la clé secrète  $d$  est assez petite :  $d < \frac{1}{3}N^{\frac{1}{4}}$ . Connaissant  $N$  et  $e$ , on peut calculer  $d$  et factoriser  $N$ .

*Démonstration.* Supposons que  $q < p < 2q$ . Puisque  $N = pq > q^2$ , alors  $q < \sqrt{N}$ . D'autre part, on a

$$N - \varphi(N) = p + q - 1 < 2q + q - 1 < 3q < 3\sqrt{N}.$$

Si  $e$  est une clé publique et  $d$  la clé privée, alors  $d \equiv e^{-1} \pmod{\phi(N)}$ , où  $\phi(N)$  est l'indicateur d'Euler. Donc il existe un entier  $k$  tel que  $ed - k\phi(N) = 1$ . Puisque  $e < \phi(N)$ , on peut donc écrire

$$k = \frac{ed - 1}{\phi(N)} < \frac{ed}{\phi(N)} < d.$$

Alors

$$\begin{aligned} \left| \frac{e}{N} - \frac{k}{d} \right| &= \frac{|ed - kN|}{Nd} \\ &= \frac{|ed - k\varphi(N) - kN + k\varphi(N)|}{Nd} \\ &= \frac{|1 - k(N - \varphi(N))|}{Nd} \\ &< \frac{k(N - \varphi(N))}{Nd} \\ &< \frac{3k\sqrt{N}}{Nd} \\ &= \frac{3k}{d\sqrt{N}}. \end{aligned}$$

Puisque  $k < d < \frac{1}{3}N^{\frac{1}{4}}$ , alors

$$\frac{3k}{d\sqrt{N}} < \frac{N^{\frac{1}{4}}}{d\sqrt{N}} = \frac{1}{dN^{\frac{1}{4}}} < \frac{1}{2d^2}.$$

Ainsi, en appliquant le théorème 2.1.5,  $\frac{k}{d}$  est une convergente de  $\frac{e}{N}$ . Connaissant  $d$  et  $k$ , on peut alors calculer  $\phi(N)$  par la relation

$$\phi(N) = \frac{ed - 1}{k}.$$

Ainsi, par la proposition 1.3.1 on peut calculer  $p$  et  $q$  et donc trouver la factorisation de  $N$ .  $\square$

L'attaque de Wiener peut donc être résumée dans l'algorithme suivant.

---

**Algorithme 7** : L'attaque de Wiener
 

---

**Entrée** : Un module RSA  $N$  et un exposant publique  $e$  pour lequel la clé secrète vérifie  $d < \frac{1}{3}N^{\frac{1}{4}}$ .

**Sortie** : La factorisation de  $N$  et la clé secrète  $d$ .

- 1: Déterminer la liste des réduites de  $\frac{e}{N}$ .
  - 2: Pour chaque réduite  $xy$  telle que  $y < \frac{1}{3}N^{\frac{1}{4}}$  :
  - 3: Calculer  $\psi = \frac{ey-1}{x}$ ,  $\delta = (N + 1 - \psi)^2 - 4N$ , et  $p_2 = \left\lfloor \frac{(N+1-\psi+\sqrt{\delta})}{2} \right\rfloor$ .
  - 4: **Si**  $\text{pgcd}(p_2, N) > 1$  **alors**
  - 5:   Afficher  $d = y$ ,  $p = p_2$  et  $q = \frac{N}{p_2}$ .
  - 6: **Fin Si**
- 

**Maple 2.2.2.**

Programme	Commentaire
<code>n:=100:Digits:=100:with(numtheory)</code>	<code>&lt;-- Initiations</code>
<code>x:=rand(2^(n/2-1)..2^(n/2))():</code>	<code>&lt;-- Une Valeur aléatoires</code>
<code>p:=nextprime(x):</code>	<code>&lt;-- Le nombre premier p</code>
<code>y:=rand(round(x/2)..x)():</code>	<code>&lt;-- Condition q&lt;p&lt;2q</code>
<code>q:= nextprime(y):</code>	<code>&lt;-- Le nombre premier q</code>
<code>evalf(p/q):</code>	<code>&lt;-- La condition 1&lt;p/q&lt;2</code>
<code>N:=p*q:</code>	<code>&lt;-- Le module RSA</code>
<code>ph:=(p-1)*(q-1):</code>	<code>&lt;-- L'indicateur d'Euler</code>
<code>sn:=trunc(1/3*(N^(1/4))):</code>	<code>&lt;-- La borne de Wiener</code>
<code>d:=rand(sn)():</code>	<code>&lt;-- Une clé privée aléatoire</code>
<code>while gcd(d,ph)&gt;1 do</code>	<code>&lt;-- d est premier avec ph</code>
<code>d:=rand(sn)() end do:</code>	
<code>e:=1/d mod ph:</code>	<code>&lt;-- La clé publique</code>
<code>convert(e/N,confrac,'pq' ):</code>	<code>&lt;-- pq est la liste des réduites</code>
<code>g:=1:i:=2:</code>	<code>&lt;-- Initiation</code>
<code>while g=1 do</code>	<code>&lt;-- Boucle</code>
<code>y:=denom(pq[i]):</code>	<code>&lt;-- Dénominateur de la réduite</code>
<code>x:=numer(pq[i]):</code>	<code>&lt;-- Numérateur de la réduite</code>
<code>psi:=(e*y-1)/x:</code>	<code>&lt;-- la valeur psi</code>
<code>delta:=(N+1-psi)^2-4*N:</code>	
<code>p2:=((N+1-psi)+sqrt(delta))/2:</code>	<code>&lt;-- Solution de l'équation</code>
<code>p2:=round(p2):</code>	
<code>g:=gcd(p2,N):</code>	<code>&lt;-- calcul de pgcd(p2,N)</code>

<pre> i:=i+1: od: print('d='):y; print('p='):p; print('q='):N/p2; </pre>	<pre> &lt;-- Affichage de d &lt;-- Affichage de p &lt;-- Affichage de q </pre>
--	--

**Magma 2.2.3.**

On vérifie maintenant l'attaque de Wiener avec un module RSA de  $n = 80$  bits.

Programme	Commentaire
<code>n:=80;</code>	<code>&lt;-- Longueur du module RSA</code>
<code>a:=Round(2^(n/2-1));</code>	<code>&lt;-- Borne inférieure</code>
<code>b:=Round(2^(n/2));</code>	<code>&lt;-- Borne supérieure</code>
<code>x:=Random(a,b);</code>	<code>&lt;-- Valeur aléatoire</code>
<code>p:=NextPrime(x);</code>	<code>&lt;-- Nombre premier</code>
<code>a:=Round(x/2);</code>	<code>&lt;-- Borne inférieure</code>
<code>b:=Round(x);</code>	<code>&lt;-- Borne supérieure</code>
<code>y:=Random(a,b);</code>	<code>&lt;-- Valeur aléatoire</code>
<code>q:=NextPrime(y);</code>	<code>&lt;-- Nombre premier</code>
<code>N:=p*q;</code>	<code>&lt;-- Module RSA</code>
<code>ph:=(p-1)*(q-1);</code>	<code>&lt;-- Fonction d'Euler</code>
<code>sn:=Truncate(1/3*(N^(1/4)));</code>	<code>&lt;-- Borne de Wiener</code>
<code>d:=Random(sn);</code>	<code>&lt;-- valeur aléatoire</code>
<code>while (GCD(d,ph) gt 1) do</code>	<code>&lt;-- d,phi(N) premiers entre eux</code>
<code>d:=Random(sn); end while;</code>	
<code>e:=Modinv(d,ph);</code>	<code>&lt;-- Inverse de d</code>
<code>c:=ContinuedFraction(e/N);</code>	<code>&lt;-- Liste des quotients partiels</code>
<code>s:=[];</code>	<code>&lt;-- Initialisation</code>
<code>t:=[];</code>	<code>&lt;-- Initialisation</code>
<code>l:=#c;</code>	<code>&lt;-- Longueur de c</code>
<code>for i in [1..l] do</code>	<code>&lt;-- Fabrication des listes</code>
<code>s:=Append(s,c[i]);</code>	<code>&lt;-- quotients partiels</code>
<code>t:=Append(t,Convergents(s));</code>	<code>&lt;-- convergentes</code>
<code>end for;</code>	
<code>i:=3;</code>	<code>&lt;-- Initialisation</code>
<code>g:=1;</code>	<code>&lt;-- Initialisation</code>
<code>while (g eq 1) do</code>	<code>&lt;-- Boucle de Wiener</code>
<code>kk:=t[i][1,2];</code>	<code>&lt;-- Valeur de k</code>
<code>dd:=t[i][2,2];</code>	<code>&lt;-- Valeur de d</code>
<code>phn:=(e*dd-1)/kk;</code>	<code>&lt;-- Valeur phn=(e*dd-1)/kk</code>

<pre>delta:=(N+1-phn)^2-4*N;   x:=(N+1-phn)+Sqrt(delta))/2; p2:=Round(x); g:=GCD(p2,N); i:=i+1; end while;</pre>	<pre>&lt;-- delta=(N+1-phn)^2-4*N &lt;-- Candidat pour p &lt;-- Candidat pour p &lt;-- PGCD &lt;-- Fin while &lt;-- Affichage de p2 &lt;-- Différence nulle</pre>
--	---



# Chapitre 3

## Cryptanalyse de RSA par l'algorithme LLL

*Les objectifs ne sont pas atteints par les souhaits, mais par le travail assidu.*

Abu Alaa Al Maary

وَمَا نَيْلُ الْمَطَالِبِ إِلَّا بِالتَّمَنِّي  
وَلَا كَيْنُ تُؤْخَذُ الدُّنْيَا غَلَابًا  
أَبُو الْعَلَاءِ الْمُتَعَرِّي

### 3.1 L'algorithme LLL

#### 3.1.1 Introduction aux réseaux

L'algorithme LLL a été inventé en 1982 et porte les initiales des ses inventeurs, A.K. Lenstra, H.W. Lenstra et L. Lovász. A l'origine, son but était de factoriser des polynômes à coefficients entiers. Depuis son invention, l'algorithme LLL a été utilisé dans de nombreux domaines, en particulier dans la résolution des équations diophantiennes et la cryptanalyse, y compris celle de certaines instances de RSA. Le domaine de l'algorithme LLL est la réduction de bases dans des sous ensembles de  $\mathbb{R}^n$ , appelés réseaux.

**Définition 3.1.1.** Soit  $n$  et  $d$  deux entiers positifs. Soit  $L$  une partie non vide de  $\mathbb{R}^n$ . On dit que  $L$  est un réseau s'il existe une famille libre  $(b_1, \dots, b_d)$  de  $\mathbb{R}^n$  telle que

$$L = \sum_{i=1}^d \mathbb{Z}b_i = \left\{ \sum_{i=1}^d x_i b_i \mid x_i \in \mathbb{Z} \right\}.$$

L'entier  $d$  est la dimension du réseau, et  $(b_1 \cdots, b_d)$  est une base de ce réseau.

Dans la plupart des applications, on a  $d = n$  et donc la matrice de la base  $(b_1 \cdots, b_d)$  est une matrice carrée. On peut en particulier calculer son déterminant, qui ne dépend pas de la base choisie.

**Définition 3.1.2.** Soit  $L$  un réseau de dimension  $n$  et  $(b_1 \cdots, b_n)$  une base de  $L$ . Le déterminant de  $L$  est

$$\det(L) = |\det(b_1 \cdots, b_n)|.$$

**Proposition 3.1.3.** Soit  $L$  un réseau de dimension  $n$ . Le déterminant de  $L$  est indépendant de la base.

*Démonstration.* Supposons que  $\det(L) = |\det(b_1 \cdots, b_n)|$ , où  $B = (b_1 \cdots, b_n)$  est une base de  $L$ . Soit  $B' = (b'_1 \cdots, b'_n)$  une autre base de  $L$ . Alors, il existe une matrice carrée  $U$ , de type  $n \times n$  à éléments dans  $\mathbb{Z}$  telle que

$$\det(U) = \pm 1, \quad B' = UB.$$

Alors

$$|\det(b'_1 \cdots, b'_n)| = |\det(U) \det(b_1 \cdots, b_n)| = |\det(b_1 \cdots, b_n)| = \det(L),$$

ce qui termine la preuve. □

Le plus souvent, la base d'un réseau n'a pas de bonnes propriétés et les calculs peuvent être compliqués. Un moyen pour rendre les calculs plus efficaces est de chercher une base orthogonale dans un réseau. Pour cela, on considère le produit scalaire habituelle de deux vecteurs et la norme euclidienne d'un vecteur.

**Définition 3.1.4.** Soient  $x = (x_1 \cdots, x_n)$  et  $y = (y_1 \cdots, y_n)$  deux vecteurs de  $\mathbb{R}^n$ .

1. Le produit scalaire de  $x$  et  $y$  est

$$\langle x, y \rangle = x^T y = \sum_{i=1}^n x_i y_i.$$

2. La norme de  $x$  est

$$\|x\| = (\langle x, x \rangle)^{\frac{1}{2}} = \left( \sum_{i=1}^n x_i y_i \right)^{\frac{1}{2}}.$$

Une des méthodes les plus utilisées pour produire une base orthogonale à partir d'une base quelconque est la méthode de Gram-Schmidt.



**Théorème 3.1.5** (Gram-Schmidt). *Soit  $V$  un sous-espace vectoriel de dimension  $n$  et  $(b_1 \cdots, b_n)$  une base de  $V$ . On considère la famille de vecteurs  $(b_1^* \cdots, b_n^*)$  définie par*

$$b_1^* = b_1, \quad b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*,$$

avec pour  $j < i$

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}.$$

Alors  $(b_1^* \cdots, b_n^*)$  est une base orthogonale de l'espace de  $V$ .

*Démonstration.* On va commencer par démontrer que  $(b_1^* \cdots, b_n^*)$  est une base de  $V$ . En écrivant

$$b_1 = b_1^*, \quad b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^*,$$

on en conclut que, sous forme matricielle, on a

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_{n-1} \\ b_n \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ \mu_{2,1} & 1 & 0 & 0 & \cdots & 0 \\ \mu_{3,1} & \mu_{3,2} & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mu_{n-1,1} & \mu_{n-1,2} & \mu_{n-1,3} & \cdots & 1 & 0 \\ \mu_{n,1} & \mu_{n,2} & \mu_{n,3} & \cdots & \mu_{n,n-1} & 1 \end{bmatrix} \begin{bmatrix} b_1^* \\ b_2^* \\ b_3^* \\ \vdots \\ b_n^* \end{bmatrix} = U \begin{bmatrix} b_1^* \\ b_2^* \\ b_3^* \\ \vdots \\ b_{n-1}^* \\ b_n^* \end{bmatrix}.$$

La matrice  $U$  est une matrice inférieure, dont la diagonale est formée de 1. Son déterminant est donc 1. Ainsi  $(b_1^* \cdots, b_n^*)$  est aussi une base de  $V$ .

On démontre maintenant que  $(b_1^* \cdots, b_n^*)$  est orthogonale. Par récurrence, puisque  $b_1^* = b_1$  et  $b_2^* = b_2 - \mu_{2,1} b_1$ , alors

$$\langle b_1^*, b_2^* \rangle = \langle b_1, b_2 - \mu_{2,1} b_1 \rangle = \langle b_1, b_2 \rangle - \mu_{2,1} \langle b_1, b_1 \rangle = \langle b_1, b_2 \rangle - \frac{\langle b_2, b_1 \rangle}{\langle b_1, b_1 \rangle} \langle b_1, b_1 \rangle = 0.$$

Supposons maintenant que la famille  $(b_1^* \cdots, b_{i-1}^*)$  est orthogonale avec  $i \geq 3$ . Alors

on a pour  $1 \leq k \leq i - 1$

$$\begin{aligned}
 \langle b_k^*, b_i^* \rangle &= \left\langle b_k^*, b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \right\rangle \\
 &= \langle b_k^*, b_i \rangle - \sum_{j=1}^{i-1} \mu_{i,j} \langle b_k^*, b_j^* \rangle \\
 &= \langle b_k^*, b_i \rangle - \mu_{i,k} \langle b_k^*, b_k^* \rangle \\
 &= \langle b_k^*, b_i \rangle - \frac{\langle b_i, b_k^* \rangle}{\langle b_k^*, b_k^* \rangle} \langle b_k^*, b_k^* \rangle \\
 &= 0.
 \end{aligned}$$

Ainsi  $(b_1^* \cdots, b_i^*)$  est orthogonale, ce qui prouve la récurrence et termine la preuve.  $\square$

La méthode de Gram-Schmidt peut être facilement mise en algorithme 8.

---

**Algorithme 8** : La méthode de Gram-Schmidt

---

**Entrée** : Une base  $(b_1 \cdots, b_n)$ .

**Sortie** : Une base orthogonale  $(b_1^* \cdots, b_n^*)$ .

- 1: Poser  $b_1^* = b_1$ .
  - 2: **Pour**  $i = 1, 2, \dots, n$ , **faire**
  - 3:   **Pour**  $j = 1, 2, \dots, i - 1$ , **faire**
  - 4:     Calculer  $\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$ .
  - 5:   **Fin Pour**
  - 6:   Calculer  $b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$ .
  - 7: **Fin Pour**
- 

On va maintenant programmer directement l'algorithme 8.

**Maple 3.1.6.**

Programme
<pre>scal:= proc (u, v) add(u[i]*v[i], i = 1 .. nops(u)); end proc:</pre>

Programme	Commentaires
<pre> gramschmidt:=proc (M) local i, j, n, B, P, u,k: with(LinearAlgebra): n := nops(M): B := []: P := []: for i from 1 to n do u := [seq(0, k = 1 .. n)]: for j from 1 to i-1 do u[j]:=scal(M[i],B[j])/scal(B[j],B[j]): end do: u[i] := 1: P := [op(P), u]: B:=[op(B), [seq(M[i][k]-add(u[j]*B[j][k], j = 1 .. i-1), k = 1 .. n)]]: end do: return(B, P): end proc: </pre>	<pre> &lt;-- Procédure &lt;-- Paramètres locaux &lt;-- Librairie LinearAlgebra &lt;-- Nombre de lignes de M &lt;-- Initiation des listes &lt;-- i=1,...,n &lt;-- Initiation de u for j from 1 to i-1 do &lt;-- Calcul de u[j] &lt;-- u[i]= 1 &lt;-- concaténation &lt;-- Calcul de B &lt;-- Sortie </pre>

Le programme suivant prend en entrée la base  $(b_1, b_2, b_3)$  dont la matrice est

$$b_1 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 1 \\ 4 \\ -2 \end{bmatrix}, \quad b_3 = \begin{bmatrix} 0 \\ -2 \\ -1 \end{bmatrix}.$$

Programme	Commentaires
<pre> M:=[[2,1,0],[1,4,-2],[0,-2,-1]]; gramschmidt(M); A:=transpose(matrix(gramschmidt(M)[1])); P := transpose(matrix(gramschmidt(M)[2])); Q:=multiply(P, A); </pre>	<pre> &lt;-- Entrée matrice M &lt;-- procédure gramshmidt &lt;-- Matrice A &lt;-- Matrice P &lt;-- Produit PA </pre>

On obtient alors les matrices :

$$A = \begin{bmatrix} 2 & -\frac{7}{5} & \frac{10}{23} \\ 1 & \frac{14}{5} & -\frac{20}{23} \\ 0 & -2 & -\frac{35}{23} \end{bmatrix}, \quad P = \begin{bmatrix} 1 & \frac{6}{5} & -\frac{2}{5} \\ 0 & 1 & -\frac{6}{23} \\ 0 & 0 & 1 \end{bmatrix}, \quad Q = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 4 & -2 \\ 0 & -2 & -1 \end{bmatrix}.$$

### Maple 3.1.7.

En fait, dans Maple, la méthode de Gram-Schmidt est programmée sous le nom de fonction **GramSchmidt** dans le package **LinearAlgebra**. Voici un exemple simple de son utilisation. On considère la base  $(b_1, b_2, b_3)$  avec

$$b_1 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 1 \\ 4 \\ -2 \end{bmatrix}, \quad b_3 = \begin{bmatrix} 0 \\ -2 \\ -1 \end{bmatrix}.$$

Programme	Commentaires
<code>with(LinearAlgebra):</code>	<code>&lt;--- package LinearAlgebra</code>
<code>b1:=Vector([2, 1, 0]):</code>	<code>&lt;--- Premier vecteur</code>
<code>b2 := Vector([1, 4, -2]):</code>	<code>&lt;--- Deuxième vecteur</code>
<code>b3 := Vector([0, -2, -1]):</code>	<code>&lt;--- Troisième vecteur</code>
<code>B := GramSchmidt([b1, b2, b3]);</code>	<code>&lt;--- La procédure de Gram-Schmidt</code>
<code>DotProduct(B[1], B[2]);</code>	<code>&lt;--- Vérification du produit scalaire</code>
<code>DotProduct(B[1], B[3]);</code>	<code>&lt;--- Vérification du produit scalaire</code>
<code>DotProduct(B[2], B[3]);</code>	<code>&lt;--- Vérification du produit scalaire</code>

On obtient alors la base orthogonale  $(b_1^*, b_2^*, b_3^*)$  avec

$$b_1^* = b_1 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \quad b_2^* = \begin{bmatrix} -\frac{7}{5} \\ \frac{14}{5} \\ -2 \end{bmatrix}, \quad b_3^* = \begin{bmatrix} \frac{10}{23} \\ -\frac{20}{23} \\ -\frac{35}{23} \end{bmatrix}.$$

### Magma 3.1.8.

Dans Magma, la méthode d'orthogonalisation de Gram-Schmidt est programmée sous le **Orthogonalize(M)** où  $M$  est une matrice carrée. Elle retourne trois valeurs  $N$ ,  $P$  et  $n$  où  $N$  est une matrice dont les colonnes représentent des vecteurs orthogonaux,  $P$  est une matrice de passage vérifiant  $N = PM$  et  $n$  est le rang de  $M$ . Voici un exemple simple de son utilisation. On considère la même base  $(b_1, b_2, b_3)$  avec

$$b_1 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 1 \\ 4 \\ -2 \end{bmatrix}, \quad b_3 = \begin{bmatrix} 0 \\ -2 \\ -1 \end{bmatrix}.$$

Programme	Programme
<code>Q:= RealField();</code>	<code>&lt;--- Ensemble des réels</code>
<code>R:=MatrixRing(Q,3);</code>	<code>&lt;--- Ensemble des matrices définie sur Q de type 3x3.</code>
<code>F:=elt&lt;R [2, 1, 0, 1, 4, -2, 0, -2, -1]&gt;;</code>	<code>&lt;--- F est la matrice</code>
<code>Orthogonalize(F) ;</code>	<code>&lt;--- L'orthogonalisation de Gram-Shmidt</code>

On obtient alors la base orthogonale  $(b_1^*, b_2^*, b_3^*)$  avec

$$b_1^* = b_1 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \quad b_2^* = \begin{bmatrix} -\frac{7}{5} \\ \frac{14}{5} \\ -2 \end{bmatrix}, \quad b_3^* = \begin{bmatrix} \frac{10}{23} \\ -\frac{20}{23} \\ -\frac{35}{23} \end{bmatrix}.$$

Le résultat suivant montre qu'on peut calculer le déterminant d'un réseau si on connaît une base orthogonale.

**Corollaire 3.1.9** (Hadamard). *Soit  $L$  un réseau de dimension  $n$ ,  $(b_1 \cdots, b_n)$  une base de  $L$  et  $(b_1^* \cdots, b_n^*)$  la famille orthogonale au sens de Gram-Schmidt. Alors*

$$\det(L) = \prod_{i=1}^n \|b_i^*\| \leq \prod_{i=1}^n \|b_i\|.$$

*Démonstration.* On a  $b_1 = b_1^*$ , donc  $\|b_1\| = \|b_1^*\|$ . Pour  $2 \leq i \leq n$ , on a

$$b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^*,$$

et comme  $\langle b_r^*, b_s^* \rangle = 0$  si  $r \neq s$ , alors

$$\|b_i\|^2 = \|b_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \|b_j^*\|^2,$$

et donc

$$\det(L)^2 = \prod_{i=1}^n \|b_i^*\|^2 \leq \prod_{i=1}^n \|b_i\|^2,$$

ce qui termine la preuve. □

Un problème très important en théorie des nombres et en cryptanalyse est la recherche d'un vecteur court dans un réseau. Deux sous-problèmes se posent alors.

**Problème du vecteur le plus court (The Shortest Vector Problem (SVP)) :**

Etant donné un réseau  $L$ . Déterminer un vecteur non nul  $v$  qui minimise la norme  $\|v\|$ .

**Problème du vecteur le plus proche (The Closest Vector Problem (CVP)) :**

Etant donné un réseau  $L$  et un vecteur  $v_0$ . Déterminer un vecteur  $v \neq v_0$  qui minimise la norme  $\|v - v_0\|$ . Une réponse théorique dans le sens de ces deux problèmes est la suivante.

**Théorème 3.1.10** (Hermitte). *Soit  $L$  un réseau de dimension  $n$ . Alors il existe un vecteur  $v$  non nul de  $L$  tel que*

$$\|v\| \leq \sqrt{n} \det(L)^{\frac{1}{n}}.$$

Ce théorème est très théorique et la détermination d'un vecteur court est difficile en général. Un moyen pratique pour trouver des vecteurs assez courts est d'utiliser l'algorithme LLL.

### 3.1.2 L'algorithme LLL

L'algorithme LLL est lié à la méthode d'orthogonalisation de Gram-Schmidt. Il concerne des bases spéciales, appelées *bases réduites*.

**Définition 3.1.11.** *Une base  $(b_1 \cdots, b_n)$  est LLL-réduite si, la base  $(b_1^* \cdots, b_n^*)$  produite par la méthode d'orthogonalisation de Gram-Schmidt vérifie*

$$(3.1) \quad |\mu_{i,j}| \leq \frac{1}{2}, \quad \text{pour } 1 \leq j < i \leq n,$$

$$(3.2) \quad \frac{3}{4} \|b_{i-1}^*\|^2 \leq \|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2, \quad \text{pour } 1 < i \leq n.$$

La deuxième condition est appelée *condition de Lovász*. Si  $\mu_{i,j} = 0$  pour tout  $i$  et  $j$ , alors la base est orthogonale, et donc minimale d'après l'inégalité de Hadamard 3.1.9. Si  $|\mu_{i,j}| \leq \frac{1}{2}$ , la base est *presque orthogonale*, donc *presque minimale*. L'algorithme LLL original est le suivant

#### Maple 3.1.12.

On va maintenant programmer l'algorithme LLL. Tout d'abord, il faut programmer la procédure produit scalaire **scal(u,v)** et la procédure **gramschmidt(M)**. On programme ensuite la procédure **redfaible(M)**.

---

**Algorithme 9** : Algorithme LLL

---

**Entrée** : Une base  $(b_1, \dots, b_n)$ **Sortie** : Une base LLL réduite  $(b_1, \dots, b_n)$ 

- 1: **Pour**  $i = 1, \dots, n$  **faire**
  - 2:    $b_i^* = b_i$
  - 3:   **Pour**  $j = 1, \dots, i - 1$  **faire**
  - 4:      $\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{B_j}$
  - 5:      $b_i^* = b_i^* - \mu_{i,j} b_j^*$
  - 6:   **Fin Pour**
  - 7:    $B_i = \langle b_i^*, b_i^* \rangle$
  - 8: **Fin Pour**
  - 9:  $k = 2$
  - 10: Appliquer **redfaible**( $k, k - 1$ )
  - 11: **Si**  $\frac{3}{4} B_{k-1} > B_k + \mu_{k,k-1}^2 B_{k-1}$  **alors**
  - 12:   Appliquer **lovasz**( $k$ )
  - 13: **Fin Si**
  - 14: Aller à l'étape 10
  - 15: **Pour**  $l = k - 2, \dots, 1$  **faire**
  - 16:   Appliquer **redfaible**( $k, l$ )
  - 17: **Fin Pour**
  - 18: **Si**  $k = n$  **alors**
  - 19:   Stop
  - 20: **Sinon**
  - 21:    $k = k + 1$
  - 22:   Aller à l'étape 10
  - 23: **Fin Si**
- 

---

**Algorithme 10** : Procédure **redfaible**

---

**Entrée** : Un couple  $(k, l)$ **Sortie** : Un vecteur  $b_k$  et des valeurs  $\mu_{k,j}$  avec  $j = 1, \dots, l - 1$  avec  $|\mu_{k,l}| \leq \frac{1}{2}$ 

- 1: **Si**  $|\mu_{k,l}| > \frac{1}{2}$  **alors**
- 2:    $b_k = b_k - \lfloor \mu_{k,l} \rfloor b_l$
- 3:    $\mu_{k,l} = \mu_{k,l} - \lfloor \mu_{k,l} \rfloor$
- 4:   **Pour**  $j = 1, \dots, l - 1$  **faire**
- 5:      $\mu_{k,j} = \mu_{k,j} - \lfloor \mu_{k,l} \rfloor \mu_{l,j}$
- 6:   **Fin Pour**
- 7: **Fin Si**

**Remarque** :  $\lfloor x \rfloor$  est l'arrondi de  $x$ , c'est à dire l'entier le plus proche de  $x$ .

---

**Algorithme 11** : Procédure **lovasz****Entrée** : Un entier  $k$ **Sortie** : La condition de Lovasz  $\frac{3}{4}B_{k-1} \leq B_k + \mu_{k,k-1}^2 B_{k-1}$  est satisfaite

- 1:  $B = B_k + \mu_{k,k-1}^2 B_{k-1}$
- 2:  $\mu_{k,k-1} = \frac{\mu_{k,k-1} B_{k-1}}{B}$
- 3:  $B_k = \frac{B_{k-1} B_k}{B}$
- 4:  $B_{k-1} = B$
- 5: Echanger  $b_k$  et  $b_{k-1}$
- 6: **Pour**  $j = 1, \dots, k - 2$  **faire**
- 7:   Echanger  $\mu_{k-1,j}$  et  $\mu_{k,j}$
- 8: **Fin Pour**
- 9: **Pour**  $i = k + 1, \dots, n$  **faire**
- 10:    $\mu_{i,k-1} = \mu_{k,k-1} \mu_{i,k-1} + (1 - \mu_{k,k-1} \mu_{k,k-1}) \mu_{i,k}$
- 11:    $\mu_{i,k} = \mu_{i,k-1} - \mu_{k,k-1} \mu_{i,k}$
- 12: **Fin Pour**
- 13: **Si**  $k > 2$  **alors**
- 14:    $k = k - 1$
- 15: **Fin Si**

Procédure redfaible	Commentaires
redfaible:=proc(M)	<-- Procédure redfaible
local i,j,k,U,N;	<-- paramètres locaux
N:=M;	<-- Initialisation
U:=gramschmidt(M)[2];	<-- Matrice de passage U
for i from 2 to nops(M) do	<-- i=2,...
for j from i-1 by -1 to 1 do	<-- j=i-1,...,1
N[i] := N[i]-round(U[i][j])*N[j];	<-- Nouveau N
for k from 1 to j do	<-- k=1,...,j
U[i][k]:=U[i][k]-round(U[i][j])*U[j][k]	<-- Nouveau U
end do	<--
end do	<--
end do:	<--
return N:	<-- renvoi de N
end proc:	<-- Fin de la procédure

On programme maintenant la procédure **lovasz(M)**.



```

Procédure lovasz

lovasz:=proc(M)
local i,n,G;
n:=nops(M);
G:=gramschmidt(M);
for i to n-1 do
  if evalb(scal(G[1][i+1],G[1][i+1])
    <(3/4-G[2][i+1][i]^2)*scal(G[1][i],G[1][i]))
  then return [false, i]
  end if:
end do:
return [true, 0]:
end proc

```

Finalement, on donne la programmation de LLL sous la forme de procédure **myLLL**(M).

```

Procédure myLLL

myLLL:=proc(M)
local N,B,x;
N:=redfaible(M):
B:=lovasz(N):
while not(B[1]) do
  x := N[B[2]]:
  N:=redfaible(subsop(B[2] = N[B[2]+1], B[2]+1 = x, N)):
  B:=lovasz(N):
end do:
return N:
end proc:

```

Avec la matrice

$$M = \begin{bmatrix} b_1 & b_2 & b_3 & b_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 7 & 9 & 4 \\ 6 & -7 & 2 & 3 \\ -1 & 2 & -1 & -1 \\ 2 & -1 & 0 & -3 \end{bmatrix},$$

on obtient en exécutant  $myLLL(M)$  la matrice suivante.

$$N = \begin{bmatrix} b_1 & b_2 & b_3 & b_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ -1 & 2 & -1 & -1 \\ 2 & 1 & -2 & -1 \\ -1 & 0 & 1 & -3 \\ 5 & 8 & 8 & 0 \end{bmatrix}.$$

Parmi les nombreuses propriétés d'une base LLL-réduite, on a les inégalités suivantes.

**Théorème 3.1.13.** *Soit  $(b_1 \cdots, b_n)$  une base LLL-réduite et  $(b_1^*, \dots, b_n^*)$  la base orthogonale associée par la méthode de Gram-Schmidt. Alors*

1.  $\|b_j^*\|^2 \leq 2^{i-j} \|b_i^*\|^2$  pour  $1 \leq j \leq i \leq n$ .
2.  $\prod_{i=1}^n \|b_i\| \leq 2^{\frac{n(n-1)}{4}} \det(L)$ .
3.  $\|b_j\| \leq 2^{\frac{i-1}{2}} \|b_i^*\|$  pour  $1 \leq j \leq i \leq n$ .
4.  $\|b_1\| \leq 2^{\frac{n-1}{4}} (\det(L))^{\frac{1}{n}}$ .
5. Pour tout vecteur non nul  $v \in L$ ,  $\|b_1\| \leq 2^{\frac{n-1}{2}} \|v\|$ .

*Démonstration.*

**Preuve de 1.** Supposons que  $(b_1 \cdots, b_n)$  une base LLL-réduite. Alors, en développant l'inégalité 3.2 et en utilisant 3.1, on a

$$\frac{3}{4} \|b_{i-1}^*\|^2 \leq \|b_i^*\|^2 + \mu_{i,i-1}^2 \|b_{i-1}^*\|^2 \leq \|b_i^*\|^2 + \frac{1}{4} \|b_{i-1}^*\|^2,$$

ce qui donne

$$\|b_{i-1}^*\|^2 \leq 2 \|b_i^*\|^2.$$

Ainsi, pour  $j \leq i$ , on obtient

$$\|b_j^*\|^2 \leq 2^{i-j} \|b_i^*\|^2$$

ce qui démontre la propriété 1.

**Preuve de 2.** Dans le processus de l'orthogonalisation de Gram-Schmidt, on a  $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$ . On obtient ainsi, en utilisant 3.1 :

$$\|b_i\|^2 = \|b_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \|b_j^*\|^2 \leq \|b_i^*\|^2 + \frac{1}{4} \sum_{j=1}^{i-1} \|b_j^*\|^2.$$

En utilisant  $\|b_j^*\|^2 \leq 2^{i-j}\|b_i^*\|^2$ , on obtient

$$\|b_i\|^2 \leq \|b_i^*\|^2 + \frac{1}{4} \sum_{j=1}^{i-1} 2^{i-j}\|b_i^*\|^2 = (2^{i-2} + 2^{-1}) \|b_i^*\|^2 \leq 2^{i-1}\|b_i^*\|^2.$$

En passant aux produits, on a alors

$$\prod_{i=1}^n \|b_i\|^2 \leq \prod_{i=1}^n 2^{i-1}\|b_i^*\|^2 = 2^{\frac{n(n-1)}{2}} \prod_{i=1}^n \|b_i^*\|^2 = 2^{\frac{n(n-1)}{2}} \det(L),$$

ce qui donne l'inégalité 2 en prenant les racines carrées.

**Preuve de 3.** En remplaçant  $i$  par  $j$  dans l'inégalité  $\|b_i\|^2 \leq 2^{i-1}\|b_i^*\|^2$  (ci-dessus), on obtient  $\|b_j\|^2 \leq 2^{j-1}\|b_j^*\|^2$ . En combinant avec l'inégalité 1, on obtient

$$\|b_j\|^2 \leq 2^{j-1}2^{i-j}\|b_i^*\|^2 = 2^{i-1}\|b_i^*\|^2,$$

ce qui démontre l'inégalité 3.

**Preuve de 4.** En prenant  $j = 1$  dans l'inégalité 3, on obtient  $\|b_1\|^2 \leq 2^{i-1}\|b_i^*\|^2$  pour  $1 \leq i \leq n$ . Alors

$$\|b_1\|^{2n} \leq \prod_{i=1}^n n2^{i-1}\|b_i^*\|^2 = 2^{\frac{n(n-1)}{2}} \prod_{i=1}^n n\|b_i^*\|^2 = 2^{\frac{n(n-1)}{2}} (\det(L))^2,$$

ce qui donne  $\|b_1\| \leq 2^{\frac{n-1}{4}} (\det(L))^{\frac{1}{n}}$  et démontre l'inégalité 4.

**Preuve de 5.** Soit  $v \in L$  un vecteur non nul. Alors, en exprimant  $v$  dans les bases  $(b_1, b_2, \dots, b_n)$  et  $(b_1^*, b_2^*, \dots, b_n^*)$ , on obtient

$$v = \sum_{i=1}^n \alpha_i b_i = \sum_{i=1}^n \alpha_i^* b_i^*, \quad \alpha_i \in \mathbb{Z} \quad \alpha_i \in \mathbb{R}.$$

En prenant la définition de  $b_i$  dans l'orthogonalisation de Gram-Schmidt, on obtient

$$v = \sum_{i=1}^n \alpha_i \left( b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \right).$$

Soit  $k$ ,  $1 \leq k \leq n$ , le plus grand indice pour lequel  $\alpha_k \neq 0$ . Alors en exprimant le produit  $\langle v, b_k^* \rangle$  de deux façons et en tenant compte de l'orthogonalité de  $(b_1^*, b_2^*, \dots, b_n^*)$ , on obtient :

$$\langle v, b_k^* \rangle = \alpha_k \|b_k^*\|^2 = \alpha_k^* \|b_k^*\|^2.$$

Ainsi  $\alpha_k = \alpha_k^*$ , avec  $|\alpha_k| \geq 1$ . En calculant  $\|v\|^2$ , on obtient

$$\|v\|^2 = \sum_{i=1}^n (\alpha_i^*)^2 \|b_i^*\|^2 \geq (\alpha_k^*)^2 \|b_k^*\|^2 \geq \|b_k^*\|^2.$$

En prenant  $j = 1$  et  $i = k$  dans l'inégalité 3, on obtient  $\|b_k^*\|^2 \geq 2^{1-k}\|b_1\|^2$ . Ainsi

$$\|v\|^2 \geq 2^{1-k}\|b_1\|^2 \geq 2^{1-n}\|b_1\|^2,$$

ce qui donne  $\|b_1\| \leq 2^{\frac{n-1}{2}}\|v\|$  et termine la preuve.  $\square$

Le théorème précédent concerne souvent le vecteur  $b_1$ . Plus généralement, on a le résultat suivant.

**Théorème 3.1.14.** *Soit  $(b_1, \dots, b_n)$  une base LLL-réduite d'un réseau. Alors pour tout  $j$ ,  $1 \leq j \leq n$ , on a*

$$\|b_j\| \leq 2^{\frac{n(n-1)}{4(n-j+1)}} (\det L)^{\frac{1}{n-j+1}}.$$

*Démonstration.* Soit  $(b_1^*, \dots, b_n^*)$  la base orthogonale associée par la méthode de Gram-Schmidt à  $(b_1, \dots, b_n)$ . Par le résultat (3) de la proposition 3.1.13, on a, pour  $1 \leq j \leq i \leq n$

$$\|b_j\| \leq 2^{\frac{i-1}{2}} \|b_i^*\|.$$

En appliquant cette inégalité pour chaque  $i = j, j+1, \dots, n$  et en multipliant, on obtient

$$\|b_j\|^{n-j+1} \leq \prod_{i=j}^n 2^{\frac{i-1}{2}} \|b_i^*\|.$$

On obtient alors en commençant à  $i = 1$  :

$$\|b_j\|^{n-j+1} \leq \prod_{i=1}^n 2^{\frac{i-1}{2}} \|b_i^*\| = \prod_{i=1}^n 2^{\frac{i-1}{2}} \prod_{i=1}^n \|b_i^*\| = 2^{\frac{n(n-1)}{4}} \det(L),$$

ce qui donne le résultat recherché.  $\square$

On donne maintenant la complexité de l'algorithme LLL.

**Théorème 3.1.15.** *Soit  $(b_1, \dots, b_n)$  une base d'un réseau  $L$  et  $B = \max_i \|b_i\|$ . L'algorithme LLL produit une base réduite en un temps polynômial :*

$$\mathcal{O}(n^4 \log^3 B).$$

### Maple 3.1.16.

Dans Maple 12, l'algorithme LLL est en fait déjà programmé sous le nom de procédure **LLL** dans le package **IntegerRelations**. On donne, par exemple la base  $(b_1, b_2, b_3, b_4)$  avec pour matrice

$$M = \begin{bmatrix} b_1 & b_2 & b_3 & b_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 7 & 9 & 4 \\ 6 & -7 & 2 & 3 \\ -1 & 2 & -1 & -1 \\ 2 & -1 & 0 & -3 \end{bmatrix}.$$

Programme	Commentaires
<code>with(IntegerRelations):</code>	<code>&lt;--- Package IntegerRelations</code>
<code>with(LinearAlgebra):</code>	<code>&lt;--- Package LinearAlgebra</code>
<code>l1 := [4, 7, 9, 4];</code>	<code>&lt;--- Première ligne</code>
<code>l2 := [6, -7, 2, 3];</code>	<code>&lt;--- Deuxième ligne</code>
<code>l3 := [-1, 2, -1, -1];</code>	<code>&lt;--- Troisième ligne</code>
<code>l4 := [2, -1, 0, -3];</code>	<code>&lt;--- Quatrième ligne</code>
<code>N:=LLL([l1, l2, l3,l4], 'integer');</code>	<code>&lt;--- Procédure LLL, paramètres entiers</code>

On obtient alors la base  $(b_1, b_2, b_3, b_4)$  dont la matrice est

$$N = \begin{bmatrix} b_1 & b_2 & b_3 & b_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ -1 & 2 & -1 & -1 \\ 2 & 1 & -2 & -1 \\ -1 & 0 & 1 & -3 \\ 5 & 8 & 8 & 0 \end{bmatrix}.$$

On peut alors vérifier que les deux bases ont le même déterminant et que  $b'_1$  est plus court que les autres vecteurs de la base.

Programme	Commentaires
<code>M:=Matrix([b1, b2, b3, b4]):</code>	<code>&lt;--- Matrice M</code>
<code>N:=Matrix([m[1], m[2], m[3], m[4]]):</code>	<code>&lt;--- Matrice N</code>
<code>Determinant(M)-Determinant(N);</code>	<code>&lt;--- Comparaison</code>
<code>for i to 4 do</code>	<code>&lt;--- Liste des modules</code>
<code>DotProduct(Vector(m[i]), Vector(m[i]))</code>	<code>et vérification que</code>
<code>end do;</code>	<code>b1 est le plus court.</code>

### Magma 3.1.17.

Dans Magma, l'algorithme LLL est programmé sous le nom **LLL**. On donne, le

même exemple avec la base  $(b_1, b_2, b_3, b_4)$  qui a pour matrice

$$M = \begin{bmatrix} b_1 & b_2 & b_3 & b_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 7 & 9 & 4 \\ 6 & -7 & 2 & 3 \\ -1 & 2 & -1 & -1 \\ 2 & -1 & 0 & -3 \end{bmatrix}.$$

Programme	Commentaires
<code>Z := IntegerRing();</code>	<code>&lt;--- Ensemble des entiers</code>
<code>R:=MatrixRing(Z,4);</code>	<code>&lt;--- Ensemble des matrices de type 4x4</code>
<code>M :=elt&lt; R [4, 7, 9, 4,</code>	<code>&lt;--- Matrice</code>
<code>          6, -7, 2, 3,</code>	
<code>          -1, 2, -1, -1,</code>	
<code>          2 , -1,0, -3] &gt;;</code>	
<code>F:=LLL(M) ;</code>	<code>&lt;--- Procédure LLL,</code>
<code>Determinant(M);</code>	<code>&lt;--- Déterminant de M</code>
<code>Determinant(F);</code>	<code>&lt;--- Déterminant de F</code>

On obtient alors la base  $(b'_1, b'_2, b'_3, b'_4)$  dont la matrice est

$$N = \begin{bmatrix} b'_1 & b'_2 & b'_3 & b'_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ -1 & 2 & -1 & -1 \\ 2 & 1 & -2 & -1 \\ -1 & 0 & 1 & -3 \\ 5 & 8 & 8 & 0 \end{bmatrix}.$$

On peut alors vérifier que les deux bases ont le même déterminant et que  $b'_1$  est plus court que les autres vecteurs de la base.

Programme	Programme
Z :=RationalField();	<--- Z :=RationalField();
V := VectorSpace(Z, 4);	V := VectorSpace(Z, 4);
x := V![-1 ,2 ,-1 ,-1];	x := V![-1 ,2 ,-1 ,-1];
Norm(x);	Norm(x);
y := V![2 , 1 ,-2, -1];	y := V![2 , 1 ,-2, -1];
Norm(y);	Norm(y);
z:= V![-1 , 0, 1, -3];	z:= V![-1 , 0, 1, -3];
Norm(z);	Norm(z);
w := V![5 , 8 , 8 , 0];	w := V![5 , 8 , 8 , 0];
Norm(w);	Norm(w);

## 3.2 Cryptanalyse de RSA par la réduction des réseaux

### 3.2.1 La méthode de Coppersmith : polynômes à une variable

En 1996, D. Coppersmith a décrit une méthode pour déterminer les petites racines modulaires d'un polynôme à une variable ainsi que les petites racines entières d'un polynôme à deux variables. Soit  $N$  un entier positif (sans factorisation connue) et  $f$  un polynôme de degré  $d$  à coefficient dans  $\mathbb{Z}$ .

$$f(x) = \sum_{i=1}^n a_i x^i.$$

Chaque terme  $x^i$  est appelé un monôme. La norme Euclidienne de  $f$  est définie par

$$\|f(x)\| = \sqrt{\sum_{i=1}^n a_i^2}.$$

Le problème de la petite racine modulaire consiste à trouver un nombre entier  $x_0$  qui vérifie

$$\begin{aligned} f(x_0) &\equiv 0 \pmod{N}, \\ |x_0| &< X, \end{aligned}$$

où  $X$  est une borne fixée.

L'idée de Coppersmith s'applique plus généralement dans le cas suivant :

**Paramètres connus :**

- Un entier  $N$ .
- L'existence d'un facteur inconnu  $b$  de  $N$  avec  $b > N^\beta$ .
- L'expression d'un polynôme  $f_b(x)$ , de degrés  $\delta$ .
- Une borne  $X$  pour laquelle  $f_b(x_0) \equiv 0 \pmod{b}$  avec  $|x_0| < X$ .

**Paramètres inconnus :**

- Le facteur  $b$  de  $\mathbb{N}$ .
- La racine  $x_0$ .

La méthode de Coppersmith permet de transformer l'équation modulaire  $f_b(x_0) \equiv 0 \pmod{b}$  en une équation entière  $f(x) = 0$ , c'est à dire sur l'ensemble des entiers. Pour déterminer l'équation entière, on fixe un entier  $m$  et on construit une série de polynômes de  $\mathbb{Z}[x]$  :

$$g_{jk}(x) = x^j (f_b(x))^k N^{m-k},$$

où les valeurs de  $j$  et  $k$  dépendent de  $m$  et du degré de  $f$ . Puisque  $f_b(x_0) \equiv 0 \pmod{b}$ , alors  $f_b(x_0) = ab$  pour un entier  $a$  et donc

$$\begin{aligned} g_{jk}(x_0) &= x_0^j (f_b(x_0))^k b^{m-k} \left(\frac{N}{b}\right)^{m-k} \\ &= a^k x_0^j b^k b^{m-k} \left(\frac{N}{b}\right)^{m-k} \\ &= a^k x_0^j b^m \left(\frac{N}{b}\right)^{m-k} \\ &\equiv 0 \pmod{b^m}. \end{aligned}$$

Ceci implique que toute combinaison linéaire  $h(x)$  des polynômes  $g_{jk}(x)$  vérifiera  $h(x_0) \equiv 0 \pmod{b^m}$ . Si en plus  $h$  vérifie  $|h(x_0)| < b^m$ , alors on a tout simplement  $h(x_0) = 0$ , ce qui est facile à résoudre. Le passage de l'équation modulaire  $h(x_0) \equiv 0 \pmod{b^m}$  à l'équation entière  $h(x_0) = 0$  peut être fixé par le théorème suivant.

**Théorème 3.2.1** (Howgrave-Graham). *Soit  $h(x) \in \mathbb{Z}[x]$  un polynôme de degré  $d$  ayant au plus  $\omega$  monômes et  $X$  un nombre positif. Si  $x_0$  est un entier et  $M$  un nombre positif tels que :*

- (1)  $|x_0| < X$ ,
- (2)  $h(x_0) \equiv 0 \pmod{M}$ ,
- (3)  $\|h(xX)\| < \frac{M}{\sqrt{\omega}}$ ,



alors  $h(x_0) = 0$  en tant qu'équation sur  $\mathbb{Z}$ .

*Démonstration.* Soit  $h(x) = \sum_i^d a_i x^i$  ayant  $\omega$  monômes. Supposons que  $|x_0| < X$ . Alors

$$|h(x_0)| = \left| \sum_i a_i x^i \right| \leq \sum_i |a_i x^i| < \sum_i |a_i X^i|.$$

D'autre part, l'inégalité de Cauchy-Schwarz donne

$$\left( \sum_i \alpha_i \beta_i \right)^2 \leq \left( \sum_i \alpha_i^2 \right) \left( \sum_i \beta_i^2 \right).$$

En utilisant cette inégalité, on obtient

$$\left( \sum_i |a_i X^i| \right)^2 \leq \left( \sum_i 1^2 \right) \left( \sum_i (a_i X^i)^2 \right) = \omega \sum_i (a_i X^i)^2.$$

Ainsi, si  $\|h(xX)\| < \frac{M}{\sqrt{\omega}}$ , alors

$$\sum_i |a_i X^i| < \sqrt{\omega} \sqrt{\sum_i (a_i X^i)^2} = \sqrt{\omega} \|h(xX)\| < M.$$

Donc  $|h(x_0)| < M$ . Si on suppose que  $h(x_0) \equiv 0 \pmod{M}$ , alors  $h(x_0) = 0$ .  $\square$

Le problème de la résolution de la congruence  $f_b(x_0) \equiv 0 \pmod{b}$  peut donc être résolu par une équation  $h(x_0) = 0$  où  $h$  vérifie le théorème 3.2.1. On observe d'abord que la condition (3) de ce théorème signifie que les coefficients de  $h$  sont assez petits et que la condition (2) avec  $M = b^m$  est satisfaite par toute combinaison linéaire des polynômes  $g_{jk}(x)$ . Ceci peut être obtenu en appliquant la réduction d'un réseau de dimension  $n$  dont une base est formée à l'aide des coefficients des polynômes  $g_{jk}(xX)$ . Avec l'algorithme LLL, on peut obtenir un vecteur  $h(xX)$  qui vérifie la condition (3). L'algorithme LLL donnera alors des vecteurs  $v_1(xX), \dots, v_n(xX)$  où  $n$  est la dimension du réseau. On sait d'après le théorème 3.1.13, que le polynôme  $v_1(xX)$  va vérifier

$$\|v_1(xX)\| \leq 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}}.$$

Ainsi, pour satisfaire la condition (3) du théorème 3.2.1, il suffit d'avoir

$$(3.3) \quad 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}} < \frac{b^m}{\sqrt{n}}.$$

Le vecteur recherché  $h(xX)$  sera donc le premier vecteur  $v_1(xX)$  de la base réduite.

En effet, on considère le réseau formé par les vecteurs colonnes de la matrice définie par les polynômes

$$\begin{aligned} g_{i,j}(x) &= x^j N^i (f_b(x))^{m-i}, \quad j = 0, \dots, \delta - 1, \quad i = m, \dots, 1, \\ h_i(x) &= x^i (f_b(x))^m, \quad i = 0, \dots, t - 1, \end{aligned}$$

où  $\delta = \deg(f_b)$  et  $m$  et  $t$  sont des entiers fixés. En explicitant les polynômes  $g_{i,j}(x)$ , on obtient les valeurs

$$(3.4) \quad \begin{array}{c|ccccc} & j = 0 & j = 1 & j = 2 & \dots & j = \delta - 1 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ i = m \rightarrow & N^m, & N^m x, & N^m x^2, & \dots & N^m x^{\delta-1}, \\ i = m - 1 \rightarrow & N^{m-1} f & N^{m-1} x f & N^{m-1} x^2 f & \dots & N^{m-1} x^{\delta-1} f \\ i = m - 2 \rightarrow & N^{m-2} f^2 & N^{m-2} x f^2 & N^{m-2} x^2 f^2 & \dots & N^{m-2} x^{\delta-1} f^2 \\ \vdots \rightarrow & \vdots & \vdots & \vdots & \vdots & \vdots \\ i = 2 \rightarrow & N^2 f^{m-2} & N^2 x f^{m-2} & N^2 x^2 f^{m-2} & \dots & N^2 x^{\delta-1} f^{m-2} \\ i = 1 \rightarrow & N f^{m-1} & N x f^{m-1} & N x^2 f^{m-1} & \dots & N x^{\delta-1} f^{m-1} \end{array}$$

On observe de cette façon que les degrés des polynômes sont croissants de la position  $(i, j) = (m, 0)$  à la position  $(i, j) = (1, \delta - 1)$ . On peut continuer ce tableau avec les polynômes  $h_i(x)$ .

$$(3.5) \quad i = 0, \dots, t - 1 \Rightarrow f^m, x f^m, x^2 f^m, \dots, x^{t-1} f^m.$$

Une fois encore les degrés sont croissants. Globalement, les degrés remplissent totalement l'intervalle  $\{0, 1, \dots, m\delta + t - 1\}$ . On peut alors considérer les matrices définies par les coordonnées des différents polynômes  $g_{i,j}(Xx)$  et  $h_i(Xx)$ , lignes par



En isolant  $X$ , on obtient alors

$$X < 2^{-\frac{1}{2}} n^{\frac{-1}{n-1}} N^{\frac{2mn\beta - m(m+1)\delta}{n(n-1)}}.$$

En considérant l'exposant de  $N$  dans l'inégalité précédente, on observe qu'il atteint son maximum pour

$$m_0 = \frac{2n\beta - \delta}{2\delta},$$

ce qui donne la borne

$$X < 2^{-\frac{1}{2}} n^{\frac{-1}{n-1}} N^{\frac{\beta^2}{\delta} + \frac{\beta^2}{(n-1)\delta} + \frac{\delta}{4n(n-1)} - \frac{\beta}{n-1}},$$

ce qui peut être écrit sous la forme

$$X < 2^{-\frac{1}{2}} N^{\frac{\beta^2}{\delta} - \varepsilon},$$

avec

$$\varepsilon = \frac{\log n}{(n-1) \log N} + \frac{\beta}{n-1} - \frac{\beta^2}{(n-1)\delta} - \frac{\delta}{4n(n-1)},$$

qui dépend de  $n$  mais qui vérifie  $\lim_{n \rightarrow +\infty} \varepsilon = 0$ .

On peut maintenant résumer cette méthode dans le théorème suivant.

**Théorème 3.2.2.** *Pour tout  $\varepsilon > 0$ , il existe un entier  $N_0$  qui vérifie la propriété : Soit  $N > N_0$  un entier de factorisation inconnue qui a un diviseur  $b > N^\beta$ . Soit  $f_b(x)$  un polynôme de degrés  $\delta$ . Toutes les solutions  $x_0$  de la congruence  $f_b(x) \equiv 0 \pmod{b}$  vérifiant*

$$|x_0| < 2^{-\frac{1}{2}} N^{\frac{\beta^2}{\delta} - \varepsilon}$$

*peuvent être déterminées en temps polynômial en  $\log N$ .*

En appliquant ce théorème avec  $b = N$  et donc  $\beta = 1$ , on obtient le théorème suivant :

**Théorème 3.2.3.** *Pour tout  $\varepsilon > 0$ , il existe un entier  $N_0$  qui vérifie la propriété : Soit  $N > N_0$  un entier de factorisation inconnue. Soit  $f(x)$  un polynôme de degrés  $\delta$ . Toutes les solutions  $x_0$  de la congruence  $f(x) \equiv 0 \pmod{N}$  vérifiant*

$$|x_0| < 2^{-\frac{1}{2}} N^{\frac{1}{\delta} - \varepsilon}$$

*peuvent être déterminées en temps polynômial en  $\log N$ .*

**Exemple 3.2.4.**

Soit  $N = 29263868053$ . On veut déterminer les solutions de la congruence

$$f(x) = -111111111 - 111111110x - 111111110x^2 + x^3 \equiv 0 \pmod{N}.$$

Le degré est  $\delta = 3$  et on peut donc déterminer, en théorie, toutes les solutions  $x_0$  qui vérifient

$$|x_0| < 2^{-\frac{1}{2}} N^{\frac{1}{\delta} - \varepsilon},$$

soit  $|x_0| < 2179$  avec  $\varepsilon = 0$ . On pose donc  $X = 2179$ . On choisissant  $m = 3$  et  $t = 1$ , on doit calculer les polynômes définies par (3.4), soit

	$j = 0$	1	2
$i = 3$	$N^3$ ,	$N^3 xX$ ,	$N^m (xX)^2$
$i = 2$	$N^2 f(xX)$	$N^2 x f(xX)$	$N^2 (xX)^2 f(xX)$
$i = 1$	$N f^2(xX)$	$N (xX) f^2(xX)$	$N (xX)^2 f^2(xX)$
$i = 0$	$f^3(xX)$		

On pose

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + x^3, \\ f^2(x) &= b_0 + b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^4 + b_5 x^5 + x^6, \\ f^3(x) &= c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5 + c_6 x^6 + c_7 x^7 + c_8 x^8 + x^9. \end{aligned}$$

Puisque  $n = \delta m + t = 10$ , on forme alors la matrice carrée  $10 \times 10$  définie par (3.6) en utilisant (3.4) avec  $m = 3$ ,  $\delta = 3$  et (3.5) avec  $t = 1$ ,

$$\begin{bmatrix} 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 & x^8 & x^9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ N^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & XN^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X^2 N^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_0 N^2 & a_1 X N^2 & a_2 X^2 N^2 & X^3 N^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_0 X N^2 & a_1 X^2 N^2 & a_2 X^3 N^2 & X^4 N^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_0 X^2 N^2 & a_1 X^3 N^2 & a_2 X^4 N^2 & X^5 N^2 & 0 & 0 & 0 & 0 \\ b_0 N & b_1 X N & b_2 X^2 N & b_3 X^3 N & b_4 X^4 N & b_5 X^5 N & X^6 N & 0 & 0 & 0 \\ 0 & b_0 X N & b_1 X^2 N & b_2 X^3 N & b_3 X^4 N & b_4 X^5 N & b_5 X^6 N & X^7 N & 0 & 0 \\ 0 & 0 & b_0 X^2 N & b_1 X^3 N & b_2 X^4 N & b_3 X^5 N & b_4 X^6 N & b_5 X^7 N & X^8 N & 0 \\ c_0 & c_1 X & c_2 X^2 & c_3 X^3 & c_4 X^4 & c_5 X^5 & c_6 X^6 & c_7 X^7 & c_8 X^8 & X^9 \end{bmatrix}$$

### Maple 3.2.5.

On ne trouve en fait aucune solution car la valeur prise par  $X$  est très grande. En effet, dans l'inégalité  $|x_0| < 2^{-\frac{1}{2}} N^{\frac{1}{\delta} - \varepsilon}$ , le rôle de  $\varepsilon$  peut être très important. En prenant la valeur  $X = 500$ , on trouve  $x_0 = 79$ .

Programme	Commentaires
<pre> with(PolynomialTools): with(LinearAlgebra): with(linalg): with(IntegerRelations): N:=29263868053; f:=x-&gt;x^3-111111110*x^2   -111111110*x-111111111; d:=degree(f(x),x): X:=trunc((2^(-1/2)*N^(1/d))): X:=500; m:=3:t:=1: n:=d*m+t: M:=Matrix(n): line:=0: for i from 1 to m do   i2:=m+1-i:   for j from 0 to d-1 do     line:=line+1:     cc:=CoefficientVector (N^i2*X^j*x^(j)*(f(X*x))^(m-i2),x):     for k from 1 to Dimension(cc) do       M[line,k]:=cc[k]:     end do:   end do: end do: for i from 0 to t-1 do   line:=line+1:   cc:=CoefficientVector (x^i*X^i*(f(x*X))^m,x):   for k from 1 to Dimension(cc) do     M[line,k]:=cc[k]:   end do: end do: VM:=[row(M,1..n)]: L := LLL(VM, 'integer'): h:=0: for i from 0 to n-1 do   h:=h+(L[1,i+1]/X^i)*x^i: end do: h: isolve(h); </pre>	<pre> &lt;-- Package Polynômes &lt;-- Package Algèbre Linéaire &lt;-- Un autre package &lt;-- Package LLL &lt;-- La valeur de N &lt;-- La fonction f &lt;-- Le degré de f &lt;-- Borne supérieure des solutions &lt;-- Une borne inférieure &lt;-- m=3 et t=1 &lt;-- La dimension du réseau &lt;-- La matrice (n,n), formée de 0 &lt;-- Initiation &lt;-- Boucle de formation de   la matrice correspondante   aux polynômes g(i,j),   qui formera   l'entrée pour LLL &lt;-- Fin de la boucle &lt;-- Boucle de formation de   la matrice correspondante   aux polynômes h(i),   qui formera   l'entrée pour LLL &lt;-- Fin de la boucle &lt;-- Formation de la matrice &lt;-- Réduction de la matrice &lt;-- &lt;-- Formation du polynôme h &lt;-- racines entière de h </pre>

**Magma 3.2.6.**

Pour Magma, on peut alors utiliser le code suivant.

Programme	Commentaires
<pre> F&lt;x&gt; := PolynomialRing (Integers()); G&lt;z&gt; := PolynomialRing(Rationals()); N:=29263868053; f:=-111111111-111111110*x   -111111110*x^2+x^3; d:=Degree(f); X:=Truncate((2^(-1/2)*N^(1/d)));X:=500; cc:=Coefficients(f); f:=0; for i:=1 to #cc do   f:=f+cc[i]*x^(i-1)*X^(i-1); end for; m:=3;t:=1; n:=d*m+t; M:=RMatrixSpace(IntegerRing(),n,n)!0; line:=0; for i:=1 to m do   i2:=m+1-i;   for j:=0 to d-1 do     line:=line+1;     cc:=Coefficients       (N^i2*X^j*x^(j)*f^(m-i2));     for k:=1 to #(cc) do       M[line,k]:=cc[k];     end for;   end for; end for; for i:=0 to t-1 do   line:=line+1;   cc:=Coefficients(x^i*X^i*f^m);   for k:=1 to #(cc) do     M[line,k]:=cc[k];   end for; end for; L := LLL(M); p:=0; pp:=0; </pre>	<pre> &lt;-- Ensemble des polynômes &lt;-- Ensemble des polynômes &lt;-- Module &lt;-- Fonction  &lt;-- Son degré &lt;-- Borne de Coppersmith &lt;-- Liste des coefficients de f &lt;-- f=0 &lt;-- Polynômes f de Coppersmith  &lt;-- Choix m=3 et t=1 &lt;-- Ordre du réseau &lt;-- Matrice carrée nxn &lt;-- line=0 &lt;-- Boucle de formation de   la matrice correspondante   aux polynômes g(i,j),   qui formera   l'entrée pour LLL  &lt;-- Boucle de formation de   la matrice correspondante   aux polynômes h(i),   qui formera   l'entrée pour LLL  &lt;-- Algorithme LLL &lt;-- p=0 &lt;-- pp=0 </pre>

for i:=0 to n-1 do	<-- Formation du polynôme h
pp:=pp+L[1,i+1]*z^i;	
p:=p+(L[1,i+1]/X^i)*z^i;	
end for;	
p;Roots(p);	<-- polynôme h et ses racines

On ne trouve en fait aucune solution si la valeur prise par  $X$  est très grande. En effet, dans l'inégalité

$$|x_0| < 2^{-\frac{1}{2}} N^{\frac{1}{8}-\varepsilon},$$

le rôle de  $\varepsilon$  peut être très important. En prenant  $X = 500$  dans le code ci-dessus, on obtient alors le polynôme :

$$\begin{aligned} h(z/X) = & 35819 * z^9 - 8381646 * z^8 + 645386742 * z^7 - 6424486034022 * z^6 \\ & + 999721772296884 * z^5 + 35322490662759665925 * z^4 \\ & + 13772627569229621478757 * z^3 - 1292162362422796441508568 * z^2 \\ & - 1292197683913738082645997 * z - 1305934988985879813073884, \end{aligned}$$

de racine 79.

En fait, dans Magma, la méthode de Coppersmith pour résoudre l'équation polynomiale

$$f(x_0) \equiv 0 \pmod{N}, \quad |x_0|X < \frac{1}{2}N^{\frac{1}{d}},$$

est implémentée sous la forme **SmallRoots(f,N,X)**. Dans l'exemple ci-dessous, on veut résoudre l'équation

$$f(x) = x^3 - 111111110 * x^2 - 111111110 * x - 111111111 \equiv 0 \pmod{29263868053},$$

avec  $|x| < 500$ .

### Magma 3.2.7.

programme	programme
F<x>:=PolynomialRing(Integers());	<-- Ensemble des polynômes
N:=29263868053;	<-- Module
f:=x^3-111111110x^2	<-- Fonction
-111111110x-111111111;	
X:=500;	<-- Borne
sol:=SmallRoots(f, N, X);	<-- Procédure de Coppersmith
sol;	<-- Ensemble des solutions

La solution obtenue 79.



### 3.2.2 Factorisation de $N$

Une autre application de la méthode de Coppersmith est la factorisation de  $N = pq$  si on connaît une fraction importante de  $p$  ou de  $q$ . Plus précisément, on a le résultat suivant :

**Théorème 3.2.8.** *Soit  $N = pq$  un module RSA dont les facteurs premiers  $p$  et  $q$  sont inconnus et tels que  $q < p$ . Si on connaît une valeur  $\tilde{p}$  telle que*

$$|\tilde{p} - p| < N^{\frac{1}{4}},$$

*alors on peut factoriser  $N$  en temps polynômial en  $\log N$ .*

*Démonstration.* Supposons que  $|\tilde{p} - p| < N^{\frac{1}{4}}$ . On considère la fonction  $f_p$  définie par  $f_p(x) = x + \tilde{p}$ . Alors on a  $f_p(p - \tilde{p}) = p \equiv 0 \pmod{p}$ . Ainsi,  $x_0 = p - \tilde{p}$  est un entier qui vérifie

$$f_p(x_0) \equiv 0 \pmod{p}, \quad |x_0| < N^{\frac{1}{4}}.$$

On peut donc appliquer le théorème 3.2.2 avec  $b = p > N^{\frac{1}{2}}$ , en prenant  $\beta = \frac{1}{2}$ .  $\square$

#### Maple 3.2.9.

Voici un exemple dans lequel  $N = 2535301200456606295881202795651$  est de la forme  $N = pq$ . On donne aussi une approximation  $p_0 = 1125899907822525$  de  $p$  et on sait que  $|p - p_0| < N^{\frac{1}{4}}$ . Dans le programme maple ci-dessous, la borne du théorème 3.2.2 avec  $\varepsilon = 0$  s'est avérée assez grande et ne donne aucune réponse. En prenant la borne

$$X < 2^{-\frac{3}{2}} N^{\frac{1}{4}}.$$

On obtient alors une réponse avec le choix  $m = 2$  et  $t = 2$  car le choix  $t = 1$  ne donne pas de solution non plus. On obtient alors la réponse  $x_0 = -979846$ , ce qui donne  $p = p_0 + x_0 = 1125899906842679$ .

Programme	Commentaires
<pre> with(PolynomialTools): with(LinearAlgebra): with(linalg): with(IntegerRelations): p := nextprime(2^50): q := nextprime(2^51): N:=p*q; p0 := p+979846: f := x-&gt;x+p0: d:=degree(f(x),x): b:=1/2: X:=trunc((2^(-3/2)*N^(b^2/d))): m:=2:t:=2: n:=d*m+t: M:=Matrix(n): line:=0: for i from 1 to m do   i2:=m+1-i:   for j from 0 to d-1 do     line:=line+1:     cc:=CoefficientVector (N^i2*X^j*x^(j)*(f(X*x))^(m-i2),x):     for k from 1 to Dimension(cc) do       M[line,k]:=cc[k]:     end do:   end do: end do: for i from 0 to t-1 do   line:=line+1:   cc:=CoefficientVector (x^i*X^i*(f(x*X))^m,x):   for k from 1 to Dimension(cc) do     M[line,k]:=cc[k]:   end do: end do: VM:=[row(M,1..n)]: L := LLL(VM, 'integer'): h:=0: for i from 0 to n-1 do   h:=h+(L[1,i+1]/X^i)*x^i: end do: isolve(h); </pre>	<pre> &lt;-- Package Polynômes &lt;-- Package Algèbre Linéaire &lt;-- Un autre package &lt;-- Package LLL &lt;-- Le nombre premier p &lt;-- Le nombre premier q &lt;-- Le module RSA &lt;-- Une approximation de p &lt;-- La fonction f &lt;-- Son degré &lt;-- L'exposant beta=1/2 &lt;-- Borne supérieure des solutions &lt;-- m=2 et t=2 &lt;-- La dimension du réseau &lt;-- La matrice (n,n), formée de 0 &lt;-- Initiation &lt;-- Boucle de formation de   la matrice correspondante   aux polynômes g(i,j),   qui formera   l'entrée pour LLL &lt;-- Fin de la boucle &lt;-- Boucle de formation de   la matrice correspondante   aux polynômes h(i),   qui formera   l'entrée pour LLL &lt;-- Fin de la boucle &lt;-- Formation de la matrice &lt;-- Réduction de la matrice &lt;-- Formation du polynôme h &lt;-- racines entière de h </pre>

**Magma 3.2.10.**

On reprend le même exemple avec  $N = pq = 2535301200456606295881202795651$ . On donne aussi une approximation  $p_0 = 1125899907822525$  de  $p$  et on sait que  $|p - p_0| < N^{\frac{1}{4}}$ . Dans le programme ci-dessous, la borne du théorème 3.2.2 avec  $\varepsilon = 0$  s'est avérée assez grande et ne donne aucune réponse. En prenant la borne

$$X < 2^{-\frac{3}{2}} N^{\frac{1}{4}}.$$

On obtient alors une réponse avec le choix  $m = 2$  et  $t = 2$  car le choix  $t = 1$  ne donne pas de solution non plus. On obtient alors la réponse  $x_0 = -979846$ , ce qui donne  $p = p_0 + x_0 = 1125899906842679$ .

**Programme**

```
F<x> := PolynomialRing (Integers());G<z> := PolynomialRing(Rationals());
p := NextPrime(2^50);q := NextPrime(2^51);N:=p*q;
p0 := p+979846;f:=x+p0;d:=Degree(f);
b:=1/2;X:=Truncate((2^(-3/2)*N^(b^2/d)));cc:=Coefficients(f);f:=0;
for i:=1 to #cc do f:=f+cc[i]*x^(i-1)*X^(i-1); end for;
m:=2;t:=2;n:=d*m+t;M:=RMatrixSpace(IntegerRing(),n,n)!0;line:=0;
for i:=1 to m do
i2:=m+1-i;
for j:=0 to d-1 do
line:=line+1;
cc:=Coefficients
(N^i2*X^j*x^(j)*f^(m-i2));
for k:=1 to #(cc) do
M[line,k]:=cc[k];
end for;end for;end for;
for i:=0 to t-1 do
line:=line+1;cc:=Coefficients(x^i*X^i*f^m);
for k:=1 to #(cc) do M[line,k]:=cc[k];end for;
end for;
L := LLL(M);h:=0;pp:=0;
for i:=0 to n-1 do pp:=pp+L[1,i+1]*z^i; h:=h+(L[1,i+1]/X^i)*z^i;end for;
h;Roots(h);
```

On obtient le polynôme

$$h(z) = 2z^3 + 2251799819564523z^2 + 4412934291333159103051z + 2162047098651212289960978150,$$

et les solutions

$$[< -1125899907822525, 1 >, < -1959781/2, 1 >, < -979846, 1 >].$$

Alors  $p_0 - 979846 = p$ .



# Bibliographie

- [1] D. Boneh, G. Durfee. Cryptanalysis of RSA with private key  $d$  less than  $N^{0.292}$ , Advances in Cryptology – Eurocrypt’99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, 1—11 (1999).
- [2] D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), 233—260 (1997).
- [3] G.H. Hardy, E.M. Wright. **An Introduction to the Theory of Numbers**. Oxford University Press, London (1965).
- [4] A. K. Lenstra, H. W. Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513—534, 1982.
- [5] A. May. New RSA Vulnerabilities Using Lattice Reduction Methods. PhD thesis, University of Paderborn (2003)  
<http://wwwcs.upb.de/cs/ag-bloemer/personen/alex/publikationen/>
- [6] R. Rivest, A. Shamir, L. Adleman. A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), 120—126 (1978).
- [7] M. Wiener. Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, 553—558 (1990).