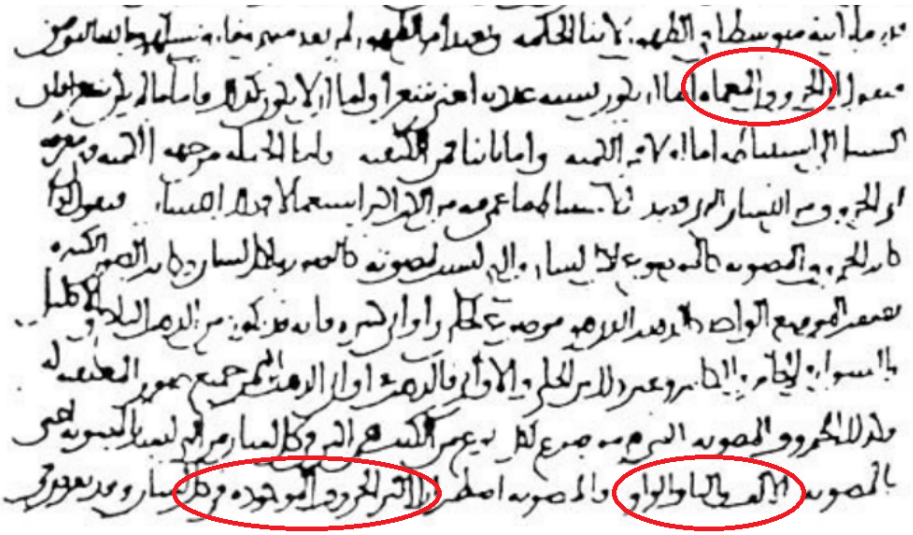
ALGORITHMIC NUMBER THEORY AND CRYPTOGRAPHY

Abderrahmane Nitaj

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen, France

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

abderrahmane.nitaj@unicaen.fr



Contents

Préface

L'invention de la cryptographie à clé publique en 1976 par Diffie et Hellman ainsi que celle du cryptosystème RSA en 1978 par Rivest, Shamir et Adleman ont contribué au développement de la théorie algorithmique des nombres. La sécurité de la plupart des cryptosystèmes modernes est basée sur des problèmes difficiles issus de la théorie de nombres, en particulier la difficulté de factoriser les grands nombres et le problème du logarithme discret. Le lien entre ces deux problèmes difficiles est la notion de nombres premiers. L'algorithmique des nombres premiers s'est alors considérablement développée et ce cours tourne autour de cette thématique. On propose ici d'étudier, tester et implémenter un grand nombre d'algorithmes nécessaires pour l'assimilation des techniques cryptographiques. Cette étude commence par les opérations arithmétiques sur les grands nombres et leurs complexités, puis continue avec les principaux tests de primalité ainsi que les principaux protocoles et cryptosystèmes modernes, en particulier RSA, Diffie-Hellman, El Gamal, NTRU et Knapsack. Toutes les implémentations sont détaillées et commentées à l'aide du system de calcul Maple.

قَالَ الشَّنْفَرَى

وَلِي دُونَكُمْ أَهلُونَ، سَيِّدٌ عَمَلَّسٌ وَ أَرْقَطُ زُهْلُولٌ وَ عَرْفَاءُ جَيْأَلُ

هُمُ الأَهْلُ لَا مُستَودَعُ السِّرِّ ذَائِعٌ لَدَيْهِمْ وَ لَا الجَانِي بِمَا جرَّ يُخْذَلُ

http://www.khayma.com/salehzayadneh/qasayed/shanfara.htm

Chapter 1

Introduction to Maple

In this chapter, we give a short introduction to the algebra system Maple and describe some basic algorithms that we will use later. Maple is a symbolic algebra system which allows computations in many fields of mathematics and engineering. We will use log to indicate the logarithm in base 2 and ln for the natural logarithm.

1.1 Basic operations

MAPLE is a symbolic algebra system which allows computations in many fields of mathematics and engineering.

```
      Maple:    Basic operations

> 10+10;
> 5*10;
> a:=790/6+3/4;
> evalf(a);
> evalf(a,8);
> evalf(a,4);
> round(a);
> floor(a);
> 2^6;
```

```
      Maple:    Digits

> Digits; evalf(1/3);
> Digits:=2;evalf(1/3);
> Digits:=50;evalf(1/3);
```

```
      Maple:    sum and product

> s:=sum(x,x=1..n);
> factor(s);
> t:=sum(x^2,x=1..n);
> factor(t);
> v:=sum(x^3,x=1..n);
> factor(v);
> product(x,x=1..10);
> w:=product(x,x=1..n);
> factor(w);
```

```
      Maple:    Trigonometry

> cos(Pi);
> sin(Pi);
> sin(Pi/4);
> tan(Pi/4);
> (cos(x))^2+(sin(x))^2;
> simplify((cos(x))^2+(sin(x))^2);
> a:=expand(sin(2x));
> combine(a);
```

```
      Maple:    Equations

> solve(x^2=4);
> solve(x^2=10);
> a:=expand((x+1)*(x^2+x+1));
> solve(a);
> isolve(a);
```

```
      Maple:    Derivatives

> diff(cos(x),x);
> diff(sin(x),x);
> diff(exp(x^2cos(x)),x);
```

```
      Maple:    Integrals

> int(cos(x),x);
> int(cos(x),x=0..Pi/2);
> int(x^2cos(x),x);
> int(x^2cos(x),x=0..Pi/2);
```

```
      Maple:    igcd

> igcd(13,10);
> igcd(15,25);
> igcd(35,42);#{what is the role of igcd(a,b)?}
```

```
      Maple:    igcdex

> igcdex(15,25,'u','v');u;v;
> 15*u+25*v;#{what is the role of igcdex?}
> igcd(151,250009);
> igcdex(151,250009,'u','v');u;v;
> 151*u+250009*v;
```

```
      Maple:    Modulo and powers

> with(numtheory):
> 10 mod 4;
> u:=7;v:=1/7 mod 10;
> u*v;
> u*v mod 10;
> 70000002^254000000;
> (70000002^254000000) mod 10;
> 70000002&^254000000 mod 10;
> modp(power(70000002, 254000000), 10);
```

1.2 Factorization and prime numbers

```
      Maple:    Factorization of polynomials

factor(x^5-1);
factor(x^12-1);
```

```
      Maple:    Factorization, details

?factor
```

```
      Maple:    Integer factorization, details

?ifactor
```

```
      Maple:    Integer factorization


ifactor(25);
ifactor(10^20-1);
```

```
      Maple:    Integer factorization, details

showstat(ifactor);
```

```
      Maple:    igcd, igcex iquo, irem

igcd(1005, 205);
igcdex(1005, 205, 'u', 'v');
u; v;
1005*u+205*v;
iquo(1005,205);
irem(1005,205);
```

```
      Maple:    Prime numbers

restart;
with(numtheory);
```

```
      Maple:    Prime numbers

nextprime(10);
nextprime(20);
prevprime(10);
prevprime(100);
isprime(12);
isprime(19);
```

```
      Maple:    Prime numbers

> restart;
> with(numtheory);
> nextprime(10);
> nextprime(20);#{what is the role of nextprime?}
> prevprime(10);
> prevprime(100);#{what is the role of prevprime?}
> isprime(12);
> isprime(19);#{what is the role of isprime?}
> ithprime(1);ithprime(2);ithprime(3);ithprime(4);ithprime(5);ithprime(6);
> ithprime(10);#{what is the role of ithprime?}
> S:=[]: for i to 100 do S:=[op(S),ithprime(i)] end do: S;
> nops(S);
> S[1];
> S[50];
> T:=[seq(ithprime(i),i=1..100)]:T;
> S-T;
> i:='i';
> sum(T[i],i=1..nops(T));
> product(T[i],i=1..nops(T));
```

1.3 Lists and arrays

```
      Maple:    Lists with brackets

> list1 := [1, 2, 3, 4, 5,99];
> list2 := [10, 20, 30, 40, 50,99];
> list1+list2;
> list1-list2;
> list1*list2;
> op(list1);
> [op(list1),op(list2)];
> nops(list1);
> [op(list1),op(list2)];
> [op(list1),1000];
> [1000, op(list1)];
> list2[1..3];
> [op(list2[1..3]),1000,op(list2[4..nops(list2)])];
> subsop(1 = a, list1);
> subsop(2 = a, list1);
> subsop(1 = NULL, list1);
> subsop(3 = NULL, list1);
```

```
      Maple:    Lists with braces

> list1 := {1, 2, 3, 4, 5,10,20};
> list2 := {10, 20, 30, 40, 50};
> list1+list2;
> list1 union list2;
> op(list1);
> {op(list1),op(list2)};
> nops(list1);
> [op(list1),op(list2)];
> list1 intersect list2;
> list1 minus {20};
> list2[1..3];
> {op(list2[1..3]),1000,op(list2[4..nops(list2)])};
> subsop(1 = a, list1);
> subsop(2 = a, list1);
> subsop(1 = NULL, list1);
> subsop(3 = NULL, list1);
```

1.4 Vectors and matrices

```
      Maple:    Modulo and power

> u := vector([1, b, c, d]);
> v := vector([1, b, c, d]);
> 2*u;
> 2*v;
> M:=matrix([[1,2],[3,4],[5,6]]);
> N:=Matrix([[1,2],[3,4],[5,6]]);
> 2*M;
> 2*N;
> M := matrix([[1, 2], [3, 4]]);
> N := matrix([[10, 20], [30, 40]]);
> multiply(M,N);
> M := Matrix([[1, 2], [3, 4]]);
> N := Matrix([[10, 20], [30, 40]]);
> multiply(M,N);
> with(LinearAlgebra);
> Multiply(M,N);
> 10*M;
> Determinant(M);
> MatrixInverse(M);
```

1.5 Procedures

```
      Maple:    If
> x:=1:y:=2:
> if (x>y) then maxi:=x else maxi:=y: end if:maxi;

> x:=5:y:=2:
> if (x>y) then maxi:=x else maxi:=y: end if:maxi;
```

```
      Maple:    Procedure with if

maxim:=proc(x,y)
    local maxi;
    if (x>y) then maxi:=x else maxi:=y:
    end if:
    return(maxi);
end proc:

maxim(10,2);
maxim(20,100);
```

```
      Maple:    Procedure

ss:=proc(n)
local i,S;
S:=0;
for i from 1 to n do
    S:=S+i^2;
end do;
return(S);
end proc:

ss(10);
ss(1000);
```

Exercice 1.5.1. 1. Copy and execute the following Maple procedure.

```
      Maple:    A procedure

count:=proc(n)
local i,S;
if n<2 then
    return( "Try n>1");
else
S:=0;
for i from 2 to n do
    if isprime(i) then
        S:=S+1;
    end if;
end do;
end if;
return S;
end proc:
```

2. Find the list of the prime numbers less than 10.
3. Execute count(10).
4. Find the list of the prime numbers less than 30.
5. Execute count(30).
6. What is the output of count(n).

Exercice 1.5.2. 1. Copy and execute the following Maple procedure.

```
      Maple:    A procedure

lprimes:=proc(n)
local i,L;
if n<2 then
    return( "Try n>1");
else
L:={};
for i from 2 to n do
    if isprime(i) then
        L:=L union {i};
    end if;
end do;
end if;
return L;
end proc:
```

2. Execute lprimes(10);
3. Execute lprimes(20);
4. What is the output of lprimes(n)?
5. Find the list of the prime numbers less than 1000.

Exercice 1.5.3. 1. Find the meaning of the following functions.

(a) nops(L)
(b) op(L)
(c) [op(L),a]
(d) [a,op(L)]
(e) op(i,L)

(f) subsop(i = a,L)

(g) subsop(1 = NULL, L)

2. What is the output of L:=lprimes(20)?

3. Find the number operands in the list L.

4. Find the second operand of the list L.

5. Add 23 at the end of the list L.

6. Add -1 at the beginning of the list L.

7. Substitute the first operand of L by 0.

Exercice 1.5.4. 1. Find the definition of **maxdigits**.

2. Execute kernelopts(maxdigits);

3. Find the number of digits of a^n with $n = 10^{10}$ and $a := 5$. Compare the result with kernelopts(maxdigits).

Chapter 2

Basic Arithmetic Algorithms

In this chapter, we describe some basic algorithms that we will use later. We will use log to indicate the logarithm in base 2 and ln for the natural logarithm.

Let a and b be positive integers. The binary representation of a is

$$a = \sum_{i=0}^{k} a_{k-i} \cdot 2^{k-i}, \quad a_i \in \{0, 1\}, \quad a_k = 1,$$

where $k = \lfloor \log_2 a \rfloor + 1$. Here, $\lfloor \log_2 a \rfloor$ is the largest integer less or equal to a.

The number of bit operations for the four basic integer operations of addition, subtraction, multiplication, and division using the classical algorithms is summarized in Table 2.1.

Operation	Notation	Complexity
Addition	$a + b$	$\mathcal{O}(\log a + \log b)$
Substraction	$a - b$	$\mathcal{O}(\log a + \log b)$
Multiplication	ab	$\mathcal{O}((\log a)(\log b))$
Division	$a = bq + r$	$\mathcal{O}((\log a)(\log b))$

Table 2.1: Complexity of basic operations.

2.1 Basic arithmetic

In algorithm analysis, it is convenient to use the $\mathcal{O}$-notation for running times of algorithms, where the involved quantities are as simple as possible.

Definition 2.1.1. For a function $f : \mathbb{N} \longrightarrow \mathbb{R}^+$, the $\mathcal{O}(f)$ is defined as

$$\mathcal{O}(f) = \left\{ g : \mathbb{N} \longrightarrow \mathbb{R}^+,\ \exists c > 0,\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geq n_0 \Longrightarrow g(n) \leq cf(n) \right\}.$$

For example, $(\log n)^4 + 10\log n + 100 \in \mathcal{O}\left((\log n)^4\right)$ since

$$(\log n)^4 + 10\log n + 100 \leq 2(\log n)^4$$

for sufficiently large n.

2.1.1 Representation in base b

To perform arithmetic operations on very large integers, it is helpful to use representations of integers in base b.

Theorem 2.1.2. *Let n and b be positive integers. Then n can be expressed in base b in the form*

$$n = \sum_{i=0}^{k-1} a_{k-1-i} b^{k-i}, \quad a_i \in \mathbb{N}, \quad 0 \leq a_i < b, \quad a_{k-1} \neq 0, \quad k = \left\lfloor \frac{\ln(n)}{\ln(b)} \right\rfloor + 1,$$

where $\lfloor x \rfloor$ is the greatest integer less than or equal to x.

Sometimes, the decomposition of n in base b is denoted $n = [a_{k-1} \dots a_0]_b$. The positive integer k is called the length of n in base b. By convention $0 = [0]_b$ in any positive base b.

Exercice 2.1.3. Suppose that $n = \sum_{i=0}^{k-1} a_{k-1-i} b^{k-i}$, $a_i \in \mathbb{N}$, $0 \leq a_i < b$, $a_{k-1} \neq 0$.

1. Show that the length of $n > 0$ in base b is $k = \left\lfloor \frac{\ln(n)}{\ln(b)} \right\rfloor + 1$ where $\lfloor x \rfloor$ is the greatest integer less than or equal to x.
2. Show that the length k of n in base b satisfies $k = \mathcal{O}(\log(n))$.
3. Prove Theorem 2.1.2 by applying successive Euclidean divisions by b.

Proof. Let k be the integer satisfying $b^{k-1} \leq n < b^k$. Then $k - 1 \leq \frac{\ln(n)}{\ln(b)} < k$ and $k - 1 = \left\lfloor \frac{\ln(n)}{\ln(b)} \right\rfloor$. Hence $k = \left\lfloor \frac{\ln(n)}{\ln(b)} \right\rfloor + 1$. Using successive Euclidean divisions, we get

$$\begin{aligned}
n &= a_{k-1} b^{k-1} + r_{k-1}, \quad r_{k-1} < b^{k-1}, \\
r_{k-1} &= a_{k-2} b^{k-2} + r_{k-2}, \quad r_{k-2} < b^{k-2}, \\
r_{k-2} &= a_{k-3} b^{k-3} + r_{k-3}, \quad r_{k-3} < b^{k-3}, \\
&\vdots = \vdots \\
r_2 &= a_1 b + r_1, \quad r_1 < b, \\
r_1 &= a_0 + r_0, \quad r_0 = 0.
\end{aligned}$$

It follows that $n = a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \ldots + a_1 b + a_0$. □

The following algorithm outputs the representation of n in base b.

Algorithm 1 Representation of n in base b

Input : Two positive integers n and b.
Output : The representation of n in base b.

If $n = 0$ **then**
  Return [0].
Else
  $k = \left\lfloor \frac{\log n}{\log b} \right\rfloor + 1$.
  $L = [\,]$.
  $q = n$.
  For i from 0 to $k-1$ **do**
    $L = L \cup \left\lfloor \frac{q}{b^{k-1-i}} \right\rfloor$ (Concatenation).
    $q = q \pmod{b^{k-1-i}}$.
  End For
End If
Return L.

Maple code 2.1.4.

```
      Maple:    Decomposition of n in base b

decomp := proc (n, b)
local k, L, q, i;
if n=0 then return [0]
else
    k := floor(ln(n)/ln(b))+1;
    L := [];
    q := n;
    for i from 0 to k-1 do
        L := [op(L), iquo(q, b^(k-1-i))];
        q := q mod  b^(k-1-i);
    end do;
end if;
return L;
end proc:
```

Exercice 2.1.5. 1. Find the decomposition of 1025 and 1023 in base 10.

2. Find the decomposition of 1025 and 1023 in base 2.

The following algorithm outputs the integer n satisfying $n = [a_{k-1} \dots a_0]_b$ using Horner's

method:

$$\begin{aligned} n &= a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \ldots + a_1 b + a_0 \\ &= b\left(a_{k-1}b^{k-2} + a_{k-2}b^{k-3} + \ldots + a_1\right) + a_0 \\ &= b\left(b\left(a_{k-1}b^{k-3} + a_{k-2}b^{k-4} + \ldots + a_2\right) + a_1\right) + a_0 \\ &= \ldots \\ &= b(b(\ldots b(b(a_{k-1}) + a_{k-2})\ldots) + a_1) + a_0. \end{aligned}$$

Algorithm 2 Composition of n in base b

Input : A positive integer b and a list $L = [a_{k-1}, \cdots, a_0]$.
Output : The integer n such that $n = [a_{k-1} \ldots a_0]_b$.

1: $k = \text{length}(L)$.
2: $n = 0$.
3: **For** i from 0 to $k-1$ **do**
4: $\quad n = bn + L[i+1]$.
5: **End For**
6: Return n.

Maple code 2.1.6.

The following Maple procedure computes the integer n given the representation of n in base b.

```
      Maple:    Composition of n in base b

comp := proc (L, b)
local k, n, i;
k:=nops(L);
n:= 0;
for i from 0 to k-1 do
    n:=b*n+L[i+1];
end do;
return n;
end proc:
```

Exercice 2.1.7.

1. Let $L_1 = [1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1]$ be the decomposition of an integer n in base 2. Find n.

2. Let $L_1 = [11, 12, 6, 1, 11, 13]$ be the decomposition of an integer n in base 16. Find n.

2.1.2 Comparison in base b

Let A and B be two positive integers with the representations in base b

$$A = [a_{k-1} \dots a_0]_b = \sum_{i=0}^{k-1} a_{k-1-i} b^{k-1-i}, \qquad B = [b_{l-1} \dots b_0]_b = \sum_{i=0}^{l-1} b_{l-1-i} b^{l-1-i}.$$

In many cases, we need to compare A and B. We can consider three cases

1. If $k > l$, then $A > B$.

2. If $k < l$, then $A < B$.

3. If $k = l$, then we must compare a_{k-i} and b_{k-i} for $i = 1, 2, \cdots$ until we find j such that $a_{k-j} \neq b_{k-j}$. Then, we distinguish two subcases

   (a) If $a_{k-j} > b_{k-j}$, then $A > B$.

   (b) If $a_{k-j} < b_{k-j}$, then $A < B$.

The following algorithm can efficiently compare A and B.

Algorithm 3 : Comparison

Input : Two lists $LA = [a_{k-1}, \cdots, a_0]_b$ and $LB = [b_{l-1}, \cdots, b_0]_b$ representing two positive integers A and B in base b.

Output : Two lists, $Lmax$ and $Lmin$ representing respectively $\max(A, B)$ and $\min(A, B)$ in base b.

1: k=length of LA.
2: l=length of LB.
3: **If** $k > l$ **then**
4: $Lmax = LA$, $Lmin = LB$.
5: **End If**
6: **If** $k < l$ **then**
7: $Lmax = LB$, $Lmin = LA$.
8: **End If**
9: **If** $k = l$ **then**
10: $i := 0$.
11: **While** $i \leq k - 1$ and $LA[i + 1] = LB[i + 1]$ **do**
12: $i := i + 1$.
13: **End While**
14: **If** $i > k - 1$ **then**
15: $Lmax = LA$, $Lmin = LB$.
16: **End If**
17: **If** $i \leq k - 1$ **then**
18: **If** $LA[i + 1] > LB[i + 1]$ **then**
19: $Lmax = LA$, $Lmin = LB$.
20: **Else**
21: $Lmax = LB$, $Lmin = LA$.
22: **End If**
23: **End If**
24: **End If**
25: Return $Lmax$, $Lmin$.

Maple code 2.1.8.

The following Maple procedure compares A and B in base b.

```
      Maple:    Comparison in base b

compare:=proc(LA, LB)
local k, l, Lmax, Lmin, i;
k:=nops(LA);
l:=nops(LB);
if l < k then
    Lmax := LA;
    Lmin := LB;
end if;
if l > k then
    Lmax := LB;
    Lmin := LA;
end if;
if k=l  then
    i:=0;
    while i<=k-1 and LA[i+1]=LB[i+1] do
            i:=i+1;
    end do;
    if  i>k-1 then
        Lmax:= LA;
        Lmin:= LB;
    end if;
    if i<=k-1 then
        if LA[i+1]>LB[i+1] then
            Lmax := LA;
            Lmin := LB;
        else
            Lmax := LB;
            Lmin := LA;
        end if;
    end if;
end if;
return Lmax, Lmin;
end proc:
```

Exercice 2.1.9. 1. Let L_1 be the decomposition of 1023 in base 2 and L_2 be the decomposition of 1025 in base 2. Compare L_1 and L_2.

2. Write a Maple procedure to compare two negative integers or a positive and a negative integer.

2.1.3 Addition in base b

Exercice 2.1.10. 1. Compute 100000×99 in base 10.

2. Compute $[b-1, b-1, b-1, b-1, b-1, b-1] - [b-1, b-1, b-1]$ in base b.

Let A and B be two positive integers with the representations in base b

$$A = [a_{k-1} \dots a_0]_b, \qquad B = [b_{l-1} \dots b_0]_b.$$

Suppose that $k > l$. Then it is possible to represent B with length k:

$$B = [b_{k-1} \dots b_0]_b, \quad b_{k-1} = b_{k-2} = \dots = b_l = 0.$$

Conversely, suppose that $k < l$. Then it is possible to represent A with length l:

$$A = [a_{l-1} \dots a_0]_b, \quad a_{l-1} = a_{l-2} = \dots = a_k = 0.$$

In the following, suppose that $k \geq l$. Then, a pseudo representation of $A + B$ in base b is

$$A + B = \sum_{i=0}^{k-1} (a_{k-1-i} + b_{k-1-i}) b^{k-1-i}.$$

This is the correct representation of $A + B$ only if $a_{k-i} + b_{k-i} < b$ for all i with $i = 0, \dots, k-1$. The correct representation of $A + B$ is obtained after the carrying process:

$$A + B = \sum_{i=0}^{h-1} c_{k-1-i} b^{k-1-i}.$$

Proposition 2.1.11. *Let $A = \sum_{i=0}^{k-1} a_{k-1-i} b^{k-1-i}$ and $B = \sum_{i=0}^{l-1} b_{l-1-i} b^{l-1-i}$ be the decomposition of A and B in base b. Suppose that $k \geq l$. Let $A + B = \sum_{i=0}^{h-1} c_{k-1-i} b^{k-1-i}$ be the decomposition of $A + B$ in base b. Let $r_{-1} = 0$, and for $i = 0, \cdots, k-1$, let r_i be the carrying value after computing $a_i + b_i + r_{i-1}$. Then*

1. *$c_i \equiv a_i + b_i + r_{i-1} \pmod{b}$,*
2. *$r_i = \left\lfloor \frac{a_i + b_i + r_{i-1}}{b} \right\rfloor$ with $0 \leq r_i \leq 1$,*
3. *length$(A + B) = k$ or length$(A + B) = k + 1$.*

Exercice 2.1.12. Prove proposition 2.1.11.

Proof. Proposition 2.1.11 can be proved by induction. Suppose that $k \geq l$. Then B can be rewritten as $B = \sum_{i=0}^{k-1} b_{l-1-i} b^{l-1-i}$ with $b_{k-1} = \ldots = b_k = 0$. Let $r_{-1} = 0$. Since $0 \leq a_0 < b$ and $0 \leq b_0 < b$, then $0 \leq a_0 + b_0 + r_{-1} < 2b$. We have $c_0 \equiv a_0 + b_0 + r_{-1} \pmod{b}$ and the carrying value is

$$r_0 = \left\lfloor \frac{a_0 + b_0 + r_{-1}}{b} \right\rfloor < 2.$$

Then $0 \leq r_0 \leq 1$. Now, suppose that $0 \leq r_{i-1} \leq 1$ for $0 \leq i$. Since $0 \leq a_i \leq b-1$ and $0 \leq b_i \leq b-1$, then $0 \leq a_i + b_i + r_{i-1} \leq 2b - 1 < 2b$. Hence, $c_i \equiv a_i + b_i + r_{i-1} \pmod{b}$ and the carrying value is

$$r_i = \left\lfloor \frac{a_i + b_i + r_{i-1}}{b} \right\rfloor < 2,$$

which implies $0 \leq r_i \leq 1$. Observe that, if $r_{k-1} = 0$, then $\text{length}(a+b) = k$, that is $h = k$, and if $r_{k-1} = 1$, then $\text{length}(a+b) = k+1$, that is $h = k+1$. □

The following algorithm outputs the representation of $A + B$ in base b.

Algorithm 4 : Addition

Input : Two lists $LA = [a_{k-1}, \cdots, a_0]_b$ and $LB = [b_{l-1}, \cdots, b_0]_b$ representing two positive integers A and B in base b.

Output : The list $LAB = [c_{h-1}, \cdots, c_0]$ that represents $A + B$ in base b.

1: $k =$ length of LA.
2: $l =$ length of LB.
3: **If** $k > l$ **then**
4: $\quad LB = [0, 0, \ldots, 0] \oplus LB$ (concatenation of $k - l$ zeros to LB).
5: **Else**
6: $\quad$ **If** $k < l$ **then**
7: $\quad\quad LA = [0, 0, \ldots, 0] \oplus LA$ (concatenation of $l - k$ zeros to LA).
8: $\quad$ **End If**
9: **End If**
10: $k = \max(k, l)$, $LAB = [\,]$, $car = 0$.
11: **For** i from 0 to $k - 1$ **do**
12: $\quad tmp = LA[i+1] + LB[i+1] + car$.
13: $\quad car = \left\lfloor \frac{tmp}{b} \right\rfloor$.
14: $\quad LAB[i+1] = tmp \pmod{b}$.
15: $\quad LAB = LAB[i+1] \oplus LAB$ (Concatenation).
16: **End For**
17: **If** $car > 0$ **then**
18: $\quad LAB = [car] \oplus LAB$ (Concatenation).
19: **End If**
20: Return LAB.

Maple code 2.1.13.

The following Maple procedure computes $A + B$ in base b.

```
      Maple:    Addition in base b

addition:=proc(LA, LB, b)
local k,  i,  LAB, l, car, tmp, La, Lb;
k:=nops(LA);
l:=nops(LB);
La := LA;
Lb := LB;
if l < k then
    for i from 1 to k-l do
        Lb := [0, op(Lb)]
    end do;
    else
        if k < l then
                for i from 1 to l-k do
                    La := [0, op(La)]
                end do;
        end if;
end if;
k := max(k, l);
LAB := [];
car := 0;
for i from 0 to k-1 do
    tmp := La[k-i]+Lb[k-i]+car;
    car := floor(tmp/b);
    LAB := [tmp mod  b, op(LAB)];
end do;
if 0 < car then
    LAB := [car, op(LAB)];
end if;
return LAB;
end proc:
```

Exercice 2.1.14. 1. Compute the decomposition $l1$ of 1023 in base 10.

2. Compute the decomposition $l2$ of 2024 in base 10.

3. Compute the decomposition $l3$ of $1023 + 2024$ in base 10.

4. Compute $l1 + l2$ in base 10 and compare with the decomposition of $1023 + 2024$ in base 10.

Proposition 2.1.15. *Let A and B be arbitrary positive integers. We can compute $A + B$ in time $O(\log A + \log B)$.*

2.1.4 Substraction in base b

Exercice 2.1.16. 1. Compute 100000×99 in base 10.

2. Compute $[1,0,0,0,0] - [b-1, b-1]$ in base b.

Let A and B be two positive integers with the representations in base b

$$A = [a_{k-1} \dots a_0]_b = \sum_{i=0}^{k-1} a_{k-1-i} b^{k-1-i}, \qquad B = [b_{l-1-i} \dots b_0]_b = \sum_{i=0}^{l-1} b_{l-1-i} b^{l-1-i},$$

where $k \geq l$. A pseudo representation of $A - B$ in base b is

$$A - B = \sum_{i=0}^{k-1} (a_{k-1-i} - b_{k-1-i}) b^{k-1-i}.$$

To be correct, the representation of $A - B$ will be obtained after the carrying process.

Proposition 2.1.17. *Let $A = \sum_{i=0}^{k-1} a_{k-1-i} b^{k-1-i}$ and $B = \sum_{i=0}^{l-1} b_{l-1-i} b^{l-1-i}$ be the decomposition of A and B in base b. Suppose that $A \geq B$. Let $A - B = \sum_{i=0}^{h-1} d_{k-1-i} b^{k-1-i}$ be the decomposition of $A - B$ in base b. Let $r_{-1} = 0$, and for $i = 0, \cdots, k-1$, let r_i be the carrying value after computing $a_i - b_i + r_{i-1}$. Then*

1. $c_i \equiv a_i - b_i + r_{i-1} \pmod{b}$,
2. $r_i = \left\lfloor \frac{a_i - b_i + r_{i-1}}{b} \right\rfloor$ *with* $-1 \leq r_i \leq 0$,
3. *length*$(A - B) \leq k$.

Exercice 2.1.18. Prove Proposition 2.1.17.

Proof. Proposition 2.1.17 can be proved by induction. Suppose that $A \geq B$ and consequently $k \geq l$. Then B can be rewritten as $B = \sum_{i=0}^{k-1} b_{l-1-i} b^{l-1-i}$ with $b_{k-1} = \ldots = b_k = 0$. Let $r_{-1} = 0$. Since $0 \leq a_0 \leq b-1$ and $0 \leq b_0 \leq b-1$, then $1-b \leq a_0 - b_0 + r_{-1} \leq b-1$. Hence

$$\frac{1}{b} - 1 \leq \frac{a_0 - b_0 + r_{-1}}{b} \leq 1 - \frac{1}{b}.$$

We have $d_0 \equiv a_0 - b_0 + r_{-1} \pmod{b}$ and the carrying value is

$$r_0 = \left\lfloor \frac{a_0 - b_0 + r_{-1}}{b} \right\rfloor \in 0, 1.$$

More precisely, we have

$$r_0 = \begin{cases} 0 & \text{if } a_0 + b_0 + r_{-1} \geq 0 \\ -1 & \text{if } a_0 + b_0 + r_{-1} < 0. \end{cases}$$

Now, suppose that $-1 \leq r_{i-1} \leq 0$ for $0 \leq i$. Since $0 \leq a_i \leq b-1$ and $0 \leq b_i \leq b-1$, we get $-b \leq a_i - b_i + r_{i-1} \leq b-1$. Then

$$-1 \leq \frac{a_i - b_i + r_{i-1}}{b} \leq 1 - \frac{1}{b}.$$

Hence, $d_i \equiv a_i - b_i + r_{i-1} \pmod{b}$ and the carrying value is

$$r_i = \left\lfloor \frac{a_i - b_i + r_{i-1}}{b} \right\rfloor \in 0, 1.$$

We have also

$$r_i = \begin{cases} 0 & \text{if } a_i - b_i + r_{i-1} \geq 0 \\ -1 & \text{if } a_i - b_i + r_{i-1} < 0. \end{cases}$$

Since $A \geq B$, let $j \in 0, \ldots, k-1$ be the smallest integer such that $a_{k-1-j} > b_{k-1-j}$. Then $a_{k-1-j} - b_{k-1-j} + r_{k-2-j} \geq 0$ and $r_{k-1-j} = 0$. Hence $\text{length}(a-b) = k - j \leq k$. □

The following algorithm enables us to efficiently compute $A - B$. Remember that $\lfloor x \rfloor$ is the greater integer less than or equal to x.

Algorithm 5 : Substraction

Input : Two lists $LA = [a_{k-1}, \cdots, a_0]$ and $LB = [b_{l-1}, \cdots, b_0]$ representing two positive integers A and B in base b.

Output : The list $LAB = [d_{h-1}, \cdots, d_0]$ that represents $A - B$ in base b.

1: $k =$ (length of LA).
2: $l =$ (length of LB).
3: **If** $k > l$ **then**
4: $\quad LB = [0, 0, \ldots, 0] \oplus LB$ (concatenation of $k - l$ zeros to LB).
5: **Else**
6: $\quad$ **If** $k < l$ **then**
7: $\quad\quad LA = [0, 0, \ldots, 0] \oplus LA$ (concatenation of $l - k$ zeros to LA).
8: $\quad$ **End If**
9: **End If**
10: $k = \max(k, l)$.
11: $LAB = [\,]$.
12: $car = 0$.
13: **For** i from 0 to $k-1$ **do**
14: $\quad tmp := LA[i] - LB[i] + car$.
15: $\quad LAB[i] = tmp \mod b$.
16: $\quad car = \left\lfloor \frac{tmp}{b} \right\rfloor$.
17: $\quad LAB = LAB[i] \oplus LAB$ (Concatenation).
18: **End For**
19: Return LAB.

Maple code 2.1.19.

The following Maple procedure computes $A - B$ in base b as well as its sign. For this procedure, we need the former procedure that compares two integers in base b, namely `compare(LA,LB,b)` which outputs $\max(LA, LB)$ and $\min(LA, LB)$ successively.

```
      Maple:    Substraction in base b

substract:=proc(LA, LB, b)
local sign, La, Lb, k, l, i, car, tmp, LAB;
La := compare(LA,LB, b)[1];
Lb := compare(LA,LB, b)[2];
if La=Lb then
    return [0];
end if;
k := nops(La);
l := nops(Lb);
if La=LA then
    sign := "+"
    else
        sign := "-";
end if;
for i from l to k-1 do
        Lb := [0, op(Lb)];
end do;
LAB := [];
car := 0;
for i from 0 to k-1 do
    tmp := La[k-i]-Lb[k-i]+car;
    car := floor(tmp/b);
    tmp := tmp mod b;
    LAB := [tmp, op(LAB)];
end do;
while LAB[1]=0 do
    LAB:=subsop(1=NULL,LAB);
end do;
return sign, LAB;
end proc:
```

Exercice 2.1.20. 1. Decompose 1023, 2024 and $1023 - 2024$ in base 2.

2. Compute $L(1023) - L(2024)$ in base 2 and compare with $L(1023 - 2024)$ in base 2.

Proposition 2.1.21. *Let A and B be arbitrary positive integers. We can compute $A - B$ in time $O(\log A + \log B)$.*

2.1.5 Multiplication in base b

Exercice 2.1.22. 1. Compute 99999×99 in base 10.

2. Compute $[b-1, b-1, b-1, b-1, b-1] \times [b-1, b-1]$ in base b.

Let A and B be positive integers with

$$A = \sum_{i=0}^{k-1} a_{k-1-i} b^{k-1-i}, \qquad B = \sum_{i=0}^{l-1} b_{l-1-i} b^{l-1-i}.$$

Exercice 2.1.23. 1. Find a formal expression for AB in terms of A and B.

2. Write a maple program to compute AB.

The algorithm for multiplying A and B can be mounted using the following observation

$$AB = \sum_{i=0}^{k+l-2} c_{k+l-1-i} b^{k+l-1-i}, \qquad c_p = \sum_{j=0}^{p} a_j b_{p-j}.$$

This will give the correct representation of AB after the carrying process. The following rule shows how to compute AB.

			b_{l-1}	b_{l-2}	$\cdots$	b_{k-1}	b_{k-2}	$\cdots$	b_3	b_2	b_1	b_0
						a_{k-1}	a_{k-2}	$\cdots$	a_3	a_2	a_1	a_0
			a_0b_{l-1}	a_0b_{l-2}	$\cdots$	a_0b_{k-1}	a_0b_{k-2}	$\cdots$	a_0b_3	a_0b_2	a_0b_1	a_0b_0
		a_1b_{l-1}	a_1b_{l-2}	$\cdots$	a_1b_{k-1}	a_1b_{k-2}	$\cdots$	a_1b_3	a_1b_2	a_1b_1	a_1b_0	
	a_2b_{l-1}	a_2b_{l-2}	$\cdots$	$\cdots$	a_2b_{k-2}	$\cdots$	$\cdots$	a_2b_2	a_2b_1	a_2b_0		
	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$			
	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$a_{k-2}b_1$	$a_{k-2}b_0$					
c_{k+l-2}	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	c_{k-1}	c_{k-2}	$\cdots$	c_3	c_2	c_1	c_0

Exercice 2.1.24. Describe the following Maple function.

Algorithm 6 : Multiplication in base b

Input : Two lists $LA = [a_{k-1}, \cdots, a_0]$ and $LB = [b_{l-1}, \cdots, b_0]$ representing two positive integers A and B in base b.

Output : The list $LAB = [c_{k+l-1}, \cdots, c_0]$ that represents AB in base b.

1: **For** i from 0 to $k + l - 1$ **do**
2: $LAB[i] = 0$.
3: **End For**
4: **For** i from 0 to $k - 1$ **do**
5: $car = 0$.
6: **For** j from 0 to $l - 1$ **do**
7: $tmp = LA[i]LB[j] + LAB[i + j] + car$.
8: $LAB[i + j] = tmp \pmod b$.
9: $car = \left\lfloor \frac{tmp}{b} \right\rfloor$.
10: **End For**
11: $LAB[l + i] = car$.
12: **End For**
13: return LAB.

```
      Maple:    Multiplication in base b

multi:= proc (LA, LB, b)
local k, l, i, c, car, j, tmp, LAB;
k := nops(LA);
l := nops(LB);
for i from 0 to k+l-1 do
    c[i] := 0
end do;
for i from 0 to k-1 do
    car := 0;
    for j from 0 to l-1 do
        tmp := LA[k-i]*LB[l-j]+c[i+j]+car;
        car := floor(tmp/b);
        c[i+j] := tmp mod b
    end do;
    c[i+l] := car
end do;
if c[k+l-1]<>0 then
    LAB := [seq(c[k+l-i], i = 1 .. k+l)];
    else LAB := [seq(c[k+l-1-i], i = 1 .. k+l-1)];
end if;
return LAB;
end proc:
```

Exercice 2.1.25. Suppose that

$$A = \sum_{i=0}^{k-1} a_{k-1-i} b^{k-1-i}, \qquad B = \sum_{i=0}^{l-1} b_{l-1-i} b^{l-1-i}.$$

1. Show that $b^{k+l-2} \leq AB \leq \left(b^k - 1\right)\left(b^l - 1\right)$.
2. Show that the length of AB in base b is $k+l-1$ or $k+l$.
3. Compute 999×999 in base 10.
4. Compute $(b-1)(b-1)(b-1) \times (b-1)(b-1)(b-1)$ in base b. Describe the carryings.

Proposition 2.1.26. *Let $A = \sum_{i=0}^{k-1} a_{k-1-i} b^{k-1-i}$ and $B = \sum_{i=0}^{l-1} b_{l-1-i} b^{l-1-i}$ be the decomposition of A and B in base b. Let $AB = \sum_{p=0}^{h-1} c_{h-1-i} b^{h-1-p}$ be the decomposition of AB in base b. Let $r_0 = 0$, and for $i = 0, \cdots, k-1$, let r_p be the carrying value after computing the pth step. Then*

1. $c_p \equiv r_p + \sum_{j=0}^{p} a_j b_{p-j}$.
2. $r_i = \left\lfloor \frac{r_{i-1} + \sum_{j=0}^{p} a_j b_{p-j}}{b} \right\rfloor$.
3. $k + l - 1 \leq length(AB) = h \leq k + l$.

Proof. Proposition 2.1.26 can be proved by induction. Similar to the product of two polynomials, we have

$$AB = a_0 b_0 + (a_0 b_1 + a_1 b_0) b + (a_0 b_2 + a_1 b_1 + a_2 b_0) b^2 + \ldots + \sum_{j=0}^{p} a_j b_{p-j} + \ldots + a_{k-1} b_{l-1}.$$

Let $r_0 = 0$. Then $c_0 \equiv a_0 b_0 + r_0 \pmod{b}$. Observe that $0 \leq a_0 b_0 + r_0 \leq (b-1)^2$. Then

$$0 \leq r_1 = \left\lfloor \frac{a_0 b_0 + r_0}{b} \right\rfloor \leq b - 2.$$

Next, we have $c_1 \equiv a_0 b_1 + a_1 b_0 + r_1$. Also, we have $0 \leq a_0 b_1 + a_1 b_0 + r_1 \leq 2(b-1)^2 + b - 2$. Then

$$0 \leq r_2 = \left\lfloor \frac{a_0 b_1 + a_1 b_0 + r_1}{b} \right\rfloor \leq 2b - 3.$$

In the third step, we get $c_2 \equiv a_0 b_2 + a_1 b_1 + a_2 b_0 + r_2 \pmod{b}$ and then

$$0 \leq r_3 = \left\lfloor \frac{a_0 b_2 + a_1 b_1 + a_2 b_0 + r_2}{b} \right\rfloor \leq 3b - 4.$$

At the pth step, we find the carried of the form $pb-(p+1)$ for $p=1,\ldots,l$. For $p=l+1,\ldots,k-l$, the carried value is the same, namely

$$0 \leq r_p \leq \left\lfloor \frac{l(b-1)^2+lb-(l+1)}{b} \right\rfloor \leq lb-(l+1).$$

For $p=k-l+1$, the carried value is

$$0 \leq r_{k-l+1} \leq \left\lfloor \frac{(l-1)(b-1)^2+lb-(l+1)}{b} \right\rfloor \leq (l-1)b-(l-1).$$

For $p=k-l+2$, the carried value is

$$0 \leq r_{k-l+2} \leq \left\lfloor \frac{(l-2)(b-1)^2+(l-1)b-(l-1)}{b} \right\rfloor \leq (l-2)b-(l-2).??$$

For $p=k-l+1,\cdots,k$, the carried value is

$$0 \leq r_p \leq (3l-p)b-(3l-p).??$$

Let h be the length of AB. We have $b^{k-1} \leq A \leq b^k-1$ and $b^{l-1} \leq A \leq b^l-1$. Then

$$b^{k+l-2} \leq AB \leq \left(b^k-1\right)\left(b^l-1\right) = \left(b^{k+l}+1-b^k-b^l\right).$$

Then $k+l-2 \leq h \leq k+l-1$. □

Proposition 2.1.27. *Let A and B be arbitrary positive integers. We can compute AB in time $O(\log A \log B)$.*

2.2 Euclidian Division and gcd

Let a and b two integers with $b \neq 0$. In this subsection, we give the definition of the Euclidean division and the greatest common divisor $\gcd(a,b)$ and the algorithm that finds $\gcd(a,b)$ efficiently.

Definition 2.2.1 (Euclidean division)**.** If a and b are integers with $b \neq 0$, then the Euclidean division of a by b consists in finding two unique integers q (the quotient) and r (the remainder) such that

$$a = bq + r, \quad \text{with} \quad |r| < |b|.$$

The remainder of the Euclidean division of a by b is denoted (a mod b).

Definition 2.2.2 (Greatest Common Divisor)**.** A positive integer d is the greatest common divisor of the integers a and b, if

1. d is a common divisor of a and b,

2. whenever $c|a$ and $c|b$, then $c|d$.

The greatest common divisor of a and b is denoted $d = \gcd(a, b)$.

The greatest common divisor of two integers a and b can be efficiently computed using the following result.

Proposition 2.2.3. *Let a and b be two positive integers. Then*

$$\gcd(a, b) = \gcd(b, (a \ mod \ b)).$$

Proof. Let $a = bq + (a \bmod b)$ be the Euclidean division of a by b. Let

$$d = \gcd(a, b) \quad \text{and} \quad d' = \gcd(b, (a \bmod b)).$$

We want to show that $d = d'$. By the definition of d, since $(a \mod b) = a - bq$, then d divides $(a \bmod b)$. Consequently, d divides $\gcd(b, (a \bmod b)) = d'$.

Conversely, since $a = bq + (a \bmod b)$, then d' divides a. Consequently, d' divides a and b and then d' divides $\gcd(b, (a \bmod b)) = d$. We then conclude that $d = d'$. □

Proposition 2.2.3 can be easily formulated in a simplest way to compute $\gcd(a, b)$.

Algorithm 7 Greatest Common Divisor

Input : Two integers a and b.
Output : $\gcd(a, b)$.

```
1: m = |a|.
2: n = |b|.
3: While n > 0 do
4:     c = (m mod n).
5:     m = n.
6:     n = c.
7: End While
8: Return m.
```

Complexity of Greatest Common Divisor: $\mathcal{O}(\log(a)\log(b))$.

Maple code 2.2.4.

```
      Maple: Greatest Common Divisor

egcd:=proc(a,b)
local m,n,c;
m:=abs(a);
n:=abs(b);
while n>0 do
    c:=m mod n;
    m:=n;
    n:=c;
od;
return(m);
end proc:
egcd(-100,420);
```

Exercice 2.2.5. Describe the following Maple procedure.

Maple code 2.2.6.

```
      Maple: Greatest Common Divisor

egcd2 := proc (a, b)
if b = 0 then return a
    else
        return egcd2(b, a mod b);
end if;
end proc:
egcd2(-100,420);
```

Let a and b two positive integers. Let $d = \gcd(a, b)$. The Euclidean algorithm applied to a and b is a repeated division process as shown in Table 2.2.

$$\begin{array}{rcll}
r_0 & = & a, & \\
r_1 & = & b, & \\
r_0 & = & r_1 q_1 + r_2, & 0 \leq r_2 < r_1, \\
r_1 & = & r_2 q_2 + r_3, & 0 \leq r_3 < r_2, \\
\vdots & & \vdots & \vdots \\
r_{i-1} & = & r_i q_i + r_{i+1}, & 0 \leq r_{i+1} < r_i. \\
\vdots & & \vdots & \vdots \\
r_{k-2} & = & r_{k-1} q_{k-1} + r_k, & 0 \leq r_k < r_{k-1}. \\
r_{k-1} & = & r_k q_k + r_{k+1}, & 0 \leq r_{k+1} < r_k.
\end{array}$$

Table 2.2: The Euclidean Algorithm.

The algorithm stops when the remainder in the division algorithm is 0. In the above representation, this corresponds to $r_k \neq 0$ and $r_{k+1} = 0$. Then $r_k = \gcd(a, b)$.

Maple code 2.2.7.

The Maple code to use for the Euclidean Algorithm could be as follows.

```
      Maple: The Euclidean Algorithm (Version 1)

ealgor:=proc(a,b)
local i;
global r,q,k;
r[0]:=a;
r[1]:=b;
i:=1;
while r[i]<>0 do
    q[i]:=iquo(r[i-1], r[i]);
    r[i+1]:=r[i-1] mod r[i];
    i:=i+1;
od;
k:=i-1;
return(k);
end proc:
ealgor(12000, 23016);
k;
R:=[seq(r[i],i=0..k+1)];
Q:=[seq(q[i],i=1..k)];
```

Exercice 2.2.8. Describe the following Maple procedure.

```
      Maple: The Euclidean Algorithm

ealgor2:=proc(a,b)
local i;
global r,q,k;
q:=[];
r:=[a,b];
i:=2;
while r[i]<>0 do
    q:=[op(q),iquo(r[i-1], r[i])]:
    r:=[op(r),r[i-1] mod r[i]]:
    i:=i+1;
od;
k:=i-1;
return(k,r[k]);
end proc:
ealgor2(12000, 23016);
k,r;q;
```

In Maple 12, the gcd of two or more integers a, b is represented by the command **igcd(a,b)**.

```
      Maple: igcd(a,b)

igcd(45,60);
```

Exercice 2.2.9. Let $\Phi = \dfrac{1+\sqrt{5}}{2}$. Show that for all $n \geq 0$, we have $\phi^n + \Phi^{n+1} = \Phi^{n+2}$.

Proposition 2.2.10. *Let a and b be positive integers. Let $(r_0, r_1, \ldots, r_k)$ be the sequence of remainders in the Euclidean algorithm. Then, for $0 \leq i \leq k$, we have*

$$\Phi^i \leq r_{k-i},$$

where $\Phi = \dfrac{1+\sqrt{5}}{2}$.

Proof. We have $\Phi^0 = 1 \leq r_k$ and $\phi < 2 \leq r_k + 1 \leq r_{k-1}$. For $i \geq 3$, suppose that

$$\Phi^{i-2} \leq r_{k-(i-2)} \quad \text{and} \quad \Phi^{i-1} \leq r_{k-(i-1)}.$$

We have

$$r_{k-i} = r_{k-(i-1)}q_{k-(i-1)} + r_{k-(i-2)} \geq r_{k-(i-1)} + r_{k-(i-2)} \geq \Phi^{i-2} + \Phi^{i-1} = \Phi^i.$$

This terminates the proof. □

As a consequence, we have the following result

Proposition 2.2.11. *Let a and b be positive integers with $a \geq b$. The Euclidean algorithm terminates after at most $1 + \frac{\log b}{\log \Phi}$ iterations where $\Phi = \dfrac{1+\sqrt{5}}{2}$.*

Proof. Using Proposition 2.2.10, we know that $\Phi^{k-1} \leq r_1 = b$. Then

$$k - 1 \leq \frac{\log b}{\log \Phi},$$

and $k \leq 1 + \frac{\log b}{\log \Phi}$. □

We give below the running time of the Euclidean algorithm.

Proposition 2.2.12. *If a and b are positive integers, then the running time of the Euclidean algorithm is $\mathcal{O}(\log(a)\log(b))$.*

Proof. The running time of the Euclidean algorithm is dominated by T where

$$T = \sum_{i=1}^{k} \log(r_i)\log(q_i) \leq \log(b) \sum_{i=1}^{k} \log(q_i).$$

We have $q_i \leq \frac{r_{i-1}}{r_i}$. Hence

$$\begin{aligned} T &\leq \log(b) \sum_{i=1}^{k} (\log(r_{i-1}) - \log(r_i)) \\ &= \log(b)\,(\log(r_0) - \log(r_k)) \\ &= \log(b)\,(\log(a) - \log(r_k))\,. \end{aligned}$$

Hence, the running time of the Euclidean algorithm is $\mathcal{O}(T) = \mathcal{O}(\log(a)\log(b))$. □

2.3 The extended Euclidean Algorithm

Let a and b two integers with $b \neq 0$. In this subsection, we present the Extended Euclidean Algorithm which is basic for many results. The algorithm finds an integral linear combination of a and b such that $ax + by = \gcd(a, b)$.

Proposition 2.3.1 (Linear Combination)**.** *If a and b are integers, then there exist integers x and y such that*

$$ax + by = \gcd(a, b).$$

Proof. If $a = 0$, then $\gcd(a, b) = b$ and $(x, y) = (0, 1)$ satisfies $ax + by = b = \gcd(a, b)$. If $b = 0$, then $\gcd(a, b) = a$ and $(x, y) = (1, 0)$ satisfies $ax + by = a = \gcd(a, b)$.. In the following, suppose that $ab \neq 0$. Let $(r_0, r_1, \ldots, r_{k+1})$ be the sequence of remainders defined by the Euclidean algorithm as shown in Table 2.2. Define integers $x_0, x_1, \ldots x_{k+1}$ and $y_0, y_1, \ldots y_{k+1}$ by

$$\begin{aligned} x_0 = 1, \quad x_1 = 0, \quad x_{i+1} = x_{i-1} - x_i q_i, \quad i = 1, \cdots k, \\ y_0 = 0, \quad y_1 = 1, \quad y_{i+1} = y_{i-1} - y_i q_i, \quad i = 1, \cdots k. \end{aligned}$$

It is obvious that $ax_0 + by_0 = r_0$ and $ax_1 + by_1 = r_1$. Suppose that $ax_{i-1} + by_{i-1} = r_{i-1}$ and $ax_i + by_i = r_i$. Then

$$\begin{aligned} ax_{i+1} + by_{i+1} &= a(x_{i-1} - x_i q_i) + b(y_{i-1} - y_i q_i) \\ &= ax_{i-1} + by_{i-1} - q_i(ax_i + by_i) \\ &= r_{i-1} - q_i r_i \\ &= r_{i+1}. \end{aligned}$$

Hence $ax_i + by_i = r_i$ for each i and for $i = k$, we get

$$ax_k + by_k = r_k = \gcd(a, b).$$

It follows that a solution to the equation $ax + by = \gcd(a, b)$ is (x_k, y_k). □

Proposition 2.3.1 can be easily formulated in a simplest way to compute $\gcd(a, b)$.

Algorithm 8 The Extended Euclidean Algorithm

Input : Two integers a and b.
Output : Three integers x, y and $\gcd(a, b)$ such that $ax + by = \gcd(a, b)$.

1: $x_0 = 1$, $x_1 = 0$.
2: $y_0 = 0$, $y_1 = 1$.
3: $r_0 = a$, $r_1 = b$.
4: $i = 1$.
5: **While** $r_i > 0$ **do**
6: $\quad q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$.
7: $\quad r_{i+1} = r_{i-1} - q_i r_i$.
8: $\quad x_{i+1} = x_{i-1} - x_i q_i$.
9: $\quad y_{i+1} = y_{i-1} - y_i q_i$.
10: $\quad i = i + 1$.
11: **End While**
12: $k = i - 1$.
13: Return $x[k], y[k], r[k]$.

Complexity of Greatest Common Divisor: $\mathcal{O}(\log(a)\log(b))$.

Maple code 2.3.2.

```
      Maple: The Extended Euclidean Algorithm

exgcd:=proc (a, b)
local i;
global r,q,k,x,y;
q:=[]; r:=[a,b];
x:=[1,0];
y:=[0,1];
i:=2;
while r[i]<>0 do
    q:=[op(q),iquo(r[i-1], r[i])];
    r:=[op(r),r[i-1] mod r[i]];
    x:=[op(x),x[i-1]-x[i]*q[i-1]];
    y:=[op(y),y[i-1]-y[i]*q[i-1]];
    i:=i+1
end do;
k:=i-1;
return x[k], y[k], r[k]:
end proc:
aa:=12570;
bb:=450;
l:=[exgcd(aa,bb)];
aa*l[1]+bb*l[2]=l[3];
```

In Maple 12, the extended gcd of two integers a, b is represented by the command **igcdex(a,b,'u','v')**.

```
      Maple: The Extended Euclidean Algorithm

aa:=12570;
bb:=450;
igcdex(aa,bb,'u','v');
aa*u+bb*v=igcd(aa,bb);
```

2.4 The Modular Exponentiation

Let a, m and n be positive integers. A practical concern in implementing many cryptographic protocols is the computation of the modular exponentiation $a^m \pmod n$. It can be performed efficiently with the repeated square-and-multiply algorithm. Let the binary

representation of m be

$$m = \sum_{i=0}^{k} m_i 2^i, \quad m_i \in \{0, 1\},$$

where $k = \lfloor \log m \rfloor$. Then

$$\begin{aligned} a^m &= \left(a^{2^k}\right)^{m_k} \cdot \left(a^{2^{k-1}}\right)^{m_{k-1}} \cdots \left(a^{2^1}\right)^{m_1} \cdot \left(a^{2^0}\right)^{m_0}, \\ a^m &= \left(\left(\left((a^{m_k})^2 \cdot a^{m_{k-1}}\right)^2 \cdot a^{m_{k-2}}\right)^2 \cdots a^{m_1}\right)^2 \cdot a^{m_0}. \end{aligned}$$

For example, for $m = 100_{10} = 1100100_2$, we get

$$a^m \equiv \left(\left(\left(\left(\left((a)^2 \cdot a\right)^2\right)^2 \cdot a\right)^2\right)^2\right)^2,$$

which gives rise to the sequence of exponents $2, 3, 6, 12, 24, 25, 50, 100$. From the above formulations, we deduce the repeated square-and-multiply algorithm for modular exponentiation. A direct consequence is that calculating $a^m \pmod n$ takes $O(\log m)$ multiplications.

Algorithm 9 Modular Exponentiation from left to right

Input : Integers a, m and n.
Output : The modular exponentiation $b \equiv a^m \pmod n$.

1: **If** $a \pmod n = 0$ **then**
2: $b = 0$.
3: **Else If** m=0 **then**
4: $b = 1$.
5: **Else**
6: Decompose $m = \sum_{i=0}^{k} m_{k-i} 2^{k-i}, \quad m_{k-i} \in \{0, 1\}$.
7: $b = a$.
8: **For** i from $k - 1$ downto 1 **do**
9: $b = b^2 \pmod n$,
10: **If** $m_i = 1$ **then**
11: $b \equiv ba \pmod n$
12: **End If**
13: **End For**
14: Return b.
15: **End If**

Maple code 2.4.1.

```
      Maple: The modular exponentiation

exponent:=proc (a,m,n)
local i,M,b,k;
if (a mod n)=0 then
    return 0;
    else
    if m=0 then
        return 1;
        else
            M:=decomp(m,2);
            b:=a;
            k:=trunc(ln(m)/ln(2))+1;
            for i from 2 to k do
                b:=b^2 mod n;
                if M[i]=1 then
                    b:=b*a mod n;
                end if;
            end do;
    end if;
end if;
return b;
end proc:
aa:=57;
mm:=1024;
nn:=212781;
exponent(aa,mm,nn);
```

Here is another Maple function that computes the modular exponentiation.

Algorithm 10 Modular Exponentiation

Input : Integers a, m and n.

Output : The modular exponentiation $b \equiv a^m \pmod{n}$.

```
1: If a (mod n) = 0 then
2:     b = 0.
3: Else If m=0 then
4:     b = 1.
5: Else
6:     b = 1.
7:     s = a.
8:     u = m.
9:     While u > 0 do
10:        If u (mod n) = 1 then
11:            b = bs (mod n).
12:        End If
13:        s = s^2 (mod n).
14:        u = ⌊u/2⌋.
15:    End While
16:    Return b.
17: End If
```

Complexity of Modular Exponentiation: $\mathcal{O}(\log m)$**.**

Maple code 2.4.2.

```
      Maple: Modular Exponentiation

modexp:=proc(a, m, n)
local s,b,u;
if (a mod n)=0 then
    b:=0;
    else if m=0 then
            b:=1;
            else
            b:=1;s:=a;u:=m;
            while u>0 do
                if u mod 2=1 then b:=b*s mod n;
                fi;
                s:=s*s mod n;
                u:=trunc(u/2);
            od;
        fi;
fi;
return(b);
end proc:
```

Example 2.4.3.

Let $a = 17$, $m = 200$ and $n = 230$. Then performing **modexp(a,m,n)**, we get $17^{200} \equiv 151 \pmod 2)30$.

Maple code 2.4.4.

In Maple 12, the modular exponentiation $a^m \pmod n$ is represented by

Power(a,m) mod n or by the expression

`a&^m mod n.`

```
      Maple: Power(a,m) mod n

aa := 457;
mm := 77;
nn := 212781;
exponent(aa, mm, nn);
aa^mm mod  nn;
`mod`(aa^mm, nn);
aa&^mm mod nn;
mod(`&^`(aa, mm), nn)
Power(aa,mm) mod nn;
```

```
      Maple: Power(a,m) mod n, a large example

aa := 457;
mm := 7000000007;
nn := 212781;
exponent(aa, mm, nn);
aa^mm mod  nn;
`mod`(aa^mm, nn);
aa&^mm mod nn;
mod(`&^`(aa, mm), nn)
Power(aa,mm) mod nn;
```

2.5 Euler's Totient Function

Definition 2.5.1. For a positive integer n, the Euler ϕ function is defined by

$$\phi(n) = \#\left\{a \in \mathbb{N} : 1 \leq a < n, \gcd(a,n) = 1\right\}.$$

Exercice 2.5.2.

1. Compute $\phi(p)$.
2. Compute $\phi(p^2)$.
3. Compute $\phi(5^7)$.
4. Compute $\phi(p^k)$.

Corollary 2.5.3. *If p is a prime number and $k \geq 1$, then $\phi(p^k) = p^{k-1}(p-1)$.*

Proof. We have

$$\begin{aligned}
\phi(p^k) &= \#\left\{a \in \mathbb{N} : 1 \leq a < p^k, \gcd(a,p) = 1\right\} \\
&= p^k - \#\left\{a \in \mathbb{N} : 1 \leq a \leq p^k, \gcd(a,p) = p\right\} \\
&= p^k - \#\left\{a \in \mathbb{N} : 1 \leq a \leq p^k, p|a\right\} \\
&= p^k - \#\left\{p, 2p, \ldots, p^k\right\} \\
&= p^k - p^{k-1} \\
&= p^{k-1}(p-1).
\end{aligned}$$

□

An important property of the Euler ϕ function is the multiplication.

Theorem 2.5.4. *For a positive integer $n = n_1 n_2 \ldots n_k$ where $\gcd(n_i, n_j) = 1$, the Euler ϕ function of n satisfies*

$$\phi(n) = \phi(n_1)\phi(n_2)\ldots\phi(n_k).$$

Proof. Apply the Chinese Theorem. □

Maple code 2.5.5.

In Maple, the Euler Totient function is simply

phi(n) .

Beware, to compute $phi(n)$, maple needs to factor n.

```
      Maple: Euler totient function

aa:=2^300*3^200;
phi(aa);

aa:=nextprime(2^300)*nextprime(3^200);
phi(aa);
```

2.6 Generators in $(\mathbb{Z}/p\mathbb{Z})^*$

Exercice 2.6.1. Let $p = 31$.

1. Let $a = 2$. Find the smallest integer $k > 0$ such that $a^k \equiv 1 \pmod{p}$.
2. Let $a = 3$. Find the smallest integer $k > 0$ such that $a^k \equiv 1 \pmod{p}$.
3. Let $a = 5$. Find the smallest integer $k > 0$ such that $a^k \equiv 1 \pmod{p}$.
4. Let $a = 26$. Find the smallest integer $k > 0$ such that $a^k \equiv 1 \pmod{p}$.
5. Give the list of (a, k) where for each $a = 2, \ldots, p-1$, k is the smallest integer such that $a^k \equiv 1 \pmod{p}$.

Maple code 2.6.2. Maple: p=31

```
p:=31;
L := [];
for a from 2 to p-1 do
    i := 1;
    while power(a, i)  mod p <> 1 do
        i := i+1;
    end do;
    L := [op(L), [a, i]];
end do:
L;
```

Definition 2.6.3 (The order of an element)**.** Let a, n be positive integers such that $\gcd(a,n)=1$. The order of a modulo n, denoted $\mathrm{ord}_n(a)$, is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$, that is

$$\mathrm{ord}_n(a) = \min\{k \in \mathbb{N}, a^k \equiv 1 \pmod{n}\}.$$

Theorem 2.6.4. *Let a, n be positive integers such that $\gcd(a,n)=1$. If $a^k \equiv 1 \pmod{n}$, then $ord_n(a)|k$.*

Proof. Let $k \in \mathbb{N}$ such that $\mathrm{ord}_n(a)|k$. Then $k = q \cdot \mathrm{ord}_n(a)$ for some integer q. Then

$$a^k \equiv a^{q\cdot \mathrm{ord}_n(a)} \equiv \left(a^{\mathrm{ord}_n(a)}\right)^q \equiv 1 \pmod{n}.$$

Conversely, suppose that $a^k \equiv 1 \pmod{n}$. Let $k = q \cdot \mathrm{ord}_n(a) + r$ be the Euclidean division of k by $\mathrm{ord}_n(a)$ with $0 \leq r < \mathrm{ord}_n(a)$. Then

$$1 \equiv a^k \equiv a^{q\cdot \mathrm{ord}_n(a)+r} \equiv \left(a^{\mathrm{ord}_n(a)}\right)^q \times a^r \equiv a^r \pmod{n}.$$

Since $\mathrm{ord}_n(a)$ is the smallest positive integer such that $a^{\mathrm{ord}_n(a)} \equiv 1 \pmod{n}$, then $r=0$. This implies that $k = q \cdot \mathrm{ord}_n(a)$ and $\mathrm{ord}_n(a)|k$. □

The former result leads to the following one.

Theorem 2.6.5. *Let a, n be positive integers such that $\gcd(a,n)=1$. Then $ord_n(a)|\phi(n)$.*

Proof. From Euler's theorem, we know that $a^{\phi(n)} \equiv 1 \pmod{n}$ whenever $\gcd(a,n)=1$. Hence, by Theorem 2.6.4, $\mathrm{ord}_n(a)|\phi(n)$. □

The following result is important for finding generators in $\mathbb{Z}^*/p\mathbb{Z}$.

Theorem 2.6.6 (Primitive Root Theorem)**.** *Let a, n be positive integers such that $\gcd(a,n) = 1$. The integers*

$$a, a^2, \ldots, a^{ord_n(a)},$$

are pairwise incongruent modulo n.

Proof. Let h and k be integers such that $1 \leq h,k \leq \mathrm{ord}_n(a)$ and $a^h \equiv a^k \pmod{n}$. Then $a^{h-k} \equiv 1 \pmod{n}$. By Theorem 2.6.4, $\mathrm{ord}_n(a)|(h-k)$. On the other hand, we have $|h-k| < \mathrm{ord}_n(a)$. Hence $h-k=0$ and $h=k$. □

Theorem 2.6.7. *Let a, n be positive integers such that $\gcd(a,n) = 1$ with the prime factorization $\phi(n) = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$. Then there exist integers $v_1, v_2, \ldots, v_k$ such that $ord_n(a) = p_1^{v_1}p_2^{v_2}\cdots p_k^{v_k}$. Moreover, for $i = 1, 2, \ldots k$, if $v_i \geq 1$, then $a^{p_1^{v_1}\cdots p_i^{v_i-1}\cdots p_k^{v_k}} \not\equiv 1 \pmod{n}$.*

Proof. Assume that $\gcd(a, n) = 1$. Consider the prime factorization $\phi(n) = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. From Theorem 2.6.5, we know that $\mathrm{ord}_n(a) | \phi(n)$. Hence $\mathrm{ord}_n(a) = p_1^{v_1} p_2^{v_2} \cdots p_k^{v_k}$ for some integers $v_1, v_2 \ldots v_k$. Assume that $v_i \geq 1$. Then, since $p_i | \mathrm{ord}_n(a)$, then $\frac{\mathrm{ord}_n(a)}{p_i}$ is an integer and $a^{\frac{\mathrm{ord}_n(a)}{p_i}} \not\equiv 1 \pmod{n}$. Hence, for all i with $v_i \geq 1$, we have $a^{p_1^{v_1} \cdots p_i^{v_i - 1} \cdots p_k^{v_k}} \not\equiv 1 \pmod{n}$. □

Exercice 2.6.8. Find a prime number p of the form $p = 2p_1p_2p_3 + 1$ where p_1, p_2, p_3 are prime numbers with $2^{10} < p_i < 2^{11}$.

Maple code 2.6.9.

```
      Maple: p=p_1p_2p_3+1

premier:=proc(n)
local p1,p2,p3,b1,b2,p;
b1:=2^n;
b2:=2^(n+1);
p1:=nextprime(rand(b1..b2)());
p2:=nextprime(rand(b1..b2)());
p3:=nextprime(rand(b1..b2)());
p:=2*p1*p2*p3+1;
while isprime(p)=false or p1>b2 or p2>b2 or p3>b2 do
    p1:=nextprime(rand(b1..b2)());
    p2:=nextprime(rand(b1..b2)());
    p3:=nextprime(rand(b1..b2)());
    p:=2*p1*p2*p3+1;
end do;
return p,p1,p2,p3;
end proc:
```

The following algorithm is an efficient way to find the order of an element a using the factorization of $\phi(n)$.

Algorithm 11 The order of an element

Input : Integers a, n and the factorization $\phi(n) = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$.
Output : The order of a modulo n.

1: $w = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$.
2: **For** i from 1 to k **do**
3: $\quad w = \frac{w}{p_i^{n_i}}$.
4: $\quad b \equiv a^w \pmod{n}$.
5: $\quad$ **While** $b \neq 1$ **do**
6: $\quad\quad b \equiv b^{p_i} \pmod{n}$.
7: $\quad\quad w = wp_i$.
8: $\quad$ **End While**
9: **End For**
10: Return w.

Maple code 2.6.10.

```
      Maple: The order of an element

myorder:=proc(a, n)
local i,w,b,p,v,fn,k;
if gcd(a,n)<>1 then
    return(not coprime);
fi;
w:=phi(n);
fn:=ifactors(w)[2];
k:=nops(fn);
for i from 1 to k do
    p:=fn[i][1];
    v:=fn[i][2];
    w:=w/p^v;
    b:=Power(a,w) mod n;
    while b<>1 do
        b:=Power(b,p) mod n;
        w:=w*p;
    od;
od;
return(w);
end proc:
```

Example 2.6.11.

```
      Maple: The order of an element

aa:=2;
nn:=2^5*3^6*5^8*7^4;
mm:=myorder(aa,nn);

aa:=11;
nn:=2^5*3^6*5^8*7^4;
mm:=myorder(aa,nn);
aa&^mm mod nn;
```

Maple code 2.6.12.

In Maple 12, the order of a modulo n can be computed using

order(a,n).

Exercice 2.6.13. 1. Find the order of 2 modulo $2^{100}+1$.

2. Find the order of 2 modulo the smallest prime number p grather than $2^{100}+1$.

Definition 2.6.14 (Primitive Root)**.** Let a and n be positive integers such that $\gcd(a,n)=1$. If the order of a modulo n is $\mathrm{ord}_n(a)=\phi(n)$, then a is called a primitive root of the integer n.

Theorem 2.6.15 (Primitive roots and reduced systems of residues)**.** *Let n be a positive integers and a a primitive root modulo n. Define the set*

$$S=\left\{a,a^2,\ldots,a^{\phi(n)}\right\},$$

Then the set S is a system of reduced residues modulo n, that is, the integers in S are pairwise incongruent modulo n and every integer b with $\gcd(n,b)=1$ is congruent modulo n to an element in S.

Proof. Let h and k be integers such that $1\leq h,k\leq\phi(n)$ and $a^h\equiv a^k \pmod n$. Then $a^{h-k}\equiv 1 \pmod n$. By Theorem 2.6.4, we get $\phi(n)|(h-k)$. On the other hand, we have $|h-k|<\phi(n)$. Hence $h-k=0$ and $h=k$. Hence the integers in S are pairwise incongruent modulo n. Consequently, S has exactly $\phi(n)$ different elements. Observe that since $\gcd(n,a)=1$, then for $k\geq 1$, $\gcd\left(n,a^k\right)=1$. Since there are exactly $\phi(n)$ different integers that are coprime to n, then if b is an integer with $\gcd(n,b)=1$, then $b\equiv a^k$ for some integer k with $1\leq k\leq\phi(n)$. □

Example 2.6.16.

Let $p=11$. Then

$$\mathbb{Z}_{11}^*=\{1,2,3,\ldots,10\}=\left\{1,2,2^2,\ldots,2^9\right\}.$$

Theorem 2.6.17. *Let a, n be positive integers such that $\gcd(a,n)=1$. Then for $k\in\mathbb{N}^*$,*

$$ord_n\left(a^k\right)=\frac{ord_n(a)}{\gcd(k,\,ord_n(a))}.$$

Proof. Suppose $\gcd(a,n)=1$. Then for $k\geq 1$, $\gcd\left(a^k,n\right)=1$. Let $h=\mathrm{ord}_n\left(a^k\right)$. Then h is the smallest positive integer such that

$$\left(a^k\right)^h\equiv a^{kh}\equiv 1 \pmod n.$$

Then, by Theorem 2.6.4, $\mathrm{ord}_n(a)|kh$ and $kh=q\cdot\mathrm{ord}_n(a)$ for some integer q. Hence

$$h=\frac{q\cdot\mathrm{ord}_n(a)}{k}=\frac{\mathrm{ord}_n(a)}{\gcd(k,\mathrm{ord}_n(a))}\cdot\frac{q\cdot\gcd(k,\mathrm{ord}_n(a))}{k}.$$

It follows that the smallest integer h satisfying this equality is

$$h=\mathrm{ord}_n\left(a^k\right)=\frac{\mathrm{ord}_n(a)}{\gcd(k,\mathrm{ord}_n(a))}.$$

□

Corollary 2.6.18. *Let a, n be positive integers such that $\gcd(a, n) = 1$. If a is a primitive root modulo n, then a^k is a primitive root modulo n if and only if $\gcd(k, \phi(n)) = 1$.*

Proof. Let a be a primitive root modulo n with $\text{ord}_n(a) = \phi(n)$. For $k \geq 1$, suppose that a^k is a primitive root modulo n, that is $\text{ord}_n\left(a^k\right) = \phi(n)$. Then, by Theorem 2.6.17, the integer k satisfies

$$\phi(n) = \frac{\phi(n)}{\gcd(k, \phi(n))}.$$

Hence $\gcd(k, \phi(n)) = 1$. Conversely, suppose that $\gcd(k, \phi(n) = 1$. Then, by Theorem 2.6.17 again, we get for $k \geq 1$,

$$\text{ord}_n\left(a^k\right) = \frac{\phi(n)}{\gcd(k, \phi(n))} = \phi(n).$$

Hence a^k is a primitive root modulo n. □

Theorem 2.6.19. *Let n be a positive integer. If n has a primitive root, then it has exactly $\phi(\phi(n))$ incongruent primitive roots.*

Proof. Suppose that n has a primitive root a. Let b be another primitive root modulo n. By Theorem 2.6.15 and Theorem 2.6.18, b is in the form $b \equiv a^k$ where $1 \leq k \leq \phi(n)$ and $\gcd(k, \phi(n)) = 1$. Since there are $\phi(\phi(n))$ such integers, then there are exactly $\phi(\phi(n))$ incongruent primitive roots modulo n. □

Theorem 2.6.20 (Existence of Primitive Roots)**.** *Let n be a positive integer. There exists a primitive root modulo n if and only if n has one of the following forms:*

1. *$n = 1, 2, 4$.*

2. *$n = p^m$, where p is an odd prime and $m \in \mathbb{N}$.*

3. *$n = 2p^m$, where p is an odd prime and $m \in \mathbb{N}$.*

The following algorithm is an efficient way to find the least primitive root a using the factorization of $\phi(n)$.

Algorithm 12 Finding a Primitive Root

Input : Integer n and the factorization $\phi(n) = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$.
Output : A primitive root a modulo n.

$w = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$.
$a = 1$.
$b = 1$.
While $b = 1$ **do**
    $a = a + 1$.
    For i from 1 to k **do**
        $b \equiv a^{w/p_i} \pmod{n}$.
        If $b = 1$ **then**
            $i := k + 1$.
        End If
    End For
End While
Return a.

Maple code 2.6.21.

```
      Maple: Finding a Primitive Root

myprimroot:=proc(n)
local a,w,i,b,p,v,fn,k;
w:=phi(n);
fn:=ifactors(w)[2];
k:=nops(fn);
a:=1;
b:=1;
while (b=1) do
    a:=a+1;
    for i from 1 to k do
        p:=fn[i][1];
        v:=fn[i][2];
        b:=Power(a,w/p) mod n;
        if (b=1) then
            i:=k+1;
        fi;
    od;
od;
return(a);
end proc:
```

Example 2.6.22.

```
      Maple: Finding a Primitive Root, examples

nn:=13;
myprimroot(nn);

nn:=17;
myprimroot(nn);

nn:=41;
myprimroot(nn);

nn:=40487^2;
myprimroot(nn);
```

Maple code 2.6.23.

In Maple 12, the smallest primitive root modulo n can be computed using

primroot(n) .

```
      Maple: Finding a Primitive Root, examples

nn:=41;
primroot(nn);

nn:=40487^2;
myprimroot(nn);
```

Theorem 2.6.24. *Let n be a positive integer. If $n = 4p + 1$ for some odd prime p, then 2 is a primitive root modulo n.*

Corollary 2.6.25. *Let p be a prime number. Then there are $\phi(p-1)$ generators of $\mathbb{Z}_p^*$ where ϕ is the Euler totient function*

$$\phi\left(p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}\right) = p_1^{n_1-1}p_2^{n_2-1}\dots p_k^{n_k-1}(p_1-1)(p_2-1)\dots(p_k-1).$$

Example 2.6.26.

Let $p = 11$. Then the set of generators of $\mathbb{Z}_{11}^*$ is $\{2, 6, 7, 8\}$. On the other hand, $\phi(p-1) = \phi(10) = \phi(2 \cdot 5) = 4$.

An interesting problem is to find an element of maximum order modulo $n = pq$ where p and q are large primes.

Corollary 2.6.27. *Let $n = pq$ be the product of two primes. Then $\mathbb{Z}_n^*$ is a non cyclic group of order $\phi(n) = (p-1)(q-1)$ and the maximum order of an element is $lcm(p-1, q-1)$.*

2.7 Square roots in $(\mathbb{Z}/p\mathbb{Z})^*$

Let p be a prime number and $a \in (\mathbb{Z}/p\mathbb{Z})^*$. The following algorithm computes a square x of a, that is finds an integer x such that $x^2 \equiv a \pmod{p}$.

Algorithm 13 Finding a Square Root

Input : Prime integer p and $a \in (\mathbb{Z}/p\mathbb{Z})^*$.
Output : A square root x of a modulo p satisfying $x^2 \equiv a \pmod{p}$.

1: Choose $g \in (\mathbb{Z}/p\mathbb{Z})^*$ such that g is not a quadratic residue modulo p, that is Legendre$(g, p) = -1$.
2: Decompose $p - 1 = 2^s t$ with odd t.
3: $e = 0$.
4: **For** i from 2 to s **do**
5: $\quad c \equiv (ag^{-e})^{(q-1)/2^i} \pmod{p}$
6: $\quad$ **If** $c \neq 1$ **then**
7: $\quad\quad e \equiv e + 2^{i-1} \pmod{p}$.
8: $\quad$ **End If**
9: **End For**
10: $d \equiv ag^{-e} \pmod{p}$.
11: $x \equiv g^{e/2} d^{(t+1)/2} \pmod{p}$.
12: Return x.

Maple code 2.7.1.

```
      Maple: Finding a square Root

with(numtheory):
mysqrroot:=proc(p,a)
local s,t,c,d,x,q,e,g,i;
g:=rand(2..p-1)();
while legendre(g,p)=1 do
    g:=rand(2..p-1)();
end do;
s:=0;
d:=p-1;
while d mod 2=0 do
    s:=s+1;
    d:=d/2;
end do;
t:=(p-1)/2^s;
e:=0;
for i from 2 to s do
    c:=a*power(g,-e) mod p;
    c:=power(c,(p-1)/2^i) mod p;
    if c<>1 then
        e:=e+power(2,(i-1)) mod p;
    end if;
end do;
d:=a*power(g,-e) mod p;
x:=(power(g,e/2) mod p)*(power(d,(t+1)/2) mod p) mod p;
return x;
end proc:
```

Example 2.7.2.

```
      Maple: Finding a Primitive Root, examples

pp:=13;aa:=12;
mysqrroot(pp,aa);
```

Corollary 2.7.3. *Let $p \equiv 3$ be prime and a a quadratic residue modulo p. Then the soloution of the equation $x^2 \equiv a \pmod{p}$ are $\pm a^{\frac{p+1}{4}}$.*

Proof. Suppose $a \equiv b^2 \pmod{p}$. Then

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv b^{p+1} \equiv b^2 \equiv a \pmod{p}.$$

The computation of a solution can be done in $\mathcal{O}(\log(p))$. □

http://stanford.edu/~jbooher/expos/sqr_qnr.pdf

Chapter 3

Tests de Primalité

3.1 Nombres premiers

Definition 3.1.1. Un entier p est nombre premier s'il n'est divisible que par 1 et par lui même.

Definition 3.1.2. On dit que deux nombres premiers p et q sont jumeaux si $|p-q|=2$.

Exercice 3.1.3.
1. Ecrire une procédure Maple qui détermine tous les nombres premiers impairs jumeaux dans un intervalle $[a, b]$.
2. Déterminer tous les nombres premiers jumeaux inférieurs à 200.
3. Déterminer tous les nombres premiers jumeaux de l'intervalle [300, 400].

Maple code 3.1.4.

```
      Nombres premiers impairs jumeaux

jum:=proc (a, b)
local ca, i, p1, p2;
if type(a, even) then ca := a+1 else ca := a end if;
p1 := isprime(ca);
for i from ca by 2 to b-2 do
    p2 := isprime(i+2);
    if p1 and p2 then lprint(i, i+2) end if;
    p1 := p2;
end do;
end proc:
```

Definition 3.1.5. On dit qu'un nombre premier p est isolé si $p-2$ et $p+2$ sont composés .

Exercice 3.1.6. 1. Ecrire une procédure Maple qui détermine tous les nombres premiers impairs isolés dans un intervalle $[a, b]$.

2. Déterminer tous les nombres premiers impairs isolés inférieurs à 200.

3. Déterminer tous les nombres premiers impairs isolés de l'intervalle [300, 400].

Maple code 3.1.7.

```
      Nombres premiers impairs isolés

isole := proc (a, b)
local ca, i, p1, p2, p3;
if type(a, even) then ca := a+1 else ca := a end if;
p1 := isprime(a);
for i from ca by 2 to b do
    p2 := isprime(i-2);
    p3 := isprime(i+2);
    if p1 and not p2 and not p3 then lprint(i) end if;
    p1 := p3;
end do;
end proc:
```

It is commonly suggested hat an RSA modulus $N = pq$ should be built using the so-called strong primes. An obvious reason is that strong primes have certain properties that make N hard to factor by specific factoring algorithms.

Definition 3.1.8. A prime number p is strong if the following conditions are satisfied

1. p is large.

2. $p - 1$ has a large prime factor. That is, $p = a_1 p_1 + 1$ for some integer a_1 and large prime p_1.

3. $p_1 - 1$ has a large prime factor. That is, $p_1 = a_2 p_2 + 1$ for some integer a_2 and large prime p_2.

4. $p+1$ has a large prime factor. That is, $p = b_1 q_1 - 1$ for some integer b_1 and large prime q_1.

Practical experiments have showed that strong primes are quite rare but easy to generate. A typical method to generate strong primes was proposed in 1979 by Williams and Schmid.

1. Choose a large prime p_2.

2. Choose a large prime q_1.

3. Compute $r \equiv -p_2^{-1} \pmod{q_1}$.

4. Find the least a such that $p_1 = 4ap_2q_1 + 4rp_2 + 3$ and $p = 2p_1 + 1$ are both prime.

Let p be a prime generated using the method of Williams and Schmid. Then, p satisfies the properties of a strong prime.

1. $rp_2 + 1 = q_1m$ for some m.

2. p is large.

3. $p - 1 = 2p_1$ where p_1 is a large prime factor.

4. $p_1 - 1 = 2(aq_1 + 2r)p_2$ where p_2 is a large prime factor.

5. $p + 1$ satisfies

$$p + 1 = 2p_1 + 2 = 8ap_2q_1 + 8rp_2 + 8 = 8ap_2q_1 + 8q_1m = 8(ap_2 + m)q_1,$$

where q_2 is a large prime factor.

This method can be easily implemented using Maple. It produces a strong prime p where p_2 and q_1 are k-bit prime.

Maple code 3.1.9.

```
    Maple:  Generation of strong primes

strongprime:=proc(k)
local m1,m2,p2,q1,r,a,p1,p;
m1:=2^(k-1);
m2:=2^(k);
p2:=nextprime(rand(m1..m2)());
q1:=nextprime(rand(m1..m2)());
r:=-1/p2 mod q1;
a:=1;
p1:=4*a*p2*q1+4*r*p2+3;
p:=2*p1+1;
while not(isprime(p1)) or not(isprime(p)) do
    a:=a+1;
    p1:=4*a*p2*q1+4*r*p2+3;
    p:=2*p1+1;
od;
return p;
end proc:
```

Example: Let $k = 20$. Then the former procedure outputs the prime number $p = 240733732119527$ which satisfies:

1. $p \approx 2^{47}$.

2. $p - 1 = 2p_1 = 2 \cdot 120366866059763$.

3. $p_1 - 1 = 2 \cdot 7 \cdot 8597633289983$.

4. $p + 1 = 2^3 \cdot 3 \cdot 604243 \cdot 16600229$.

Exercice 3.1.10. 1. Find a strong prime of 100 bits.

2. Find an RSA modulus with strong prime factors of size 50 bits each.

3.2 Factorisation

3.2.1 Introduction

Theorem 3.2.1. *Tout nombre entier $n \geq 2$ admet une factorisation de la forme*

$$n = p_1^{n_1} \cdots p_k^{n_k},$$

où $p_1 < p_2 < \cdots < p_k$ sont des nombres premiers et $n_1, \ldots, n_k \in N^*$ sont des entiers positifs.

Maple code 3.2.2.

```
      ifactor

?ifactor;
n:=5*8*61;
ifactor(n);
```

Exercice 3.2.3. 1. Exécuter les commandes suivante:

```
      ifactor

interface(verboseproc = 2);
print(ifactor);
```

2. Copier et factoriser le grand nombre qui apparait dans la procédure.

3. Interpréter ce nombre.

Maple code 3.2.4.

Dans Maple , il est possible d'utiliser une méthode spécifique en utilisant la procédure **ifactor(n,méthode)**.

```
      Factorisations selon Maple

n:=10^32+11;
st := time():ifactor(n, mpqs):duree := time()-st;
st := time():ifactor(n, morrbril):duree := time()-st;
st := time():ifactor(n, squfof):duree := time()-st;
st := time():ifactor(n, pollard):duree := time()-st;
st := time():ifactor(n, lenstra):duree := time()-st;
st := time():ifactor(n, mpqsmixed):duree := time()-st;
st := time():ifactor(n, mixed):duree := time()-st;
```

Pour déterminer les petits facteurs d'un grand nombre entier, Maple 12 propose la fonction **ifactor(n,easy)**.

```
      Factorisations avec easy de Maple

n:=10^69+11;
st := time():ifactor(n, easy);duree := time()-st;

n:=10^70+11;
st := time():ifactor(n, easy);duree := time()-st;
```

Aussi, on peut limiter le temps de la factorization.

```
      Factorisations avec easy de Maple

n:=10^69+11;
timelimit(5, ifactor(n));

n:=10^70+11;
timelimit(5, ifactor(n));
```

3.2.2 Factorisation par des divisions successives

La méthode la plus simple pour factoriser un nombre n est de tester si n est divisible par 2 et par tous les nombres impaires $3, 5, 7, 9, \cdots, \lfloor\sqrt{n}\rfloor$ où $\lfloor x\rfloor$ désigne la partie entière de n.

Maple code 3.2.5.

```
      Factorisation par des divisions successives

trial:=proc(n)
local i,l,a,lim;
l:=NULL; a:=n;
    lim:=trunc(evalf(sqrt(n)));
    for i from 2  to lim do
            while a mod i = 0 do
                a:=a/i;
                l:=l,i;
            od;
    od;
if (a<>1) then l:=l,a;fi;
print(l);
end:
```

```
      Factorisation par des divisions successives

st := time();
trial(11*2^10*3^4*5^8*1001);
duree := time()-st;
```

3.2.3 Factorisation par la suite des nombres premiers

Une autre méthode simple pour factoriser un nombre n est de tester si n est divisible par tous les nombres premiers $2, 3, 5, 7, \ldots, q$ où q est le plus grand nombre premier tel que $q \leq \lfloor \sqrt{n} \rfloor$.

Maple code 3.2.6.

```
      Factorisation par la suite des nombres premiers

trialp:=proc(n)
local p,l,a,lim;
l:=NULL; a:=n;
lim:=trunc(evalf(sqrt(n)));
p:=2;
while p<=lim do
         while a mod p = 0 do
            a:=a/p;
            l:=l,p;
         od;
         p:=nextprime(p);
od;
if (a<>1) then l:=l,a;fi;
return l;
end:
```

```
      Factorisation par la suite des nombres premiers

st := time();
trial(11*2^10*3^4*5^8*1001);
duree := time()-st;
```

3.3 Tests de Primalité

3.3.1 Test par les divisions successives

Dans ce test, pour factoriser n, il faut le diviser par tous les nombres $2, \cdots, m$ où $m = \lfloor \sqrt{n} \rfloor$.

Algorithm 14 Trial Division Test

Input : An integer n.

Output : An indication of whether n is really composite or really prime.

If $n \equiv 0 \pmod 2$ **then**
    Return "n is composite".
Else
    $a = 3$.
    While $a < \sqrt{n}$ and $n \not\equiv 0 \pmod a$ **do**
        $a = a + 2$
    End While
    If $a > \sqrt{n}$ **then**
        Return "n is prime".
    Else
        Return "n is composite".
    End If
End If

Complexity of Trial Division Test: $\mathcal{O}\left(\sqrt{n}\right) = \mathcal{O}\left(2^{\frac{1}{2}\log n}\right)$.

Maple code 3.3.1.

Maple code 3.3.2.

```
      Maple: Trial Division Primality Test

trialtest:=proc(n)
local m,a;
if n mod 2=0 then return(n is composite);
 else   m:=trunc(sqrt(n));
        a:=3;
        while (a<= m) and (n mod a<>0) do
            a:=a+2;
        od;
        if a>m then return(n is prime);
            else return(n is composite);
        fi;
fi;
end proc:
```

```
      Maple: Trial Division Primality Test, examples

trialtest(2000002);
trialtest(557);
```

3.3.2 Le petit théorème de Fermat

Most modern primality tests depend on the converse of Fermat's Little Theorem: Given a number n, if there exists an integer a with $1 < a < n$ and $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite. Since $a^{n-1} \pmod{n}$ can be computed in $\log(n)$, the former condition is very easy to check.

Theorem 3.3.3 (Fermat's Little Theorem)**.** *Let p be a prime and a any positive integer. If $\gcd(a, p) = 1$, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. Suppose that p is prime and let a be an integer with $\gcd(a, p) = 1$. Consider the set

$$E_1 = \{a \pmod{p}, 2a \pmod{p}, \ldots, (p-1)a \pmod{p}\}.$$

If $ma = na \pmod{p}$ for some m and n with $1 \leq m, n \leq p-1$, then $(m-n)a \equiv 0 \pmod{p}$. Since $\gcd(a, p) = 1$, then $m - n \equiv 0 \pmod{p}$. On the other hand, we have $0 \leq |m - n| \leq p - 2$. Hence $m - n = 0$ and $m = n$. It follows that the cardinality of E_1 is $\#E_1 = p - 1$. Rearranging, we get

$$E_1 = \{1, 2, \ldots, p-1\}.$$

Next, multiplying the numbers in $E_1 = \{a \pmod{p}, 2a \pmod{p}, \ldots, (p-1)a \pmod{p}\}$, we get $a^{p-1}(p-1)! \pmod{p}$. Similarly, multiplying the numbers in $E_1 = \{1, 2, \ldots, p-1\}$, we get $(p-1)! \pmod{p}$. Equating, we get

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Since $\gcd((p-1)!, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. □

Example 3.3.4.

Consider the prime number $n = 23$ and let $a = 17$. We get $17^{23-1} \equiv 1 \pmod{23}$.

The converse of Fermat's Little Theorem will reveal whether an integer n is composite or not.

Theorem 3.3.5 (Fermat's Primality Test)**.** *Let n be a positive integer. If there exists a positive integer a such that*

$$\gcd(a, n) \neq 1 \quad \textit{or} \quad a^{n-1} \not\equiv 1 \pmod{n},$$

then n is composite.

Example 3.3.6.

Consider the number $n = 231$ and let $a = 5$. We get $a^{n-1} \equiv 67 \pmod{n}$. Hence 231 is a composite number. Indeed, we have $231 = 3 \cdot 7 \cdot 11$.

Maple code 3.3.7.

```
      Maple:    Le petit théorème de Fermat

p:=17;a:=5;a^(p-1) mod p;
p:=18;a:=5;a^(p-1) mod p;
p:=230;a:=17;a^(p-1) mod p;
p:=nextprime(10^10);a:=5;a^(p-1) mod p;
```

Le dernier calcul produit une erreur "overflow". Ceci est dû au fait que le nombre est très grand pour Maple. Pour y remédier, Maple propose d'exécuter **modp(power(a,p-1),p)** ou encore `a&^(p-1) mod p;`

Algorithm 15 The Fermat Test

Input : An integer n, a number k of tests.
Output : An indication of whether n is really composite or probably prime after k tests.

If $n \equiv 0 \pmod 2$ **then**
    Return "n is composite".
Else
    $i = 1$.
    While $i \leq k$ **do**
        Generate a random $a \in \{2, \ldots, n-1\}$.
        If $\gcd(a, n) \neq 1$ **then**
            Return "n is composite".
            Break.
        End If
        Compute $b = a^{n-1} \pmod n$.
        If $b \neq 1$ **then**
            Return "n is composite".
            Break.
        End If
        $i = i + 1$.
    End While
    Return "n is probably prime".
End If

Complexity of The Fermat Test: $\mathcal{O}(k \log n)$.

Maple code 3.3.8.

Maple code 3.3.9.

```
      Maple: The Fermat Test

Fermattest:=proc(n,k)
local i,a,b;
if n mod 2=0 then
    return(n is composite);
    else
        i:=1;
        while i<=k do
            a:=rand(2..n-1)();
            if gcd(a,n)<>1 then
                return(n is composite);
            fi;
            b:=a&^(n-1) mod n;
            if b<>1 then
                return(n is composite);
            fi;
            i:=i+1;
        od;
        return(n is probably prime);
fi;
end proc:
```

Example 3.3.10.

Performing **Fermattest(93,1)**, Maple returns **93 is composite**, while performing **Fermattest(3828001,10)**, Maple returns **3828001 is probably prime** which is incorrect since $3828001 = 101 \cdot 151 \cdot 251$.

The probability of a composite number n passing k Fermat's tests for k different bases $a_1, a_2, \ldots, a_k$ is at most $\frac{1}{2^k}$. Hence, an integer is declared prime after k Fermat's tests with a probability at least $1 - \frac{1}{2^k}$.

3.3.3 Les nombres pseudo premiers

Definition 3.3.11. Soit n un entier composé. Soit a un entier avec $\gcd(a, n) = 1$. On dit que n est pseudo-premier en base a si $a^{n-1} \equiv 1 \pmod{n}$.

Dans la plupart des cas, l'égalité $a^{n-1} \equiv 1 \pmod{n}$ a lieu pour des nombres premiers n, mais l'entier n peut être composé.

Maple code 3.3.12.

```
      Maple: Les nombres pseudo premiers

n:=341;a:=2;modp(power(a,n-1),n);ifactor(n);
```

Ainsi 341 est pseudo-premier en base 2.

Algorithm 16 Pseudoprime Test

Input : An integer n and a number a such that $\gcd(n, a) = 1$.
Output : An indication of whether n is pseudoprime in base a or not.

1: **If** $\gcd(n, a) \neq 1$ **then**
2: Return "n and a are not coprime".
3: **Else**
4: **If** $a^{n-1} \not\equiv 1 \pmod{n}$ **then**
5: Return "n is not pseudoprime to the base a".
6: **Else**
7: Return "n is pseudoprime to the base a".
8: **End If**
9: **End If**

Maple code 3.3.13.

The following procedure tests whether a integer n is pseudoprime to the base a. Here, we used the procedure **modexp(a,n-1,n)** to compute $a^{n-1} \pmod{n}$ which can be supplied by the Maple function

```
{a &\^ (n-1) mod n}
```

```
      Maple:  Pseudoprime Test

pseudoprime:=proc(n,a)
local b;
if gcd(n,a)<>1 then
    return cat(n, a, " are not coprime ");
    else
        b:=a&\^(n-1) mod n;
        if b<>1 then return cat(n, " is not pseudoprime to the base ", a);
            else return cat(n, " is pseudoprime to the  base ", a);
        fi;
fi;
end proc:
```

```
      Maple:  Pseudoprime Test


nn:=341;
aa:=2;
pseudoprime(nn,aa);
ifactor(nn);
```

Exercice 3.3.14. 1. Write a procedure that gives a list of pseudoprimes to a base a up to the bound B.

2. Write a procedure that gives a list of bases for which a number n is pseudoprime.

```
      Maple: Les nombres pseudo premiers en une base

pseudo := proc (a, B)
local i, l;
l := NULL;
for i from 2 to B do
    if not(isprime(i)) and modp(power(a,i-1),i) = 1 then
        l := l, i;
    end if;
end do;
RETURN(l);
end proc:
pseudo(4, 1000);
```

```
      Maple: Les  bases pour un entier

pseudo2 := proc (n)
local a, l;
l := NULL;
for a from 2 to n do
    if  modp(power(a,n-1),n) = 1 then
        l := l, n;
    end if;
end do;
RETURN(l);
end proc:
pseudo(561);
```

3.3.4 Les nombres de Carmichael

Il existe des nombres composés n qui sont pseudo-premiers dans toutes les bases a avec $2 \leq a \leq n-1$ et $\gcd(a,n) = 1$.

Definition 3.3.15 (Nombres de Carmichael)**.** Soit $n \geq 2$ un nombre entier composé. On dit que n est un nombre de Carmichael s'il est pseudo-premier en base a pour tous les entiers a avec $2 \leq a \leq n-1$ et $\gcd(a,n) = 1$.

Algorithm 17 Carmichael number

Input : A composite integer n.
Output : An indication of whether n is a Carmichael number or not.

```
1: If n is prime then
2:     Return "n is a prime number".
3: End If
4: For a = 2 to n − 1 do
5:     If gcd(n, a) = 1 then
6:         If a^{n−1} ≢ 1 (mod n) then
7:             Return "n is not a Carmichael number in base a".
8:         End If
9:     End If
10: End For
11: Return "n is a Carmichael number".
```

Maple code 3.3.16.

Complexity of Carmichael number Test: $\mathcal{O}(n \log n)$**.**

Maple code 3.3.17.

```
      Maple: Carmichael number

carmichael:=proc(n)
local a,b;
if isprime(n) then
    return cat(n, " is a prime number ");
end if;
for a from 2 to n-1 do
    if gcd(n,a)=1 then
        b:=modp(power(a,n-1),n);
        if b<>1 then
            return cat(n, " is not Carmichael number in base ", a);
        fi;
    fi;
od;
return cat(n, " is a Carmichael number");
end proc:
```

Example 3.3.18.

Running carmichael(561), we find that a 561 is a Carmichael number while $561 = 3 \cdot 11 \cdot 17$.

Exercice 3.3.19. An easy way to build Carmichael numbers is to find $n = pqr$ where $p = 6m + 1$, $q = 12m + 1$, $r = 18m + 1$ and p, q and r are all primes.

1. Show that $(s - 1)|(n - 1)$ where $s = p$, $s = q$ or $s = r$.

2. Write a Maple program and find at least 10 Carmichael numbers.

```
      Maple: Carmichael number

listcarm:=proc(B)
local l,m,p,r,q,n;
l:=NULL;
for m from 1 to B do
    p:=6*m+1;
    if isprime(p) then
        q:=12*m+1;
        if isprime(q) then
            r:=18*m+1;
            if isprime(r) then
                n:=p*q*r;
                l:=l,n;
            fi;
        fi;
    fi;
end do;
return l;
end proc:
```

3.3.5 Les nombres pseudo-premiers forts

Soit n un nombre entier impair. Alors on peut écrire de façon unique $n = 2^r m + 1$ avec $r \geq 1$ et m est impair.

Algorithm 18 Decomposition

Input : A odd integer n.
Output : The decomposition $n = 2^r m + 1$ where $r \geq 1$ and m est odd.

1: **If** n is even **then**
2: Return "n is even".
3: **End If**
4: $m = n - 1$, $r = 0$.
5: **While** m is even **do**
6: $m = \frac{m}{2}$.
7: $r = r + 1$.
8: **End While**
9: Return m and r.

Maple code 3.3.20.

```
      Décomposition sous la forme n=2^rm+1

decomp:=proc(n)
local r,m;
if type(n,even) then
    return cat(m,"is even");
end if;
m:=n-1;r:=0;
while type(m,even) do
  m:=iquo(m,2):r:=r+1:
 end do:
return r,m;
end proc:
```

Definition 3.3.21. Soit $n = 2^r m + 1$ un entier impair composé avec m impair. Soit a un entier. On dit que n est pseudo-premier fort en base a si une des deux conditions suivantes est satisfaite:

1. $a^m \equiv 1 \pmod{n}$,

2. il existe un entier i avec $0 \leq i \leq r-1$ tel que $a^{2^i m} \equiv -1 \pmod{n}$.

Exercice 3.3.22.

1. Let $n = 561$. Find m and r such that $n = 2^r m + 1$. Show that 561 is not a strong pseudoprime in base 5.

2. Let $n = 18721$. Find m and r such that $n = 2^r m + 1$. Show that 18721 is a strong pseudoprime in base 3.

La procédure suivante permet de tester si un nombre composé et impair n est pseudo-premier fort en une base a.

Maple code 3.3.23.

```
      Maple:    Nombres pseudo-premiers forts

pspfort:=proc(a,n)
local r,m,i;
m:=n-1;r:=0;
while type(m,even) do
    m:=iquo(m,2):r:=r+1:
end do:
if a&^m mod n=1 then RETURN(n, "est pseudo premier fort en", a);fi;
for i from 0 to r-1 do
    if a&^(2^i*m) mod n=n-1 then
        RETURN(n, "est pseudo premier fort en", a);
    fi;
od;
RETURN(n, "n'est pseudo premier fort en base", a);
end proc:
```

3.3.6 Le test de primalité Miller-Rabin

Le test Rabin-Miller a été développé par Rabin en utilisant les idées de Miller. C'est un test probabilistique assez rapide. Il utilise la propriété suivante.

Proposition 3.3.24. *Si p est un nombre premier, alors l'équation $x^2 \equiv 1 \pmod{p}$ n'admet que les solutions $x = 1$ et $x = p - 1 \pmod{p}$.*

Proof. Observe that $x = 1$ and $x = p - 1$ are solutions to the equation $x^2 \equiv 1 \pmod{p}$. Suppose that there is another solution of the equation $x^2 \equiv 1 \pmod{p}$ with $2 \leq x \leq p-2$. Then $x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{p}$ and $p|(x-1)(x+1)$. If $\gcd(x+1, p) = 1$, then $p|(x-1)$ which contradicts the assumption $2 \leq x \leq p-2$. Also, if $\gcd(x-1, p) = 1$, then $p|(x+1)$ which contradicts the assumption $2 \leq x \leq p-2$. If $\gcd(x+1, p) = p$, then $n|(x+1)$ which also contradicts the assumption $2 \leq x \leq p-2$. Similarly, if $\gcd(x-1, p) = p$, then $p|(x-1)$ which also contradicts the assumption $2 \leq x \leq p-2$. □

Le test de Miller-Rabin est basé sur la généralisation suivante du théorème de Fermat.

Theorem 3.3.25. *Soit $n = 2^r m + 1$ un nombre premier avec $r \geq 1$ et m impair. Pour tout entier a avec $2 \leq a \leq n-2$, on a une des deux éventualités:*

1. $a^m \equiv 1 \pmod{n}$,
2. *Il existe un entier $0 \leq i \leq r-1$ tel que $a^{m2^i} \equiv -1 \pmod{n}$,*

Proof. Suppose that $n > 2$ is prime and $n = 2^r m + 1$. Since n is prime, then Fermat's Little Theorem implies that $a^{n-1} - 1 \equiv 0 \pmod{n}$. Then, we get recursively

$$\begin{aligned} a^{n-1} - 1 &= a^{2^r m} - 1 \\ &= (a^m)^{2^r} - 1 \\ &= \left((a^m)^{2^{r-1}} - 1\right)\left((a^m)^{2^{r-1}} + 1\right) \\ &= \left((a^m)^{2^{r-2}} - 1\right)\left((a^m)^{2^{r-2}} + 1\right)\left((a^m)^{2^{r-1}} + 1\right) \\ &= \cdots \\ &= (a^m - 1)(a^m + 1)\left(a^{2m} + 1\right)\cdots\left((a^m)^{2^{r-1}} + 1\right). \end{aligned}$$

Since n is prime, then n divides one of the factors. Hence $a^m \equiv 1 \pmod{n}$, or $a^{2^i m} \equiv -1 \pmod{n}$ for some i with $0 \leq i \leq r-1$. □

Assuming the Generalized Riemann Hypothesis, the following theorem is the key ingredient.

Theorem 3.3.26 (The Miller-Rabin Test)**.** *Let n be an odd number such that $n-1 = 2^r m$ with odd m. If for all a with $1 \leq a \leq 2(\log n)^2$ one has one of the following assertions*

1. *$a^m \equiv 1 \pmod{n}$, or*

2. *there exists i with $0 \leq i \leq r-1$ such that $a^{m2^i} \equiv -1 \pmod{n}$,*

then n is a prime number.

This theorem can be transformed into an easy test.

Algorithm 19 The Miller-Rabin Test

[The Miller-Rabin Test]

Input : An odd integer n and a number k of tests.

Output : An indication whether n is composite or probably prime.

For i from 1 to k **do**
  Randomly choose $a \in [2, n-2]$.
  If $\gcd(n, a) > 1$ **then**
    Return "n is composite".
  End If
  If $a^{n-1} \not\equiv 1 \pmod{n}$ **then**
    Return "n is composite".
  End If
  Find $r \geq 1$ and m such that $n - 1 = 2^r m$ and m is odd.
  $g_0 = a^m \pmod{n}$.
  If $g_0 = 1$ **then**
    Return "n is probably prime".
  Else
    $i := 0$.
    While $i < r$ and $g_i \neq n - 1$ **do**
      $i := i + 1$.
      Compute $g_i = a^{2^i m} \pmod{n}$.
    End While
    If $i = r$ **then**
      Return "n is composite".
    Else
      Return "n is probably prime".
    End If
  End If
End For

Complexity of the Miller-Rabin Test: $\mathcal{O}(k \log n)$.

The probability of success of the Miller-Rabin test to declare n as prime after k tests is at least $1 - \frac{1}{4^k}$. In practice, it is acceptable that a number is prime if it passes the Miller–Rabin test for 100 tests.

Maple code 3.3.27.

```
      The Miller-Rabin Test

MillerRabin:=proc(n,lim)
local i,j,a,r,m,b,g;
if type(n,even) then
    return cat(n," is composite");
end if;
for i from 1 to lim do
    a:=rand(1..n-1)();
    if gcd(a,n)<>1 then
        return cat(n, " is composite");
    fi;
    b:=modp(power(a,n-1),n);
    if b<>1 then
        return cat(n, " is composite");
    fi;
    r:=1;m:=(n-1)/2;
    while gcd(m,2)=2 do
        r:=r+1;m:=m/2;
    od;
    g:=modp(power(a,m),n);
    if g=1 then
        return (n, " is probably prime");
        else
            j:=0;
            while j<r and g<>n-1 do
                j:=j+1;
                g:=modp(power(a,2^j*m),n);
            end do;
            if j=r then
                return cat(n, " is composite");
                else
                    return cat(n, " is probably prime");
            fi;
    fi;
od;
end proc:
```

3.3.7 Le test de primalité Solovay-Strassen

Le test de Solovay-Strassen est basé sur une combinaison du théorème de Fermat et des symboles de Legendre et de sa généralisation par Jacobi. Le symbole de Legendre est

basé sur la notion de résidu quadratique.

Definition 3.3.28 (Résidu quadratique)**.** Soit p un nombre premier et a un entier non nul. On dit que a est un résidu quadratique modulo p si l'équation $x^2 \equiv a \pmod{p}$ admet une solution. Dans le cas contraire, a est appelé non-résidu quadratique modulo p.

Maple dispose de la fonction **msolve(eq,m)** pour résoudre certaines équations modulaires.

Maple code 3.3.29.

```
      msolve

?msolve;
p:=nextprime(10^5):a:=141^2 mod p:msolve(x^2=a,p);
p:=nextprime(10^5):a:=141^2 mod p:msolve(x^2=-a,p);
p:=nextprime(10^5):a:=141^7+141^2-141+1 mod p:msolve(x^7+x^2-x+1=a,p);
```

Exercice: Résoudre les équations

$x^4 \equiv 1 \pmod{121}$, $x^4 \equiv 1 \pmod{30}$, $3^x \equiv 1 \pmod{34}$, $3x+4y = 7 \pmod{101}$.

Definition 3.3.30 (Symbole de Legendre)**.** Soit p un nombre premier et a un entier non nul. Le symbole de Legendre $\left(\frac{a}{p}\right)$ est défini par:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{Si } \gcd(a,p) = p, \\ 1 & \text{Si } a\text{est un résidu quadratique modulo } p, \\ -1 & \text{Si } a\text{n'est pas un résidu quadratique modulo } p. \end{cases}$$

Maple dispose de la fonction **legendre(a,p)** pour calculer le symbole de Legendre.

Maple code 3.3.31.

```
      Maple:    Legendre

?legendre;
with(numtheory):
legendre(5,17);
legendre(5,18);
legendre(51,nextprime(10^10));
```

Complexity of Legendre Symbol: $\mathcal{O}(\log p)$**.**

Exercice 3.3.32. Résoudre les équations à l'aide de **msolve**.

$x^4 \equiv 1 \pmod{121}$, $x^4 \equiv 1 \pmod{30}$, $3^x \equiv 1 \pmod{34}$, $3x+4y = 7 \pmod{101}$.

Le symbole de Legendre peut être calculé à l'aide d'une exponentiation modulaire.

Theorem 3.3.33 (Symbole de Legendre)**.** *Soit p un nombre premier et a un entier non nul. Alors*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Proof. Si a est un résidu quadratique, alors a est de le forme $a \equiv x^2 \pmod{p}$ et $\left(\frac{a}{p}\right) = 1$. D'autre part, d'après le théorème de Fermat, on a $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$. □

Le symbole de Jacobi est une généralisation du symbole de Legendre.

Definition 3.3.34 (Symbole de Jacobi)**.** Soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ la factorisation d'un entier positif. Soit a un entier non nul. Le symbole de Jacobi est défini par

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i}.$$

Maple dispose de la fonction **jacobi(a,n)** pour calculer le symbole de Jacobi.

Maple code 3.3.35.

```
      Maple:    Jacobi

?jacobi;
with(numtheory):
jacobi(5,18);
legendre(5,18);
jacobi(51,10*nextprime(10^10));
```

Complexity of Jacobi symbol: $\mathcal{O}((\log n)^2)$.

Le test de Solovay et Strassen de la primalité d'un entier n est basé sur l'égalité du symbole de Legendre $\left(\frac{a}{n}\right)$ et de la valeur de $a^{\frac{n-1}{2}} \pmod{n}$.

Algorithm 20 Solovay-Strassen Test

[Solovay-Strassen Test]

Input : A positive odd integer n and a number k of tests.

Output : An indication whether n is composite or probably prime.

1: **For** i from 1 to k **do**
2: Choose a random $a \in \{1, \ldots, n-1\}$.
3: **If** $\gcd(n, a) <> 1$ **then**
4: Return "n is composite".
5: **Else If** $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \pmod{n}$ **then**
6: Return "n is composite".
7: **End If**
8: **End For**
9: Return "n is probably prime".

Complexity of the Solovay-Strassen Test: $\mathcal{O}(k \log n)$.

Maple code 3.3.36.

```
      Maple:    Solovay-Strassen Test

SolovayStrassen:=proc(n,k)
local i,a;
for i from 1 to k do
    a:=rand(1..n-1):a:=a();
    if gcd(a,n)<>1 then
        return cat(n, " is composed");
        else
            if modexp(a,(n-1)/2,n)<>jacobi(a,n) mod n then
                return cat(n, " is composed");
            fi;
    fi;
    i:=i+1;
od;
return cat(n, " is probably prime");
end proc:
```

The following result is the basis for the probability success for the Solovay–Strassen primality test.

Theorem 3.3.37. *Suppose n is an odd composite number. Then for a random integer $a \in \{1, \ldots, n-1\}$, the probability that the following conditions*

$$\gcd(n, a) = 1 \quad \textit{and} \quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right),$$

are satisfied is at most $\frac{1}{2}$.

As a consequence, we get the following result.

Corollary 3.3.38. *Suppose* n *is an odd number. Then if*

$$\gcd(n,a)=1 \quad \textit{and} \quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right),$$

for k *random integers* $a \in \{1,\dots,n-1\}$*, then we consider* n *to be prime with a probability of at least* $1-\frac{1}{2^k}$.

3.3.8 Le test de primalité AKS

Le test AKS a été proposé en 2004 par Agrawal, Kayal et Saxena [1]. C'est le seul algorithme déterministe connu. Ce test est basé sur une généralisation du théorème de Fermat aux polynômes.

Theorem 3.3.39. *Soit* $a \in \mathbb{Z}$, $n \in \mathbb{N}$ *avec* $\gcd(a,n)=1$. *Alors* n *est un nombre premier si et seulement si*

$$(X+a)^n \equiv X^n + a \pmod{n}.$$

Proof. We have

$$(X+a)^n - (X^n+a^n) = \sum_{i=1}^{n-1} C_n^i X^i X^{n-i}, \quad \text{with} \quad \binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{1\cdots i}.$$

Suppose that n is prime. Then $a^n \equiv a \pmod{n}$ and $\binom{n}{i} \equiv 0 \pmod{n}$. Hence $(X+a)^n \equiv X^n + a \pmod{n}$.

Suppose now that $(X+a)^n \equiv X^n + a \pmod{n}$ with $\gcd(a,n)=1$. If n is not prime, then there exists a prime factor q of n such that $n = q^k q'$ with $\gcd(q,q')=1$. In the development of $(X+a)^n$, the coefficient of the term X^q is

$$\binom{n}{q} a^{n-q} = \frac{n(n-1)\cdots(n-q+1)}{1\cdots q} a^{n-q} = \frac{q^{k-1}q'(n-1)\cdots(n-q+1)}{1\cdots(q-1)} a^{n-q}.$$

Since q does not divide the product $q'(n-1)\cdots(n-q+1)a^{n-q}$, then $\binom{n}{q}$ is divisible by q^{k-1} but not by q^k. Hence $\binom{n}{q} \not\equiv 0 \pmod{q^k}$ and $\binom{n}{q} \not\equiv 0 \pmod{n}$. This contradicts the congruence $(X+a)^n \equiv X^n + a \pmod{n}$. It follows that n is prime. □

Exercice 3.3.40. Démontrer que si n est premier, alors n divise C_n^i pour tout $0 < i < n$.

Un autre résultat relatifs aux polynômes est le suiant. Le nombre $O_r(n)$ désigne le plus petit entier k vérifiant

$$n^k \equiv 1 \pmod{r}.$$

Algorithm 21 Test AKS

Input : Un nombre entier n.
Output : n est premier ou n est composé.

If $n = m^k$ **then**
    Sortir "n est composé". Stop.
End If
Déterminer le plus petit entier r tel que $O_r(n) > 4(\log n)^2$.
For a de 1 à $2\sqrt{r}\log n$ **do**
    If $\gcd(n, a) > 1$ **then**
        Sortir "n est composé". Stop.
    End If
    If $(X + a)^n \equiv X^n + a \ (\pmod{n}, X^r - 1)$ **then**
        Sortir "n est composé". Stop.
    End If
    Sortir "n est premier". Stop.
End For

Theorem 3.3.41. *Soit n un nombre entier. Soit r le plus petit entier tel que l'ordre $O_r(n)$ de n vérifie $O_r(n) > 4(\log n)^2$. Si pour tout entier a avec $0 < a \leq 2\sqrt{r}\log n$ ona*

$$(X + a)^n \equiv X^n + a \pmod{(n, X^r - 1)},$$

alors n est un nombre premier.

Ce théorème donne lieu au test AKS.

Chapter 4

Le Cryptosystème RSA

4.1 Principe de RSA

4.1.1 Le module de RSA

Below we describe in detail the initial schemes of the RSA Cryptosystem.

- **RSA Key Generation**
  INPUT: The bitsize k of the modulus.
  OUTPUT: A public key (N, e) and a private key (N, d).

  1. Generate two large random and distinct $(k/2)$-bit primes p and q.
  2. Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$.
  3. Choose a random integer e such that $3 \leq e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$.
  4. Compute the unique integer d such that $1 \leq e < \phi(N)$ and $ed \equiv 1 \pmod{\phi(N)}$.
  5. Return the public key (N, e) and the private key (N, d).

- **RSA Encryption**
  INPUT: The public key (N, e) and the plaintext $\mathbf{m}$.
  OUTPUT: The ciphertext C.

  1. Represent the message $\mathbf{m}$ as an integer M with $1 \leq M \leq N-1$.
  2. Compute $C \equiv M^e \pmod{N}$.
  3. Return the ciphertext C.

- **RSA Decryption**
  INPUT: The private key (N, d) and the the ciphertext C.
  OUTPUT: The message $\mathbf{m}$.

1. Compute $M \equiv C^d \pmod{N}$.
2. Transform the number M to the message **m**.
3. Return the message **m**.

Algorithm 22 : Fabrication du module RSA

Input : Une taille $2t$ pour le module du cryptosytème RSA.
Output : Deux nombres premiers de tailles t et un module RSA N de taille $2t$.

1: Prendre un nombre premier aléatoire p dans l'intervalle $[2^t, 2^{t+1}]$.
2: Prendre un nombre premier aléatoire q dans l'intervalle $[2^t, 2^{t+1}]$.
3: **If** $p = q$ **then**
4: Aller à l'étape 2.
5: **Else**
6: $N = pq$.
7: **End If**

Exercice 4.1.1. 1. Ecrire une procédure pour produire deux nombres premiers p et q ayant chacun t bits avec $q < p$ ainsi qu'un module RSA $N = pq$.

2. Donner un module RSA de 1024 bits.

Maple code 4.1.2.

```
      Programme

rsa:=proc(t)
local m1,m2,p,q,N;
m1:=2^(t-1);m2:=2^(t);
p:=nextprime(rand(m1..m2)());
q:=nextprime(rand(m1..m2)());
while p=q or p>m2 or q>m2 do
    p:=nextprime(rand(m1..m2)());
    q:=nextprime(rand(m1..m2)());
end do;
N:=p*q;
return min(p,q),max(p,q),N;
end proc:
```

```
      Programme

t:=512:
l:=rsa(t);
p:=l[1];q:=l[2];N:=l[3];
```

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

Maple code 4.1.3.

Programme	Commentaires
`with(numtheory):`	`<- Package numtheory "Théorie des Nombres"`
`N:=5*8*61:phi(N);`	`<- un exemple simple et calcul de phi(n)`
`N:=nextprime(10^26)*nextprime(10^27):`	
`st := time():phi(N);duree := time()-st;`	

4.1.2 Les clés publiques et privées

Algorithm 23 : Fabrication des clés e et d

Input : Deux nombres premiers p et q.
Output : Une une clé publique e et clé privée d.

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

Exercice: a) Pour p et q donnés, écrire une procédure pour produire un une clé publique e telle que $\gcd(e, \phi(N)) = 1$ et son inverse d modulo $\phi(N)$. a) Donner une clé publique et une clé privée pour un module RSA de 1024 bits.

Maple code 4.1.4.

Programme
`cle:=proc(p,q)`
`local N, phii,e,d;`
`phii:=(p-1)*(q-1):`
`e:=rand(3..phii-1)():`
`while(gcd(e,phii) <> 1) do`
`  e:=rand(3..phii)();`
`od:`
`d := 1/e mod  phii:`
`return e,d;`
`end proc:`

```
      Programme

l:=rsa(512):p:=l[1]:q:=l[2]:N:=l[3]:
l:=cles(p,q);
e:=l[1];d:=l[2];
e*d mod (p-1)*(q-1);
```

4.1.3 Envoi d'un message

Algorithm 24 : Chiffrement d'un message

Input : Un message clair et la clé publique (N, e).
Output : Un message chiffré C.
1: Transformer le message en un nombre entier M de l'intervalle $[2, N]$.
2: Calculer $C \equiv M^e \pmod{N}$.
3: Envoyer le message C.

Maple code 4.1.5.

Pogramme de chiffrement.

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

4.1.4 Déchiffrement d'un message

Algorithm 25 : Déchiffrement d'un message

Input : Un message chiffré C et la clé privée (N, d).
Output : Un message clair M.
1: Calculer $M \equiv C^d \pmod{N}$.
2: Transformer le nombre M en un message clair.

Maple code 4.1.6.

Pogramme déchiffrement.

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

4.1.5 Signature d'un message

Algorithm 26 : Signature d'un message

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

Output : 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 code 4.1.7.

Programme Signature

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

Algorithm 27 : Vérification d'une signature

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

Output : Vérification d'une signature.

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

Maple code 4.1.8.

Programme vérification

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

4.1.6 Un exemple d'utilisation de RSA

Rabat est la capitale de Maroc Numérique 2013

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 code 4.1.9.
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)**.

Maple code 4.1.10.

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

Maple code 4.1.11.

Pogramme de vérification.

```
      Programme

mt:="Rabat est la capitale de Maroc Numérique 2013";
m:=convert(m,bytes);
c:=[];
for i from 1 to nops(m) do
    c:=[op(c),power(m[i],e) mod N];
end do:
c;

m2:=[];
for i from 1 to nops(c) do
    m2:=[op(m2),power(c[i],d) mod N];
end do:
m2;
m2-m;
```

Maple code 4.1.12.

Pogramme de vérification.

```
      Programme

l:=rsa(50):p:=l[1]:q:=l[2]:N:=l[3]:
l:=cles(p,q):e:=l[1]:d:=l[2]:
message:="Rabat est la capitale de maroc Numérique 2013":
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;
```

4.2 Cryptanalyses élémentaires de RSA

4.2.1 Cryptanalyse de RSA connaissant $\varphi(N)$

Proposition 4.2.1. *Soit N un module RSA. Si on connait $\varphi(N)$, alors on peut factoriser N.*

Maple code 4.2.2.

Programme de résolution

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

Exercice 4.2.3. 1. Démontrer la proposition.

2. Pogrammer cette proposition à l'aide de Maple et déterminer la valeur de p et q sachant que (ne pas utliser **ifactor**)

$$\begin{aligned} N &= 1027243749104935631846892836072899922149, \\ \phi(N) &= 1027243749104935631691380684862943278060. \end{aligned}$$

4.2.2 Utilisation du même module et deux exposants différents

Proposition 4.2.4. *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.*

Exercice 4.2.5. Démontrer cette proposition.

Maple code 4.2.6.

Programme	Commentaires
N:=22900724415936720487705353O7:	<--- Le module RSA
e1:=4543322112211:	<--- Le premier exposant publique
e2:=787654321187:	<--- Le deuxième exposant publique
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

4.2.3 Utilisation de modules différents pour le même message.

Theorem 4.2.7. *Si les entiers $N_1, N_1, \cdots, N_k$ sont deux à deux premiers entre eux, alors le système*

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

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 $M_i \equiv P_i^{-1} \pmod{N_i}$.

Dans Maple, le théorème des restes chinois est la fonction

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

Voici un exemple pour résoudre le système

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

Maple code 4.2.8.

Programme	Commentaires
`x:=chrem([1,2,3],[101,103,201]):`	`<--- Le théorème des restes chinois`
`x;`	`<--- On obtient x=1482378`
`mod(x, 101);`	`<--- Vérification`
`mod(x, 103);`	`<--- Vérification`
`mod(x, 201);`	`<--- Vérification.`

Proposition 4.2.9. *Soit $k \geq 2$ un nombre entier. On considère 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.*

Proof. Supposons que le même message clair M est chiffré k fois par

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

pour $i = 1, \cdots, k$. 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 code 4.2.10.

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

4.2.4 Attaque cyclique (Cycling Attack)

Dans cette partie, on considère RSA avec un module $N = pq$, une clé publique e et un message m. Soit c le message crypté:

$$c \equiv m^e \pmod{N}.$$

Theorem 4.2.11. *Soit $N = pq$ un module RSA, e une clé publique et c un message crypté d'un message claire m inconnu. On suppose qu'on connait le plus petit entier k tel que*

$$\gcd\left(c^{e^k} - c, N\right) > 1.$$

Alors on peut déterminer le message m ou factoriser le module N.

Proof. On suppose que

$$\gcd\left(c^{e^k} - c, N\right) > 1.$$

On distingue alors deux cas:

- Soit

$$\gcd\left(c^{e^k} - c, N\right) = p, \qquad \text{ou} \qquad \gcd\left(c^{e^k} - c, N\right) = q,$$

ce qui donne la factorisation de N.

- Soit

$$\gcd\left(c^{e^k} - c, N\right) = N,$$

alors

$$c^{e^k} \equiv c \pmod{N},$$

et en posant

$$m' \equiv c^{e^{k-1}} \pmod{N},$$

on obtient $m'^e \equiv c \pmod{N}$, donc $m = m'$ car k est le plus petit entier vérifiant $c^{e^k} \equiv c \pmod{N}$. □

Maple code 4.2.12.

Programme	Commentaires

```
Digits := 100:
p := nextprime(round(7.5^12));
q := nextprime(round(7.5^11.8));
N := p*q:
e:=3;
c := 175406449694505885461:
x0:=c;
x:=modp(x0&^e,N);
g:=gcd(x-c,N);
while g =1 do
    x0:=x;
    x:=modp(x0&^e,N);
    g:=gcd(x-c,N);
end do;
if g<N then
    print('Un facteur premier de N est', g):
    else print('Le message clair est', x0):
end if:
```

4.2.5 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.

Lemma 4.2.13. *Let $N = pq$ be an RSA modulus with $|p-q| < cN^{1/4}$ where c is a positive constant. Then one can factor N in time polynomial in c.*

Proof. Fermat's method for factoring $N = pq$ consists in finding two integers x, y such that

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

If $x - y \neq 2$, then the factorization of N is given by

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

Observe that, if $p - q < c\sqrt{N}$, then $p \approx q \approx \sqrt{N}$ and $p + q \approx 2\sqrt{N}$. To find x, y, we consider the sequence of candidates for x and y defined by

$$x_i = \left\lfloor 2\sqrt{N} \right\rfloor + 1 + i, \quad \text{and} \quad y_i = \sqrt{x_i^2 - 4N}, \quad i = 0, 1, \cdots, k,$$

where $\lfloor x \rfloor$ is the integral part of x. We stop the process when $x_k^2 - 4N$ is a perfect square. Since $p = \frac{x_k+y_k}{2}$ and $q = \frac{x_k-y_k}{2}$, then $x_k = p + q$. Now, suppose that $|p - q| < cN^{1/4}$. Then, since $2\sqrt{N} \leq \left\lfloor 2\sqrt{N} \right\rfloor + 1$ and $p + q > 2\sqrt{N}$, we get

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

It follows that Fermat's method can factor N in less than $\frac{c^2}{4}$ steps, which is efficient for small values of c. □

Maple code 4.2.14.

```
            Programme

fermat:=proc(N)
local i,x,y,p,q;
x:=trunc(2*sqrt(N));
y:=sqrt(x^2-4*N);
while y<>round(y) do
    x:=x+1;
    y:=sqrt(x^2-4*N);
end do;
p:=(x+y)/2;
q:=(x-y)/2;
return p,q;
end proc;

fermat(43361741);
fermat(17090864954662304167505112728173352240867);
fermat(177722816726901365646785214427104985842720418574284701311);
```

Maple code 4.2.15.

A complete example

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

4.2.6 Cryptanalyse de RSA en utilisant deux messages et un polynôme

EXERCICE 1.

1) Démontrer le théorème suivant:

Theorem 4.2.16. *Soient $N = pq$ un module RSA, e une clé publique et f un polynôme. Soit M un message satisfaisant*

$$\begin{aligned} C_1 &\equiv M^e \pmod N, \\ C_2 &\equiv (f(M))^e \pmod N, \\ x - M &\equiv pgcd(x^e - C_1, (f(x))^e - C_2) \mod N. \end{aligned}$$

Connaissant N, e, f, C_1 et C_2, on peut déterminer M.

2) Pogrammer ce théorème à l'aide de Maple et déterminer la valeur de M sachant que

$$\begin{aligned} N &= 22900724415936720487705353 07, \\ e &= 7, \\ f(x) &= x^2 - 751, \\ C_1 &= 50898847680285003503506 6764, \\ C_2 &= 13247370961014078164695 6648. \end{aligned}$$

Chapter 5

Diffie-Hellman and El Gamal

5.1 Introduction

The Diffie-Hellman key agreement protocol was developed by Diffie and Hellman [7] in 1976 and published in the famous paper "New Directions in Cryptography". Their protocol is still widely used to this day. The protocol uses mainly two public parameters, a large prime number p and an element g of the finite group $\mathbb{Z}_p^*$ with a large order. The success of the Diffie-Hellman protocol is based on the difficulty of solving some problems related to the discrete logarithm problem. In 1985, T. El Gamal proposed a crytosystem for both encryption and signature. El Gamal suggested a way to turn the idea of the Diffie-Hellman protocol into a regular public key cryptosystem.

In this note, we describe the the Diffie-Hellman protocol as well as the ElGamal cryptosystem and review the Discrete Logarithm Problem and the way to choose the prime numbers that make the schemes secure.

5.2 The Diffie-Hellman Key Exchange protocole

The Diffie-Hellman key agreement protocol allows two users, Ali and Baba to obtain a shared secret key over a public communication channel. The first step is for the two users to agree on a large prime p and an integer g modulo p having a large prime order.

Definition 5.2.1. Let p and a be integers such that $\gcd(a, p) = 1$. The order of a modulo p is the smallest integer r such that $a^r \equiv 1 \pmod{p}$.

The basic arithmetical operations of the Diffie-Hellman protocol make use of the structure of the cyclic group $\mathbb{Z}_p^*$.

Theorem 5.2.2 (Primitive Root Theorem)**.** *Let p be a prime number. Then there exists*

an element $g \in \mathbb{Z}_p^*$ such that

$$\mathbb{Z}_p^* = \left\{1, g, g^2, \ldots, g^{p-2}\right\}.$$

Such elements are called generators or primitive roots of $\mathbb{Z}_p^*$.

If the factorization of $p-1$ is known, it is easy to find a generator of $\mathbb{Z}_p^*$.

Lemma 5.2.3. *Let p be a prime number. A number g is a generator of $\mathbb{Z}_p^*$ if and only if $g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ for every prime q that divides $p-1$.*

The Diffie-Hellman protocol enables two parties, Ali and Baba to share a common key. The protocol works as follows.

- **The Diffie-Hellman Protocol**
  INPUT: The prime number p and an integer g of large prime order.
  OUTPUT: A shared secret key K.

  1. Ali chooses a secret integer a.
  2. Ali computes $A \equiv g^a \pmod{p}$.
  3. Ali sends A to Baba.
  4. Baba chooses a secret integer b.
  5. Baba computes $B \equiv g^b \pmod{p}$.
  6. Baba sends B to Ali.
  7. Ali computes $K \equiv B^a \pmod{p}$ using his private integer a.
  8. Baba computes $K \equiv A^b \pmod{p}$ using his private integer b.
  9. The shared key is K.

The correctness of the Diffie-Hellman protocol is based on the following equalities

$$K \equiv B^a \equiv \left(g^b\right)^a \equiv \left(g^a\right)^b \equiv A^b \equiv K \pmod{p}.$$

Maple code 5.2.4.

The following procedure outputs a prime number $p \in [2^n, 2^{n+1}]$ and a generator g of $(\mathbb{Z}/p\mathbb{Z})^*$.

```
      Maple:    Diffie-Hellman public parameters

dhpublic:= proc (n)
local p,g,fset,k,test,t,i,a,ga;
with(numtheory):
p:=nextprime(rand(2^n,2^(n+1))());
fset:=factorset(p-1);
k:=nops(fset);
g:=1;test:=1;
while test=1 do
    test:=2;
    g:=g+1;
    for i from 1 to k do
        t:=g&^((p-1)/fset[i]) mod p;
        if t=1 then
            test:=1;
        end if;
    end do;
end do;
return p,g;
end proc:
```

Maple code 5.2.5.

The following procedure shows the computations that Ali will execute.

```
      Maple:    DH, first part of the shared key.

dhA:= proc (p,g)
local a,A;
a:=rand(2..p-2)();
A:=g&^a mod p;
return a,A;
end proc:
```

Maple code 5.2.6.

Similarly, the following procedure shows the computations that Baba will execute.

```
      Maple:    DH, second part of the shared key.

dhB:= proc (p,g)
local b,B;
b:=rand(2..p-2)();
B:=g&^b mod p;
return b,B;
end proc:
```

Maple code 5.2.7.

To obtain the shared key, Ali will execute the following procedure.

```
      Maple:    Ali's shared key.

dhkeyA:= proc (p,a,B)
local K;
K:=B&^a mod p;
return K;
end proc:
```

Maple code 5.2.8.

Similarly, Baba will execute the following procedure.

```
      Maple:    Baba's shared key.

dhkeyB:= proc (p,b,A)
local K;
K:=A&^b mod p;
return K;
end proc:
```

Maple code 5.2.9.

The following procedure summarize the hole Diffie-Hellman protocol.

```
      Maple:    Baba's shared key.

dh:= proc(n)
local public,p,g,LA,a,A,LB,b,B,K1,K2;
public:=dhpublic(n);
    p:=public[1];
    g:=public[2];
LA:=dhA(p,g);
    a:=LA[1];
    A:=LA[2];
LB:=dhB(p,g);
    b:=LB[1];
    B:=LB[2];
K1:=dhkeyA(p,a,B);
K2:=dhkeyB(p,b,A);
return K1,K2;
end proc:
```

5.3 The ElGamal cryptosystem

In 1985, T. El Gamal [8] proposed a public-key encryption based on the discrete logarithm problem in $\mathbb{Z}_p^*$. Here, we present the ElGamal encryption scheme. We suppose that Baba wishes to send a message m to Ali. They will take the following steps.

- **Key generation by Ali.**
  To generate a public and a private key, Ali proceeds as follows.
  1. Ali generates a large prime p.
  2. Ali chooses an element $g \in (\mathbb{Z}/p\mathbb{Z})^*$ of large order.
  3. Ali chooses a random a such that $1 \leq a \leq p-2$ and computes $g^a \pmod p$.
  4. Ali publishes the public key (p, g, g^a).
  5. Ali retains the private key a.
- **Encryption by Baba.**
  To encrypt a message M using the public key (p, g, g^a), Baba proceeds as follows.
  1. Baba obtains Ali's public key (p, g, g^a).
  2. Baba converts the message into an integer $m \in \{1, \ldots, p-1\}$.
  3. Baba chooses a random k with $1 \leq k \leq p-2$.
  4. Baba computes $\gamma \equiv g^k \pmod p$ and $\delta \equiv m(g^a)^k \pmod p$.

5. Baba sends (γ, δ) to Ali.

- **Decryption by Ali.**
  To decrypt the ciphertext (γ, δ), Ali proceeds as follows.

  1. Ali computes $m \equiv \gamma^{-a}\delta \pmod{p}$.

The correctness of decryption follows from the equalities

$$\gamma^{-a}\delta \equiv \left(g^k\right)^{-a} m \left(g^a\right)^k \equiv m \pmod{p}.$$

Maple code 5.3.1.

The following procedure outputs a prime number $p \in [2^n, 2^{n+1}]$ and a generator g of $(\mathbb{Z}/p\mathbb{Z})^*$.

```
      Maple:    El Gamal public and secret keys

elgamalkeys:= proc (n)
local p,g,fset,k,test,t,i,a,ga;
with(numtheory):
p:=nextprime(rand(2^n,2^(n+1))());
fset:=factorset(p-1);
k:=nops(fset);
g:=1;test:=1;
while test=1 do
    test:=2;
    g:=g+1;
    for i from 1 to k do
        t:=g&^((p-1)/fset[i]) mod p;
        if t=1 then
            test:=1;
        end if;
    end do;
end do;
a:=rand(2..p-2)();
ga:=g&^a mod p;
return p,g,ga,a;
end proc:
```

Maple code 5.3.2.

The following procedure enables to encrypt a message m and to output the quantities γ and δ.

```
      Maple:    El Gamal encryption

elgamalencrypt:= proc (p,g,ga)
local m,k,gamma,delta;
m:=rand(2..p-1)();
k:=rand(2..p-2)();
gamma:=g&^k mod p;
delta:=m*(ga&^k mod p) mod p;
return gamma,delta,m;
end proc:
```

Maple code 5.3.3.

The following procedure enables to decrypt a message (γ, δ) and to output the original message m.

```
      Maple:    El Gamal decryption

elgamaldecrypt:= proc (p,a,gamma,delta)
local m,k;
m:=(delta*(gamma&^(-a) mod p)) mod p;
return m;
end proc:
```

Maple code 5.3.4.

The following procedure simulates the hole El Gamal encryption scheme.

```
      Maple:    El Gamal cryptosystem

elgamal:=proc(n);
local s,p,g,ga,a,t,gamma,delta,m,u;
s:=elgamalkeys(n);
    p:=s[1];
    g:=s[2];
    ga:=s[3];
    a:=s[4];
t:=elgamalencrypt(p,g,ga);
    gamma:=t[1];
    delta:=t[2];
    m:=t[3];
u:=elgamaldecrypt(p,a,gamma,delta);
return m,u;
end proc:
```

Exercice 5.3.5. Perform the ElGamal cryptosystem with the following parameters
Ali: $p = 1009$, $g = 11$, $a = 37$.
Baba: $m = 543$, $k = 218$.

Maple code 5.3.6. Maple: El Gamal

```
p:=1009;g:=11;a:=37;m:=543;k:=218;
G:=power(g,a) mod p;
gama:=power(g,k) mod p;
delta:=m*power(G,k) mod p;
m2:=delta/(power(gama,a) mod p) mod p;
m2-m;
```

Exercice 5.3.7. Perform the ElGamal cryptosystem with the following parameters
Ali: $p = 1009$, $g = 11$, $a = 37$.
Baba: $m =$ "$RabatCasa$", $k = 218$.

Maple code 5.3.8. Maple: El Gamal

```
p:=1009;g:=11;a:=37;m:=543;k:=218;
G:=power(g,a) mod p;
gama:=power(g,k) mod p;
mt:="Rabat Casa";
m:=convert(mt,bytes);
delta:=[];
for i from 1 to nops(m) do
    delta:=[op(delta),m[i]*power(G,k) mod p];
end do:
delta;
m2:=[];
for i from 1 to nops(delta) do
    m2:=[op(m2),delta[i]/(power(gama,a) mod p) mod p];
end do:
m2;
m2-m;


m2:=delta/(power(gama,a) mod p) mod p;
m2-m;
```

5.4 The Discrete Logarithm Problem (DLP)

In the Diffie-Hellman process, the following equations are involved.

$$\begin{aligned} A &\equiv g^a \pmod{p} \quad \text{with the unknown } a. \\ B &\equiv g^b \pmod{p} \quad \text{with the unknown } b. \end{aligned}$$

Similarly, the following equations appear during the ElGamal scheme.

$$\begin{aligned} \gamma_a &\equiv g^a \pmod{p} \quad \text{with the unknown } a, \\ \gamma &\equiv g^k \pmod{p} \quad \text{with the unknown } k, \\ \delta &\equiv m(g^a)^k \pmod{p} \quad \text{with the unknown } m, \ a \text{ and } k. \end{aligned}$$

It is clear that the Diffie-Hellman and the ElGamal scheme share a common problem: the discrete problem.

Definition 5.4.1 (Discrete Logarithm Problem (DLP))**.** Let p be a prime number and let g be a generator of $\mathbb{Z}_p^*$. Given $a \in \mathbb{Z}_p^*$, find a positive integer x such that

$$g^x \equiv a \pmod{p}.$$

The number x is called the discrete logarithm of a to the base g and is denoted by $\log_g(a)$.

The following theorem concerns the solutions of the DLP.

Proposition 5.4.2. *Let p be a prime number and let g be a generator of $\mathbb{Z}_p^*$. Given $a \in \mathbb{Z}_p^*$, there are infinitely many integers x such that*

$$g^x \equiv a \pmod{p}.$$

Proof. Since g is a generator of $\mathbb{Z}_p^*$ and $a \in \mathbb{Z}_p^*$, then there exists an integer x_0 such that $g^{x_0} \equiv a \pmod{p}$. Define $x = x_0 + m(p-1)$ for an integer m. By Fermat's little theorem, we get

$$g^x \equiv g^{x_0+m(p-1)} \equiv g^{x_0} \cdot \left(g^{p-1}\right)^m \equiv g^{x_0} \equiv a \pmod{p}.$$

Hence, there are infinitely many solutions to the DLP. □

Observe that in the Diffie-Hellamn protocol, the values $A \equiv g^a \pmod{p}$ and $B \equiv g^b \pmod{p}$ are public. Nevertheless, it seems very difficult to build $g^{ab} \pmod{p}$ using $g^a \pmod{p}$ and $g^b \pmod{p}$. This is the Diffie-Hellman Problem.

Definition 5.4.3 (The Diffie-Hellman Problem)**.** Let p be a prime number and g an integer. The Diffie-Hellman Problem is the problem of computing the value of $g^{ab} \pmod{p}$ from the known values of $g^a \pmod{p}$ and $g^b \pmod{p}$.

Clearly, if we can solve the DLP, then we can solve the Diffie-Hellamn Problem. It is not known if the opposite direction is true in general.

5.5 Recommendations for the primes for Diffie-Hellman and ElGamal

5.5.1 Recommendations for the structure of the prime

Fact 5.5.1. The prime number should satisfy $p-1=2q$ where q is a prime number.

This recommendation is practical in view of the following result.

Proposition 5.5.2. *Suppose that the prime number p is such that $p-1=2q$ where q is a prime number. Then each element of $\mathbb{Z}_p^*$ has order 1, 2, q or $p-1$.*

Proof. Let $a \in \mathbb{Z}_p^*$. By Lagrange's theorem, we know that the order of a is a divisor of $p-1=2q$. It follows that the order of a is one of the values 1, 2, q or $p-1$. □

5.5.2 Recommendations for the size of the order

Fact 5.5.3. The base should have a large order.

Let p be a prime number and g an element of order q. This recommendation is in relation with two methods to solve the discrete logarithm problem: Exhaustive search with running time $\mathcal{O}(q)$ and Shanks's Babystep–Giantstep Algorithm. Suppose that $a \equiv g^x \pmod{p}$ with $1 \leq x \leq p-2$. Let $k = \lfloor \sqrt{q} \rfloor + 1$. Shanks's Babystep–Giantstep Algorithm computes the lists

$$\begin{array}{ll} \text{Baby Step:} & 1, g^2, g^3, \ldots, g^k, \\ \text{Giant Step:} & a, ag^{-k}, ag^{-2k}, \ldots, ag^{-k^2}. \end{array}$$

For some integers i and j, we have $g^i \equiv ag^{-jk} \pmod{p}$. Then $a \equiv g^{i+jk} \mod p$. It follows that $x \equiv i+jk \pmod{p-1}$. It is proved that the running time of this method is $\mathcal{O}(k \log k) = \mathcal{O}\left(\sqrt{q} \log q\right)$.

5.5.3 Recommendations for the structure of the order

Fact 5.5.4. The base should have an order with a large prime divisor.

This recommendation follows the Pohlig-Hellman method for logarithms. Given the factorization of the order q of the base g as

$$q = \prod_{i=1}^{k} p_i^{e_i},$$

the running time of the Pohlig-Hellman method is

$$\mathcal{O}\left(\sum_{i=1}^{k} e_i \left(\log q + \sqrt{p_i}\right)\right).$$

Chapter 6

Cryptanalyse de RSA par les Fractions Continues

6.1 Les fractions continues

6.1.1 Définitions et propriétés

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

Maple code 6.1.1.

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,....]`

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 $x = 1 + 7^{\frac{1}{3}}$.

Maple code 6.1.2.

Proramme	Commentaires
restart:	<--- Remise à zéro
with(numtheory):	<--- Fonctionnalités "Théorie des Nombres"
Digits:=100:	<--- Précision
x:=1+7^(1/3):	<--- Un nombre réel
s:=cfrac(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

Theorem 6.1.3. *Soit $[a_0, a_1, a_2, \cdots]$ la fraction continue d'un nombre x. Alors les convergentes $\frac{p_n}{q_n}$ de x vérifient pour tout $n \geq -2$*

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

Maple code 6.1.4.

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):	
long:=100:	
s:=cfrac(x,long,'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)

Programme	Commentaires

`for n from -2 to long-1 do`
`  r := nu(n)*de(n+1)-nu(n+1)*de(n);`
`  dif := (-1)^(n+1)-r;`
`  print(n, dif):`
`end do:`	

Corollary 6.1.5. *Les convergentes* $\frac{p_n}{q_n}$ *d'un nombre réel* x *vérifient* $pgcd(p_n, q_n) = 1$ *pour tout* $n \geq 0$.

Maple code 6.1.6.

Programme	Commentaires

`for n from 0 to long-1 do`
`  g := gcd(nu(n), de(n)):`
`  print(n, g):`
`end do:`	

Theorem 6.1.7. *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 :*

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

Maple code 6.1.8.

Programme	Commentaires

`for n from 0 to trunc((1/2)*long) do`
`  dif1:= nu(2*n-2)/de(2*n-2)-nu(2*n)/de(2*n):`
`  print(n, sign(dif1)):`
`end do:`
`for n from 0 to trunc((1/2)*long) do`
`  dif2 := nu(2*n)/de(2*n)-evalf(x):`
`  print(n, sign(dif2)):`
`end do:`
`for n from 0 to trunc((1/2)*long)-1 do`
`  dif3 := evalf(x)-nu(2*n+1)/de(2*n+1):`
`  print(n, sign(dif3)):`
`end do:`
`for n from 1 to trunc((1/2)*long)-1 do`
`  dif4:=nu(2*n+1)/de(2*n+1)-nu(2*n-1)/de(2*n-1):`
`  print(n, sign(dif4)):`
`end do`	

Corollary 6.1.9. *Si $[a_0, a_1, a_2, \cdots]$ 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 $n \geq 0$, $|q_{n+1}x - p_{n+1}| < |q_n x - p_n|$.*

Maple code 6.1.10.

Programme	Commentaires

```
for n from 0 to long-1 do
    dif1 := de(n)*evalf(x)-nu(n);
    dif2 := de(n+1)*evalf(x)-nu(n+1);
    print(n, sign(dif1)*sign(dif2)):
end do:
for n from 0 to long-1 do
    dif3 := abs(de(n)*evalf(x)-nu(n)):
    dif4 := abs(de(n+1)*evalf(x)-nu(n+1)):
    dif := dif4-dif3:
    print(n, sign(dif)):
end do:
```

Proposition 6.1.11. *Si $x = [a_1, a_2, a_3, \cdots]$, alors les convergentes $\frac{p_n}{q_n}$ de x vérifient pour tout $n \geq 0$,*

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

Maple code 6.1.12.

Programme	Commentaires

```
for n from 0 to long-1 do
    dif := abs(evalf(x)-nu(n)/de(n))-1/(de(n)*de(n+1)):
    print(n, sign(dif)):
end do:
```

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

Theorem 6.1.13 (Meilleurs approximations)**.** *Soit $[a_1, a_2, a_3, \cdots]$ 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 $|q_n x - p_n| \leq |qx - p|$.*
2. *Si $q \leq q_n$, alors $\left| x - \frac{p_n}{q_n} \right| \leq \left| x - \frac{p}{q} \right|$.*

Proof. 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 6.1.3. En effet, on a $p_n q_{n+1} - p_{n+1} q_n = (-)^{n+1}$ et donc

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

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. □

Proposition 6.1.14. *Si $[a_0, a_1, a_2, \cdots]$ est la fraction continue d'un nombre x, alors pour $n \geq 0$, on a*

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

Maple code 6.1.15.

Programme	Commentaires

```
for n from 0 to long-1 do
    dif1:=abs(evalf(x)-nu(n)/de(n))-1/(2*de(n)^2):
    dif2:=abs(evalf(x)-nu(n+1)/de(n+1))-1/(2*de(n+1)^2):
    print(n,sign(dif1),sign(dif2)):
    if sign(dif1)+sign(dif2)>1 then
        print(FAUX)
    end if:
end do:
```

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

Theorem 6.1.16. *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.

Proof. 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 6.1.13 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

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

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

6.2 Cryptanalyse de RSA par les fractions continues

6.2.1 L'attaque de Wiener

Proposition 6.2.1. *Soit $N = pq$ un module RSA où les nombres premiers p et q vérifient $q < p < 2q$. Alors*

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}.$$

Exercice: Démontrer la proposition.

Proposition 6.2.2. *Soit $N = pq$ un module RSA où les nombres premiers p et q vérifient $q < p < 2q$. Alors*

$$2\sqrt{N} < p + q < \frac{3\sqrt{2}}{2}\sqrt{N}.$$

Exercice: a) Démontrer la proposition.
b) Donner un encadrement de $\phi(N)$ en fonction de N.

Theorem 6.2.3. *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.*

Proof. 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 $ed - k\varphi(N) = 1$. 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 6.1.16, $\frac{k}{d}$ 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 4.2.1 on peut calculer p et q et donc trouver la factorisatio de N. □

Exercice 6.2.4.

1. Write a maple procedure wiener(N, e) that computes $k, d, \phi(N), p, q$ when $ed - k\phi(N) = 1$ and $d < \frac{1/3}{N}^{\frac{1}{4}}$.
2. Find the factorization of $N = 1235882707637$ with $e = 434466294109$ using wiener(N, e).

Maple code 6.2.5.

```
        Programme

wiener:=proc(N,e)
local cv,i,k,d,phin,q,delta;
cfrac(e/N,10,'cv'):
for i from 2 to nops(cv) do
    k:=numer(cv[i]);
    d:=denom(cv[i]);
    phin:=(e*d-1)/k;
    if round(phin)=phin then
        delta:=(phin-N-1)^2-4*N;
        if delta>0 then
            q:=(-(phin-N-1)-sqrt(delta))/2;
            if round(q)=q then
                return q,N/q,phin,d,k;
            end if;
        end if;
    end if;
end do;
end proc:

N:=1235882707637;
e:=434466294109;
wiener(n,e);
```

Maple code 6.2.6.

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

EXERCICE 3.

1) Démontrer le théorème suivant:

Theorem 6.2.7. *Soit d un entier positif, qui n'est pas un carré parfait. Si x et y sont deux nombres entiers positifs qui vérifient l'équation :*

$$x^2 - dy^2 = 1,$$

alors $\frac{x}{y}$ est une convergente de $\sqrt{d}$.

2) Programmer ce théorème et déterminer une solution (x, y) lorsque $d = 1237$. **EXERCICE 4.**

1) Démontrer le théorème suivant:

Theorem 6.2.8. *Soit a, b et N des entiers positifs. Si x et y sont deux entiers positifs qui vérifient $pgcd(x, y) = 1$ et*

$$ax^2 + by^2 = N,$$

alors il existe une solution t de la congruence $at^2 + b \equiv 0 \pmod{N}$ et un entier u tel $x = Nu - ty$. De plus, $\frac{u}{y}$ est une convergente de $\frac{t}{N}$.

2) Programmer ce théorème et déterminer une solution (x, y) lorsque

$$a = 127, \qquad b = 1547, \qquad N = 324655759005538.$$

sachant que les solutions de la congruence $at^2 + b \equiv 0 \pmod{N}$ s'obtiennet en effectuant **msolve**$(a * t^2 + b = 0, N)$.

Chapter 7

Réductions des Réseaux

7.1 Introduction aux Réseaux

L'algorithme LLL a été inventé en 1982 et porte les initiales de 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.

Definition 7.1.1. Soit n et d deux un 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 $(b_1 \cdots, b_d)$ 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.

If $\mathcal{L} \subset \mathbb{R}^n$ is a lattice of dimension d, then it is a discrete additive subgroup of $\mathbb{R}^n$.

Proposition 7.1.2. *Let $\mathcal{L}$ be a lattice of dimension d and rank n. Then $\mathcal{L}$ can be written as the rows of an $d \times n$ matrix with real entries.*

Proof. Let $(b_1 \cdots, b_d)$ be a basis of $\mathcal{L}$ such that, for $1 \leq i \leq d$,

$$b_i = \begin{bmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{ni} \end{bmatrix}.$$

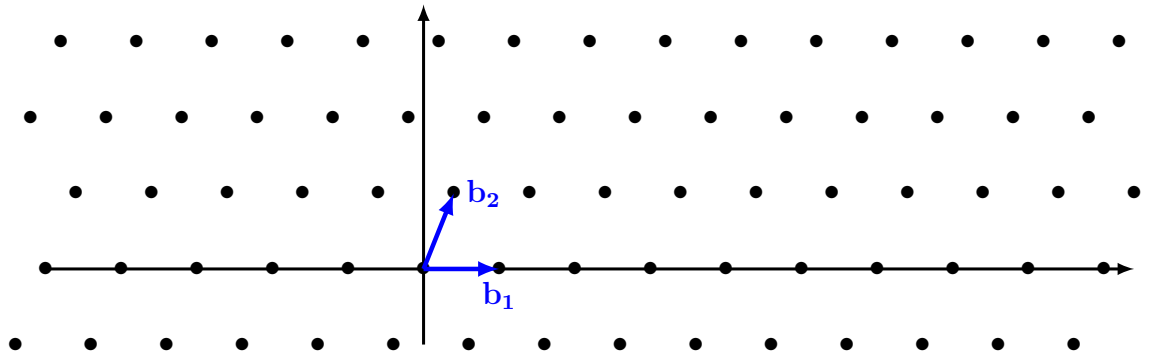


Figure 7.1: A lattice with the basis (b_1, b_2)

Let v be a vector of $\mathcal{L}$. Then $v = \sum_{i=1}^{d} x_i b_i$ for $x_i \in \mathbb{Z}$. Hence v can be rewritten as

$$v = x_1 \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{bmatrix} + x_2 \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{bmatrix} + \ldots + x_d \begin{bmatrix} a_{1d} \\ a_{2d} \\ \vdots \\ a_{nd} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & \cdots & a_{2d} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nd} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{bmatrix}.$$

The involved matrix is constructed using the coordinates of the basis $(b_1 \cdots, b_d)$ as follows

$$\begin{bmatrix} b_1 & b_2 & \cdots & b_d \\ \downarrow & \downarrow & \cdots & \downarrow \\ a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & \cdots & a_{2d} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nd} \end{bmatrix}.$$

□

The following result shows that in a lattice $\mathcal{L}$ with dimension $d \geq 2$, any two couples of bases are related with a unimodular matrix.

Proposition 7.1.3. *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice of dimension d. Let $(b_1 \cdots, b_d)$ and $(b'_1 \cdots, b'_d)$ be two bases of $\mathcal{L}$. Then there exists a $d \times d$ matrix U with entries in $\mathbb{Z}$ and $\det(U) = \pm 1$ such that*

$$\begin{bmatrix} b'_1 \\ b'_2 \\ \vdots \\ b'_d \end{bmatrix} = U \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_d \end{bmatrix}.$$

Proof. Let $(b_1 \cdots, b_d)$ and $(b'_1 \cdots, b'_d)$ be two bases of $\mathcal{L}$. Since every vector $b'_i \in \mathcal{L}$, then

$$\begin{bmatrix} b'_1 \\ b'_2 \\ \vdots \\ b'_d \end{bmatrix} = \begin{bmatrix} u_{11}b_1 + u_{12}b_2 + \ldots + u_{1d}b_d \\ u_{21}b_1 + u_{22}b_2 + \ldots + u_{2d}b_d \\ \vdots \\ u_{d1}b_1 + u_{d2}b_2 + \ldots + u_{dd}b_d \end{bmatrix} = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1d} \\ u_{21} & u_{22} & \cdots & u_{2d} \\ \vdots & \vdots & \vdots & \vdots \\ u_{d1} & u_{d2} & \cdots & u_{dd} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_d \end{bmatrix} = U \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_d \end{bmatrix},$$

where U is a $d \times d$ matrix with integer entries. This can be rewritten as

$$(b'_1, b'_2, \ldots, b'_d)^t = U(b_1, b_2, \ldots, b_d)^t.$$

Similarly, there exist a $d \times d$ matrix U' with integer entries such that

$$(b_1, b_2, \ldots, b_d)^t = U'(b'_1, b'_2, \ldots, b'_d)^t.$$

Hence,

$$(b'_1, b'_2, \ldots, b'_d)^t = UU'(b'_1, b'_2, \ldots, b'_d)^t,$$

which implies $UU' = I_d$ where I_d is the $d \times d$ identity matrix. Taking determinant, we get $\det(U)\det(U') = 1$. Since the entries of U and U' are integers, then $\det(U), \det(U') \in \mathbb{Z}$ and $\det(U) = \det(U') = \pm 1$. □

Observe that any $d \times d$ triangular matrix U with diagonal entries equal to ± 1 satisfies $\det(U) = \pm 1$. This shows that a lattice $\mathcal{L}$ with dimension $d \geq 2$ has infinitely many bases.

Definition 7.1.4. Let $\mathcal{L}$ be a lattice with a basis $(b_1 \cdots, b_d)$. The volume or determinant of $\mathcal{L}$ is

$$\det(\mathcal{L}) = \sqrt{\det(BB^t)},$$

where B is the $d \times n$ matrix of formed by the rows of the basis.

Proposition 7.1.5. *Let $\mathcal{L}$ be a lattice of dimension d. Then the* $\det(\mathcal{L})$ *is independent of the choice of the basis.*

Proof. Let $(b_1 \cdots, b_d)$ and $(b'_1 \cdots, b'_d)$ be two bases of $\mathcal{L}$ with matrices B and B'. Then there exists a $d \times d$ matrix U with entries in $\mathbb{Z}$ and $\det(U) = \pm 1$ such that $B' = UB$. Then since $B'B'^t = UBB^tU^t$, we get

$$\det(B'B'^t) = \det\left(UBB^tU^t\right) = \det(U)\det\left(BB^t\right)\det\left(U^t\right) = \det\left(BB^t\right),$$

where we used $\det(UU^t) = \det(U)^2 = 1$. Hence $\sqrt{\det(B'B'^t)} = \sqrt{\det(BB^t)} = \det(\mathcal{L})$. □

When $d = n$, that is L is a full-rank lattice, the matrix of the basis is a $n \times n$ matrix and the following property holds.

Lemma 7.1.6. *Let $\mathcal{L}$ be a full-rank lattice of dimension n. If $(b_1 \cdots, b_n)$ is a basis of $\mathcal{L}$ with matrix B, then*

$$\det(L) = |\det(B)|.$$

Proof. Since $\det(B^t) = \det(B)$, then

$$\det(\mathcal{L}) = \sqrt{\det(BB^t)} = \sqrt{\det(B)\det(B^t)} = \sqrt{\det(B)^2} = |\det(B)|.$$

□

The determinant of a lattice can be considered as the volume of its fundamental domain.

Definition 7.1.7. Let $\mathcal{L}$ be a lattice with a basis $(b_1 \cdots, b_d)$. The fundamental domain or parallelepipede for $\mathcal{L}$ is the set

$$\mathcal{P}(b_1 \cdots, b_d) = \left\{ \sum_{i=1}^{d} x_i b_i, \ | \ 0 \leq x_i < 1 \right\}.$$

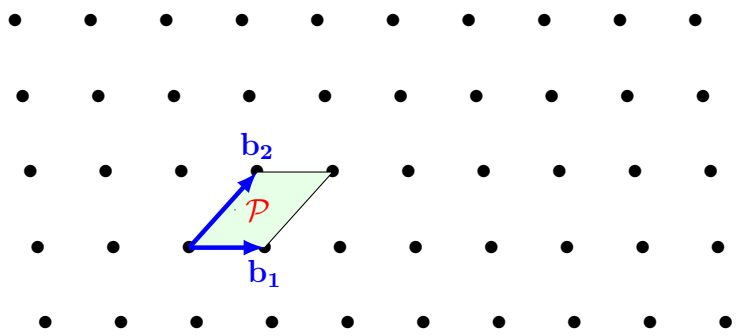


Figure 7.2: The fundamental domain for the basis (b_1, b_2)

Proposition 7.1.8. *Let $\mathcal{L}$ be a lattice with a basis $(b_1, \ldots, b_d)$. Then the volume $\mathcal{V}$ of the fundamental domain $\mathcal{P}(b_1, \ldots, b_d)$ satisfies*

$$\mathcal{V}(\mathcal{P}(b_1, \ldots, b_d)) = \det(\mathcal{L}).$$

The former result shows that any two bases of a lattice have the same volume $\mathcal{V}$ of the fundamental domain. This shows again that $\det(\mathcal{L})$ is an important invariant in a lattice.

When $d = n$, that is L is a full-rank lattice, the matrix of the basis is a $n \times n$ matrix and the following property holds. Lattices whose bases have integer coordinates are very convenient for various problems. Such lattices are called *integral lattices*. Also, many problems in lattice theory involve inner product of vectors and distance minimization and the most intuitive way to measure distance in a lattice is by using the Euclidean norm.

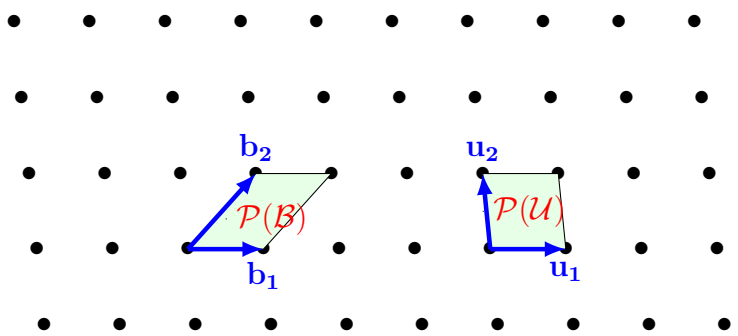


Figure 7.3: The fundamental domain for the bases (b_1, b_2) and (u_1, u_2)

7.2 The Gram-Schmidt Orthogonalization

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, la plus orthogonale possible dans un réseau. Pour cela, on considère le produit scalaire habituel de deux vecteurs et la norme euclidienne d'un vecteur.

Definition 7.2.1. 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

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

Exercice 7.2.2. 1. Programmer le produit scalaire à l'aide de Maple.

2. Calculer $\langle u, v \rangle$ avec $u = (1, 2, 3, 4)$ et $v = (-1, -2, -3, -4)$.

Maple code 7.2.3.

```
      maple: Produit Scalaire

scal:= proc (x, y)
add(x[i]*y[i], i = 1 .. nops(x));
end proc:
```

```
      Maple: Exemple Produit Scalaire

u := [1, 2, 3, 4]; v := [-1, -2, -3, -4];
scal(u, v);
```

Dans Maple, le produit scalaire est la fonction **DotProduct(u,v)**.

Maple code 7.2.4.

```
      Maple: Exemple Produit Scalaire

with(LinearAlgebra):
u := [1, 2, 3, 4]; v := [-1, -2, -3, -4];
DotProduct(u, v);
```

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

Theorem 7.2.5 (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*

$$b_1^* = b_1, \quad \text{et pour } i \geq 2, \quad b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*,$$

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.

Proof. 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

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_{n-1} \\ b_n \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ \mu_{2,1} & 1 & 0 & 0 & \cdots & 0 \\ \mu_{3,1} & \mu_{3,2} & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mu_{n_1,1} & \mu_{n-1,2} & \mu_{n-1,3} & \cdots & 1 & 0 \\ \mu_{n,1} & \mu_{n,2} & \mu_{n,3} & \cdots & \mu_{n,n-1} & 1 \end{bmatrix} \begin{bmatrix} b_1^* \\ b_2^* \\ b_3^* \\ \vdots \\ b_{n-1}^* \\ b_n^* \end{bmatrix} = U \begin{bmatrix} b_1^* \\ b_2^* \\ b_3^* \\ \vdots \\ b_{n-1}^* \\ b_n^* \end{bmatrix}.$$

La matrice U est est une matrice triangulaire dont la diagonale est formée de 1. Donc $\det(U) = 1$. 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 $1 \leq k \leq i-1$

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

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

Exercice 7.2.6. Orthogonaliser les vecteurs suivants :

1. $b_1 = (3, 1)$, $b_2 = (1, 2)$.

2. $b_1 = (3, 2, 5)$, $b_2 = (2, 4, -1)$, $b_3 = (-2, -1, 6)$.

Maple code 7.2.7.

```
      Maple: Gram-Schmidt

with(LinearAlgebra):
b1 := Vector([3, 1]);
b2 := Vector([1, 2]);
bb1 := b1;
u21 := DotProduct(b2, b1)/DotProduct(b1, b1);
bb2 := -b1*u21+b2;
```

Maple code 7.2.8.

```
      Maple: Gram-Schmidt

with(LinearAlgebra):
b1 := Vector([3, 2, 5]);
b2 := Vector([2, 4, -1]);
b3:=Vector([-2, -1, 6]);
bb1 := b1;
u21 := DotProduct(b2, b1)/DotProduct(b1, b1);
bb2 := -b1*u21+b2;
u31 := DotProduct(b3,bb1)/DotProduct(bb1, bb1);
u32 :=DotProduct(b3,bb2)/DotProduct(bb2, bb2);
bb3 := -bb1*u31-bb2*u32+b3;
DotProduct(bb1, bb2);
DotProduct(bb1, bb3);
DotProduct(bb2, bb3);
```

La méthode de Gram-Schmidt, décrite dans Theorem 41 peut être facilement mise en algorithme, comme dans l'algorithme 41.

Algorithm 28 : La méthode de Gram-Schmidt

Input : Une base $(b_1 \cdots, b_n)$.
Output : Une base orthogonale $(b_1^* \cdots, b_n^*)$.
1: Poser $b_1^* = b_1$.
2: **For** $i = 1, 2, \cdots n$, **do**
3: **For** $j = 1, 2, \cdots i-1$, **do**
4: Calculer $\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$.
5: **End For**
6: Calculer $b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$.
7: **End For**

Example 7.2.9.

1. Programmer la méthode de Gram-Schmidt avec pour entrée une matrice carrée.

2. Orthogonaliser la base (b_1, b_2, b_3) avec $b_1 = (3, 2, 5)$, $b_2 = (2, 4, -1)$, $b_3 = (-2, -1, 6)$.

```
      La méthode de Gram-Schmidt

gramschmidt:=proc(B)
local i, j, n, M, P, u, k;
with(LinearAlgebra);
n:=nops(B);
for i to n do
    M[i]:=B[i];
    for j to i-1 do
        u[j]:= DotProduct(B[i],M[j])/DotProduct(M[j],M[j]);
        M[i]:= M[i]-M[j]*u[j];
    end do;
end do;
M :=seq(M[i], i = 1 .. n);
return M;
end proc:
```

Le programme suivant prend en entrée la base (b_1, b_2, b_3) dont les vecteurs sont $b_1 = (3, 2, 5)$, $b_2 = (2, 4, -1)$, $b_3 = (-2, -1, 6)$ et sort la base orthogonale $b_1^* = (3, 2, 5)$, $b_2^* = \left(\frac{49}{38}, \frac{67}{19}, -\frac{83}{38}\right)$, $b_3^* = \left(-\frac{1738}{717}, \frac{1027}{717}, \frac{632}{717}\right)$.

Maple code 7.2.10.

```
      La méthode de Gram-Schmidt

b1 :=[3, 2, 5];
b2 :=[2, 4, -1];
b3:=[-2, -1, 6];
B:=[b1,b2,b3];
gramschmidt(B);
```

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 $b_1 = (3, 2, 5)$, $b_2 = (2, 4, -1)$, $b_3 = (-2, -1, 6)$.

Programme	Commentaires
`with(LinearAlgebra):`	`<--- package LinearAlgebra`
`b1:=Vector([3,2,5]):`	`<--- Premier vecteur`
`b2 := Vector([2,4,-1]):`	`<--- Deuxième vecteur`
`b3 := Vector([-2,-1,6]):`	`<--- Troisième vecteur`
`B := GramSchmidt([b1, b2, b3]);`	`<--- La procédure de Gram-Schmidt`
`DotProduct(B[1], B[2]);`	`<--- Vérification du produit scalaire`
`DotProduct(B[1], B[3]);`	`<--- Vérification du produit scalaire`
`DotProduct(B[2], B[3]);`	`<--- Vérification du produit scalaire`

La base $(b_1^*, \cdots, b_n^*)$ a plusieurs propriétés remarquables, comme dans l'exemple ci-suivant.

Lemma 7.2.11. *Soient $(b_1 \cdots, b_n)$ une famille indépendante de vecteurs. On considère la famille de vecteurs $(b_1^* \cdots, b_n^*)$ produite par l'orthogonalisation de Gram-Schmidt. Alors*

1. $\|b_i^*\| \leq \|b_i\|$ *pour* $1 \leq i \leq n$.
2. $\langle b_i, b_i^* \rangle = \langle b_i^*, b_i^* \rangle$ *pour* $1 \leq i \leq n$.

Proof. 1. On a $\|b_1^*\| = \|b_1\|$ et pour $2 \leq i \leq n$,

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

avec pour $j < i$

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

Alors, puisque les vecteurs $b_1, \ldots, b_i$ sont deux à deux orthogonaux, on obtient

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

Ainsi $\|b_i^*\| \leq \|b_i\|$.

2. On a $\langle b_1, b_1^* \rangle = \langle b_1^*, b_1^* \rangle$ et pour $2 \leq i \leq n$,

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

□

Corollary 7.2.12 (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*

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

Proof. Par définition, on sait que $\det(L) = |\det(b_1 \cdots, b_n)|$. On sait aussi par Théorème 7.2.5 que $(b_1 \cdots, b_n)^t = U(b_1^*, \cdots, b_n^*)^t$ où U est une matrice triangulaire inférieure avec $\det(U) = 1$. Alors, puisque les vecteurs $b_1^*, \cdots, b_n^*$, sont orthogonaux deux à deux et $\|b_i^*\| \leq \|b_i\|$ pour $1 \leq i \leq n$, on obtient:

$$\det(L) = \det(U) |\det(b_1^* \cdots, b_n^*)| = \prod_{i=1}^{n} \|b_i^*\| \leq \prod_{i=1}^{n} \|b_i\|.$$

□

Exercice 7.2.13. On considère le réseau L engendré par la base $(b_1, \ldots, b_n)$. Ecrire une procédure Maple qui calcule $\det(L)$.

```
      Maple: procédure det

with(LinearAlgebra)
deter:=proc(B);
local GS,n,d,i;
GS:= GramSchmidt(B);
n:=nops(B);
d:=1;
for i from 1 to n do
    d:=d*sqrt(DotProduct(GS[i],GS[i]));
end do;
return d;
end proc:
```

Exercice 7.2.14. On considère le réseau L engendré par la base (b_1, b_2, b_3) avec $b_1 = (3, 2, 5)$, $b_2 = (2, 4, -1)$, $b_3 = (-2, -1, 6)$.

1. Calculer $\det(L)$.

2. Comparer $\det(L)$ et $\prod_{i=1}^{3} \|b_i\|$.

Maple code 7.2.15.

```
      Maple: exemple

b1:=Vector([3,2,5]):
b2 := Vector([2,4,-1]):
b3 := Vector([-2,-1,6]):
B := [b1, b2, b3]:
d1:= simplify(deter(B));
d2:=Determinant(Matrix(B));
d3:=1;
for i from 1 to 3 do
    d3:=d3*sqrt(DotProduct(B[i],B[i]));
end do:
d3;
```

7.3 Les vecteurs courts d'un réseau

Lattices are used as a fundamental tool for cryptanalysis of various public key cryptosystems such as knapsack cryptosystems, RSA, NTRU and GGH. On the other hand, lattices are used as a theoretical tool for security analysis of several cryptosystems such as NTRU and LWE. These cryptosystems are related to hard computational problems in the theory of lattices such shortest nonzero vectors and minimal distances.

Definition 7.3.1. Let L be a lattice. The minimal distance λ_1 of $\mathcal{L}$ is the length of the shortest nonzero vector of $\mathcal{L}$:

$$\lambda_1 = \inf\{\|v\| \in \mathcal{L} \mid v \in \mathcal{L}\backslash\{0\}\} = \inf\{\|v-u\| \in \mathcal{L} \mid v, u \in \mathcal{L},\ v \neq u\}.$$

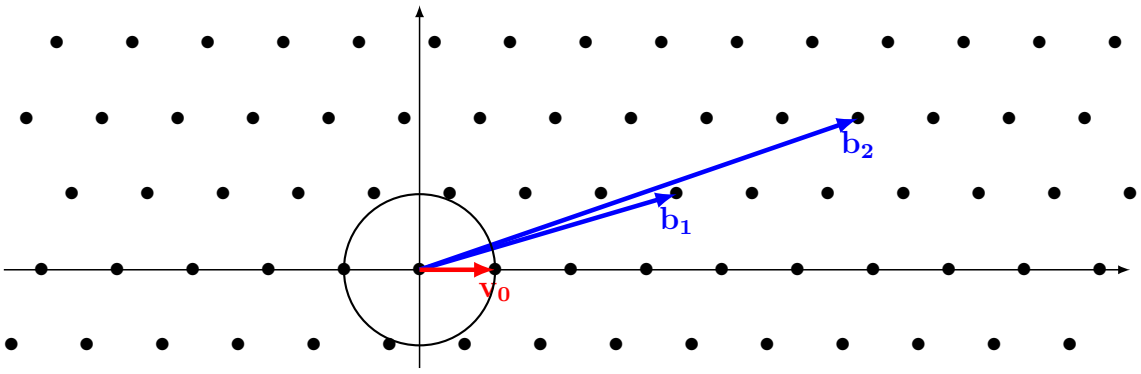


Figure 7.4: The shortest vectors are v_0 and $-v_0$

Example 7.3.2.

In dimension 2, finding the shortest vector in a lattice is very easy. Let $\mathcal{L}$ be a lattice with a basis (b_1, b_2) with

$$b_1 = \begin{bmatrix} 19239 \\ 2971 \end{bmatrix}, \quad b_1 = \begin{bmatrix} 22961 \\ 3546 \end{bmatrix}.$$

Then the shortest vector is in the form

$$v_0 = x_1 b_1 + x_2 b_2 = \begin{bmatrix} 19239x_1 + 22961x_2 \\ 2971x_1 + 3546x_2 \end{bmatrix},$$

for some integers $(x_1, x_2) \neq (0, 0)$ for which the norm

$$\|v_0\| = \left((19239x_1 + 22961x_2)^2 + (2971x_1 + 3546x_2)^2\right)^{1/2},$$

is as small as possible. We write this as $v_0 \approx 0$, that is

$$\begin{cases} 19239x_1 + 22961x_2 \approx 0 \\ 2971x_1 + 3546x_2 \approx 0 \end{cases}$$

Assume that $x_2 \neq 0$. Then

$$\frac{x_1}{x_2} \approx -\frac{22961}{19239}, \text{ and } \frac{x_1}{x_2} \approx -\frac{3546}{2971}.$$

This means that $\frac{x_1}{x_2}$ is a good approximation for $-\frac{22961}{19239}$ and $-\frac{3546}{2971}$, which can be found among their common convergents. Indeed, the common convergents are

$$-2, -1, -\frac{6}{5}, -\frac{31}{26}, -\frac{37}{31}.$$

Plugging the common convergents in $x_1b_1 + x_2b_2 = v_0$ and computing $\|v_0\|$, we get

$$\begin{aligned}
&(x_1, x_2) = (2, -1), \quad v_0 = [15517, 2396], \quad \|v_0\| = \sqrt{246518105}, \\
&(x_1, x_2) = (1, -1), \quad v_0 = [-3722, -575], \quad \|v_0\| = \sqrt{14183909}, \\
&(x_1, x_2) = (6, -5), \quad v_0 = [629, 96], \quad \|v_0\| = \sqrt{404857}, \\
&(x_1, x_2) = (31, -26), \quad v_0 = [-577, -95], \quad \|v_0\| = \sqrt{341954}, \\
&(x_1, x_2) = (37, -31), \quad v_0 = [52, 1], \quad \|v_0\| = \sqrt{2705}.
\end{aligned}$$

Using some extra algebra, one can show that $v_0 = 37b_1 - 31b_2$ is the shortest vector in the lattice $\mathcal{L}$.

Programme

```
with(numtheory):
m1:=-22961/19239:
cfrac(m1,20,'cv1'):cv1;
m1:=-3546/2971:
cfrac(m2,20,'cv2'):cv2;
```

Exercice 7.3.3. Let $\mathcal{L}$ be a lattice with a basis (b_1, b_2) with $b_1 = (412157, -14578)$, $b_2 = (21571, 695743)$. Find the shortest non-zero vector of $\mathcal{L}$.

Example 7.3.4.

In dimension $n \geq 3$, finding the shortest vector in a lattice is not so easy. For example, let $\mathcal{L}$ be a lattice with a basis (b_1, b_2, b_3) with

$$b_1 = \begin{bmatrix} 124797 \\ 2971 \\ 4781 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 95874 \\ 3546 \\ 7895 \end{bmatrix}, \quad b_3 = \begin{bmatrix} 56871 \\ 35462 \\ 16539 \end{bmatrix}.$$

Then the shortest vector is in the form

$$v_0 = x_1b_1 + x_2b_2 + x_3b_3 = \begin{bmatrix} 124797x_1 + 95874x_2 + 56871x_3 \\ 2971x_1 + 3546x_2 + 35462x_3 \\ 4781x_1 + 7895x_2 + 16539x_3 \end{bmatrix},$$

for some integers $(x_1, x_2, x_3) \neq (0, 0, 0)$ for which the $\|v_0\|^2$ is as small as possible. We have

$$\begin{aligned}\|v_0\|^2 =&(124797x_1 + 95874x_2 + 56871x_3)^2 + (2971x_1 + 3546x_2 + 35462x_3)^2 \\ &+ (4781x_1 + 7895x_2 + 16539x_3)^2.\end{aligned}$$

As we will see below, finding the shortest vector in a lattice is very hard in general. The short vector in the lattice $\mathcal{L}$ is

$$v_0 = -3b_1 + 4b_2 = \begin{bmatrix} 9105 \\ 5271 \\ 17237 \end{bmatrix}.$$

Definition 7.3.5. Let L be a lattice of dimension n. For $i = 1, \dots n$, the ith successive minimum of the lattice is

$$\lambda_i = \min\{\max\{\|v_1\|, \dots, \|v_i\|\} \mid v_1, \dots, v_i \in \mathcal{L} \text{ are linearly independent}\}.$$

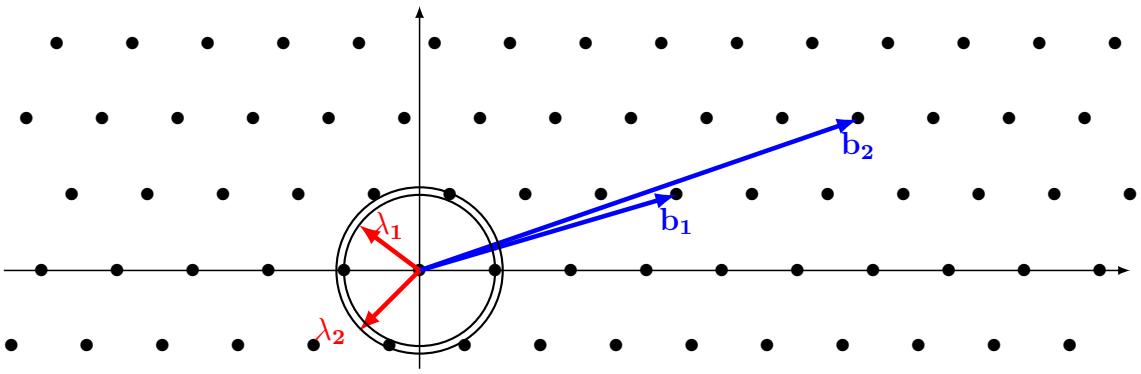


Figure 7.5: The first minima λ_1 and the second minima λ_2

Finding a vector v such that $\|v\| = \lambda_1$ is very hard in general. Nevertheless, in low dimension, the problem can be solved. For example, in dimension 2, Gauss'algorithm finds a basis (b_1, b_2) such that $\|b_1 = \lambda_1$ and $\|b_2\| = \lambda_2$ (see Subsection 7.3.1).

In the following, we list some computational problems that seem to be hard in general and on which some cryptographic systems have been based. An overview of many hard lattice problems and their interconnections is presented in [26].

Definition 7.3.6. Let $\mathcal{L}$ be a full rank lattice of dimension n in $\mathbb{Z}^n$.

1. **The Shortest Vector Problem (SVP):** Given a basis matrix B for $\mathcal{L}$, compute a non-zero vector $v \in \mathcal{L}$ such that $\|v\|$ is minimal, that is $\|v\| = \lambda_1(\mathcal{L})$.
2. **The Closest Vector Problem (CVP):** Given a basis matrix B for $\mathcal{L}$ and a vector $v \notin \mathcal{L}$, find a vector $u \in \mathcal{L}$ such that $\|v - u\|$ is minimal, that is $\|v - u\| = \mathrm{d}(v, \mathcal{L})$ where $\mathrm{d}(v, \mathcal{L}) = \min_{u \in \mathcal{L}} \|v - u\|$.
3. **The Shortest Independent Vectors Problem (SIVP):** Given a basis matrix B for $\mathcal{L}$, find n linearly independent lattice vectors $v_1, v_2, \ldots, v_n$ such that $\max_i \|v_i\| \leq \lambda_n$, where λ_n is the nth successive minima of $\mathcal{L}$.
4. **The approximate SVP problem (γSVP):** Fix $\gamma > 1$. Given a basis matrix B for $\mathcal{L}$, compute a non-zero vector $v \in \mathcal{L}$ such that $\|v\| \leq \gamma\lambda_1(\mathcal{L})$ where $\lambda_1(\mathcal{L})$ is the minimal Euclidean norm in $\mathcal{L}$.
5. **The approximate CVP problem (γSVP):** Fix $\gamma > 1$. Given a basis matrix B for $\mathcal{L}$ and a vector $v \notin \mathcal{L}$, find a vector $u \in \mathcal{L}$ such that $\|v - u\| \leq \gamma\lambda_1\mathrm{d}(v, \mathcal{L})$ where $\mathrm{d}(v, \mathcal{L}) = \min_{u \in \mathcal{L}} \|v - u\|$.

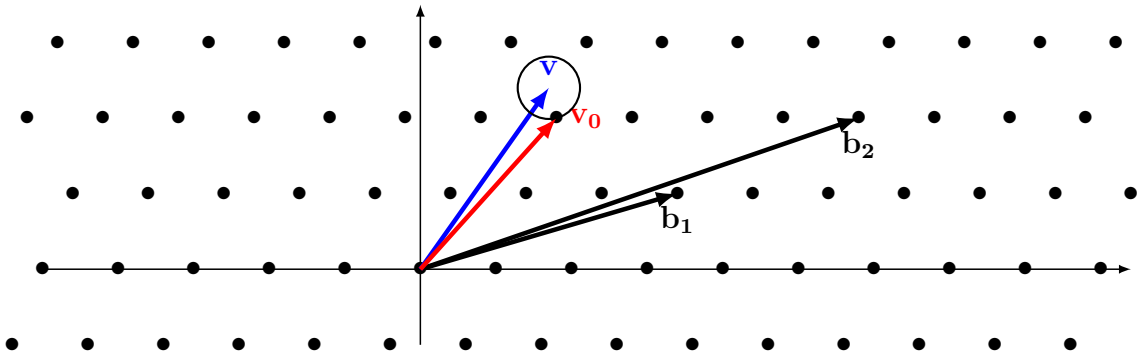


Figure 7.6: The closest vector to v is v_0

Some of such problems have been shown to be NP-hard, and in general, are known to be hard when the dimension is sufficiently large. No efficient algorithm is known to find the shortest vector nor the closest vector in a lattice. The next result, due to Minkowski gives a theoretical explicit upper bound in terms of $\dim(\mathcal{L})$ and $\det(\mathcal{L})$.

Theorem 7.3.7 (Minkowski)**.** *Let $\mathcal{L}$ be a lattice with dimension n. Then there exists a nonzero vector $v \in \mathcal{L}$ satisfying*

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

On the other hand, the Gaussian Heuristic implies that the expected shortest non-zero vector in a lattice $\mathcal{L}$ is approximately $\sigma(\mathcal{L})$ where

$$\sigma(\mathcal{L}) = \sqrt{\frac{\dim(\mathcal{L})}{2\pi e}} \left(\det(\mathcal{L})\right)^{\frac{1}{\dim(\mathcal{L})}}.$$

Exercice 7.3.8. On considère le réseau L muni de la base (b_1, b_2) avec $b_1 = (19239, 2971)$, $b_2 = (22961, 3546)$ et le vecteur le plus court $v_0 = 37b_1 - 31b_2$.

1. Vérifier l'inégalité de Minkowski.
2. Vérifier l'inégalité de l'heuristique de Gauss.

Maple code 7.3.9.

```
      Maple: Minkowski and Gauss heuristic

with(LinearAlgebra):
b1 := [19239, 2971];
b2 := [22961, 3546];
v0 := 37*b1-31*b2;
d:=Determinant(Matrix([b1, b2]));
Mink:=evalf(sqrt(DotProduct(v0,v0))/(sqrt(2)*d^(1/2)));
Gauss:=evalf(sqrt(DotProduct(v0,v0))/((sqrt(2/(2*Pi*exp(1)))*d^(1/2))));
```

7.3.1 Gauss'algorithm

Suppose that $\mathcal{L}$ is a lattice with a basis (b_1, b_2). Gauss'algorithm is used to find an optimal basis for $\mathcal{L}$ which is short and almost orthogonal. More precisely, it outputs a basis with length λ_1 and λ_2.

Lemma 7.3.10. *Let b_1 and b_2 non-zero vectors. Define b_2^* by*

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

Then b_2^* is the projection of b_2 onto the orthogonal line of b_1.

Proof. Let

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

Then

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

This means that b_2^* is orthogonal to b_1. Moreover, since $\langle b_1, b_2\rangle = \|b_1\|\|b_2\|\cos(b_1, b_2)$, then

$$\begin{aligned}\|b_2^*\|^2 &= \|b_2\|^2 - \frac{2\langle b_1, b_2\rangle^2}{\|b_1\|^2} + \frac{\langle b_1, b_2\rangle^2}{\|b_1\|^2}\\ &= \|b_2\|^2 - \|b_2\|^2\cos^2(b_1, b_2)\\ &= \|b_2\|^2\left(1 - \cos^2(b_1, b_2)\right)\\ &= \|b_2\|^2\sin^2(b_1, b_2).\end{aligned}$$

Hence $|b_2^*\| = \|b_2\|\sin(b_1, b_2)|$. This means that b_2^* is the projection of b_2 onto the orthogonal line of b_1. □

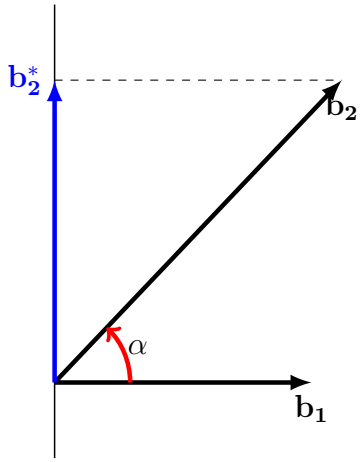


Figure 7.7: The orthogonal projection b_2^* of b_2 with $\alpha = (b_1, b_2)$

Since b_2^* is not necessary in $\mathcal{L}$, we replace the basis (b_1, b_2) by a basis (u_1, u_2) where

$$u_1 := b_1, \quad u_2 = b_2 - \left\lfloor \frac{\langle b_1, b_2\rangle}{\|b_1\|^2} \right\rceil b_1,$$

where $\lfloor x \rceil$ is the nearest integer to x.

Proposition 7.3.11. *Let b_1, b_2 be two linearly independent vectors. Define*

$$u_2 = b_2 - \left\lfloor \frac{\langle b_1, b_2\rangle}{\|b_1\|^2} \right\rceil b_1.$$

Then

$$-\frac{1}{2} < \frac{\langle b_1, u_2\rangle}{\|b_1\|^2} \leq \frac{1}{2}.$$

Proof. Let $m = \left\lfloor \frac{\langle b_1, b_2 \rangle}{\|b_1\|^2} \right\rceil$. Then

$$m - \frac{1}{2} < \frac{\langle b_1, b_2 \rangle}{\|b_1\|^2} \leq m + \frac{1}{2}.$$

Hence

$$-\frac{1}{2} < \frac{\langle b_1, b_2 \rangle}{\|b_1\|^2} - m \leq \frac{1}{2}.$$

We have

$$\frac{\langle b_1, b_2 \rangle}{\|b_1\|^2} - m = \frac{\langle b_1, b_2 \rangle - m\|b_1\|^2}{\|b_1\|^2} = \frac{\langle b_1, b_2 - mb_1 \rangle}{\|b_1\|^2} = \frac{\langle b_1, u_2 \rangle}{\|b_1\|^2}.$$

Consequently, we get

$$-\frac{1}{2} < \frac{\langle b_1, u_2 \rangle}{\|b_1\|^2} \leq \frac{1}{2}.$$

This terminates the proof. □

Exercice 7.3.12. Let b_1, b_2 be two linearly independent vectors. Define

$$u_1 = b_1, \qquad u_2 = b_2 - \left\lfloor \frac{\langle b_1, b_2 \rangle}{\|b_1\|^2} \right\rceil b_1.$$

Show that, if (b_1, b_2) is a basis of a lattice L, then $(u_1, u2)$ is also a basis of L.

If $\|u_1\| \geq \|u_2\|$, we swap u_1 and u_2 and continue the process.
The Gaussian reduction algorithm is described in Algorithm 29.

Algorithm 29 : Gauss' algorithm

Input : A basis (b_1, b_2) of a lattice $\mathcal{L} \subset \mathcal{R}^2$.
Output : A basis (u_1, u_2) such that $\|u_1\| = \lambda_1$ and $\|u_2\| = \lambda_2$.

1: Set $u_1 = b_1$ and $u_2 = b_2$.
2: **If** $\|u_1\| > \|u_2\|$ **then**
3: Swap u_1 and u_2.
4: **End If**
5: **While** $\|u_1\| < \|u_2\|$, **do**
6: Compute $\mu = \frac{\langle u_1, u_2 \rangle}{\|u_1\|^2}$.
7: Compute $u_2 = u_2 - \lfloor \mu \rceil u_1$.
8: Swap u_1 and u_2.
9: **End While**
10: Swap u_1 and u_2.
11: Return (u_1, u_2).

Exercice 7.3.13. Apply Gauss algorithm with the basis (b_1, b_2) with $b_1 = (6, 3)$ and $b_2 = (5, 1)$.

We get $u_1 = (1, 2)$ and $b_2 = (4, -1)$.

Maple code 7.3.14.

The algorithm 29 can be easily encoded using maple.

```
      Maple: Gauss'algorithm

gauss:=proc(b1,b2)
local u1,u2,v,mu:
with(VectorCalculus):
u1:=convert(b1, Vector);
u2:=convert(b2, Vector);
if Norm(1.0*u1)>= Norm(1.0*u2) then
    v:=u1;
    u1:=u2;
    u2:=v;
end if;
while Norm(1.0*u1)<Norm(1.0*u2) do
    mu:=DotProduct(u1,u2)/Norm(u1)^2:
    u2:=u2-round(mu)*u1:
    v:=u1;
    u1:=u2;
    u2:=v;
end do;
v := u1;
u1 := u2;
u2 := v;
u1:=convert(u1, Vector);
u2:=convert(u2, Vector);
return(u1, u2):
end proc:
```

Example 7.3.15.

Let $\mathcal{L}$ be the lattice with the basis (b_1, b_2) with

$$b_1 = \begin{bmatrix} 19239 \\ 2971 \end{bmatrix}, \quad b_1 = \begin{bmatrix} 22961 \\ 3546 \end{bmatrix}.$$

```
      Maple: Gauss'algorithm,  example1

b1 := [19239, 2971];
b2 := [22961, 3546];
gauss(b1, b2);
```

Then, applying Gauss'algorithm, we find a new basis (u_1, u_2) with

$$u_1 = \begin{bmatrix} -52 \\ -1 \end{bmatrix}, \quad u_2 = \begin{bmatrix} 5 \\ 84 \end{bmatrix}.$$

Then, we get

$$\lambda_1 = \|u_1\| = \sqrt{2705}, \quad \lambda_2 = \|u_2\| = \sqrt{7081}.$$

Observe that

$$u_1 = [b_1, b_2] \begin{bmatrix} -37 \\ 31 \end{bmatrix}, \quad u_2 = [b_1, b_2] \begin{bmatrix} -438 \\ 367 \end{bmatrix},$$

and that the fractions -$\frac{37}{31}$ and $-\frac{438}{367}$ are among the convergents of the continued fraction expansion of $-\frac{22961}{19239}$ as explained in Example 7.3.2.

Observe that the Gaussian algorithm can be applied to any two linearly independent vectors b_1, b_2 in the $\mathbb{R}^n$ for any $n \geq 2$.

Exercice 7.3.16. Apply Gauss algorithm with the basis (b_1, b_2) with $b_1 = (49, 70, -35)$ and $b_2 = (58, 89, -48)$.

We get $u_1 = (13, -6, 17)$ and $b_2 = (9, 19, -13)$.

7.4 L'algorithme LLL

L'algorithme de Gauss permet de réduire une base (b_1, b_2) et déterminer une base (u_1, u_2) avec de bonnes proprités, à savoir, u_1 et u_2 sont les plus courts possibles dans le réseau et sont presque orthogonaux. Pour généraliser la réduction à un nombre n de vecteurs indépendants $(b_1, \ldots, b_n)$, on utilise l'algorithme LLL de Lenstra, Lenstra et Lovász [15].

The LLL algorithm is the most useful tool in the algorithmic study of lattices. It provides a partial answer to SVP since it runs in polynomial time and approximates the shortest vector of a lattice of dimension n up to a factor of $2^{n/2}$. Babai gave an algorithm that approximates the CVP problem by a factor of $\left(3/\sqrt{2}\right)^n$. In some cases, LLL gives extremely striking results both in theory and practice that are enough to solve the problem. LLL uses the well known Gram-Schmidt orthogonalization method. The Gram-Schmidt process is an iterative method to orthonormalize the basis of a vector space. The LLL algorithm is connected to the Gram-Schmidt orthogonolization process and produces a basis that satisfies the LLL-reduction notion as in the following definition.

Definition 7.4.1. A basis $(b_1 \cdots, b_n)$ of a lattice $\mathcal{L}$ is said to be LLL-reduced if the Gram-Schmidt orthogonalization $(b_1^* \cdots, b_n^*)$ satisfies

$$|\mu_{i,j}| = \frac{|\langle b_i, b_j^* \rangle|}{\langle b_j^*, b_j^* \rangle} \leq \frac{1}{2}, \quad \text{for} \quad 1 \leq j < i \leq n, \tag{7.1}$$

$$\frac{3}{4}\|b_{i-1}^*\|^2 \leq \|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2, \quad \text{for} \quad 1 < i \leq n. \tag{7.2}$$

Using

$$|\mu_{i,j}| = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} = \frac{\|b_i\|}{\|b_j^*\|} |\cos(b_i, b_j^*)|,$$

we see that if $\mu_{i,j} = 0$ for all i and j, then the basis is orthogonal, and consequently is minimal according to Hadamard's inequality as in Corollary 7.2.12.
Also, the condition (7.1) means that the norm of b_i onto the line spanned by b_j^* is less than half of the norm of b_j^* and that the vector b_i is almost orthogonal the space spanned by the vectors $b_1, \ldots, b_{i-1}$.
The condition (7.2) is called Lovász' condition. It means that the norm of the projection of b_i onto the orthogonal space spanned by $(b_1, \cdots, b_{i-1})$ is larger than $\frac{3}{4}$ times the norm of the projection of b_{i-1} onto the orthogonal space spanned by $(b_1, \cdots, b_{i-2})$. Also, it can be transformed into the inequality

$$\|b_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|b_{i-1}^*\|^2.$$

Since a lattice has infinitely many basis, some basis are better than others. A *good basis* is generally a basis with short and almost orthogonal vectors. Consequently, a LLL-reduced basis is a candidate for a good basis.

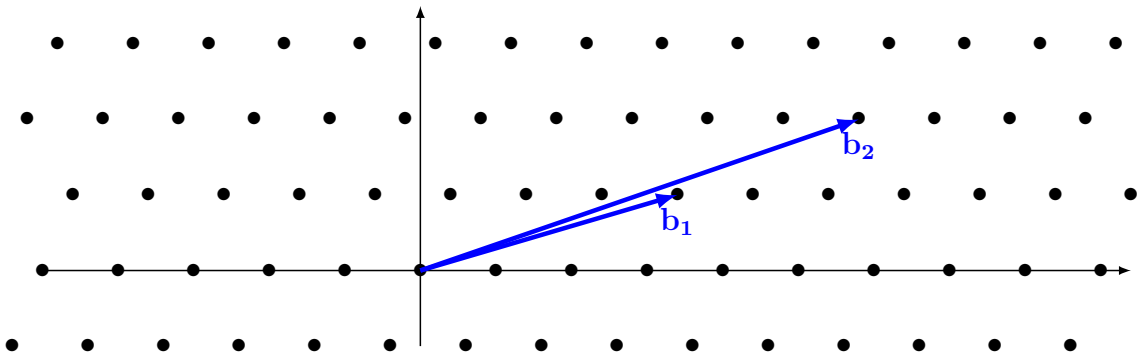


Figure 7.8: A lattice with *a bad* basis (b_1, b_2)

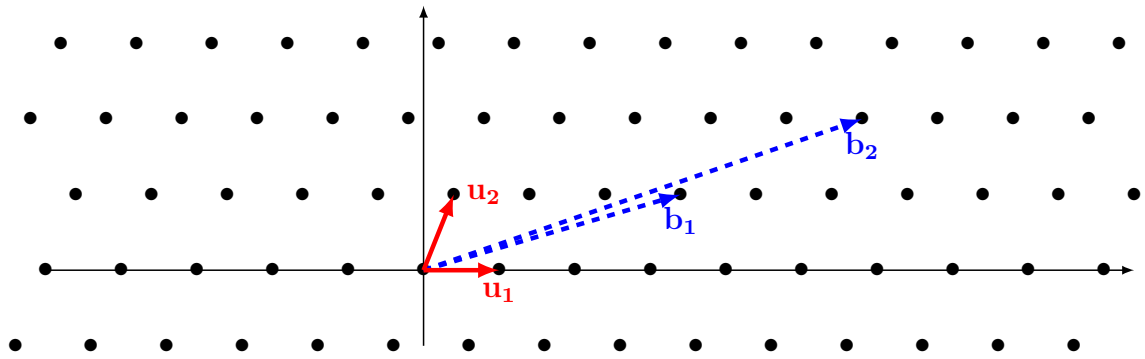


Figure 7.9: The same lattice with *a good* basis (u_1, u_2)

The original version of the LLL algorithm is presented in Algorithm (30).

Maple code 7.4.2.

Using the description of the LLL algorithm in Algorithm (30) and the procedures 31 and 32 , we can encode it using maple. The corresponding code needs the procedure **scal(u,v)** for the inner product and the procedure **gramschmidt(M)** for the Gram-Schmidt orthogonolization process. We start by encoding the procedure **redfaible(M)**.

Procedure 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`

Maple code 7.4.3.

Algorithm 30 : LLL Algorithm

Input : A basis $(b_1, \cdots, b_n)$

Output : A LLL reduced basis $(b_1, \cdots, b_n)$

For $i = 1, \cdots, n$ **do**
  $b_i^* = b_i$
  For $j = 1, \cdots, i-1$ **do**
    $B_j = \langle b_j^*, b_j^* \rangle$
    $\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{B_j}$
    $b_i^* = b_i^* - \mu_{i,j} b_j^*$
  End For
  $B_i = \langle b_i^*, b_i^* \rangle$
End For
$k = 2$
Apply the procedure **redfaible**$(k, k-1)$ [31]
If $\frac{3}{4} B_{k-1} > B_k + \mu_{k,k-1}^2 B_{k-1}$ **then**
  Apply **lovasz**(k) [32]
End If
Goto 10
For $l = k-2, \cdots, 1$ **do**
  Apply the procedure **redfaible**(k, l) [31]
End For
If $k = n$ **then**
  Stop
Else
  $k = k + 1$
  Goto 10
End If

Algorithm 31 : Procedure **redfaible**

Input : Two integers k and l.

Output : A vector b_k and $l-1$ values $\mu_{k,j}$ with $j = 1, \cdots l-1$ such that $|\mu_{k,l}| \leq \frac{1}{2}$

If $|\mu_{k,l}| > \frac{1}{2}$ **then**
  $b_k = b_k - \lfloor \mu_{k,l} \rceil b_l$ where $\lfloor x \rceil$ is the nearest integer to x.
  $\mu_{k,l} = \mu_{k,l} - \lfloor \mu_{k,l} \rceil$
  For $j = 1, \cdots, l-1$ **do**
    $\mu_{k,j} = \mu_{k,j} - \lfloor \mu_{k,l} \rceil \mu_{l,j}$
  End For
End If

Algorithm 32 : Procedure **lovasz**

Input : An integer k

Output : Test if the condition $\frac{3}{4}B_{k-1} \leq B_k + \mu_{k,k-1}^2 B_{k-1}$ is satisfied.

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: Swap b_k and b_{k-1}.
6: **For** $j = 1, \cdots, k-2$ **do**
7: Swap $\mu_{k-1,j}$ and $\mu_{k,j}$
8: **End For**
9: **For** $i = k+1, \cdots, n$ **do**
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: **End For**
13: **If** $k > 2$ **then**
14: $k = k - 1$
15: **End If**

Next, we encode the procedure **lovasz(M)**.

```
      Procedure 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:
```

Maple code 7.4.4.

Finally, we encode the LLL algorithm as the procedure **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:
```

Example 7.4.5.

We will need the scalr product of two vectors.

```
      Produit Scalaire

scal:= proc (x, y)
add(x[i]*y[i], i = 1 .. nops(x));
end proc:
```

Also, we will need the Gram-Schmidt orthogonalization.

```
      La méthode de Gram-Schmidt

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:
```

```
      Commentaires

<-- Procédure
<-- Paramètres locaux
<-- Librairie LinearAlgebra
<-- Nombre de lignes de M
<-- Initiation des listes
<-- i=1,...,n
<-- Initiation de u
 for j from 1 to i-1 do
<-- Calcul de u[j]

<-- u[i]= 1
<-- concaténation
<-- Calcul de B



<-- Sortie
```

Example 7.4.6.

Define the lattice $\mathcal{L}$ by the basis (b_1, b_2, b_3, b_4) with

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

Maple code 7.4.7.

The corresponding maple code is as follows.

```
      Programme

M1 := [4, 7, 9, 4];
M2 := [6, -7, 2, 3];
M3 := [-1, 2, -1, -1];
M4 := [2, -1, 0, -3];
M := [M1, M2, M3, M4];
M5 := Matrix(myLLL(M));
```

Then, the procedure **myLLL(M)** outputs the basis (u_1, u_2, u_3, u_4) with the matrix

$$N = \begin{bmatrix} -1 & 2 & -1 & -1 \\ 2 & 1 & -2 & -1 \\ -1 & 0 & 1 & -3 \\ 5 & 8 & 8 & 0 \end{bmatrix}.$$

Maple code 7.4.8.

The LLL algorithm is implemented in maple with the procedure **LLL** in the package **IntegerRelations**.
Using the same lattice $\mathcal{L}$ with the basis (b_1, b_2, b_3, b_4) as in Example 7.4.6, we can use the following code.

```
      Programme

with(IntegerRelations):
M := [M1, M2, M3, M4]:
N:=LLL(M,'integer');
```

This outputs the LLL-reduced basis (u_1, u_2, u_3, u_4) with the matrix

$$N = \begin{bmatrix} -1 & 2 & -1 & -1 \\ 2 & 1 & -2 & -1 \\ -1 & 0 & 1 & -3 \\ 5 & 8 & 8 & 0 \end{bmatrix}.$$

Using the lattice as in Example 7.4.6, we can check that the bases (b_1, b_2, b_3, b_4) and (u_1, u_2, u_3, u_4) have the same determinant and that u_1 is shorter than the other vectors of the basis (u_1, u_2, u_3, u_4).

Maple code 7.4.9.

The following procedure tests whether $\det(b_1, b_2, b_3, b_4) = \det(u_1, u_2, u_3, u_4)$ and compares the norms of the vectors u_1, u_2, u_3, u_4.

```
      Programme

B := Matrix([M1, M2, M3, M4]):
U := Matrix(N):
Determinant(B)-Determinant(U):
for i to 4 do
    print(U[i], "has norm", DotProduct(Vector(U[i]), Vector(U[i]))):
end do;
```

The LLL algorithm outputs a reduced basis that has many interesting properties such as the following ones.

Theorem 7.4.10. *Let $(b_1 \cdots, b_n)$ be an LLL-reduced basis with Gram-Schmidt orthogonolization $(b_1^*, \cdots, b_n^*)$. Then*

1. $\|b_j^*\|^2 \leq 2^{i-j}\|b_i^*\|^2$ *for* $1 \leq j \leq i \leq n$.
2. $\det(L) \leq \prod_{i=1}^{n} \|b_i\| \leq 2^{\frac{n(n-1)}{4}} \det(L)$.
3. $\|b_j\| \leq 2^{\frac{i-1}{2}}\|b_i^*\|$ *for* $1 \leq j \leq i \leq n$.
4. $\|b_1\| \leq 2^{\frac{n-1}{4}}(\det(L))^{\frac{1}{n}}$.

Proof.
`Proof of 1.` Suppose that $(b_1 \cdots, b_n)$ is an LLL-reduced basis. Then, expanding the inequality (7.2) and using (7.1), we get

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

from which we deduce

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

Hence, for $j \leq i$, we get

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

which proves the property 1.
`Proof of 2.` In the Gram-Schmidt orthogonalization process, we have $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$. Combining with (7.1), we get

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

Using $\|b_j^*\|^2 \leq 2^{i-j}\|b_i^*\|^2$, we get

$$\|b_i\|^2 \leq \|b_i^*\|^2 + \frac{1}{4} \sum_{j=1}^{i-1} 2^{i-j} \|b_i^*\|^2 = \left(1 + 2^{i-2} + 2^{-1}\right) \|b_i^*\|^2 \leq 2^{i-1}\|b_i^*\|^2. \tag{7.3}$$

Taking the product and using Corollary 7.2.12, we get

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

Taking square roots, this proves the property 2.
`Proof of 3.` Replacing i by j in the inequality 7.3, we get $\|b_j\|^2 \leq 2^{j-1}\|b_j^*\|^2$. Combining with property 1, we get

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

which proves the property 3.
`Proof of 4.` If we take $j = 1$ in the inequality 3, we get $\|b_1\|^2 \leq 2^{i-1}\|b_i^*\|^2$ for $1 \leq i \leq n$. Then

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

which gives $\|b_1\| \leq 2^{\frac{n-1}{4}} (\det(L))^{\frac{1}{n}}$ and proves the inequality in 4. □

Theorem 7.4.11. *Let $(b_1 \cdots, b_n)$ be an LLL-reduced basis with Gram-Schmidt orthogonolization $(b_1^*, \cdots, b_n^*)$. Then for any non zero vector $v \in L$, $\|b_1\| \leq 2^{\frac{n-1}{2}}\|v\|$.*

Proof. Let $v \in L$ be a nonzero vector. Writing v simultaneously in the bases $(b_1, b_2, \cdots, b_n)$ and $(b_1^*, b_2^*, \cdots, b_n^*)$, we get

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

Let k be the greatest integer with $1 \leq k \leq n$ and $\alpha_k \neq 0$, that is $|\alpha_k| \geq 1$ and $\alpha_i = 0$ for $i = k+1, \ldots, n$. Using b_i as in the Gram-Schmidt orthogonalization process, we get

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

Then

$$\alpha_k^* = \alpha_k + \sum_{i=k+1}^{n} \alpha_i \mu_{i,k} = \alpha_k.$$

Expanding $\|v\|^2$ in $(b_1^*, b_2^*, \cdots, b_n^*)$, we get

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

Taking $j = 1$ and $i = k$ in the inequality in (3) of Proposition 7.4.10, we get

$$\|b_k^*\|^2 \geq 2^{1-k} \|b_1\|^2.$$

Hence

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

which gives $\|b_1\| \leq 2^{\frac{n-1}{2}} \|v\|$ and terminates the proof. □

Observe that, as shown in property 5 of Proposition 7.4.11, the LLL algorithm outputs a basis where the first vector is short. It is the shortest vector in the lattice up to the factor $2^{\frac{n-1}{2}}$. Frequently, in low dimensions, it is the shortest nonzero vector in the lattice.
The following result gives the size of the the vectors of an LLL-reduced basis when $\mathcal{L} \subset \mathbb{Z}^n$, that is when the coordinates of the basis vectors are integers.

Theorem 7.4.12. *Let $(b_1, \cdots, b_n)$ be an LLL-reduced basis of a lattice $\mathcal{L} \subset \mathbb{Z}^n$. Then for $1 \leq j \leq n$, we have*

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

Proof. Let$(b_1^*, \cdots, b_n^*)$ be the orthogonal basis associated to $(b_1, \cdots, b_n)$ in the Gram-Schmidt process. Using property (3) of Theorem 7.4.10, we get, for $1 \leq j \leq i \leq n$,

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

Applying this successively for $i = j, j+1, \cdots, n$ and multiplying all the inequalities, we get

$$\|b_j\|^{n-j+1} \leq \prod_{i=j}^{n} 2^{\frac{i-1}{2}} \|b_i^*\|. \tag{7.4}$$

Using Property (3) of Theorem 7.4.10 with $j = 1$, we get, for $1 \leq i \leq n$,

$$\|b_1\| \leq 2^{\frac{i-1}{2}} \|b_i^*\|.$$

Then, since $\mathcal{L} \subset \mathbb{Z}^n$, then, for $1 \leq i \leq n$,

$$2^{\frac{i-1}{2}} \|b_i^*\| \geq \|b_1\| \geq 1,$$

and

$$\prod_{i=1}^{j-1} 2^{\frac{i-1}{2}} \|b_i^*\| \geq \|b_1\| \geq 1,$$

Then, transforming (7.4), we get

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

which leads the inequality of the theorem. □

Note that the LLL algorithm provides a basis of reasonably short vectors and can be used to approximate the shortest vector problem. The next result shows that the LLL algorithm is a polynomial time algorithm.

Theorem 7.4.13. *Let $(b_1, \cdots, b_n)$ be a basis of a lattice $\mathcal{L}$. Define $B = \max_i \|b_i\|$. The LLL algorithm computes an LLL-reduced basis with running time*

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

Chapter 8

Cryptanalyse de RSA par la Méthode de Coppersmith

8.0.1 La méthode de Coppersmith : polynômes à une variable

An important application of lattice reduction found by Coppersmith [5] in 1996 is finding small roots of low-degree polynomial equations. This includes modular univariate polynomial equations, and bivariate integer equations.

Let M be some large integer of unknown factorization and

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

be a polynomial of degree d with integer coefficients. Consider the equation $f(x) \equiv 0 \pmod{M}$. In general there is no known efficient algorithm that find integer roots of the above equation. However, Coppersmith [5] introduced an efficient method for finding small integer solutions using the LLL algorithm. Suppose we know that there exists an integer x_0 such that $f(x_0) \equiv 0 \pmod{M}$ and that $|x_0| < N^{\frac{1}{d}}$. The problem is to find x_0. The main idea is that if the coefficients of f are small enough so that $|f(x_0)| = \sum_{i=1}^{d} |a_i x^i| < M$, then one might have $f(x_0)$ over the integers. Coppersmith's idea is to build from $f(x)$ a polynomial $h(x)$ which has small coefficients and the same solution x_0. Soon after Coppersmith proposed his method in 1996, Howgrave-Graham [**?**] proposed in 1997 a a new method for finding all small integer roots. Suppose we know an upper bound X such that $|x_0| < X$. The following theorem by Howgrave-Graham reformulates Coppersmith's idea of finding modular roots. We define the Euclidean norm of a polynomial $f(x)$ as

$$\|f(x)\| = \left(\sum_{i=0}^{d} a_i^2 \right)^{\frac{1}{2}}.$$

Theorem 8.0.14 (Howgrave-Graham)**.** *Let $h(x) \in \mathbb{Z}[x]$ be a polynomial of at most ω monomials satisfying*

(1) $|x_0| < X$, for some positive integer X.

(2) $h(x_0) \equiv 0 \pmod{M}$, for some positive integer M.

(3) $\|h(xX)\| < \frac{M}{\sqrt{\omega}}$.

Then $h(x_0) = 0$ over $\mathbb{Z}$.

Proof. Let $h(x) = \sum_i^d a_i x^i$ with ω monomials. Suppose $|x_0| < X$. Then

$$|h(x_0)| = \left|\sum_i a_i x_0^i\right| \leq \sum_i \left|a_i x_0^i\right| < \sum_i \left|a_i X^i\right|. \tag{8.1}$$

Recall that Cauchy-Schwarz inequality asserts that for $\alpha, \beta \in \mathbb{R}$, we have

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

Using this, we get

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

If $\|h(xX)\| < \frac{M}{\sqrt{\omega}}$, then, using (8.1), we get

$$|h(x_0)| < \sum_i \left|a_i X^i\right| < \sqrt{\omega}\sqrt{\sum_i \left(a_i X^i\right)^2} = \sqrt{\omega}\|h(xX)\| < M.$$

Hence $|h(x_0)| < M$. Finally, if $h(x_0) \equiv 0 \pmod{M}$, then $h(x_0) = 0$ over $\mathbb{Z}$ which terminates the proof. □

To solve $f(x_0) \equiv 0 \pmod{M}$, Theorem 8.0.14 suggests we should look for a polynomial $h(x)$ of small norm satisfying $h(x_0) \in Z$. To do this we will build a lattice of polynomials related to f and use LLL to find short vectors in the lattice. The following result, as given below, is from May [17].

Theorem 8.0.15. *For every $\varepsilon > 0$ there exists an N_0 such that the following holds: Let $N > N_0$ be an integer with unknown factorization which has a divisor $b > N^\beta$. Let $f_b(x)$ be a monic univariate polynomial of degree δ. All solutions x_0 of the congruence $f_b(x) \equiv 0 \pmod{b}$, such that*

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

can be found in time polynomial in $\log(N)$.

Proof. Fix two positive integers m and t and consider the polynomials

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

where $\delta = \deg(f_b)$. Observe that all the polynomials share the root x_0 modulo N^m. Rewriting the polynomials explicitly, we get

	$j=0$	$j=1$	$j=2$	$\cdots$	$j=\delta-1$
$i=m$	N^m,	$N^m x$,	$N^m x^2$,	$\cdots$	$N^m x^{\delta-1}$,
$i=m-1$	$N^{m-1} f_b(x)$	$N^{m-1} x f_b(x)$	$N^{m-1} x^2 f_b(x)$	$\cdots$	$N^{m-1} x^{\delta-1} f_b(x)$
$i=m-2$	$N^{m-2} f_b(x)^2$	$N^{m-2} x f_b(x)^2$	$N^{m-2} x^2 f_b(x)^2$	$\cdots$	$N^{m-2} x^{\delta-1} f_b(x)^2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i=2$	$N^2 f_b(x)^{m-2}$	$N^2 x f_b(x)^{m-2}$	$N^2 x^2 f_b(x)^{m-2}$	$\cdots$	$N^2 x^{\delta-1} f_b(x)^{m-2}$
$i=1$	$N f_b(x)^{m-1}$	$N x f_b(x)^{m-1}$	$N x^2 f_b(x)^{m-1}$	$\cdots$	$N x^{\delta-1} f_b(x)^{m-1}$

(8.2)

Observe that the maximal degree is $\delta - 1 + (m-1)\delta = m\delta - 1$. The details of the polynomials $h_i(x)$ are as follows

$$i = 0, \cdots, t-1 \Rightarrow f_b^m(x), x f_b^m(x), x^2 f_b^m(x), \cdots, x^{t-1} f_b^m(x). \tag{8.3}$$

Observe here that the maximal degree is $t - 1 + m\delta > m\delta - 1$. Replacing x by Xx in the rows $i = m, m-1, \ldots, 1$ of the table (8.2) and in the sequence (8.3) and expressing in the basis $\left(1, x, x^2, \cdots, x^{m\delta+t-1}\right)$, we get a sequence of matrices of the shape

$$M_m = \begin{bmatrix} N^m & & & \\ & N^m X & & \\ & & \ddots & \\ & & & N^m X^{\delta-1} \end{bmatrix},$$

$$M_{m-1} = \begin{bmatrix} - & - & - & - & N^{m-1}X^{\delta} & & & \\ - & - & - & - & - & N^{m-1}X^{\delta+1} & & \\ - & - & - & - & - & - & \ddots & \\ - & - & - & - & - & - & - & N^{m-1}X^{2\delta-1} \end{bmatrix},$$

$$\vdots = \vdots$$

$$M_1 = \begin{bmatrix} - & - & \cdots & - & NX^{(m-1)\delta} & & & \\ - & - & \cdots & - & - & NX^{(m-1)\delta+1} & & \\ - & - & \cdots & - & - & - & \ddots & \\ - & - & \cdots & - & - & - & - & NX^{(m-1)\delta+\delta-1} \end{bmatrix},$$

$$M_0 = \begin{bmatrix} - & - & \cdots & - & X^{m\delta} & & & \\ - & - & \cdots & - & - & X^{m\delta+1} & & \\ - & - & \cdots & - & - & - & \ddots & \\ - & - & \cdots & - & - & - & - & X^{m\delta+t-1} \end{bmatrix}.$$

Gathering the matrices, we get a triangular matrix of the form

$$M = \begin{bmatrix} M_m \\ M_{m-1} \\ \vdots \\ M_1 \\ M_0 \end{bmatrix}, \tag{8.4}$$

which generates a lattice $\mathcal{L}$. Obviously, we have

$$\det(\mathcal{L}) = N^{m\delta} \cdot N^{(m-1)\delta} \cdot \ldots \cdot N^{\delta} X^{1+2+\cdots+n-1} = N^{\frac{1}{2}m(m+1)\delta} X^{\frac{1}{2}n(n-1)},$$

where $n = m\delta + t$. Using the LLL-algorithm, we can find a small element in $\mathcal{L}$ that corresponds to a polynomial $h(x)$ satisfying (4) of Theorem 7.4.10, namely

$$\|h(xX)\| \leq 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}} = 2^{\frac{n-1}{4}} N^{\frac{m(m+1)\delta}{2n}} X^{\frac{1}{2}(n-1)}.$$

In order to apply Theorem 8.0.14 on $h(x)$, it is sufficient that $\|h(xX)\| \leq \frac{b^m}{\sqrt{n}}$, holds. This is satisfied if

$$2^{\frac{n-1}{4}} N^{\frac{m(m+1)\delta}{2n}} X^{\frac{1}{2}(n-1)} < \frac{b^m}{\sqrt{n}}.$$

Plugging $b > N^{\beta}$, we find

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

Solving for X, we get

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

Consider the exponent of N as a polynomial in m. The exponent is maximal for

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

which leads to the bound

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

This can be rewritten as

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

where

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

Observe that ε depends on n and satisfies $\lim_{n \to +\infty} \varepsilon = 0$. □

Example 8.0.16.

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

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

Maple code 8.0.17.

Programme	Commentaires
restart;	
with(PolynomialTools):	<-- Package Polynômes
with(LinearAlgebra):	<-- Package Algèbre Linéaire
with(linalg):	<-- Un autre package
with(IntegerRelations):	<-- Package LLL
N:=29263868053;	<-- La valeur de N
f:=x->x^3-111111110*x^2	<-- La fonction f
-111111110*x-111111111;	
d:=degree(f(x),x):	<-- Le degré de f
X:=trunc((2^(-1/2)*N^(1/d))):	<-- Borne supérieure des solutions
X:=500;	<-- Une borne inférieure
m:=3:t:=1:	<-- m=3 et t=1
n:=d*m+t:	<-- La dimension du réseau
M:=Matrix(n):	<-- La matrice (n,n), formée de 0
line:=0:	<-- Initiation
for i from 1 to m do	<-- Boucle de formation de
i2:=m+1-i:	la matrice correspondante
for j from 0 to d-1 do	aux polynômes g(i,j),
line:=line+1:	qui formera
cc:=CoefficientVector(	l'entrée pour LLL
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:	<-- Fin de la boucle
for i from 0 to t-1 do	<-- Boucle de formation de
line:=line+1:	la matrice correspondante
cc:=CoefficientVector(	aux polynômes h(i),
x^i*X^i*(f(x*X))^m,x):	qui formera
for k from 1 to Dimension(cc) do	l'entrée pour LLL
M[line,k]:=cc[k]:	
end do:	
end do:	<-- Fin de la boucle
VM:=[row(M,1..n)]:	<-- Formation de la matrice
L := LLL(VM, 'integer'):	<-- Réduction de la matrice
h:=0:	<--
for i from 0 to n-1 do	<-- Formation du polynôme h
h:=h+(L[1,i+1]/X^i)*x^i:	
end do:	
h:	
isolve(h);	<-- racines entière de h
f(79) mod N;	<-- Vérification

8.0.2 Factorisation de N

Theorem 8.0.15 has various applications in cryptography. We will now present an attack on RSA - also due to Coppersmith - that finds the factorization of $N = pq$, provided that one knows half of the bits of one of the factors.

Theorem 8.0.18. *Let $N = pq$ be an RSA modulus with $p > q$. If $\tilde{p}$ is an approximation of p with*

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

then N can be factored in polynomial time in $\log N$.

Proof. Suppose we know an approximation $\tilde{p}$ of p with $|\tilde{p} - p| < N^{\frac{1}{4}}$. Consider the polynomial $f_p(x) = x + \tilde{p}$. Then $f_p(p - \tilde{p}) = p \equiv 0 \mod p$. Hence, $x_0 = p - \tilde{p}$ satisfies

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

Since $p > N^{\frac{1}{2}}$, one can then apply Theorem 8.0.15 with $b = p$, $f_p(x) = x + \tilde{p}$, $\delta = 1$ and $\beta = \frac{1}{2}$. This gives explicitly x_0 which leads to $p = x_0 + \tilde{p}$. □

Example 8.0.19.

Voici un exemple dans lequel $N = 25353012004566062958812027956 51$ 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 8.0.15 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 $p = p_0 + x_0 = 1125899906842679$.

Maple code 8.0.20.

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

Chapter 9

Le Cryptosystème NTRU

9.1 Introduction au cryptosystème NTRU

Le cryptosystème NTRU utilise plusieurs sortes de paramètres, en particulier les paramètres N, p et q.

Soit N un nombre entier. Les opérations de NTRU ont pour domaine l'anneau des polynômes suivant:

$$\mathcal{P} = \mathbb{Z}[X]/\left(X^N - 1\right).$$

Ainsi, les éléments f de $\mathcal{P}$ peuvent être représentés sous la forme

$$f = (f_0, f_1, \cdots, f_{N-1}) = \sum_{i=0}^{N-1} f_i X^i.$$

L'addition de deux polynômes $f, g \in \mathcal{P}$ se fait de façon naturelle terme à terme de même degrés, alors que la multiplication se fait par un produit de convolution noté ici $*$. Si $f * g = h$ avec $f = \sum_{i=0}^{N-1} f_i X^i$ et $g = \sum_{i=0}^{N-1} g_i X^i$, alors $h = \sum_{i=0}^{N-1} h_i X^i$ avec pour tout $0 \leq k \leq N-1$,

$$h_k = \sum_{i+j \equiv k \mod N} f_i g_j = \sum_{i=0}^{k} f_i g_{k-i} + \sum_{i=k+1}^{N-1} f_i g_{N+k-i}.$$

Different descriptions of NTRUEncrypt, and different proposed parameter sets, have been in circulation since 1996. The 2005 instantiation of NTRU is set up by six public integers N, p, q, d_f, d_g, d_r and four public spaces $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_m$, $\mathcal{L}_r$.

- N is prime and sufficiently large to prevent lattice attacks.
- p and q are relatively prime numbers.

- q is much larger than p.
- $\mathcal{L}_f = \mathcal{B}(d_f)$ is a set of small polynomials from which the private keys are selected.
- $\mathcal{L}_g = \mathcal{B}(d_g)$ is a similar set of small polynomials from which other private keys are selected.
- $\mathcal{L}_m = \mathbb{Z}_p[X]/\left(X^N - 1\right)$ is the plaintext space. It is a set of polynomials $m \in \mathbb{Z}_p[X]/(X^N - 1)$ that represent encryptable messages.
- $\mathcal{L}_r = \mathcal{B}(d_r)$ is a set of polynomials from which the blinding value used during encryption is selected.

The key generation, encryption and decryption primitives are as follows:

1. **Key generation**
   - Randomly choose a polynomial $f \in \mathcal{L}_f$ such that f is invertible in $\mathcal{P}$ modulo p and modulo q.
   - Compute $f_p \equiv f^{-1} \pmod{p}$ and $f_q \equiv f^{-1} \pmod{q}$.
   - Randomly choose a polynomial $g \in \mathcal{L}_g$.
   - Compute $h \equiv g * f_q \pmod{q}$.
   - Publish the public key (N, h) and the set of parameters p, q, $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_r$ and $\mathcal{L}_m$.
   - Keep the private key (f, f_p).
2. **Encryption**
   - Represent the message as a polynomial $m \in \mathcal{L}_m$.
   - Randomly choose a polynomial $r \in \mathcal{L}_r$.
   - Encrypt m with the public key (N, h) using the rule $e \equiv p * r * h + m \pmod{q}$.
3. **Decryption**
   - The receiver computes $a \equiv f * e \pmod{q}$.
   - Using a centering procedure, transform a to a polynomial with coefficients in the interval $\left[-\frac{q}{2}, \frac{q}{2}\right[$.
   - Compute $m \equiv f_p * a \pmod{p}$.

The decryption process is correct if the polynomial $p*r*g+f*m \pmod q$ is actually equal to $p*r*g+f*m \in \mathbb{Z}[X]/\left(X^N-1\right)$, that is without using modulo q. We have

$$\begin{aligned} a &\equiv f*e \pmod q \\ &\equiv f*(p*r*h+m) \pmod q \\ &\equiv f*r*(p*g*f_q)+f*m \pmod q \\ &\equiv p*r*g*f*f_q+f*m \pmod q \\ &\equiv p*r*g+f*m \pmod q. \end{aligned}$$

Hence, if $a=p*r*g+f*m$ in $\mathbb{Z}[X]/\left(X^N-1\right)$, then

$$a*f_p \equiv (p*r*g+f*m)*f_p \equiv m \pmod p.$$

We note that if the parameters are chosen properly, the decryption process never fails. A sufficient condition for this is to choose q much larger than p.

Maple code 9.1.1.

Avec Maple 12, la procédure suivante permet de calculer $f*g$ dans l'anneau $\mathcal{P}$.

Programme (Maple)	Commentaires
`star:=proc (N,f,g)`	`<--- Procedure star`
`local k, h, i, s;`	`<--- Variables locales`
`for k from 0 to N-1 do`	`<--- Création de la`
`  h[k] := 0;`	`  suite h_k`
`  for i from 0 to k do`	`<--- Partie i=0..k`
`h[k]:=h[k]+coeff(f,X,i)*coeff(g,X,k-i)`	
`  end do;`	`<--- Fin partie i=0..k`
`  for i from k+1 to N-1 do`	`<--- Partie i=k+1..N-1`
`h[k]:=h[k]+coeff(f,X,i)*coeff(g,X,N+k-i)`	
`  end do;`	`<--- Fin partie i=k+1..N-1`
`end do;`	
`s := 0;`	`<--- Formation du`
`for k from 0 to N-1 do`	`  polynôme h=f*g`
`  s := s+h[k]*X^k`	
`end do;`	`<--- Fin`
`return s;`	`<--- Sortie de h=f*g`
`end proc;`	`<--- Fin de la procédure`

Pour illustrer cette procédure, on considère $N=17$, $f=X^{16}-1$ et $g=X^{15}+1$. Le programme suivant permet de calculer $s=f+g$ et $h=f*g$ dans $\mathcal{P}=\mathbb{Z}[X]/\left(X^{17}-1\right)$.. On suppose donc que la procédure **star(N,f,g)** est déjà exécutée.

Programme (Maple)	Commentaires
N:=17;	<--- Valeur de N
f:=X^16-1;	<--- Polynôme f
g:=X^15+1;	<--- Polynôme g
h:=star(N,f,g);	<--- h=f*g=-1+X^14-X^15+X^16

Soient $p, q \in \mathcal{P}$ deux entiers premiers entre eux. Une notion importante dans NTRU est le calcul de l'inverse d'un polynôme f dans $\mathcal{P}_p$ et $\mathcal{P}_q$. L'inverse de f dans $\mathcal{P}_p$ est un polynôme $f_p \in \mathcal{P}_p$ tel que

$$f * f_p \equiv 1 \pmod{p}.$$

De même, l'inverse de f dans $\mathcal{P}_q$ est un polynôme $f_q \in \mathcal{P}_q$ vérifiant

$$f * f_q \equiv 1 \pmod{q}.$$

Maple code 9.1.2.

Avec Maple 12, la procédure suivante permet de calculer l'inverse f_p de f dans $\mathcal{P}_p$. Pour l'algorithme de calcul, on peut consulter [21]. On suppose que la procédure **star(N,f,g)** est déjà exécutée.

Programme (Maple)

```
invp := proc (N, p, a)
with(MatrixPolynomialAlgebra);
k := 0;
b := 1;
c := 0;
f := a;
g := X^N-1;
while true do
    f0 := coeff(f, X, 0);
    while f0 = 0 do
        f := expand(f/X);
        c := expand(c*X);
        k := k+1;
        f0 := coeff(f, X, 0)
    end do;
    if degree(f) = 0 then
        b := `mod`(b/f0, p);
        fp := star(N, b, X^(`mod`(-k, N)));
        break
    end if;
    if degree(f) < degree(g) then
        t := f; f := g; g := t;
        t := b; b := c; c := t
    end if;
    f0 := coeff(f, X, 0);
    g0 := coeff(g, X, 0);
    u := `mod`(f0/g0, p);
    f := `mod`(f-u*g, p);
    b := `mod`(b-u*c, p)
end do;
return fp;
end proc:
```

Pour illustrer cette procédure, on considère l'exemple suivant $N = 11$, $p = 3$ et $f = 1 + X - X^3 + X^5 - X^6$. Le programme suivant permet de calculer f_p dans $\mathcal{P}_p$.

Programme (Maple)	Commentaires
N:=11;	
p:=3;	
f:=1+X-X^3+X^5-X^6;	
fp:=invp(N,p,f);	<-- fp=2X^8+2X^7+2X^6+X^5+2X^4+2*X^3+2X^2+X+2
star(N,f,fp) mod p;	<-- vérification f*fp=1 mod p

De même, le programme ci-dessous permet de calculer l'inverse f_q de f dans $\mathcal{P}_q$. Pour l'algorithme de calcul, on peut aussi consulter [21]. On suppose que les procédures **star(N,f,g)** et **inv(N,p,f)** sont déjà exécutées.

```
      Programme  (Maple)

invq := proc (N,p,r,a)
q := p^r;
b := invp(N, p, a);
qq := p;
while qq < q do
    qq := qq*p;
    b := `mod`(star(N, b, 2-star(N, a, b)), q)
end do;
return b;
 end proc:
```

Pour illustrer cette procédure, on considère l'exemple suivant $N = 11$, $p = 2$, $r = 3$ et $f = 1 + X - X^3 + X^5 - X^6$. Le programme suivant permet de calculer f_q dans $\mathcal{P}_q$.

Programme (Maple)	Commentaires
N:=11;	
p:=2;	
r:=3;	
f:=1+X-X^3+X^5-X^6;	
fq:=invp(N,p,r,f);	<-- fq=X^10+7X^9+7X^8+7X^7+5X^6+2X^5+3X^4+4X^3+X+4
star(N,f,fq) mod q;	<-- vérification f*fq=1 mod q

Maple code 9.1.3.

The following procedure transforms a polynomial f modulo q to a centered polynomial f modulo q, that is with coefficients in the interval $\left[-\frac{q}{2}, \frac{q}{2}\right[$

```
   Programme  (Maple)

center:=proc(N,f,q)
local i,ci,di,g;
g:=0;
for i from 0 to N-1 do
 ci:=coeff(f,X,i);
 di:=ci mod q;
 if di>q/2 then
    di:=di-q;
 end if;
 g:=g+di*X^i;
end do;
return(g);
end proc:
```

Maple code 9.1.4.
Le programme ci-dessous permet de vérifier la validité de NTRU à l'aide de Maple. On suppose que les procédure **star**, **invp** et **invq** sont déjà initialisées.

```
      Programme  (Maple)

N := 13: q := 8: p := 3:
f := X^12+X^11+X^10+X^9+X^8+X^7+1:
g := X^12+X^5-X^4+X^3-X^2+X-1:
fp := invp(N, p, f):
fq := invq(N, 2, 3, f):
h := `mod`(star(N, fq, g), q):
m := X^10+X^8+X^7+X^4+X^3+1:
r := X^12+X^11+X^8+X^7+1:
e := `mod`(star(N, p*r, h)+m, q):
a := `mod`(star(N, f, e), q):
a:=center(N,a,q);
m2 := `mod`(star(N, fp, a), p):
m2:=center(N,m2,p);
m-m2;
```

La différence entre le message d'origine m est le message $m2$, obtenu après décryptage est nulle, ce qui confirme l'exactitude de NTRU.

9.2 Application de LLL à NTRU

Juste après la publication de NTRU, Coppersmith et Shamir [5] ont proposé une attaque contre la clé publique pour les petites valeurs du paramètre N. Dans NTRU, la clé

publique $h \equiv f_q * g \pmod q$ vérifie $f * h \equiv g \pmod q$. Alors, il existe un polynôme $u \in \mathcal{P} = \mathbb{Z}/\left(X^N - 1\right)$ tel que

$$f * h - q * u = g.$$

On considère alors l'ensemble

$$\mathcal{L} = \left\{(f, g) \in \mathcal{P}^2 \mid \exists u \in \mathcal{P},\ f * h - q * u = g\right\}.$$

On vérifie facilement que $\mathcal{L}$ est un réseau et sous forme matricielle, ceci s'écrit sous la forme :

$$(f, -u) * \begin{bmatrix} 1 & h \\ 0 & q \end{bmatrix} = (f, g).$$

Avec les coordonnées de f, g et h, l'égalité ci-dessus prend la forme

$$\left[\begin{array}{c} f_0 \\ f_1 \\ \vdots \\ \hline\hline f_{N-1} \\ \hline -u_1 \\ -u_2 \\ \vdots \\ -u_{N-1} \end{array}\right] * \left[\begin{array}{cccc||cccc} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_0 \\ \hline\hline 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{array}\right] = \left[\begin{array}{c} f_0 \\ f_1 \\ \vdots \\ \hline\hline f_{N-1} \\ \hline g_0 \\ g_1 \\ \vdots \\ g_{N-1} \end{array}\right]$$

Ainsi, la matrice

$$M(L) = \begin{bmatrix} I_N & h_N \\ 0 & qI_N \end{bmatrix}$$

du réseau vérifie $\det(M(L)) = q^N$. D'autre part, on suppose que $f \in \mathcal{T}(d_f, d_f - 1)$ et $g \in \mathcal{T}(d_g, d_g)$ avec $d_f = d_g \approx \frac{N}{3}$. Alors

$$\|(f, g)\| = \left(\sum_{i=0}^{N-1} f_i^2 + \sum_{i=0}^{N-1} g_i^2\right)^{1/2} \approx \sqrt{4d_f} \approx 2\sqrt{\frac{N}{3}}.$$

En appliquant l'algorithme LLL au réseau $\mathcal{L}$, on produit un vecteur v_1 assez court, plus précisement

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

Ainsi, on peut avoir $v_1 = (f, g)$ si la condition suivante est vérifiée:

$$2\sqrt{\frac{N}{3}} \leq 2^{\frac{2N-1}{4}} \det(L)^{\frac{1}{2N}} \quad \Longleftrightarrow \quad 2^{-\frac{2N-5}{2}} N \leq 3q.$$

Pour illustrer l'utilisation de LLL, on prend l'exemple ci-dessous:

$$\begin{aligned}
N &= 13, \quad p = 3 \quad q = 8,\\
f &= 1 - X + X^{12},\\
f_p &= 1 + 2X + 2X^2 + 2X^4 + X^5 + X^6 + X^8 + 2X^9 + 2X^10 + 2X^12,\\
f_q &= 1 + X + X^3 + 7X^4 + 2X^5 + 5X^6 + 5X^7 + 5X^9 + 3X^10 + 2X^11 + X^12,\\
g &= 1 + X - X^8 + X^{11},\\
h &= 6X + 3X^2 + 3X^3 + 3X^5 + 5X^6 + 6X^7 + 7X^8 + 6X^9 + X^{10} + 5X^11 + 5X^{12} \pmod q.
\end{aligned}$$

La matrice du réseau est alors

$$M(L) = \begin{bmatrix} I_N & h_N \\ 0_N & qI_N \end{bmatrix}$$

où 0_N est la matrice carrée nulle, I_N est la matrice unité et h_N est la matrice circulaire. En appliquant l'algorithme LLL à la matrice $M(L)$, on obtient une matrice sous la forme

$$\begin{bmatrix} M_f & M_g \end{bmatrix}.$$

Si l'algorithme LLL réussit, les coefficients de f sont parmi les lignes de M_f et ceux de g sont parmi les lignes de M_g. Les lignes 26 de M_f et de M_g nous donnent

$$\begin{aligned}
f(LLL) &= 1 - X + X^{12} = f,\\
g(LLL) &= 1 + X - X^8 + X^{11} = g.
\end{aligned}$$

On retrouve ainsi les clés privées f et g qui ont permi de fabriquer la clé plublique h.

Maple code 9.2.1.

Dans Maple 12, le programme ci-dessous permet de retrouver f et g à partir de h.

Programme (Maple)	Commentaires
`with(IntegerRelations):`	`<--- Package LLL:`
`N := 13;`	`<--- N= 13`
`q := 8;`	`<--- q = 8`
`P := 6*X+3*X^2+3*X^3+3*X^5+5*X^6+6*X^7`	`<--- Polynôme h`
`+7*X^8+6*X^9+X^10+5*X^11+5*X^12;`	
`for i from 0 to N-1 do`	`<--- Coefficients de h`
`h[i] := coeff(P, X, i)`	
`end do:`	
`delta := proc (i, j)`	`<--- delta(i,j)=1 si i=j`
`if i = j then return 1`	`delta(i,j)=0 sinon`
`else return 0`	
`end if end proc:`	
`for i from 0 to N-1 do`	`<--- Matrice I_N`
`l[i+1]:=seq(delta(i, j),j=0..N-1)`	
`end do:`	
`for i from 0 to N-1 do`	`<--- Matrice h_N`
`ll[i+1]:=seq(h[‘mod‘(N-i+j, N)],j=0..N-1)`	
`end do:`	
`for i from 0 to N-1 do`	`<--- Matrice [I_N H_N]`
`b[i+1]:=[l[i+1],ll[i+1]]`	
`end do:`	
`delta2 := proc (i, j)`	`<--- Matrice 0_N`
`if i = j then return q`	
`else return 0`	
`end if`	
`end proc:`	
`for i from 0 to N-1 do`	`<--- Matrice q_N`
`l[N+i+1] := seq(delta2(i, j),j=0..N-1)`	
`end do:`	
`for i from 0 to N-1 do`	`<--- Matrice [0_N q_N]`
`b[N+i+1]:=[seq(0,j=0..N-1),l[N+i+1]]`	
`end do:`	
`ML := seq(b[i+1], i = 0 .. 2*N-1):`	`<--- Matrice ML`
`MLL := LLL([ML], 'integer');`	`<--- Application de LLL`

Pour vérifier que toutes les lignes sont des solutions, on peut appliquer le programme ci-dessous et remarquer que $f * P - g \equiv 0 \pmod{q}$.

```
      Programme  (Maple)

for i from 1 to 2*N do
    f:=0;
    for j from 1 to N do
        f:=f+MLL[i,j]*X^(j-1);
    end do;
    g:=0;
    for j from N+1 to 2*N do
        g:=g+MLL[i,j]*X^(j-N-1);
    end do;
    dif:=(star(N, P, f)-g) mod q;
    if (dif=0) then print(i,dif);end if;
end do:
```

Chapter 10

Le Cryptosystème Knapsack de Merkle et Hellman

10.1 Introduction au problème du sac à dos

Soit $n \geq 2$ un nombre entier. Soient a_i, $1 \leq i \leq n$, et S des nombres entiers fixés. Le problème du sac à dos consiste en la recherche d'une solution $(x_1, \cdots, x_k) \in \{0,1\}^n$ de l'équation:

$$a_1 x_1 + \cdots + a_n x_n = S.$$

Definition 10.1.1. Une suite supercroissante est une suite $(a_1, \cdots, a_n)$ telle que pour tout k avec $2 \leq k \leq n$, on a $b_k > \sum_{i=1}^{k-1} b_i$.

Proposition 10.1.2. *Soit $(a_1, \cdots, a_n)$ une suite supercroissante et S un entier tel que $S = a_1 x_1 + \cdots + a_n x_n$ avec $x_i \in \{0,1\}$. Alors l'algorithme suivant permet de déterminer la solution $(x_1, \cdots, x_n) \in \{0,1\}^n$.*

Maple code 10.1.3.

Dans Maple 12, le programme suivant permet déterminer la solution de l'équation $S = a_1 x_1 + \cdots + a_n x_n$ avec $x_i \in \{0,1\}$ où $(a_1, \cdots, a_n)$ est une suite supercroissante. Dans ce programme, on pose $a = \{a_1, \cdots, a_n\}$.

Algorithm 33 : Résolutions du problème sac à dos pour une suite supercroissante

Input : La suite supercroissante $(a_1, \cdots, a_n)$ et un entier $S = a_1x_1 + \cdots + a_nx_n$ avec $x_i \in \{0, 1\}$.

Output : La solution $(x_1, \cdots, x_n) \in \{0, 1\}^n$.

1: $i = n$.
2: **While** $i \geq 1$ **do**
3: **If** $S \geq a_i$ **then**
4: $x_i = 1$,
5: $S = S - a_i$,
6: **Else**
7: $x_i = 0$.
8: **End If**
9: $i = i - 1$.
10: **End While**
11: Sortir $(x_1, \cdots, x_n)$.

Programme (Maple 12)	Commentaires
`sol := proc (a, S)`	`<--- procédure sol`
`n := nops(a);`	`<--- n:=nombre d'éléments de a`
`x := [seq(0, i = 1 .. n)];`	`<--- Changement de variable;`
`Z := S; i := n;`	`<--- initialisation de i`
`while 0 < i do`	`<--- Début de la boucle`
`if a[i] <= Z then`	`<--- Test`
`x[i] := 1;`	`<--- x[i] = 1`
`Z := Z-a[i]`	`<--- S := S-a[i]`
`else x[i] := 0`	`<--- Sinon x[i] := 0`
`end if;`	`<--- Fin du test`
`i := i-1`	`<--- Décrémentation de i`
`end do;`	`<--- Fin de la boucle`
`return x;`	`<--- Sortie de la solution`
`end proc:`	

On peut tester ce programme avec l'exemple suivant

$$a = \{4, 6, 11, 25, 50, 110\}, \quad S = a[1] + a[2] + a[3] + a[6] = 131.$$

Programme (Maple 12)	Commentaires
`a:={4, 6, 11, 25, 50, 110};`	`<--- Liste a`
`S:=a[1]+a[2]+a[3]+a[6];`	`<--- Expression de S`
`sol(a,S);`	`<--- procédure sol(a,S);`

On obtient alors la solution $(1, 1, 1, 0, 0, 1)$.

10.2 Le cryptosysteme de Merkle et Hellman

Pour utliser le cryptosystème Merkle et Hellman par deux entités **A** et **B**, ils doivent procéder comme suit, où on suppose que **B** veut envoyer un message M à **B**. Pour celà, **A** doit préparer ses clés secrètes et publiques.

Génération des clés par A:

1. Choisir une suite super croissante $(a_1, \cdots, a_n)$.
2. Choisir un entier N tel que $N > \sum_{i=1}^{n} a_i$.
3. Choisir un entier d tel que $\gcd(d, N) = 1$.
4. Calculer $e_i = da_i \pmod N$ pour $1 \leq i \leq n$.
5. Publier la clé publique $(e_1, \cdots, e_n)$.
6. Conserver la clé secrète $(N, d, (a_1, \cdots, a_n))$.

Maintenant, **B** peut coder et envoyer son message M.

Chiffrement par B:

1. Transformer le message M en une suite binaire $X = (x_1, \cdots, x_n) \in \{0, 1\}^n$.
2. Calculer $S = \sum_{i=1}^{n} x_i e_i$.
3. Envoyer le message S à **A**.

En recevant le message chiffré S, **A** peut alors le déchiffrer.

Déchiffrement par A:

1. Calculer $S' \equiv Sd^{-1} \equiv \pmod N$.
2. Résoudre l'équation $S' = \sum_{i=1}^{n} x_i a_i$.
3. Calculer $M = \sum_{i=1}^{n} x_i 2^i$.

Maple code 10.2.1.

Avec Maple 12, le programme suivant illustre une utilisation du cryptosystème de Merkle et Hellman. Dans ce programme, on pose $a = \{a_1, \cdots, a_n\}$, et on suppose que la procédure **sol** est à été exécutée.

Programme (Maple 12)	Commentaires
`#Génération des clés par A:`	`<--- Génération des clés par A:`
`a := [4, 6, 11, 25, 50, 110];`	`<--- Choix de la suite a`
`n := nops(a);`	`<--- n := #a`
`T := 0:`	`<--- Initialisation de T`
`for i from 1 to n do`	`<--- T=somme des termes de a`
`  T := T+a[i]`	
`end do:`	
`N := (rand(T .. 2*T))();`	`<--- Choix d'un nombre`
`d:=N:`	`  aléatoire dans [T,2T]`
`while gcd(d,N)>1 do`	`<--- Création d'un nombre d`
`  d:=rand(2..N-1)():`	
`end do:`	
`e:=[seq(mod(d*a[i],N),i=1..n)];`	`<--- Création de la suite e`
`# Chiffrement par B`	`<--- Chiffrement par B`
`M:=61;`	`<--- Choix du message M`
`a2:=[seq(2^i, i = 0 .. n-1)];`	`<--- Suite a2=(1,2,...2^{n-1}`
`X :=sol(a2, M);`	`<--- Décomposition de M dans a2`
`S := 0:`	`<--- Initialisation de S`
`for i from 1 to n do`	`<--- S=somme X*e`
`  S := S+X[i]*e[i];`	
`end do:`	
`# Déchiffrement par A`	`<--- Déchiffrement par A`
`S2:=(S*modp(1/d, N)) mod N;`	`<--- Calcul de S2=S/d mod N`
`X2 := sol(a, S2);`	`<--- X2=suite binaire de S2 dans a`
`M2 := 0:`	`<--- Initialisation de M2`
`for i from 0 to n-1 do`	`<--- Calcul du nombre`
`  M2 := M2+X2[i+1]*2^i`	`  M2=somme X2[i+1]*2^i`
`end do:`	
`M2-M;`	`<--- Vérification de l'égalité M2=M`

10.3 Application de LLL au problème du sac à dos

Supposons que les entités **A** et **B** sont entrain d'utliser le cryptosystème de Merkle et Hellman. Les paramètres publiques sont donc :

- La clé publique $(e_1, \cdots, e_n)$ de **A**.
- Le message S envoyé par **B** à **A**.

On sait aussi que ces paramètres vérifient une relation secrète $S = \sum_{i=1}^{n} x_i e_i$ pour une suite $(x_1, \cdots, x_n) \in \{0,1\}^n$. On considère le vecteur

$$U = \left(x_1, x_2, \cdots, x_n, \sum_{i=1}^{n} x_i e_i - S \right).$$

On peut écrire alors le vecteur U sous la forme

$$U = \sum_{i=1}^{n} x_i b_i + b_{n+1},$$

avec

$$\begin{array}{rcl} b_1 & = & (1,0,0,\cdots,0,e_1 C), \\ b_2 & = & (0,1,0,\cdots,0,e_2 C), \\ b_3 & = & (0,0,1,\cdots,0,e_3 C), \\ \vdots & \vdots & \vdots \\ b_n & = & (0,0,0,\cdots,1,e_n C), \\ b_{n+1} & = & (0,0,0,\cdots,0,-SC), \end{array}$$

où C est un nombre à déterminer plus tard pour garantir le succés de la méthode. Ceci nous amène à considérer le résau L défini par:

$$L := \left\{ \sum_{i=1}^{n+1} a_i b_i \mid a_i \in \mathbb{Z} \right\}.$$

La matrice associé à ce résau est alors:

$$M(L) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & e_1 C \\ 0 & 1 & 0 & \cdots & 0 & e_2 C \\ 0 & 0 & 1 & \cdots & 0 & e_3 C \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & 0 & \vdots & 1 & e_n C \\ 0 & 0 & 0 & \vdots & 0 & -SC \end{pmatrix}.$$

En réduisant le réseau, on peut alors déterminer un vecteur court $V = (y_1, \cdots, y_n, y_{n+1})$. Pour que la suite $(y_1, \cdots, y_n)$ soit une solution pour le problème, on doit avoir $\sum_{i=1}^{n} y_i e_i = S$ et donc $y_{n+1} = 0$, ce qui donne les conditions:

$$\begin{cases} |y_{n+1}| = 0 \\ |y_i| \leq 1 \quad \text{pour } 1 \leq i \leq n \\ \sum_{i=1}^{n} y_i e_i = S. \end{cases} \tag{10.1}$$

Pour illustrer l'application de l'algorithme au problème du sac à dos, on prend l'exemple:

$$e = [205, 119, 281, 56, 112, 171], \qquad S = 825.$$

La matrice formée par les vecteurs de la base du réseau L est donc sous la forme

$$M(L) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 205C \\ 0 & 1 & 0 & 0 & 0 & 0 & 119C \\ 0 & 0 & 1 & 0 & 0 & 0 & 281C \\ 0 & 0 & 0 & 1 & 0 & 0 & 56C \\ 0 & 0 & 0 & 0 & 1 & 0 & 112C \\ 0 & 0 & 0 & 0 & 0 & 1 & 171C \\ 0 & 0 & 0 & 0 & 0 & 0 & 825C \end{pmatrix}.$$

En appliquant l'algorithme LLL sous Maple 12 avec C=10, on obtient la matrice

$$\begin{pmatrix} 0 & 0 & 0 & -2 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ -1 & -3 & 2 & 0 & 0 & 0 & 0 \\ 2 & -3 & 0 & 0 & -2 & 1 & 0 \\ 1 & -2 & -2 & 0 & 1 & -2 & 0 \\ -1 & -1 & -3 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & -1 & -2 & 0 & 10 \end{pmatrix}.$$

Seul le vecteur $(1, 0, 1, 1, 1, 1, 0)$ vérifie les conditions 10.1 et donne

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (1, 0, 1, 1, 1, 1),$$

ce qui permet d'avoir $205 + 281 + 56 + 112 + 171 = 825$.

Maple code 10.3.1.

Avec Maple 12, l'exemple ci-dessus peut être réalisé comme ci-dessous.

Programme (Maple 12)	Commentaires
`restart;`	
`with(IntegerRelations):`	`<--- Package LLL et PSLQ:`
`with(LinearAlgebra):`	`<--- Matrices et vecteurs`
`n:=6;`	`<--- Nombre d'inconnues`
`S:=825;`	`<--- Valeur de S`
`C:=10;`	`<--- Valeur de C`
`e[1]:=205*C;e[2]:=119*C;e[3]:=281*C;`	`<--- Valeurs de la suite e`
`e[4]:=56*C;e[5]:=112*C;e[6]:=171*C;`	
`e[7]:=-S*C;`	
`for i to n+1 do`	`<--- Construction de`
`  for j to n+1 do`	`<--- la base b`
`  if i=j then b[i, j]:=1;`	
`  else b[i, j]:=0 ;`	
`  end if;`	
`  end do;`	
`end do;`	`<--- Fin`
`for i to n+1 do`	`<--- Construction de`
`  b[i, n+1]:=e[i]`	`  la base b`
`end do;`	
`for i to n+1 do`	
`  for j to n+1 do`	
`  b[i]:=[seq(b[i, j],j=1..n+1)];`	
`  end do;`	
`end do;`	`<--- Fin`
`ML:=[seq(b[i], i = 1 .. n+1)];`	`<--- La matrice M(L)`
`N:=LLL(ML,'integer');`	`<--- N=Application de LLL`
`i := 0;`	`<--- Initialisation`
`while i < n+1 do`	`<--- Vérification des`
`  i:=i+1;`	`<--- conditions:`
`  if N[i,n+1]=0 then`	`<--- y_{n+1}>0`
`  j := 0;`	
`  while j<n+1 do`	
`  j:=j+1;`	
`  if abs(N[i, j])>1`	`<--- abs(y_i)=0 ou 1`
`  then j:=n+1`	
`  else if j=n+1 then`	
`print("La solution est dans :",N[i]);`	`<--- La solution`
`  i := n+1`	
`  end if;`	
`  end if;`	
`  end do;`	
`  end if;`	
`end do;`	`<--- Réponse [1,0,1,1,1,1,0]`

Chapter 11

The Lattice Based Cryptosystems GGh and LWE

In this chapter, we give a short introduction to two lattice based cryptosystems, GGH and LWE. While GGH has been broken, LWE is a promising scheme since it is one of the candidates to post quantum cryptography. The chapter is illustrated with many examples and codes using the computer algebra system Maple.

In the following, we list some computational problems that seem to be hard in general and on which some cryptographic systems have been based. An overview of many hard lattice problems and their interconnections is presented in [26].

Definition 11.0.2. Let $\mathcal{L}$ be a full rank lattice of dimension n in $\mathbb{Z}^n$.

1. **The Shortest Vector Problem (SVP):** Given a basis matrix B for $\mathcal{L}$, compute a non-zero vector $v \in \mathcal{L}$ such that $\|v\|$ is minimal, that is $\|v\| = \lambda_1(\mathcal{L})$.

2. **The Closest Vector Problem (CVP):** Given a basis matrix B for $\mathcal{L}$ and a vector $v \notin \mathcal{L}$, find a vector $u \in \mathcal{L}$ such that $\|v - u\|$ is minimal, that is $\|v - u\| = \mathrm{d}(v, \mathcal{L})$ where $\mathrm{d}(v, \mathcal{L}) = \min_{u \in \mathcal{L}} \|v - u\|$.

3. **The Shortest Independent Vectors Problem (SIVP):** Given a basis matrix B for $\mathcal{L}$, find n linearly independent lattice vectors $v_1, v_2, \ldots, v_n$ such that $\max_i \|v_i\| \leq \lambda_n$, where λ_n is the nth successive minima of $\mathcal{L}$.

4. **The approximate SVP problem (γSVP):** Fix $\gamma > 1$. Given a basis matrix B for $\mathcal{L}$, compute a non-zero vector $v \in \mathcal{L}$ such that $\|v\| \leq \gamma\lambda_1(\mathcal{L})$ where $\lambda_1(\mathcal{L})$ is the minimal Euclidean norm in $\mathcal{L}$.

5. **The approximate CVP problem (γSVP):** Fix $\gamma > 1$. Given a basis matrix B for $\mathcal{L}$ and a vector $v \notin \mathcal{L}$, find a vector $u \in \mathcal{L}$ such that $\|v - u\| \leq \gamma\lambda_1\mathrm{d}(v, \mathcal{L})$ where $\mathrm{d}(v, \mathcal{L}) = \min_{u \in \mathcal{L}} \|v - u\|$.

11.1 GGH

In 1996, Goldreich, Goldwasser and Halevi [9] proposed an new way to use lattice theory to build a public key cryptosystem and digital signature scheme inspired by McEliece cryptosystem. This cryptosystem, called GGH was based on the appproximate Closest Vector Problem γCVP 11.0.2. GGH was brocken by Nguyen [19] in 1999 for low dimensions.

Algorithm 34 : GGH key generation

Input : A lattice $\mathcal{L}$ of dimension n.
Output : A public key B and a private key A.

1: Find a "good basis" A of $\mathcal{L}$.
2: Find a "bad basis" B of $\mathcal{L}$.
3: Publish B as the public key.
4: Keep A as the secret key.

Algorithm 35 : GGH encryption

Input : A lattice $\mathcal{L}$, a parameter $\rho > 0$, a public key B and a plaintext $m \in \mathbb{Z}^n$.
Output : A ciphertext c.

1: Compute $v = mB \in \mathcal{L}$.
2: Choose a small vector $e \in [-\rho, \rho]^n$.
3: The ciphertext is $c = v + e$.

Algorithm 36 : GGH decryption

Input : A lattice $\mathcal{L}$, a private key A and a ciphertext c.
Output : A plaintext $m \in \mathbb{Z}^n$.

1: Use an efficient reduction algorithm and the good basis A to find the closest vector $v \in \mathcal{L}$ of the ciphertext c.
2: Compute $m = vB^{-1}$.

The security of GGH is based on the following assumptions.

- Given a "good basis" A of $\mathcal{L}$, it is easy to find a "bad basis" B of $\mathcal{L}$.
- Given a "bad basis" B of $\mathcal{L}$, it is hard to find a "good basis" A of $\mathcal{L}$.
- Given a "good basis" A of $\mathcal{L}$, it is easy to solve the CVP.
- Given a "bad basis" B of $\mathcal{L}$, it is hard to solve the CVP.

Nevertheless, Ngyuen's attack [19] shows that GGH is vulnerable for lattices with small dimension ($\dim(\mathcal{L}) \leq 350$). Consequently, to ensure security, GGH requires lattices with higher dimension. This makes GGH not practical at all for implementations.

Maple code 11.1.1. To start with Maple, we need to initialize the worksheet with the following packages.

```
      Maple:    Initialization

restart:Digits:=50:
with(numtheory):with(linalg):
with(LinearAlgebra):with(IntegerRelations):
```

Maple code 11.1.2. The following procedure creates a $n \times n$ matrix with large random integer entries and determinant 1.

```
      Maple:    Creating a matrix (n,n) with det=1


matinv:=proc(n)
local M1,M2,M;
M1 := randmatrix(n, n, unimodular):
M2 := transpose(randmatrix(n, n, unimodular)):
M := multiply(M1, M2):
return matrix(M);
end proc:
```

Then, we can check that $\det(M) = 1$.

```
      Maple:    Checking that det(M)=1


n:=4;
M:=matinv(n);
Determinant(M);
```

We get always 1.

Maple code 11.1.3. The following procedure creates a $n \times n$ matrix with nonzero determinant.

```
      Maple:    Creating a matrix (n,n) with det=1

mat:=proc(n)
local dd,M;
M:=randmatrix(n,n);
dd:=Determinant(Matrix(M));
while dd=0 do
    M:=randmatrix(n,n);
    dd:=Determinant(Matrix(M));
end do;
return Matrix(M);
end proc:

mat(5);
```

Maple code 11.1.4. The following procedure creates public key B and a private A as in the GGH key generation process.

```
      Maple:    Public and private keys for GGH

GGHkeys:=proc(n)
local B,A,U,i,b,j,M;
B:=mat(n);
M:=[seq(Row(B,i),i=1..n)];
A:=LLL(M, 'integer');
U:=matinv(n);
B:=multiply(U,A);
return Matrix(A),Matrix(B);
end proc:

n:=4;
key:=GGHkeys(n):
A:=key[1];
B:=key[2];
```

Maple code 11.1.5. The following procedure creates a a random plaintext message $m \in \mathbb{Z}^n$.

```
      Maple:    Random message

message:=proc(n)
local m;
m:=RandomMatrix(1, n, generator = -100 .. 100);
return m;
end proc:

m:=message(n);
```

Maple code 11.1.6. Let A be a GGH private key and B a GGH public key. Let $m \in \mathbb{Z}^n$ be a plaintext. The following procedure creates the ciphertext $c = mB + e$ where $e \in [-\rho, \rho]^n$ B for a fixed ρ.

```
      Maple:    GGH encryption

GGHencrypt:=proc(n,B,m,r)
local v,e,c;
v:=multiply(m,B);
e:=RandomMatrix(1, n, generator = -r .. r);
c:=matadd(v, e);
return Matrix(c);
end proc:

c:=GGHencrypt(n,B,m,2);
```

Maple code 11.1.7. Let A be a GGH private key and B a GGH public key. Let $c \in \mathbb{Z}^n$ be a ciphertext. The following procedure outputs the plaintext m such that $c = mB + e$.

```
      Maple:    GGH decryption

GGHdecrypt:=proc(n, A, B, c)
local T1, T, j, M1, M;
T1:=multiply(c, inverse(A));
T:=[seq(round(T1[1,i]), i = 1 .. n)];
M1:=multiply(T,A);
M:=multiply(M1,inverse(B));
return Matrix(M);
end proc:

mm:=GGHdecrypt(n,A,B,c);
m;
```

11.2 LWE

In this section we describe LWE, the Learning With Errors cryptosystem. LWE was invented by Regev [23] in 2005. It is a lattice-based cryptosystem and is supported by a theoretical proof of security. LWE is parameterized by integers n, m, l, t, r, q and a probability distribution χ over $\mathbb{Z}_q$, typically taken to be a rounded normal distribution.

Maple code 11.2.1. The following Maple code prepares a list LWE=$[n0, m0, l0, t0, r0, q]$ to be used throughout the LWE cryptosystem.

```
      LWE List

n0:=3:
m0:=3:
l0:=6:
t0:=10:
r0:=9:
q0:=23:
LWE:=[n0,m0,l0,t0,r0,q0];
```

The key generation, encryption and decryption algorithms are presented in Algorithm 37, Algorithm 38 and Algorithm 39.

Algorithm 37 : LWE Key Generation

Input : Integers n, m, l, q.
Output : A private key S and a public key (A, P).

1: Choose $S \in \mathbb{Z}_q^{n\times l}$ at random.
2: Choose $A \in \mathbb{Z}_q^{m\times n}$ at random.
3: Choose $E \in \mathbb{Z}_q^{m\times l}$ according to χ.
4: Compute $P = AS + E \pmod q$. Hence $P \in \mathbb{Z}_q^{m\times l}$.
5: The private key is S.
6: The public key is (A, P).

Maple code 11.2.2. The following Maple code computes a private key S and a public key (A, P) to be used by LWE.

```
      LWE Key Generation

lwekey:= proc(L);
local n,m,l,t,r,q,S,A,E,P;
n:=L[1]:m:=L[2]:l:=L[3]:t:=L[4]:r:=L[5]:q:=L[6]:
S:=randmatrix(n,l,entries=rand(0 .. q-1));
A:=randmatrix(m,n,entries=rand(0 .. q-1));
E:=randmatrix(m,l,entries=rand(0 .. 0));
P:=Matrix(multiply(A,S))+Matrix(E) mod q;
return matrix(S),matrix(A),P;
end proc:
```

We choose E to be nil for decryption reason. Here is an example for lwekey.

```
      LWE Key Generation, example

ll:=lwekey(LWE):
S0:=ll[1];
A0:=ll[2];
P0:=ll[3];
```

The output is

$$S = \begin{bmatrix} 17 & -6 & 9 & 8 \\ -9 & -4 & -18 & 16 \\ -16 & -18 & 8 & -21 \end{bmatrix},\ A = \begin{bmatrix} -5 & 6 & -18 \\ -3 & -10 & 15 \end{bmatrix},\ P = \begin{bmatrix} 11 & 6 & 3 & 18 \\ 4 & 18 & 22 & 7 \end{bmatrix}$$

Maple code 11.2.3. In LWE, the message is a vector $M \in \mathbb{Z}_t^{l\times 1}$. The following Maple code outputs a random message.

```
      LWE Random Message Generation

lwemessage:= proc(L)
local n,m,l,t,r,q,M;
n:=L[1]:m:=L[2]:l:=L[3]:t:=L[4]:r:=L[5]:q:=L[6]:
M:=randmatrix(l,1,entries=rand(0 .. t-1));
return matrix(M);
end proc:
```

Here is an example for lwemessage.

```
      LWE Random Message Generation, example

M0:=lwemessage(LWE);
```

The output is

$$M = [8, 1, 8, 4, 9, 6]^T.$$

Algorithm 38 : LWE Encryption

Input : Integers n, m, l, t, r, q, a public key (A, P) and a plaintext $M \in \mathbb{Z}_t^{l\times 1}$.
Output : A ciphertext (u, c).

1: Choose $a \in [-r, r]^{m\times 1}$ at random.
2: Compute $u = A^T a \pmod q \in \mathbb{Z}_q^{n\times 1}$.
3: Compute $c = P^T a + \left[\frac{Mq}{t}\right] \pmod q \in \mathbb{Z}_q^{l\times 1}$.
4: The ciphertext is (u, c).

Maple code 11.2.4. The LWE encryption process can be encoded in Maple as in the following.

```
      LWE Encryption

lweencrypt:=proc(A,P,M,L);
local n,m,l,t,r,q,a,u,c1,c2,c;
n:=L[1]:m:=L[2]:l:=L[3]:t:=L[4]:r:=L[5]:q:=L[6]:
a:=randmatrix(m,1,entries=rand(-r..r));
u:=evalm(transpose(A)&*a);
u:=Matrix(u) mod q;
c1:=evalm(transpose(P)&*a);
c2:=evalm(round(q*M/t));
c:=evalm(c1+c2);
c :=Matrix(c) mod q;
return evalm(u),evalm(c);
end proc:
```

Here is an example

```
      LWE Encryption, an example

ll:=lweencrypt(A0,P0,M0,LWE):
u0:=ll[1];
c0:=ll[2];
```

The output is

Algorithm 39 : LWE Decryption

Input : Integers n, m, l, t, r, q, a private key S and a ciphertext (u, c).
Output : A plaintext M.

1: Compute $v = c - S^T u$ and $M = \left\lfloor \frac{tv}{q} \right\rceil$.

Maple code 11.2.5. The LWE encryption process can be encoded in Maple as in the following.

```
      LWE Decryption

lwedecrypt:=proc(S,L,u,c);
local n,m,l,t,r,q,a,c1,c2,v,M;
n:=L[1]:m:=L[2]:l:=L[3]:t:=L[4]:r:=L[5]:q:=L[6]:
c1:=evalm(transpose(S)&*u);
v:=evalm(c-c1);
v:=Matrix(v) mod q;
v :=matrix(v);
M:=evalm(round(t*v/q));
M:=Matrix(M) mod t;
return evalm(M);
end proc:
```

Here is an example for the decryption.

```
      LWE decryption, an example

ll:=lwedecrypt(S0,LWE,u0,c0);
```

The output is

The parameters of LWE are chosen to guarantee the correctness of the decryption. We have

$$\begin{aligned} v &= c - S^T u \\ &= (AS + E)^T a - S^T A^T a + \left\lfloor \frac{Mq}{t} \right\rceil \\ &= E^T a + \left\lfloor \frac{Mq}{t} \right\rceil . \end{aligned}$$

Hence

$$\left\lfloor \frac{tv}{q} \right\rceil = \left\lfloor \frac{tE^T a}{q} + \frac{t}{q} \left\lfloor \frac{Mq}{t} \right\rceil \right\rceil .$$

With suitable parameters, the term $\frac{tE^T a}{q}$ is negligible with high probability according to the form of the probability χ (see [16] for more details). Consequently

$$\left\lceil \frac{tv}{q} \right\rfloor = M.$$

This ensures the correctness of the decryption process.

The security of LWE is based on the following problem:

LWE Problem. Given $P \in \mathbb{Z}_q^{m \times l}$ and $A \in \mathbb{Z}_q^{m \times n}$, find $S \in \mathbb{Z}_q^{n \times l}$ and $E \in \mathbb{Z}_q^{m \times l}$ such that $P = AS + E \pmod{q}$.

In [23], it is shown that the LWE problem can be reduced to special worst-case lattice problems using a quantum algorithm. This means that the LWE problem is hard.

Chapter 12

Elliptic Curves

In this chapter, we describe the main theory of the elliptic curve and its application in cryptography. We propose an implementation of the algorithms using Maple a computer algebra system.

12.1 Methods for Encoding Plaintext

In this section, we review some practical methods for encoding a plaintext M to a point on an elliptic curve $E_p(a, b)$ defined by the Wierstrass equation

$$E_p(a, b): \quad y^2 = x^3 + ax + b \pmod{p}.$$

12.1.1 Koblitz's Method for Encoding Plaintexts

In the following method, the parameters p, K and $E_p(a, b)$ are public. The goal is to transform a plaintext M into a point $P(x, y)$ of the elliptic curve $E_p(a, b)$. To do this, M should be transformed into an integer $m < p$ using the ASCII code for example. If the plaintext is too long, then M can be transformed to a series of numbers $m_1 \| m_2 \| \cdots \| m_n$ with $m_i < p$ for each i.

Algorithm 40 : Koblitz's Method: mapping a plaintext to a point

Input : A prime number p, an elliptic curve $E_p(a,b)$ over $\mathbb{F}_p$, an integer K and a message m with $m < p$.

Output : A point $P = (x, y)$ on the elliptic curve E_p.

1: **For** $i = 1, 2, \cdots, K-1$, **do**
2: Compute $x = mK + i \pmod{p}$.
3: Compute $z = x^3 + ax + b \pmod{p}$.
4: Compute the Legendre's symbol $ls = \left(\frac{z}{p}\right)$.
5: **If** $ls = 1$ **then**
6: Compute $y = z^{\frac{1}{2}} \pmod{p}$.
7: Output (x, y).
8: **End If**
9: **End For**
10: **If** $ls = 1$ **then**
11: Output "Impossible to map M to a point on E_p".
12: **End If**

The inverse operation, that is mapping a point (x, y) on $E_p(a, b)$ to a message $m < p$ can be obtained by computing $m = \left\lfloor \frac{x}{K} \right\rfloor$.

Algorithm 41 : Koblitz's Method: mapping a point to a plaintext

Input : A prime number p, an elliptic curve E_p over $\mathbb{F}_p$, an integer K and a point (x, y) on $E_p(a, b)$.

Output : A message $m < p$.

1: Compute the floor integer $m = \left\lfloor \frac{x}{K} \right\rfloor$.

Maple code 12.1.1. It is easy to transform Koblitz's Method into a Maple code as follows.

```
      Koblitz's Method: mapping a plaintext to a point

restart;with(numtheory):with(linalg):Digits:=100:
koblitz1:=proc(p,a,b,K,m)
local i,x,z,ls,sol,y;
for i from 0 to K-1 do
    x:=m*K+i;
    z:=x^3+a*x+b mod p;
    ls:=legendre(z,p);
    if ls=1 then
        sol := Roots(y^2-z) mod p;
        y:=sol[1][1];
        return  [x, y];
    end if;
end do;
if ls=1 then
    return "Impossible";
end if;
end proc:
```

The inverse operation is as follows.

```
      Koblitz's Method: mapping a point to a message


koblitz2:=proc(p,a,b,K,x)
local m;
m:=trunc(x/K);
return m;
end proc:
```

We present below a complete example.

```
      Koblitz's Method: mapping a point to a message

p0:=nextprime(10^8);
a0:=23;
b0:=1271;
K0:=371;
m0:=123456;
k:=koblitz1(p0,a0,b0,K0,m0):
x0:=k[1];
m1:=koblitz2(p0,a0,b0,K0,x0);
if m1=m0 then yes else no end if;
```

Here is a very simple example. Suppose we want to map the message

"**M0= Marrakech is the prettiest city in North Africa**"

using the elliptic curve $E_p(a,b): \quad y^2 = x^3 + ax + b \pmod p$, where

$$p = 377986153, \quad a = 2484325, \quad b = 5958404.$$

We first transform the message using the ASCII code. The following table shows some ASII codes.

Character	a	A	b	z	0	1	2	"space"	à	+
ASCII code	097	065	098	122	048	049	050	32	224	43

Maple code 12.1.2. The corresponding maple code is as follows.

```
      ASCII Code

M0:="Marrakech is the prettiest city in North Africa";
list1:=convert(M0, bytes);
```

This gives a list in the form list1=$[77, 97, \ldots, 99, 97]$. The inverse maple code is as follows.

```
      Inverse ASCII Code

M2:=convert(list1, bytes);
```

This gives M2:="Marrakech is the prettiest city in North Africa". Now, we can map list1 in the elliptic curve $E_p(a,b): \quad y^2 = x^3 + ax + b \pmod p$ using the procedure **koblitz1(p,a,b,K,m)**.

```
      Mapping the message

mapp:=proc(p,a,b,K,M)
local i,m,points;
m:=convert(M, bytes);
points:=[seq(koblitz1(p,a,b,K,m[i]),i=1..nops(m))];
return points;
end proc:
```

Let us perform the following example.

```
      Mapping the message: An example

p0:=377986153;
a0:=2484325;
b0:=5958404;
K0:=451;
M0:="Marrakech is the prettiest city in North Africa";
lp0:=mapp(p0,a0,b0,K0,M0);
```

We get a list of points in the form $[[34728, 183110874], \ldots, [43747, 246788448]]$. The inverse mapping is to transform a list of points lp on the elliptic curve to a plaintext using the procedure **koblitz2(p,a,b,K,x)**.

```
      Inverse mapping

invmapp:=proc(p,a,b,K,lp)
local i,M2,listx;
listx:=[seq(koblitz2(p,a,b,K,lp[i][1]),i=1..nops(lp))];
M2:=convert(listx, bytes);
return M2;
end proc:
```

Let us perform the following example.

```
      Mapping the message: An example

p0:=377986153;
a0:=2484325;
b0:=5958404;
K0:=451;
M0:="Marrakech is the prettiest city in North Africa";
lp0:=mapp(p0,a0,b0,K0,M0):
Plain:=invmapp(p0,a0,b0,K0,lp0);
```

We get "Marrakech is the prettiest city in North Africa" as expected.

12.2 Equation de Wierstrass

12.2.1 Forme projective

Soit K un corps. Par exemple, $K = \mathbb{Q}$, $K = \mathbb{R}$, $K = \mathbb{C}$, $K = \mathbb{F}_p$ ou $K = \mathbb{F}_{p^r}$, où p est un nombre premier et $r \geq 1$. On note $\overline{K}$ la cloture algébrique de K et K^* l'ensemble des éléments inversibles de K. Le plan projectif $P^2(K)$ sur K est l'ensemble des classes d'équivalence de la relation $\sim$ définie sur K^3 $\{(0,0,0)\}$ par

$$(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2) \quad \text{si et seulement si} \quad \frac{X_1}{X_2} = \frac{Y_1}{Y_2} = \frac{Z_1}{Z_2} \in K^*.$$

Une classe d'équivalence contenant (X, Y, Z) sera notée $(X : Y : Z)$ et représente un point du plan projectif $P^2(K)$ avec les coordonnées homogènes X, Y, Z.

Un polynôme $F \in \overline{K}[X, Y, Z]$ est un polynôme homogène de degré d s'il vérifie pour tout $a \in \overline{K}$ l'égalité :

$$F(aX, aY, aZ) = a^d F(X, Y, Z),$$

Definition 12.2.1. Une équation de Weierstrass en coordonnées projectives définie sur K est une équation cubique homogène de la forme

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

avec $a_1, a_2, a_3, a_4, a_5, a_6 \in K$.

Les points satisfaisants une équation de Weierstrass sont les racines du polynôme

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - \left(X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\right),$$

et sont notés $P = (X, Y, Z)$.

Definition 12.2.2. Une équation de Weierstrass est dite non singulière si pour tout point $P = (X, Y, Z) \in P^2(\overline{K})$ satisfaisant $F(X, Y, Z) = 0$, on a

$$\frac{\partial F}{\partial X}(P) \neq 0, \quad \text{ou} \quad \frac{\partial F}{\partial Y}(P) \neq 0, \quad \text{ou} \quad \frac{\partial Z}{\partial Z}(P) \neq 0.$$

Si pour un point P, on a $\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial Z}{\partial Z}(P) = 0$, on dit que l'équation est singulière et le,point est un point singulier. On remarque que le point particulier $O = (0, 1, 0)$ est solution de toutes les équations de Weierstrass. La classe d'équivalence $\mathcal{O} = (0 : 1 : 0)$ est appelée point à l'infini.

Example 12.2.3. On considère l'équation définie par $Y^2 = X^3+X^2Z$. Alors $F(X,Y,Z) = Y^2 - X^3 - X^2Z$ et tous les points $P = (0,Y,0)$ satisfont $F(X,Y,Z) = 0$. De plus

$$\frac{\partial F}{\partial X}(P) = -3X^2 - 2XZ = 0, \quad \frac{\partial F}{\partial Y}(P) = 2Y = 0, \quad \frac{\partial F}{\partial Z}(P) = -X^2 = 0.$$

Ainsi, l'équation $Y^2 = X^3 + X^2Z$ est singulière.

Example 12.2.4. Pour $K = \mathbb{R}$, on considère l'équation définie par $Y^2 = X^3 + XZ^2$. Alors $F(X,Y,Z) = Y^2 - X^3 - XZ^2$ et pour tous les points $P = (X,X,Z) \neq (0,0,0)$ on a

$$\frac{\partial F}{\partial X}(P) = -3X^2 - Z, \quad \frac{\partial F}{\partial Y}(P) = 2Y, \quad \frac{\partial F}{\partial Z}(P) = -2XZ.$$

Si les trois dérivées partielles sont nulles, alors $X = Y = Z = 0$ et $P = (0,0,0)$ ce qui contredit la définition de $P^2(K)$. Ainsi, l'équation $Y^2 = X^3 + XZ^2$ est non singulière.

On donne maintenant la définition d'une courbe elliptique.

Definition 12.2.5. Une courbe elliptique E définie sur K à coordonnées projectives est une courbe dont l'équation de Weierstrass est une équation cubique non singulière

$$E: \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

avec $a_1, a_2, a_3, a_4, a_5, a_6 \in K$. L'ensemble des points $P = (X,Y,Z)$ vérifiant l'équation est noté $E(K)$.

Pour signifier que la courbe elliptique est définie sur K, on note E/K.

12.2.2 Forme affine

Si on considère un triplet $P = (X,Y,0)$ vérifiant l'équation de Weierstrass, alors $X = 0$ et on retrouve le triplet $(O,Y,0)$ qui est dans la classe $\mathcal{O}$. Ainsi, toutes autres solutions (X,Y,Z) de l'équation de Weierstrass vérifient $Z \neq 0$. La classe de ces solutions peut donc être $\left(\frac{X}{Z} : \frac{X}{Z} : 1\right)$. En notant $x = \frac{X}{Z}$ et $y = \frac{X}{Z}$, on obtient une équation dans le plan affine :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

On a alors la définition suivante.

Definition 12.2.6. Une équation de Weierstrass en coordonnées affines est une équation cubique homogène de la forme

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

avec $a_1, a_2, a_3, a_4, a_5, a_6 \in K$.

En coordonnées affines, la définition d'une courbe elliptique est la suivante.

Definition 12.2.7. Une courbe elliptique E définie sur K à coordonnées affines est une courbe dont l'équation de Weierstrass est une équation non singulière

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

en plus du point à l'infini $\mathcal{O} = (0 : 1 : 0)$. L'union de $\{\mathcal{O}\}$ et de l'ensemble des points $P = (X, Y)$ de la courbe est noté $E(K)$.

12.2.3 Représentation graphique

Maple code 12.2.8.

Avec Maple 12, on peut facilement tracer la représentation graphique d'une curbe elliptique $E/\mathbb{R}$ d'équation de Weierstrass

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Voici un exemple avec la courbe elliptique

$$y^2 + xy + 3y = x^3 - 2x^2 - 4x - 6.$$

Le programme fait appel à la librairie plots qui contient les fonctions graphiques. le paramètre **numpoints**=10^6 indique le nombre minimum de points à tracer et le paramètre **thickness = 4** indique sa largeur.

Programme	Commentaires
`with(plots):`	
`a1:=1;a2:=-2;a3:=3;`	
`a4:=-4;a6:=6:`	`<--- librairie graphique`
`E:= (x,y)->y^2+a1*x*y+a3*y-x^3-a2*x^2-a4*x-a6:`	`<--- Coefficients`
`implicitplot(E(x,y),x=-3..5,y=-20..10,numpoints=10^2):`	`<--- Définition`
	`<--- Tracer la courbe`

On obtient ainsi la courbe ci-dessous.

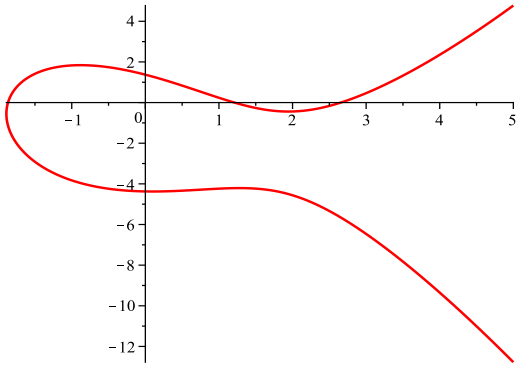


Figure 12.1: Courbe $y^2 + xy + 3y = x^3 - 2x^2 - 4x - 6$

Voici un deuxième exemple avec la courbe elliptique

$$y^2 = x^3 - 2x + 2.$$

Programme	Commentaires
`with(plots):`	`<--- librairie graphique`
`a1:=0;a2:=0;a3:=0;`	`<--- Coefficients de l'équation`
`a4:=-2;a6:=+2;`	
`E:= (x,y)->y^2+a1*x*y`	`<--- Définition de la courbe`
`+a3*y-x^3-a2*x^2-a4*x-a6:`	
`implicitplot`	
`(E(x,y),x=-2..3,`	`<--- Tracer la courbe`
`y=-6..6,thickness=4):`	`dans le rectangle`
	`[-2,3]x[-6,6]`

On obtient ainsi la courbe ci-dessous.

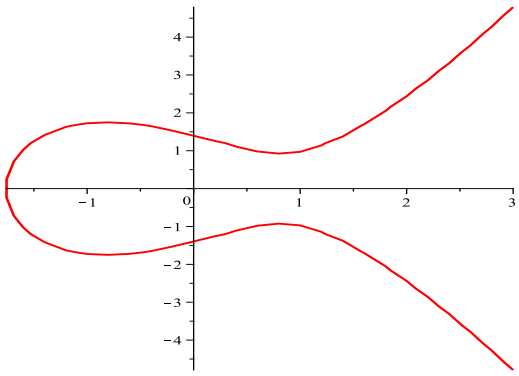


Figure 12.2: Courbe $y^2 = x^3 - 2x + 2$

12.2.4 Invariants des courbes elliptiques

Soit E/K une courbe elliptique définie par son équation de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Un grand nombre de paramètres peuvent alors être définis.

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= 2a_4 + a_1a_3,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= \frac{c_4^3}{\Delta}, \quad \text{si} \quad \Delta \neq 0.
\end{aligned}$$

Les éléments Δ et j s'appellent respectivement le discriminant et le j-invariant de la courbe elliptique. Avec ces quantités, on alors le critère suivant.

Proposition 12.2.9. *la courbe d'équation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

est non singulière si et seulement si $\Delta \neq 0$.

Maple code 12.2.10.

Avec Maple 12, on peut facilement programmer toutes les quantités relatives à une courbe elliptique.

```
      Programme

elliptic:=proc(a1,a2,a3,a4,a6)
global b2,b4,b6,b8,c4,c6,Dis,E,j:
b2:=a1^2+4*a2:
b4:=a1*a3+2*a4:
b6:=a3^2+4*a6:
b8:=a1^2*a6-a1*a3*a4+4*a2*a6+a2*a3^2-a4^2:
c4:=b2^2-24*b4:
c6:=-b2^3+36*b2*b4-216*b6:
Dis:=-b2^2*b8-8*b4^3-27*b6^2+9*b2*b4*b6:
if Dis<>0 then j:=c4^3/Dis
else print("courbe singulière");
end if;
E:=[a1,a2,a3,a4,a6,b2,b4,b6,b8,c4,c6,Dis,j]:
end:
```

La définition suivante permet de grouper les courbes elliptiques en classes d'équivalence ou d'isomorphisme.

Definition 12.2.11. Deux courbes elliptiques E_1/K et E_2/K définies par

$$\begin{array}{rcl} E & : & y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \\ E' & : & y'^2 + a'_1x'y' + a'_3y' = x'^3 + a'_2x'^2 + a'_4x' + a'_6, \end{array}$$

sont isomorphes sur K s'il existe des paramètres $r, s, t, u \in K$ avec $u \neq 0$ tels que la correspondance

$$(x, y) \mapsto \left(u^2x' + r, u^3y' + u^2sx' + t\right),$$

transforme E en E'. On écrit dans ce cas $E \cong E'$.

On a alors la proposition suivante.

Proposition 12.2.12. *Soient E, E', E'' des courbes elliptiques défine sur K. Alors*

1. *on a $E \cong E$.*
2. *si $E \cong E'$, alors $E' \cong E$.*
3. *si $E \cong E'$ et $E' \cong E''$, alors $E \cong E''$.*

Proof. Preuve de 1. Cette propriété est évidente avec $(r, s, t, u) = (0, 0, 0, 1)$.

Preuve de 2. Si $E \cong E'$, alors le changement de variables

$$(x, y) \mapsto \left(u^2x' + r, u^3y' + u^2sx' + t\right),$$

transforme E en E'. On vérifie alors que, inversement, le changement de variables

$$(x', y') \mapsto \left(u^{-2}(x - r), u^{-3}(y - sx + rs - t)\right),$$

transforme E' en E.

Preuve de 3. Si $E \cong E'$ et $E' \cong E''$, alors les changements de variables

$$\begin{array}{rcl} (x, y) & \mapsto & \left(u^2x' + r, u^3y' + u^2sx' + t\right), \\ (x', y') & \mapsto & \left(u'^2x'' + r, u'^3y'' + u'^2sx'' + t'\right), \end{array}$$

transforment E en E', puis E' en E''. Alors, le changement de variables

$$(x, y) \mapsto \left(U^2x'' + R, U^3y'' + U^2Sx'' + T\right),$$

avec

$$U = uu', \quad R = u^2r', \quad S = us' + s, \quad T = u^3t'' + u^2sr' + t$$

transforme E en E''. □

On a de même la proposition suivante.

Proposition 12.2.13. *Soient E et E' deux courbes elliptiques défine sur K telles que $E \cong E'$. Si*

$$\begin{cases} x = u^2x' + r, \\ y = u^3y' + u^2sx' + t, \end{cases}$$

alors

$$\begin{aligned} a'_1 &= u^{-1}(a_1 + 2s) \\ a'_2 &= u^{-2}\left(a_2 - sa_1 + 3r - s^2\right) \\ a'_3 &= u^{-3}\left(a_3 + ra_1 + 2t\right) \\ a'_4 &= u^{-4}\left(a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st\right) \\ a'_6 &= u^{-6}\left(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1\right) \\ \Delta' &= u^{-12}\Delta \\ j' &= j. \end{aligned}$$

Proof. Il suffit de faire le changement de variables $x = u^2x' + r$ et $y = u^3y' + u^2sx' + t$ dans l'équation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

de diviser ensuite par u^6 et par identification, on obtient les quantités a'_1, a'_2, a'_3, a'_4 et a'_6. □

12.2.5 Courbes elliptiques et caractéristiques

Dans cette partie, on va donner des formes courtes de l'équation de Weierstrass suivant la caractéristiques char$K$ du corps K.

Proposition 12.2.14. *Soit E/K une courbe elliptique d'équation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

Si car$(K) = 2$, alors une forme courte de E est

$$\begin{cases} Y^2 + XY = X^3 + a'_2X^2 + a'_6 & si \quad a_1 \neq 0, \\ Y^2 + a'_3Y = X^3 + a'_4X^2 + a'_6 & si \quad a_1 = 0. \end{cases}$$

Proof. Supposons char$K = 2$. Si $a_1 \neq 0$, alors le changement de variables

$$(x, y) \mapsto \left(a_1^2X + \frac{a_3}{a_1}, a_1^3Y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right),$$

signifie que

$$u = a_1, \quad r = \frac{a_3}{a_1}, \quad s = 0, \quad t = \frac{a_1^2 a_4 + a_3^2}{a_1^3}.$$

En reportant ces valeurs dans la proposition 12.2.13, on obtient

$$a_1' = a_1^6, \quad a_2' = (a_1 a_2 + 3a_3)a_1^3, \quad a_3' = 0, \quad a_4' = 0, \quad a_6' = a_6 - \frac{a_3 a_4}{a_1} - \frac{a_4^2 - a_2 a_3^2}{a_1^2} - \frac{a_3^3}{a_1^3} - \frac{a_3^4}{a_1^6}.$$

ce qui, après avoir divisé par a_1^6, permet d'obtenir l'équation

$$Y^2 + XY = X^3 + aX^2 + b,$$

avec $a = a_1^{-6} a_2'$ et $b = a_1^{-6} a_6'$.

Si $a_1 = 0$, alors le changement de variables

$$(x, y) \mapsto (X + a_2, Y),$$

permet d'obtenir

$$a_1' = 0, \quad a_2' = 0, \quad a_3' = a_3, \quad a_4' = a_4 - a_2^2, \quad a_6' = a_6 + a_2 a_4.$$

On obtient alors l'équation

$$Y^2 + a_3' Y = X^3 + a_4' X^2 + a_6'.$$

□

Proposition 12.2.15. *Soit E/K une courbe elliptique d'équation*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

Si car$K \neq 2$, alors une forme courte de E est

$$y^2 = x^3 + \frac{1}{4} b_2 x^2 + \frac{1}{2} b_4 x + \frac{1}{4} b_6.$$

Proof. Si car$K \neq 2$, alors le changement de variable

$$(x, y) \mapsto \left(x', y' - \frac{1}{2}(a_1 x' + a_3) \right),$$

permet d'obtenir l'équation

$$y'^2 = x'^3 + \frac{1}{4} b_2 x'^2 + \frac{1}{2} b_4 x' + \frac{1}{4} b_6.$$

□

Maple code 12.2.16.

Avec Maple 12, la proposition 12.2.15 peut être programmée comme ceci.

```
      Programme

car2:=proc(a1,a2,a3,a4,a6)
global b2,b4,b6,b8,c4,c6,Dis,E:
b2:=a1^2+4*a2:
b4:=a1*a3+2*a4:
b6:=a3^2+4*a6:
b8:=a1^2*a6-a1*a3*a4+4*a2*a6+a2*a3^2-a4^2:
c4:=b2^2-24*b4:
c6:=-b2^3+36*b2*b4-216*b6:
Dis:=-b2^2*b8-8*b4^3-27*b6^2+9*b2*b4*b6:
E:=[a1,a2,a3,a4,a6,b2,b4,b6,b8,c4,c6,Dis]:
return y^2=x^3+b2/4*x^2+b4/2*x+b6/4
end:
```

On considère maintenant le cas où la caractéristique de K est 3.

Proposition 12.2.17. *Soit E/K une courbe elliptique d'équation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

Si car$(K) = 3$, alors une forme courte de E est

$$\begin{cases} Y^2 = X^3 + a'_4X + a'_6 & si \quad j(E) = 0, \\ Y^2 = X^3 + a'_2X^2 + a'_6 & si \quad j(E) \neq 0, \end{cases}$$

Proof. Supposons car$K = 3$. Le changement de variables

$$(x, y) \mapsto \left(X, Y - \frac{a_1}{2}X - \frac{a_3}{2}\right),$$

dans l'équation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, permet d'obtenir

$$Y^2 = X^3 + \frac{b_2}{4}X^2 + \frac{b_4}{2}X + \frac{b_6}{4},$$

et alors $j(E) = \frac{b_2^6}{\Delta}$.

Si $j(E) = 0$, alors $b_2 = 0$ et on obtient l'équation $Y^2 = X^3 + a'_4X + a'_6$ avec $a'_4 = \frac{b_4}{2}$, $a'_6 = \frac{b_6}{4}$, $\Delta = -8b_4^3$ et $j(E) = 0$.

Si $j(E) \neq 0$, alors $b_2 \neq 0$ et le changement de variables

$$(X, X) \mapsto \left(X + 2\frac{b_4}{b_2}, Y\right),$$

permet d'obtenir l'équation

$$Y^2 = X^3 + \frac{b_2}{4}X^2 + \frac{2b_2^2b_4^2 + 2b_4^3 + b_2^3b_6}{b_2^3}.$$

Alors $\Delta =$ et $j(E) =$. □

Proposition 12.2.18. *Soit E/K une courbe elliptique d'équation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

Si $carK \neq 2$ et $carK \neq 3$, alors une forme courte de E est

$$y^2 = x^3 - 27c_4x - 54c_6.$$

Proof. Si car$K \neq 2$ et car$K \neq 3$, alors le changement de variable

$$(x, y) \mapsto \left(\frac{x' - 3b_2}{36}, \frac{y}{216}\right),$$

permet d'obtenir l'équation

$$y'^2 = x'^3 - 27c_4x' - 54c_6.$$

□

Maple code 12.2.19.

Avec Maple 12, la proposition 12.2.17 peut être programmée comme ceci.

```
      Programme

car23:=proc(a1,a2,a3,a4,a6)
global b2,b4,b6,b8,c4,c6,Dis,E:
b2:=a1^2+4*a2:
b4:=a1*a3+2*a4:
b6:=a3^2+4*a6:
b8:=a1^2*a6-a1*a3*a4+4*a2*a6+a2*a3^2-a4^2:
c4:=b2^2-24*b4:
c6:=-b2^3+36*b2*b4-216*b6:
Dis:=-b2^2*b8-8*b4^3-27*b6^2+9*b2*b4*b6:
E:=[a1,a2,a3,a4,a6,b2,b4,b6,b8,c4,c6,Dis]:
return y^2=x^3-27*c4*x-54*c_6
end:
```

On termine cette partie avec la proposition suivante.

Proposition 12.2.20. *Si car$K > 3$, alors la courbe de Weierstrass*

$$y^2 = x^3 + ax + b,$$

est non singulière si $4a^3 + 27b^2 \neq 0$.

Proof. Soit

$$F(x, y) = y^2 - x^3 - ax - b.$$

Si $P(x, y)$ un point singulier de la courbe, alors

$$\frac{\partial F}{\partial x}(P) = -3x^2 - a = 0, \quad \frac{\partial F}{\partial Y}(P) = 2y = 0.$$

On obtient ainsi $a = -x^2$ et $x^3 + ax + b = 0$ puis $b = 2x^3$ ce qui permet de vérifier $4a^3 + 27b^2 = 0$. □

12.3 Loi de groupe des courbes elliptiques

Dans cette partie, on s'intéresse à la structure de l'ensemble $E(K)$. Nous verrons qu'on peut définir une addition sur $E(K)$ qui lui permet d'avoir une structure de groupe commutatif.

12.3.1 Corde et tangente

Proposition 12.3.1. *Soient E/K une courbe elliptique et P et Q deux points de $E(K)$. Soit L la droite définie par*

$$L \text{ est } \begin{cases} \text{la droite passant par } P \text{ et } Q & \text{si } P \neq Q, \\ \text{la droite tangente en } P & \text{si } P = Q. \end{cases}$$

Soit R le troisième point d'intersection de E et de L. Soit V_R la droite verticale passant par R. On définit $P + Q$ comme étant le deuxième point d'intersection de E et de V_R.

Proof. Voir par exemple [25]. □

Pour illustrer cette proposition, voici un exemple d'addition de deux points différents de $E(\mathbb{R})$.

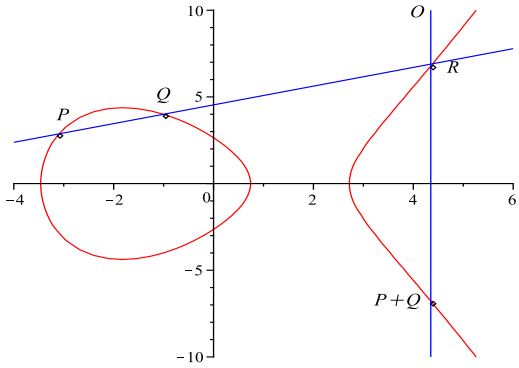


Figure 12.3: Courbe $y^2 = x^3 - 10x + 7$

Voici maintenant un exemple de doublement d'un point de $E(\mathbb{R})$.

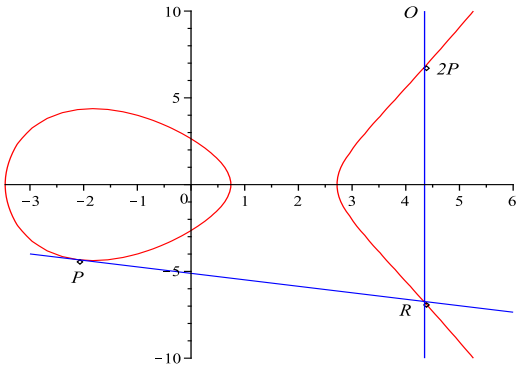


Figure 12.4: Courbe $y^2 = x^3 - 10x + 7$

12.3.2 L'opposé d'un point

Proposition 12.3.2. *Soient E/K une courbe elliptique et P un point de $E(K)$. Soit V_P la droite verticale passant par P. On définit $-P$ comme étant le deuxième point d'intersection de E et de V_P.*

Proof. Voir par exemple [25]. □

Pour illustrer cette proposition, voici un exemple de l'opposé d'un point P de $E(\mathbb{R})$.

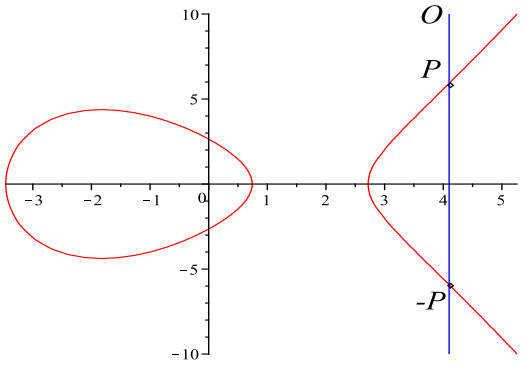


Figure 12.5: Courbe $y^2 = x^3 - 10x + 7$

12.3.3 L'opposé d'un point: formules explicites

On donne ci-dessous les formules explicites qui permettent de calculer explicitement l'opposé d'un point d'une courbe elliptique.

Proposition 12.3.3. *Soient E/K une courbe elliptique définie par l'équation de Weierstrass*

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

et $P = (x_1, y_1)$ un point de $E(K)$. Alors

$$-P = (-x_1, -y_1 - a_1x_1 - a_3).$$

Proof. Si $P = ((x_1, y_1)$ est un point de $E(K)$. La droite $x = x_1$ coupe la courbe en deux points $P = (x_1, y_1)$ et $-P = (x_2, y_2)$ avec $x_2 = x_1$. Avec le point P, on a

$$y^2 + (a_1x_1 + a_3)y_1 - \left(x_1^3 + a_2x_1^2 + a_4x_1 + a_6\right) = 0.$$

Or, sous forme factorisée, on peut écrire

$$y^2 + (a_1x_1 + a_3)y_1 - \left(x_1^3 + a_2x_1^2 + a_4x_1 + a_6\right) = (y - y_1)(y - y_2).$$

Ainsi, les racines y_1 et y_2 vérifient $y_1 + y_2 = -a_1x_1 - a_3$, ce qui donne $y_2 = -y_1 - a_1x_1 - a_3$. □

12.3.4 Doublement d'un point: formules explicites

On donne ci-dessous les formules explicites qui permettent de calculer le double d'un point d'une courbe elliptique.

Proposition 12.3.4. *Soient E/K une courbe elliptique définie par l'équation de Weierstrass*

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

et $P_1 = (x_1, y_1)$ un point de $E(K)$. Si $2y_1 + a_1x_1 + a_3 \neq 0$, on pose

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

Si $2y_1 + a_1x_1 + a_3 = 0$, alors $2P_1 = \mathcal{O}$, sinon $2P_1 = P_3 = (x_3, y_3)$ avec

$$\begin{aligned} x_3 &= -2x_1 - a_2 + a_1\lambda + \lambda^2, \\ y_3 &= -y_1 - (x_3 - x_1)\lambda - a_1x_3 - a_3. \end{aligned}$$

Proof. Soit $P_1 = (x_1, y_1)$. On définit la fonction

$$f(x, y) = y^2 + a_1xy + a_3y - \left(x^3 + a_2x^2 + a_4x + a_6\right).$$

Soit T la tangente en $P_1 = (x_1, y_1)$. Son équation est

$$\frac{\partial f}{\partial y}(x_1, y_1)(y - y_1) + \frac{\partial f}{\partial x}(x_1, y_1)(x - x_1) = 0$$

On peut alors distinguer deux cas suivant la valeur de $\frac{\partial f}{\partial y}(x_1, y_1) = 2y_1 + a_1x_1 + a_3$.

Si $2y_1 + a_1x_1 + a_3 = 0$, alors l'équation de la tangente T est $x = x_1$ qui est verticale, ce qui veut dire que $2P_1 = \mathcal{O}$.

Si $2y_1+a_1x_1+a_3 \neq 0$, on peut alors écrire l'équation de T plus simplement $y = \lambda(x-x_1)+y_1$ avec

$$\lambda = -\frac{\frac{\partial f}{\partial x}(x_1, y_1)}{\frac{\partial f}{\partial y}(x_1, y_1)} = \frac{3x_1^2 + a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

La tangente T coupe la courbe en un autre point $P_3' = (x_3', y_3')$. En reportant $y = \lambda(x - x_1) + y_1$ dans l'équation de Weierstrass, le coefficient de x^2 est

$$-\left(a_2 - a_1\lambda - \lambda^2\right)x^2.$$

La nouvelle expression de l'équation de Weierstrass est en fait de la forme $-(x-x_1)^2(x-x_3')$. Alors, par identification des coefficients de x^2, on obtient

$$x_3' = -2x_1 - a_2 + a_1\lambda + \lambda^2,$$

et donc $y_3' = \lambda(x_3' - x_1) + y_1$. On en déduit $P_3 = (x_3, y_3) = -P_3'$ par la proposition 12.3.3

$$x_3 = -x_1 - x_2 - a_2 + a_1\lambda + \lambda^2, \quad y_3 = -y_1 - \lambda(x_3 - x_1) - a_1x_3 - a_3.$$

□

12.3.5 Somme de deux points distincts: formules explicites

On donne ci-dessous les formules explicites qui permettent de calculer la somme de deux points distincts d'une courbe elliptique.

Proposition 12.3.5. *Soient E/K une courbe elliptique définie par l'équation de Weierstrass*

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

et $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points de $E(K)$ avec $P_1 \neq P_2$. Si $x_1 = x_2$, alors $P_1 + P_2 = \mathcal{O}$, sinon $P_1 + P_2 = P_3 = (x_3, y_3)$ avec

$$\begin{aligned} x_3 &= -x_1 - x_2 - a_2 + a_1\lambda + \lambda^2, \\ y_3 &= -y_1 - (x_3 - x_1)\lambda - a_1x_3 - a_3. \end{aligned}$$

et

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Proof. Soient $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points de $E(K)$ avec $P_1 \neq P_2$.

Supposons d'abord que $x_1 = x_2$. Comme $P_1 \neq P_2$, alors la droite passant par P_1 et P_2 a pour équation $x = x_1$ et est verticale, donc $P_1 + P_2 = \mathcal{O}$.

Supposons maintenant que $x_1 \neq x_2$. Soit L la droite passant par P_1 et P_2. Son équation est alors $y = \lambda(x - x_1) + y_1$ avec

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Cette droite coupe la courbe en un troisième point $P_3' = (x_3', y_3')$. En reportant $y = \lambda(x - x_1) + y_1$ dans l'équation de Weierstrass, le coefficient de x^2 est

$$-\left(a_2 - a_1\lambda - \lambda^2\right) x^2.$$

La nouvelle expression de l'équation de Weierstrass est en fait de la forme $-(x - x_1)(x - x_2)(x - x_3')$. Alors, par identification des coefficients de x^2, on obtient

$$x_3' = -x_1 - x_2 - a_2 + a_1\lambda + \lambda^2,$$

et donc $y_3' = \lambda(x_3' - x_1) + y_1$. On en déduit $P_3 = (x_3, y_3) = -P_3'$ par la proposition 12.3.3

$$x_3 = -x_1 - x_2 - a_2 + a_1\lambda + \lambda^2, \quad y_3 = -y_1 - \lambda(x_3 - x_1) - a_1x_3 - a_3.$$

□

Bibliography

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. Annals of Mathematics, 160(2):781–793, 2004.

[2] J.P. Buhler, H.W. Lenstra, and C. Pomerance, The development of the number field sieve, Volume 1554 of Lecture Notes in Computer Science, Springer-Verlag, 1994, pp. 50–94.

[3] 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).

[4] H. Cohen, A Course in Computational Number Theory, Graduate Texts in Mathematics, Springer, 1993.

[5] D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), 233—260 (1997).

[6] D. Coppersmith and A. Shamir, Lattice attacks on NTRU. In Advances in cryptology—EUROCRYPT '97, volume 1233 of Lecture Notes in Comput. Sci., pages 52–61. Springer, Berlin, 1997.

[7] W. Diffie, E. Hellman, New Directions in Cryptography, IEEE Trans- actions on Information Theory, 22, 5 (1976), pp. 644–654.

[8] T. El Gamal, A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory IT-31, 496-473,1976.

[9] Goldreich, O., Goldwasser, S., Halevi, S.: Public-Key Cryptosystems from Lattice Reduction Problems. Tech. rep., Massachusetts Institute of Technology (1996).

[10] G. Hanrot, LLL: A Tool for Effective Diophantine Approximation, in: The LLL Algorithm Survey and Applications, Phong Q. Nguyen and Brigitte Vallée Ed. Springer, 2010.

[11] G.H. Hardy, E.M. Wright. **An Introduction to the Theory of Numbers**. Oxford University Press, London (1965).

[12] J. Hoffstein, J. Pipher, and J. H. Silverman, NTRU: A Ring Based Public Key Cryptosystem in Algorithmic Number Theory. Lecture Notes in Computer Science 1423, Springer-Verlag, pages 267–288, 1998.

[13] J. Hoffstein, J. Pipher, and J. H. Silverman, An Introduction to Mathematical Cryptography, Springer-Verlag, UTM, 2008.

[14] B. King, Mapping an Arbitrary Message to an Elliptic Curve when Defined over GF(2^n), International Journal of Network Security, Vol.8, No.2, PP.169–176, Mar. 2009

[15] A. K. Lenstra, H. W. Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513—534, 1982.

[16] D. Micciancio and O. Regev. Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput., 37(1): pp. 267–302, 2007. Preliminary version in FOCS 2004.

[17] 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/`

[18] R. C. Merkle, M. E. Hellman, Hiding information and signatures in trap door knapsacks, IEEE Transactions on Information Theory, IT-24(5), pp. 525-530, 1978.

[19] P. Nguyen, Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from crypto'97. In M. Wiener, eds, Advances in Cryptology - CRYPTO'99, volume 1666 of Lecture Notes in Computer Science, pp. 790–790. Springer, 1999.

[20] 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).

[21] J. H. Silverman, Almost Inverses and Fast NTRU Key Creation," Tech. Rep. 14, NTRU Cryptosystems, Inc., March 1999. Version 1.

[22] D. Simon, Selected applications of LLL in number theory (2008) `www.math.unicaen.fr/~simon/maths/lll25_Simon.pdf`.

[23] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, STOC 2005, ACM (2005) pp. 84–93.

[24] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Computing 26, pp. 1484-1509 (1997).

[25] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, Springer-Verlag, 106 (1986)

[26] T. Laarhoven, J. van de Pol, B. de Weger, Solving hard lattice problems and the security of lattice-based cryptosystems, Cryptology ePrint Archive, No. 2012/533 (2012).

[27] M. Wiener. Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, 553—558 (1990).