ARITHMETIQUE

Ce chapitre est propre aux MPSI

PLAN

I : L'anneau $\mathbb{Z}$

1– Diviseurs communs, PGCD

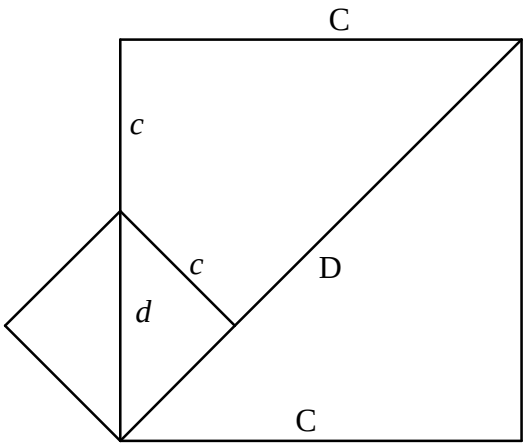
On appelle diviseur commun de deux entiers a et b un nombre d tel que d divise a et d divise b. On s'intéresse en particulier au plus grand d'entre eux, le PGCD (plus grand commun diviseur). Cette notion intervient couramment quand on cherche à simplifier une fraction rationnelle. Il est avantageux de diviser numérateur et dénominateur par leur PGCD.

A noter que les Grecs se posaient un problème comparable pour des grandeurs quelconques. Le problème était le suivant : étant données deux grandeurs A et B (longueurs, aires, mais aussi entiers), trouver une quantité X mesure commune à A et B, i.e. trouver X tel que A et B soient des multiples entiers de X. A l'époque pythagoricienne (VI^{ème} siècle avant J.C.) l'existence de X ne faisait pas de

doute. Un algorithme pour trouver X existait probablement déjà. Il est clairement exposé dans les *Eléments* d'Euclide (315-255 avant J.C.) :

> Si A > B, retrancher B de A autant de fois que possible.
> S'il reste une quantité R à A, recommencer sur B et R.
> S'il ne reste rien, X est la plus petite des deux quantités considérées.

Pour des quantités A et B quelconques, on peut se poser la question de savoir si l'algorithme se termine. Si oui, les quantités A et B sont dites commensurables (Aujourd'hui, on dirait A/B est rationnel), sinon, elles sont incommensurables (A/B est irrationnel). La découverte de grandeur incommensurable a été un événement marquant des mathématiques grecques. Prenons par exemple le cas de $\sqrt{2}$.



Prenons un petit carré sur la pointe, et construisons un grand carré dont le côté a pour longueur C, somme des longueurs de la diagonale d et du côté c du petit carré. On a un grand côté $C = d + c$, et une grande diagonale D. On a :

$D = 2c + d$ (car $D^2 = 2C^2 = 2c^2 + 4cd + 2d^2 = (2c + d)^2$ puisque $d^2 = 2c^2$)

$C = c + d$.

On va chercher la mesure commune à $A = C + D$ et à $B = C$. On voit que C va deux fois dans C + D. Donc le premier quotient est égal à 2. Le premier reste est c car $C + D - 2C = D - C = c$. On est donc maintenant amené à comparer C et c, c'est-à-dire $c + d$ et c. Ainsi, ayant fait l'opération une fois, on trouve pour quotient 2, et les deux nouvelles quantités à considérer sont c et le grand côté $C = c + d$. C'est exactement la même chose que ce dont on était parti, car, par homothétie, les deux rapports sont égaux. Par conséquent, les quotients successifs valent tous 2, jusqu'à l'infini. Ceci démontre que le rapport est irrationnel.

PROPOSITION

Pour deux entiers, l'algorithme d'Euclide se termine nécessairement et donne le PGCD.

Démonstration :

Soit deux entiers a et b. L'algorithme d'Euclide consiste successivement à diviser a par b, puis b par le reste obtenu précédemment, puis les deux restes entre eux, etc.... Pour $a = 1236$ et $b = 96$, on obtient successivement :

1236	96	$1236 = 96 \times 12 + 84$
84	96	$96 = 84 + 12$
84	12	$84 = 12 \times 7$

Sur cet exemple, on observe bien que la "mesure commune" à 1236 et 96 est 12.

Plus généralement :

Soit a et b deux entiers, $a > b$. On a :

$a = bq_1 + r_1$ avec $0 \leq r_1 < b$

$b = r_1q_2 + r_2$ avec $0 \leq r_2 < r_1$

$r_1 = r_2q_3 + r_3$ avec $0 \leq r_3 < r_2$

...

$r_{n-1} = r_nq_{n+1} + r_{n+1}$ avec $0 \leq r_{n+1} < r_n$

jusqu'à obtenir un reste nul (par exemple r_{n+1}). L'algorithme est nécessairement fini, sinon (r_n) formerait une suite strictement décroissante d'entiers, ce qu'on sait impossible. Montrons que le dernier reste calculé r_n est le PGCD :

❑ r_n divise a et b. En effet, r_n divise r_{n-1} puisqu'on a $r_{n+1} = 0$. Il se divise également lui-même. Par récurrence descendante, si r_n divise r_{p+1} et r_p, il divise r_{p-1} (car $r_{p-1} = r_pq_{p+1} + r_{p+1}$). Donc r_n divise r_1 et r_2, puis r_1 et b, puis a et b.

❑ un diviseur d commun à a et b divise également r_1 (car $r_1 = a - bq_1$). Il divise également r_2 (car $r_2 = b - r_1q_2$). Par récurrence ascendante, si d divise r_{p-1} et r_p, il divise r_{p+1} (car $r_{p+1} = r_{p-1} - q_{p+1}r_p$). d divise donc r_n.

Ainsi, r_n est un diviseur commun à a et à b et tout diviseur commun à a et b divise r_n. r_n est bien le plus grand diviseur commun de a et b, au sens de la relation de divisibilité. C'est le PGCD de a et b, noté PGCD(a, b) ou $a \wedge b$.

L'algorithme est le suivant. La fonction *mod* (*mod* pour modulo) donne le reste de la division euclidienne :

```
lire(A,B);                  # A = A0, B = B0,
                            #       A0 et B0 valeurs initiales.
                            #       PGCD(A,B) = PGCD(A0,B0)
tant que B ≠ 0 faire        # invariant de boucle :  PGCD(A0,B0) = PGCD(A,B)
        R ← A mod B;        # PGCD(A0,B0) = PGCD(A,B) = PGCD(R,B) car (A, B) et (B, R) ont
                            #     mêmes diviseurs communs donc même PGCD
        A ← B;              # PGCD(A0,B0) = PGCD(A,R)
        B ← R;              # PGCD(A0,B0) = PGCD(A,B)
fin faire                   # On quitte la boucle quand B = 0 donc quand PGCD(A0,B0) = A
resultat ← A;
```

Si $d = 1$, on dit que a et b sont *premiers entre eux*, ce qu'on note $a \wedge b = 1$. On peut également définir le PGCD de n nombres. Si celui–ci vaut 1, ces nombres sont dits *premiers entre eux dans leur ensemble* (exemple : 6, 10, 15)

2– Egalité de Bézout

Soit a et b deux entiers, et d leur PGCD. On cherche à exprimer d sous la forme $ax + by$, avec x et y élément de $\mathbb{Z}$. Est–ce possible ? On part de :

$a \times 1 + b \times 0 = a$

$a \times 0 + b \times 1 = b$

$a - bq_1 = r_1$

Si l'on a :

$ax_{p-1} + by_{p-1} = r_{p-1}$

$ax_p + by_p = r_p$

[où (r_p) est la suite des restes de la division euclidienne de a par b], on retranche q_{p+1} fois [où (q_p) est la suite des quotients] la deuxième de la première pour obtenir :

$$ax_{p+1} + by_{p+1} = r_{p+1}$$

avec $r_{p-1} = q_{p+1}r_p + r_{p+1}$

$x_{p+1} = x_{p-1} - q_{p+1}x_p$

$y_{p+1} = y_{p-1} - q_{p+1}y_p$

Si l'on définit les vecteurs $W_p = (r_p, x_p, y_p)$ avec $W_{-1} = (a, 1, 0)$ et $W_0 = (b, 0, 1)$ alors, les trois égalités précédentes s'interprètent vectoriellement par :

$$W_{p+1} = W_{p-1} - q_{p+1}W_p$$

On continue jusqu'au dernier reste non nul, obtenant ainsi r_n, PGCD de a et b.

EXEMPLE :

$a = 123$ et $b = 27$

	$1 \times a + 0 \times b = 123$	$[L_1]$	
	$0 \times a + 1 \times b = 27$	$[L_2]$	or $123 = 27 \times 4 + 15$
$\Rightarrow$	$a - 4b = 15$	$[L_3 = L_1 - 4L_2]$	or $27 = 15 \times 1 + 12$
$\Rightarrow$	$-a + 5b = 12$	$[L_4 = L_2 - L_3]$	or $15 = 12 \times 1 + 3$
$\Rightarrow$	$2a - 9b = 3$	$[L_5 = L_3 - L_4]$	

dernier calcul puisque 3 divise 12.

En particulier, si deux entiers a et b sont premiers entre eux, alors il existe x et y tels que $ax + by = 1$. Réciproquement, si cette relation est vérifiée, alors tout diviseur de a et divise 1 donc vaut 1, donc le PGCD de a et b est 1, et a et b sont premiers entre eux.

Un algorithme de l'identité de Bézout est le suivant :

X1,Y1,X2,Y2	sont des entiers, coefficients utilisés dans deux lignes successives de calcul
R,Q	sont des entiers, reste et quotient provisoires
Temp	est un entier, variable temporaire de transfert

Les commentaires prouvent la validité de l'algorithme.

```
lire(A,B)                          # A = A0, B = B0, valeurs initiales
                                   # PGCD(A0,B0) = PGCD(A,B)
X1 ← 1
Y1 ← 0                             # A0.X1 + B0.Y1 = A
X2 ← 0
Y2 ← 1                             # A0.X2 + B0.Y2 = B
tant que B ≠ 0 faire               # Les invariants de boucles sont :
                                   # A0.X1 + B0.Y1 = A
                                   # A0.X2 + B0.Y2 = B
                                   # PGCD(A0,B0) = PGCD(A,B)
    R ← A mod B
    Q ← A//B                       # on note ainsi le quotient de A par B
    Temp ← X1                      # A0.X1 + B0.Y1 = A et Temp = X1
                                   # A0.X2 + B0.Y2 = B
    X1 ← X2                        # A0.Temp + B0.Y1 = A
                                   # A0.X1 + B0.Y2 = B et X1 = X2
    X2 ← Temp – X2*Q               # A0.Temp + B0.Y1 = A
                                   # A0.X1 + B0.Y2 = B et X2 = Temp – X1.Q
                                   # ce qui implique :
```

	# A0.Temp + B0.Y1 = A
	# A0.X1 + B0.Y2 = B
	# A0.X2 + A.X1.Q + B0.Y1 = A
Temp ← Y1	# Temp = Y1
	# A0.X1 + B0.Y2 = B
	# A0.X2 + A.X1.Q + B0.Temp = A
Y1 ← Y2	# Y1 = Y2
	# A0.X1 + B0.Y1 = B
	# A0.X2 + A.X1.Q + B0.Temp = A
Y2 ← Temp – Y2*Q	# Y2 = Temp – Y1.Q
	# A0.X1 + B0.Y1 = B
	# A0.X2 + A.X1.Q + B0.Y2 + B0.Y1.Q = A
	# ce qui implique
	# A0.X2 + B0.Y2 = A – B.Q
	# PGCD(A0,B0) = PGCD(A,B) = PGCD(B,R)
A ← B	# A0.X1 + B0.Y1 = A
	# A0.X2 + B0.Y2 = R
	#PGCD(A0,B0) = PGCD(A,R)
B ← R	# A0.X1 + B0.Y1 = A
	# A0.X2 + B0.Y2 = B
	# PGCD(A0,B0) = PGCD(A,B)
jusqu'à B = 0	# lorsque B = 0, le PGCD est A.

On a bien obtenu les coefficients (X1, Y1) de l'égalité de Bézout

Nous pouvons énoncer :

PROPOSITION

Soit a et b deux entiers. Il existe x et y entiers tels que :

$ax + by = d$

où d est le PGCD de a et b.

La condition nécessaire et suffisante pour que a et b soient premiers entre eux est qu'il existe x et y tels que $ax + by = 1$.

On remarquera que, si on pose $a = da'$ et $b = db'$, alors a' et b' sont premiers entre eux.

3– Le théorème de Gauss

Le fait qu'un entier u divise un entier v est noté $u \mid v$.

PROPOSITION

Soit trois entiers a,b et c tels que $c \mid ab$, *et que* $c \wedge a = 1$. *Alors* $c \mid b$.

Démonstration :

Puisque $c \wedge a = 1$, il existe x et y tels que $ax + cy = 1$ donc $abx + bcy = b$ or $\exists\, q$, $ab = cq$ donc $b = c(qx + by)$ donc c divise b.

COROLLAIRES :

(i) Si on a une solution (x, y), comment s'obtiennent les autres ? Soit a' tel que $a = da'$ et b' tel que $b = db'$, avec $d = a \wedge b$. Soit (x', y') une autre solution de l'identité de Bézout. On a:

$$\begin{cases} ax + by = d \\ ax' + by' = d \end{cases} \Rightarrow \begin{cases} a'x + b'y = 1 \\ a'x' + b'y' = 1 \end{cases}$$

$\Rightarrow a'(x' - x) = b'(y - y')$. Or a' est premier avec b', donc divise $y - y'$. Il existe k tel que $y = y' + ka'$. En remplaçant, on obtient $x' = x + kb'$. Les solutions sont donc :

$$a(x + kb') + b(y - ka') = d$$

Le raisonnement précédent appliqué à $a = 123$ et $b = 27$ pour qui $2a - 9b = 3$ donnera :

$$a(2 + 9k) - b(9 + 41k) = 3$$

(ii) $\forall\, n \in \mathbb{Z}$, $a \wedge b = a \wedge (b + na)$

En effet, un diviseur commun a a et b est diviseur commun à a et $b + na$, et inversement. Cette règle permet parfois de calculer le PGCD de deux nombres plus vite qu'avec l'algorithme d'Euclide. Par exemple, par l'algorithme d'Euclide, on a :

$144 \wedge 89 = 89 \wedge 55 = 55 \wedge 34 = 34 \wedge 21 = 21 \wedge 13 = 13 \wedge 8 = 8 \wedge 5 = 5 \wedge 3 = 3 \wedge 2 = 2 \wedge 1 = 1$

alors que :

$144 \wedge 89 = 89 \wedge 34$ obtenu en remplaçant 144 par $2 \times 89 - 144 = 34$
$= 34 \wedge 13$ obtenu en remplaçant 89 par $3 \times 34 - 89 = 13$
$= 13 \wedge 5$ obtenu en remplaçant 34 par $3 \times 13 - 34 = 5$
$= 5 \wedge 2$ obtenu en remplaçant 13 par $3 \times 5 - 13 = 2$
$= 2 \wedge 1$ obtenu en remplaçant 5 par $5 - 2 \times 2 = 1$

soit cinq calculs au lieu de neuf.

(iii) $\begin{cases} a \wedge b = 1 \\ c \text{ divise } a \end{cases} \Rightarrow c \wedge b = 1$

En effet, il existe d tel que $a = dc$, et il existe u et v tel que :

$au + bv = 1$
$\Rightarrow \quad cdu + bv = 1$
$\Rightarrow \quad c \wedge b = 1$

(iv) $c \wedge a = 1 \Rightarrow a \wedge b = a \wedge (bc)$

En effet, un diviseur commun de a et b est évidemment diviseur commun de a et bc. Inversement, soit d diviseur commun de a et bc. On a, d'après la propriété précédente $d \wedge c = 1$. Or d divise bc. Il résulte du théorème de Gauss que d divise b. Ainsi a et b ont même diviseurs que a et bc et donc même PGCD. Cette règle permet également d'accélérer les calculs de PGCD. Par exemple :

$144 \wedge 89 = (4 \times 36) \wedge 89$ or $4 \wedge 89 = 1$ donc le PGCD cherché est égal à $36 \wedge 89$, ou à $9 \wedge 89 = 1$.

(v) $b \wedge c = 1 \Rightarrow a \wedge bc = (a \wedge b) \times (a \wedge c)$

Soit $d = a \wedge bc$, $q = a \wedge b$ et $r = a \wedge c$. Il existe u, v, x, y tels que :

$ax + by = q$
$au + cv = r$

donc $(ax + by)(au + cv) = qr = a(axu + xcv + byu) + bcvy = a\mathrm{X} + bc\mathrm{Y}$

donc qr est un multiple de d.

Par ailleurs, q divise a et b, donc divise a et bc donc divise d. De même, r divise d. Enfin, q est premier avec r car un diviseur commun de q et r est aussi un diviseur commun de b (que divise q) et de c (que divise r). Comme q et r divise d et sont premiers entre eux, qr divise d (cf viii ci-dessous).

Donc $qr = d$.

(vi) Si a est premier avec n nombres $b_1, b_2, ..., b_n$, alors a est premier avec leur produit

Par récurrence, on a :

$a \wedge b_1 ... b_k = 1$

Cette propriété est vraie pour $k = 1$. Soit k quelconque. Supposons que $a \wedge b_1 ... b_k = 1$. Alors $a \wedge b_1 ... b_k b_{k+1} = a \wedge b_1 ... b_k = 1$ puisque $a \wedge b_{k+1} = 1$, (en utilisant la règle (iv) du paragraphe précédent).

(vii) Si a et b sont premiers entre eux, alors, pour tout m et p, a^m et b^p sont premiers entre eux.
$a \wedge b = 1$, donc en appliquant (v) sur p fois b, on obtient $a \wedge b^p = 1$, puis en appliquant m fois (v) sur a, on obtient $a^m \wedge b^p = 1$.

(viii) Si a est divisible par $b_1, b_2, ..., b_n$ est que les b_i sont premiers entre eux deux à deux, alors a est divisible par le produit des b_i.
$a = b_1q_1$ et b_1q_1 est divisible par b_2. Or b_1 est premier avec b_2 donc b_2 divise q_1 d'après le théorème de Gauss. Donc il existe q_2 tel que $q_1 = b_2q_2$ et $a = b_1b_2q_2$. Par récurrence, supposons que $a = b_1b_2...b_kq_k$. b_{k+1} divise a donc divise $b_1b_2...b_kq_k$, mais b_{k+1} est premier avec $b_1b_2...b_k$ (d'après vi) donc, d'après le théorème de Gauss, b_{k+1} divise q_k donc il existe q_{k+1} tel que $q_k = b_kq_{k+1}$ et $a = b_1b_2...b_{k+1}q_{k+1}$

(ix) Si $p_1, ..., p_k$ sont des nombres premiers, et si $p_i^{n_i}$ divise a, alors a est divisible par le produit.
On appelle *nombre premier* tout entier naturel strictement supérieur à 1, divisible uniquement par 1 et par lui–même. Les premiers entiers premiers sont :
2 3 5 7 11 13 17 19 23 29 31 37 41 ...
Un nombre qui n'est pas premier est dit *composé*.
Le (ix) est une application directe du (viii), en remarquant que les $p_i^{n_i}$ sont premiers entre eux deux à deux d'après (vi).
Par exemple : 4 divise n et 9 divise $n \Rightarrow$ 36 divise n.

(x) Si p est premier et ne divise pas a, alors p et a sont premiers entre eux.
Un diviseur commun à a et p est un diviseur de p, donc vaut 1 ou p. Or ce n'est pas p, donc c'est 1.

(xi) Si p est premier et divise un produit de facteurs, alors p divise l'un des facteurs.
Sinon, p serait premier avec chacun des facteurs, donc avec le produit. Si on raisonne modulo p (i.e. à un multiple entier de p près), cela se traduit de la façon suivante : si un produit de facteurs est nul modulo p premier, alors l'un des facteurs est nul modulo p. On cherchera un exemple prouvant que ce résultat est faux si p n'est pas premier.

Voici une application qui généralise l'irrationalité de $\sqrt{2}$. Soit n entier. Alors $\sqrt{n}$ est soit irrationnel (par exemple $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, ...), soit entier (par exemple $\sqrt{16}$, $\sqrt{25}$ ...)
En effet, si $\sqrt{n}$ est rationnel, égal à $\frac{a}{b}$ avec $\frac{a}{b}$ qu'on peut supposer irréductible, on a $nb^2 = a^2$. Or a est premier avec b, donc (vi) a^2 est premier avec b^2. Mais b^2 divise a^2. Donc le PGCD de a^2 et b^2 est égal d'une part à 1, d'autre part à b^2. Ainsi $b^2 = 1$, $n = a^2$ et $\sqrt{n}$ est entier.

4– PPCM

On appelle multiple commun de deux entiers a et b un entier m qui est multiple de a et multiple de b. On s'intéresse au plus petit d'entre eux, le PPCM (plus petit commun multiple). Le PPCM intervient couramment quand on cherche à additionner deux rationnels. Il est intéressant de minimiser le dénominateur final en prenant comme dénominateur commun le PPCM des dénominateurs des deux fractions.

PROPOSITION
Soit m le PPCM *et d le* PGCD *de a et b. Alors ab = md.*

Démonstration :

Posons $a = da'$, et $b = db'$ avec $a' \wedge b' = 1$. Posons $m = \frac{ab}{d}$. On a donc $m = da'b' = ab' = ba'$ ce qui montre que m est multiple commun à a et à b. Soit maintenant n multiple de a et b. On a :
$n = ax = by \Leftrightarrow n = da'x = db'y \Rightarrow a'x = b'y$. Ainsi, b' divise $a'x$. Or b' est premier avec a'. Donc b' divise x. Il existe donc q tel $x = b'q$ donc $a'x = a'b'q$ donc $n = da'b'q = mq$. Donc tout multiple n de a et b est multiple de m. m est bien le plus petit multiple commun.

Le PPCM de a et b est noté PPCM(a, b) ou $a \vee b$.

On notera que si a et b sont premiers entre eux, le PGCD vaut 1 et le PPCM vaut ab.

5– Les nombres premiers

Rappelons que l'on appelle *nombre premier* tout entier naturel supérieur à 1, divisible uniquement par 1 et par lui–même. Les premiers entiers premiers sont :

2 3 5 7 11 13 17 19 23 29 31 37 41 ...

Un nombre qui n'est pas premier est dit *composé*.

PROPOSITION

Tout entier naturel supérieur strictement à 1 *se décompose de manière unique (à commutativité près) en produit (éventuellement réduit à un seul terme) de nombres premiers.*

Démonstration :

Montrons l'existence de la décomposition. Nous donnons trois démonstrations utilisant les trois principes équivalents fondamentaux de $\mathbb{N}$.

a) Principe de la descente infinie de Fermat : Si n est un nombre ne se décomposant pas en facteurs premiers, alors n n'est lui–même pas premier (sinon, $n = n$ est une décomposition). Donc, n s'écrit $n = ab$, avec $1 < a < n$ et $1 < b < n$. n ne se décomposant pas en facteurs premiers, nécessairement, a ou b ne se décompose pas en facteurs premiers. On trouve donc, pour tout entier ne se décomposant pas en facteurs premiers, un entier strictement plus petit ne se décomposant pas en facteurs premiers. Ce qui est impossible, car en itérant le procédé, on construirait une suite strictement décroissante d'entiers.

b) Principe du bon ordre : Soit A l'ensemble des entiers n'admettant pas de décomposition. Nous voulons montrer que A est vide. S'il était non vide, il y aurait un plus petit élément a. Si a n'admet pour diviseur que 1 et lui–même, a est premier. $a = a$ est une décomposition de a en facteurs premiers, ce qui est contraire à l'hypothèse. Donc a admet au moins deux diviseurs b et c. a étant le minimum de A, b et c ne sont pas éléments de A, et se décomposent donc en produit de facteurs premiers. Il en est donc de même de a.

c) Principe de récurrence : On suppose que tout entier inférieur ou égal à n se décompose en produits de facteurs premiers (ce qui est vrai pour $n \leq 2$). Considérons $n + 1$.

- ❑ Si $n + 1$ est premier, alors $n + 1 = n + 1$ est une décomposition.
- ❑ Sinon, $n + 1 = ab$, avec $1 < a < n + 1$, et $1 < b < n + 1$. L'hypothèse de récurrence s'applique sur a et b, qui se décomposent donc en produits de facteurs premiers. Il en est donc de même de $n + 1$.

Montrons l'unicité de la décomposition. Si :

$p_1^{r_1}...p_n^{r_n} = p_1^{s_1}...p_n^{s_n}$ avec $r_i \geq 0$ et $s_i \geq 0$ (on complète éventuellement les deux membres par des p^0 pour avoir les mêmes facteurs premiers dans les deux membres). Le théorème de Gauss permet de dire que $p_1^{r_1}$ divise le membre de droite, mais est premier avec p_2, ..., p_n, donc divise $p_1^{s_1}$, donc $r_1 \leq s_1$. Symétriquement, $s_1 \leq r_1$. Ainsi $s_1 = r_1$, et de même pour les autres puissances.

PROPOSITION

Si $a = p_1^{r_1}...p_n^{r_n}$ et $b = p_1^{s_1}...p_n^{r_n}$, *où les* p_i *sont des nombres premiers, alors* :

le PGCD *est égal à* $p_1^{t_1}...p_n^{t_n}$, *où* $t_i = \text{Min}(s_i, r_i)$.

le PPCM *est égal à* $p_1^{t_1}...p_n^{t_n}$, *où* $t_i = \text{Max}(s_i, r_i)$.

Par exemple :

$156 = 2^2 \times 3 \times 13$

$24 = 2^3 \times 3$

Donc le PGCD vaut $2^2 \times 3 = 12$; $156 = 12 \times 13$ et $24 = 12 \times 2$

le PPCM vaut $2^3 \times 3 \times 13 = 312 = 156 \times 2 = 24 \times 13$

La puissance de p intervenant dans la décomposition d'un nombre n s'appelle valuation p-adique de n, votée $v_p(n)$. Les notations précédentes se traduisent donc sous la forme :

$v_p(a \wedge b) = \text{Min}(v_p(a), v_p(b))$ pour tout facteur premier p

$v_p(a \vee b) = \text{Max}(v_p(a), v_p(b))$

Démonstration :

Soit $d = p_1^{t_1}...p_n^{t_n}$. Comme, pour tout i, $t_i \leq r_i$ et $t_i \leq s_i$, il est clair que d divise a et b. Montrons que c'est le plus grand diviseur. Considérons un diviseur q quelconque et décomposons-le en facteurs premiers. Comme q divise a, pour tout nombre premier p, $p^{v_p(q)}$ divise q donc divise a, donc $p^{v_p(q)}$ divise $p^{v_p(a)}$ donc $v_p(q) \leq v_p(a)$. De même $v_p(q) \leq v_p(b)$. Donc $v_p(q) \leq \text{Min}(v_p(a), v_p(b)) = v_p(d)$. Le même raisonnement ayant lieu pour tout facteur premier p, on a q diviseur de d.

Si $m = \text{PPCM}(a, b)$, comme $m = \frac{ab}{d}$, on a, pour tout p premier :

$v_p(m) = v_p(a) + v_p(b) - v_p(d) = v_p(a) + v_p(b) - \text{Min}(v_p(a), v_p(b)) = \text{Max}(v_p(a), v_p(b))$

comme on le vérifiera aisément

PROPOSITION

L'ensemble des nombres premiers est infini.

Démonstration ;

La démonstration est connue depuis Euclide. En effet, soit p_1, ..., p_n n nombres premiers. Montrons qu'il en existe nécessairement un autre. On considère la quantité $p_1p_2...p_n + 1$. Soit q un nombre premier divisant cette quantité. Alors q est nécessairement différent de tous les p_i. Car s'il existe i tel que $q = p_i$, q divise $p_1p_2...p_n$ d'une part, et divise $p_1p_2...p_n + 1$ d'autre part, donc divise la différence 1, ce qui est impossible. Ainsi, la famille de nombres premiers ne peut être finie.

On notera qu'il se peut que $p_1p_2...p_n + 1$ lui–même soit premier. En fait, on ignore si la quantité $p_1p_2...p_n + 1$ prend une infinité de fois une valeur première, ou si elle prend une infinité de fois une valeur non première. Par ailleurs, si $p_1 = 2$ et si on pose p_n le plus petit premier diviseur de $p_1p_2...p_{n-1} + 1$, on construit une suite infinie de nombres premiers distincts deux à deux . Voici les premiers termes de la suite :

2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17,...

On conjecture que tous les nombres premiers apparaissent dans la liste ci-dessus. La même conjecture s'applique également à la variante suivante : on prend $q_1 = 3$ et on définit q_n comme le plus petit premier de la suite $q_1q_2...q_{n-1} - 1$ dont les premiers termes sont :

3, 2, 5, 29, 11, 7, 13, 37, 32222189, 131, 136013303998782209, 31, 197, 19, 157, 17...

Les démonstrations de l'infinitude des nombres premiers sont innombrables. En voici une autre, datant de 1955 (preuve de Furstenberg). Pour tout a et b entiers, notons $a + b\mathbb{Z} = \{a + nb, n \in \mathbb{Z}\}$. Pour tout entier n, l'ensemble des non-multiples de n est :

$$\mathrm{NM}(n) = \{m, m \text{ ne divise pas } n\} = (1 + n\mathbb{Z}) \cup (2 + n\mathbb{Z}) \cup ... \cup (n-1 + n\mathbb{Z})$$

On note par ailleurs que, pour toute famille finie (r_i) et (n_i), $i \in \mathrm{I}$, n_i étant non nuls, $\bigcap_{i\in 1} r_i + n_i\mathbb{Z}$ est vide ou infinie. Car si x appartient à cette intersection, alors il en est de même de tous les $x + k\prod_{i\in \mathrm{I}} n_i$, $k \in \mathbb{Z}$. Supposons maintenant que la famille des nombres premiers soit une famille finie P. L'ensemble $\bigcap_{p\in \mathrm{P}} \mathrm{NM}(p)$ est constituée des entiers relatifs multiples d'aucun nombre premier. Il s'agit donc simplement de l'ensemble constitué de deux éléments {–1, 1}. Mais on a également :

$$\bigcap_{p\in \mathrm{P}} \mathrm{NM}(p) = \bigcap_{p\in \mathrm{P}} \bigcup_{k=1}^{p-1} k + p\mathbb{Z}$$

Or $\cap$ est distributif par rapport à $\cup$ de sorte qu'une intersection finie de réunion finie de $k + p\mathbb{Z}$ est également une réunion finie d'une intersection finie de tels ensembles. Mais nous avons vu qu'une telle intersection est vide ou infinie. Il en est a fortiori vraie pour la réunion qui, vide ou infinie, ne peut en aucun cas être égale à {–1, 1}.

Les records de nombres premiers sont (en 2016) :

$2^{86243} - 1$	qui possède 25 962 chiffres (1983 par Slowinski)
$2^{132049} - 1$	qui possède 39 751 chiffres (1984 par Slowinski)
$2^{216091} - 1$	qui possède 65 050 chiffres (1985 par Slowinski)
$391581 \times 2^{216193} - 1$	qui possède 65 087 chiffres (1989 par Brown)
$2^{756839} - 1$	qui possède 227 832 chiffres (1992 Slowinski et Gage)
$2^{859433} - 1$	qui possède 258 716 chiffres (1994 Slowinski et Gage)
$2^{1257787} - 1$	qui possède 378 632 chiffres (1996 Slowinski et Gage)
$2^{1398269} - 1$	qui possède 420 921 chiffres (1996 Armengaud/[Gimps])
$2^{2976221} - 1$	qui possède 895 932 chiffres (1997 Spence/[Gimps])
$2^{3021377} - 1$	qui possède 909 526 chiffres (1998 Clarkson/[Gimps])
$2^{6972593} - 1$	qui possède 2 098 960 chiffres (1999 Hajratwala/[Gimps])
$2^{13466917} - 1$	qui possède 4 053 946 chiffres (2001 Cameron/[Gimps])
$2^{20996011} - 1$	qui possède 6 320 430 chiffres (2003 Shafer/[Gimps])
$2^{24036583} - 1$	qui possède 7 235 733 chiifres (2004 Findley/[Gimps])
$2^{25964951} - 1$	qui possède 7 816 230 chiffres (2005 Nowak/[Gimps])
$2^{30402457} - 1$	qui possède 9 152 052 chiffres (2005, Boone, Cooper/[Gimps])
$2^{32582657} - 1$	qui possède 9 808 358 chiffres (2006, Boone, Cooper/[Gimps])
$2^{43112609} - 1$	qui possède 12 978 189 chiffres (2008, Cooper/[Gimps])
$2^{57885161} - 1$	qui possède 17 425 170 chiffres (2013, Cooper[GIMPS])
$2^{74\,207\,281} - 1$	qui possède 22 338 618 chiffres (2016, Cooper[GIMPS])

On pourra consulter le site internet **http://www.mersenne.org** pour de plus amples renseignements. On voit que la plupart de ces nombres sont de la forme $2^n - 1$. Ce sont les nombres de Mersenne, pour lesquels Lucas a défini au XIXème un algorithme efficace permettant de déterminer leur primalité.

On consultera l'annexe V pour de plus amples renseignements sur les difficultés à déterminer si un nombre est premier ou composé.

6– Le petit théorème de Fermat

Il s'énonce comme suit :

PROPOSITION

Soit p premier et a non multiple de p. Alors $a^{p-1} \equiv 1 \bmod p$.

On peut aussi l'énoncer sous la forme suivante : pour tout a, on a $a^p \equiv a \bmod p$. Cette deuxième formulation est équivalente à la première car $a^p \equiv a \bmod p$ signifie que p divise $a^p - a$ et donc divise $a(a^{p-1} - 1)$. Donc, a étant premier avec n, le théorème de Gauss permet de conclure que p divise $a^{p-1} - 1$.

Démonstration :

La relation $a^p \equiv a \bmod p$ se montre par exemple par récurrence sur a. Elle est vraie pour $a = 1$, et si elle est vraie pour un nombre a, on a :

$$(a+1)^p = \sum_{k=0}^{n} \binom{p}{k} a^k = a^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k$$

Or $\binom{p}{k} = \dfrac{p(p-1)\ldots(p-k+1)}{k!}$ est un entier donc $k!$ divise $p(p-1)\ldots(p-k+1)$. Par ailleurs $p > k$ donc p ne divise aucun nombre inférieur ou égal à k, donc p est premier avec tous les nombres inférieurs ou égaux à k donc p est premier avec leur produit $k!$. Puisque $k!$ divise $p(p-1)\ldots(p-k+1)$ et que $k!$ est premier avec p, $k!$ divise $(p-1)\ldots(p-k+1)$. Donc $\binom{p}{k} = p \times$ un entier, donc $\binom{p}{k} \equiv 0 \bmod p$. Il en résulte que :

$(a+1)^p \equiv a^p + 1 \bmod p \equiv a + 1 \bmod p$ en appliquant l'hypothèse de récurrence.

On consultera l'annexe VII sur les tests de primalité pour voir comment on utilise ce théorème de Fermat dans la recherche de nombres premiers.

II : L'anneau des polynômes K[X]

Les propriétés des polynômes sont en tout point comparables à celles des entiers. C'est pour cette raison que ce paragraphe a été placé dans le chapitre *Arithmétique* et non dans le chapitre *Polynômes*.

1– Algorithme du calcul du PGCD

On cherche le plus grand diviseur commun à deux polynômes A et B, le plus grand signifiant pour le moment de degré maximal. L'algorithme d'Euclide, appliqué à deux entiers, admet une traduction pour les polynômes. Cherchons le PGCD de $X^3 + 2X^2 - X - 2$ et de $X^2 + 4X + 3$. On a :

$X^3 + 2X^2 - X - 2 = (X^2 + 4X + 3)(X - 2) + 4X + 4$

$X^2 + 4X + 3 = (4X + 4)(\frac{X}{4} + \frac{3}{4})$

Le PGCD est donc 4X + 4, ou plutôt X + 1, l'habitude étant de donner le polynôme normalisé ou unitaire, i.e. celui dont le coefficient du terme de plus haut degré vaut 1. Prouvons que la démarche suivie donne bien le PGCD. La démonstration pourra être comparée avec ce qui se passe dans **Z**.

Soit A et B deux polynômes, deg(A) ≥ deg(B). On a :

$A = BQ_1 + R_1$ avec $\deg(R_1) < \deg(B)$

$B = R_1Q_2 + R_2$ avec $\deg(R_2) < \deg(R_1)$

$R_1 = R_2Q_3 + R_3$ avec $\deg(R_3) < \deg(R_2)$

...

$R_{n-1} = R_nQ_{n+1} + R_{n+1}$ avec $\deg(R_{n+1}) < \deg(R_n)$

jusqu'à obtenir un reste nul (par exemple R_{n+1}). L'algorithme est nécessairement fini, sinon ($\deg(R_n)$) formerait une suite strictement décroissante d'entiers, ce qu'on sait impossible. Le dernier reste calculé R_n est le PGCD. La démonstration est identique à celle des entiers.

Les diviseurs communs de A et B sont exactement les diviseurs de R_n. Le PGCD est donc R_n. Le PGCD est en fait défini à une constante non nulle multiplicative près (car les diviseurs restent les mêmes). On choisit donc le polynôme unitaire correspondant. Le qualificatif de *plus grand* s'applique non seulement au sens de *diviseur commun de plus haut degré* mais également aussi au sens de *diviseur commun multiple de tout autre diviseur commun*, comme pour les entiers.

Si D = 1, on dit que A et B sont *premiers entre eux*. On peut également définir le PGCD de *n* polynômes. Si celui–ci vaut 1, ces polynômes sont dits *premiers entre eux dans leur ensemble* (exemple : (X + 1)(X + 2), (X + 1)(X + 3), (X + 2)(X + 3))

On appelle *polynôme irréductible* tout polynôme de degré supérieur ou égal à 1, divisible uniquement par 1 et par lui–même (à une constante multiplicative près). Les polynômes irréductibles jouent dans $\mathbb{K}[X]$ le même rôle que les nombres premiers dans $\mathbb{Z}$.

2– Egalité de Bézout

Soit A et B deux polynômes, et D leur PGCD. On cherche à exprimer D sous la forme AP + BQ, avec P et Q élément de $\mathbb{K}[X]$. Est–ce possible ? Il suffit de reprendre l'algorithme donné dans $\mathbb{Z}$, qui s'adapte mot à mot.

EXEMPLE :

$A = X^4 + X^3 - 2X + 1$ et $B = X^2 + X + 1$. On a:

$A + 0B = X^4 + X^3 - 2X + 1$

$0A + B = X^2 + X + 1$ or $X^4+X^3-2X+1 = (X^2+X+1)(X^2-1) - X + 2$

$\Rightarrow$ $A - (X^2 - 1)B = - X + 2$ or $X^2+X+1 =(-X+2)(-X-3) + 7$

$\Rightarrow$ $(X + 3)A - (X^3 + 3X^2 - X - 4)B = 7$

Les deux polynômes sont premiers entre eux.

On retiendra en particulier que deux polynômes A et B sont premiers entre eux si et seulement si il existe P et Q tels que AP + BQ = 1 (ou égale une constante non nulle).

Nous pouvons énoncer :

PROPOSITION

Soit A et B deux polynômes. Il existe P et Q polynômes tels que :

$$AP + BQ = D$$

où D est le PGCD de A et B.
La condition nécessaire et suffisante pour que A et B soient premiers entre eux est qu'il existe P et Q tels que AP + BQ = 1.

On remarquera que, si on pose A = DA' et B = DB', alors A' et B' sont premiers entre eux.

3– Le théorème de Gauss

PROPOSITION
Soit trois polynômes A,B et C tels que C divise le produit AB, et que C soit premier avec A. Alors C divise B

Démonstration :
Identique aux entiers. On peut la rappeler rapidement : il existe P et Q tels que AP + CQ = 1 donc ABP + BCQ = B. On voit alors facilement que C divise le premier membre, donc divise B.

Tous les corollaires énoncés dans le cas des entiers s'appliquent ici. Citons par exemple :

i) Si A est premier avec n polynômes B_1, B_2, ..., B_n, alors A est premier avec leur produit

ii) Si A est divisible par B_1, B_2, ..., B_n est que les B_i sont premiers entre eux deux à deux, alors A est divisible par le produit des B_i.

iii) Si P_1, ..., P_k sont des polynômes irréductibles, et si $P_i^{n_i}$ divise A, alors A est divisible par le produit.

iv) Si P est irréductible et ne divise pas A, alors P et A sont premiers entre eux.

v) Si P est irréductible et divise un produit de facteurs, alors P divise l'un des facteurs.

Voici une application de ce qui précède :

PROPOSITION
Soit P un polynôme non nul de degré n. Alors le nombre de ses racines, comptées avec leur ordre de multiplicité est inférieur ou égal à n.

Démonstration :
Soit a_i de multiplicité k_i les racines. Alors P est divisible par $(X - a_i)^{k_i}$. Or ces facteurs sont premiers entre eux deux à deux. Donc P est divisible par le produit. Le degré du produit ne pouvant excéder le degré de P, on en déduit que la somme des k_i est inférieure ou égale au degré de P.

COROLLAIRE
Soit P un polynôme de degré inférieur ou égal à n, et admettant plus de n racines. Alors P est nul.

COROLLAIRE
Soit P un polynôme à coefficients dans un sous–corps de $\mathbb{C}$. Alors, si la fonction polynomiale associée à P est identiquement nulle, P a tous ses coefficients nuls.

Démonstration :
Si la fonction polynomiale est nulle, elle admet une infinité de racines. Le polynôme ne peut donc qu'être nul.

4– Les polynômes irréductibles

On appelle *polynôme irréductible* tout polynôme de degré supérieur ou égal à 1, divisible uniquement par 1 et par lui–même (à une constante multiplicative près). Voici des exemples de polynômes irréductibles :

Dans $\mathbb{C}[X]$: $X - 2$, $X + i$

Dans $\mathbb{R}[X]$: $X - 2$, $X^2 + 1$

Dans $\mathbb{Q}[X]$: $X - 2$, $X^2 + 1$, $X^2 - 2$

On voit que la condition d'irréductibilité dépend du corps sur lequel on travaille.

PROPOSITION

Tout polynôme unitaire de degré supérieur ou égal à 1 *se décompose de manière unique (à commutativité près) en produit (éventuellement réduit à un seul terme) de polynômes irréductibles unitaires.*

Démonstration analogue à celle des entiers :

Montrons l'existence de la décomposition. Soit E l'ensemble des polynômes n'admettant pas de décomposition. Nous voulons montrer que E est vide. Raisonnons par l'aburde. S'il était non vide, il y aurait un polynôme de plus petit degré A. Si A n'admet pour diviseur que 1 et lui–même, A est irréductible. A = A est une décomposition de A en facteurs premiers, ce qui est contraire à l'hypothèse. Donc A admet au moins deux diviseurs B et C. A étant de degré minimum dans E, B et C ne sont pas éléments de E, et se décomposent donc en produit de facteurs irréductibles. Il en est donc de même de A, ce qui conduit à une contradiction.

Montrons l'unicité de la décomposition. Si :

$P_1^{r_1}...P_n^{r_n} = P_1^{s_1}...P_n^{s_n}$ avec $r_i \geq 0$

le théorème de Gauss permet de dire que $P_1^{r_1}$ divise le membre de droite, mais il est premier avec P_2, ..., P_n, donc il divise $P_1^{s_1}$, donc $r_1 \leq s_1$. Symétriquement, $s_1 \leq r_1$. Ainsi $s_1 = r_1$, et de même pour les autres puissances.

Si $A = P_1^{r_1}...P_n^{r_n}$ et $B = P_1^{s_1}...P_n^{s_n}$, où les P_i sont des polynômes irréductibles, alors le PGCD est égal à $P_1^{u_1}...P_n^{u_n}$, où $u_i = \text{Inf}(s_i, r_i)$. Par exemple, le PGCD de $(X - 2)^3(X + 1)^2$ et de $(X - 2)^2(X + 1)^4(X + 3)$ est égal à $(X - 2)^2(X + 1)^2$, mais en général, on ne possède pas d'algorithme pour décomposer un polynôme en facteurs irréductibles. Il est plus efficace de calculer le PGCD par l'algortihme d'Euclide donné plus haut.

L'ensemble des polynômes irréductibles est infini. Une fois de plus, la démonstration est parfaitement identique à celle de $\mathbb{Z}$. En effet, soit P_1, ..., P_n n polynômes irréductibles. Montrons qu'il en existe nécessairement un autre. On considère la quantité $P_1P_2...P_n + 1$. Soit Q un facteur irréductible divisant cette quantité. Alors Q est nécessairement différent de tous les P_i. Car si $Q = P_i$, Q divise $P_1P_2...P_n$ d'une part, et divise $P_1P_2...P_n + 1$ d'autre part, donc divise la différence 1, ce qui est impossible.

5– PPCM

On appelle PPCM de A et B (respectivement de A_1, A_2, ..., A_n) le polynôme unitaire multiple commun à A et B (ou à A_1, ..., A_n) de plus bas degré.

Si $A = P_1^{r_1}...P_n^{r_n}$ et $B = P_1^{s_1}...P_n^{s_n}$, où les P_i sont des polynômes irréductibles, alors le PPCM est égal à $P_1^{t_1}...P_n^{t_n}$, où $t_i = \text{Sup}(s_i, r_i)$. Par exemple, le PPCM de $(X - 2)^3(X + 1)^2$ et de $(X - 2)^2(X + 1)^4(X + 3)$ est égal à $(X - 2)^3(X + 1)^4(X + 3)$. On a également AB = MD, où D est le PGCD de A et B, et M le PPCM (Si les polynômes ne sont pas unitaires, il y a une constante en facteur). La démonstration est identique à celle des entiers.

Les annexes qui suivent sont de lecture difficile. Elles montrent diverses applications de l'arithmétique et mettent en évidence le fait que ce chapitre n'est qu'une maigre introduction à ce vaste domaine.

Annexe I : Le numéro INSEE

❑ Le numéro INSEE est constitué de 15 chiffres. Le nombre A constitué des treize premiers identifie la personne alors que le nombre B constitué des deux derniers chiffres sert de contrôle. On peut détecter une erreur sur un chiffre, ou bien on peut détecter la permutation de deux chiffres consécutifs. B est défini par la formule B = 97 – (A mod 97). Considérons par exemple le nombre purement fictif A = 0630215012026. Alors B = 34.

Pour tester la validité du numéro 063021501202634, on calcule A + B, soit 630215012060 et on vérifie que c'est un multiple de 97. Si tel est le cas, le numéro est considéré comme valide. Dans le cas contraire, il y a une erreur.

Ce sera le cas si un chiffre est faux. En effet, dans ce cas, A + B est en fait égal modulo 97 à un nombre de la forme $x10^n$, où x est un chiffre de 0 à 9. Celui-ci n'étant pas divisible par 97, l'erreur est détectée.

Il en est de même si on a permuté deux chiffres consécutifs. En effet, dans ce cas, A + B est égal modulo 97 à un nombre de la forme $y \times 10^n + x \times 10^{n-1} - x \times 10^n - y \times 10^{n-1}$ soit $9 \times 10^{n-1} \times (y - x)$ qui n'est pas divisible par 97.

❑ Un procédé comparable est utilisé pour le relevé d'identité bancaire (RIB) : les deux derniers chiffres forment une clef choisie de façon que le nombre formé par la suite des différents codes (établissement, guichet, compte, clef) soit divisible par 97.

❑ Quant au code ISBN des livres (*International Standard Book Number*), il est constitué de dix chiffres a_i, $1 \le i \le 10$, dont les neufs premiers identifient l'éditeur et le livre, et le dernier est une clef choisie de façon que $\sum_{i=1}^{10} i a_{11-i}$ soit divisible par 11. Là aussi, une erreur sur un chiffre est détectée. Si la clef doit se voir attribuer la valeur 10, elle sera notée X. Par exemple :

0-387-97993-X

(code ISBN d'un livre remarquable dont on ne peut que recommander la lecture ☺)

Annexe II : Utilisation d'un corps fini dans le codage des transmissions

Le Minitel est un objet devenu obsolète depuis le développement d'Internet, mais la description de son mode de communication est représentatif de procédés encore utilisés actuellement dans tous les moyens de communication numériques modernes (téléphone portable, téléviseur, ...). Les messages envoyés par Minitel étaient codés de façon à pouvoir détecter une erreur et la corriger. Pour cela, on utilise $\mathbb{F}_{128}$, corps fini possédant 128 éléments.

$\mathbb{F}_{128}$ se construit de la façon suivante. On considère $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Ce dernier ensemble possède uniquement les deux éléments 0 et 1, avec la règle de calcul 1 + 1 = 0 (0 peut être considéré comme

représentant les nombres pairs et 1 les nombres impairs. On a alors impair + impair = pair). Dans l'anneau des polynômes $\mathbb{F}_2[X]$, on prouve que le polynôme $X^7 + X^3 + 1$ est irréductible. De même qu'on construit $\mathbb{C}$ à partir de $\mathbb{R}$ en introduisant un symbole i racine de $X^2 + 1$, nous construisons $\mathbb{F}_{128}$ en introduisant un symbole α racine de $X^7 + X^3 + 1$. Les éléments de $\mathbb{F}_{128}$ sont de la forme $a_0\alpha^6 + a_1\alpha^5 + ... + a_5\alpha + a_6$, les a_i étant éléments de $\mathbb{F}_2$. α vérifie donc : $\alpha^7 + \alpha^3 + 1 = 0$. On montre que :

i) à isomorphisme près, $\mathbb{F}_{128}$ est unique.

ii) $\mathbb{F}_{128} - \{0\}$ est un groupe multiplicatif cyclique, engendré par α, c'est-à-dire que l'on a $\mathbb{F}_{128} = \{0, 1, \alpha, \alpha^2, ..., \alpha^{126}\}$ (et $\alpha^{127} = 1\}$

Ainsi, les éléments de $\mathbb{F}_{128}$ peuvent être considérés indifféremment :

- comme des polynômes en α à coefficient 0 ou 1, avec la règle de calcul $\alpha^7 + \alpha^3 + 1 = 0$ et $1 + 1 = 0$.
- comme des éléments de la forme α^k, $0 \le k \le 126$, auquel on adjoint 0, avec la règle de calcul $\alpha^{127} = 1$.

A titre d'exemples plus simples, voici ci-dessous la description précise de corps finis plus petits. Pour cela, il nous faut trouver des polynômes irréductibles de $\mathbb{F}_2[X]$. Il suffit de partir des deux polynômes élémentaires X et 1+X, puis de chercher leurs produits. On obtient ainsi tous les polynômes réductibles. Les autres sont irréductibles. On obtient ainsi :

degré	polynômes réductibles	polynômes irréductibles
1		X, $X+1$
2	X^2, X^2+X, $X^2+1 = (X+1)^2$	X^2+X+1
3	$XP(X)$ ... $X^3+1 = (X+1)(X^2+X+1)$ $X^3+X^2+X+1 = (X+1)^3$	X^3+X^2+1 X^3+X+1
4	$XP(X)$ (8 polynômes) $X^4+1 = (X+1)^4$ $X^4+X^3+X+1 = (X+1)^2(X^2+X+1)$ $X^4+X^2+X+1 = (X+1)(X^3+X^2+1)$ $X^4+X^3+X^2+1 = (X+1)(X^3+X+1)$ $X^4+X^2+1 = (X^2+X+1)^2$	$X^4+X^3+X^2+X+1$ X^4+X^3+1 X^4+X+1
5	$XP(X)$ (16 polynômes) $(X+1)P(X)$ (8 autres polynômes) $X^5+X+1 = (X^2+X+1)(X^3+X^2+1)$ $X^5+X^4+1 = (X^2+X+1)(X^3+X+1)$	$X^5+X^4+X^3+X^2+1$ $X^5+X^4+X^3+X+1$ $X^5+X^4+X^2+X+1$ $X^5+X^3+X^2+X+1$ X^5+X^3+1 X^5+X^2+1

etc ...

On définit alors :
$\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ avec $\alpha^2 = \alpha + 1$
$= \{0, 1, \alpha, \alpha^2\} = \{0, 1, \alpha, 1 + \alpha\}$

$\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ avec $\alpha^3 = \alpha + 1$, par exemple.
Les éléments de $\mathbb{F}_8$ sont :

0
1
α
α^2
$\alpha^3 = \alpha + 1$
$\alpha^4 = \alpha^2 + \alpha$
$\alpha^5 = \alpha^2 + \alpha + 1$
$\alpha^6 = \alpha^2 + 1$

($\alpha^7 = 1$)
Les racines de $X^3 + X + 1$ sont α, α^2, α^4.
Les racines de $X^3 + X^2 + 1$ sont α^3, α^5, α^6.

$\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$ avec $\alpha^4 = \alpha + 1$, par exemple.
Les éléments de $\mathbb{F}_{16}$ sont :

0
1
α
α^2
α^3
$\alpha^4 = \alpha + 1$
$\alpha^5 = \alpha^2 + \alpha$
$\alpha^6 = \alpha^3 + \alpha^2$
$\alpha^7 = \alpha^3 + \alpha + 1$
$\alpha^8 = \alpha^2 + 1$
$\alpha^9 = \alpha^3 + \alpha$
$\alpha^{10} = \alpha^2 + \alpha + 1$
$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^{13} = \alpha^3 + \alpha^2 + 1$
$\alpha^{14} = \alpha^3 + 1$

On a $\alpha^{15} = 1$.
Les racines de $X^4 + X^3 + X^2 + X + 1$ sont α^3, α^6, α^9 et α^{12}.
Les racines de $X^4 + X^3 + 1$ sont α^7, α^{11}, α^{13} et α^{14}. Les racines de $X^4 + X + 1$ sont α, α^2, α^4 et α^8

$\mathbb{F}_{32} = \mathbb{F}_2[X]$ avec $\alpha^5 = \alpha^2 + 1$.
etc ...

Revenons au Minitel et à $\mathbb{F}_{128}$. Pour envoyer un message de 15 octets (soit 120 bits) de la forme $M = b_0 b_1 ... b_{119}$, où les b_i sont des bits, éléments de $\mathbb{F}_2$, on considère l'élément de $\mathbb{F}_{128}$ égal à $T = b_0 \alpha^{126} + ... + b_{119} \alpha^7$. Cet élément est en fait égal à un élément de $\mathbb{F}_{128}$ de la forme $b_{120} \alpha^6 + ... + b_{125} \alpha + b_{126}$. On envoie le message $b_0 b_1 ... b_{119} b_{120} ... b_{126}$, soit 127 caractères. (Si on ajoute également un bit de parité, on obtient exactement 16 octets. Nous n'en tenons pas compte ici). Le message envoyé correspond donc dans $\mathbb{F}_{128}$ au nombre :

$$S = b_0 \alpha^{126} + ... + b_{119} \alpha^7 + b_{120} \alpha^6 + ... + b_{125} \alpha + b_{126} = T + T = (1 + 1)T = 0$$

(qui est nul puisque $1 + 1 = 0$). Le message reçu est :

$$S' = b'_0 \alpha^{126} + ... + b'_{119} \alpha^7 + b'_{120} \alpha^6 + ... + b'_{125} \alpha + b'_{126}$$

où certains b_i sont susceptibles d'avoir été changés en b'_i à la suite d'une erreur de transmission. Les 120 premiers bits $b'_0 ... b'_{119}$ forme un message M' que l'on souhaite être égal au message initial M.

A l'arrivée, on calcule S' dans $\mathbb{F}_{128}$. Si S' = 0, on considère qu'il n'y a pas eu d'erreur de transmission et que M' = M. Sinon, on suppose que les erreurs de transmission sont suffisamment rares pour qu'une seule erreur se soit produite, par exemple au bit k. On a donc :

$b'_i = b_i$ pour $i \neq k$

$b'_k = b_k + 1$

De sorte que $S' = S + \alpha^{126-k} = \alpha^{126-k}$ puisque S = 0. Or connaissant la valeur de S' (il y a 127 valeurs possibles non nulles dans $\mathbb{F}_{128}$), il suffit de déterminer parmi les 127 puissances possibles distinctes de α celle qui est égale à la valeur de S'. Une et une seule puissance de α convient. L'indice k correspondant permet de corriger l'erreur de transmission.

La démarche suivie par le Minitel avec $\mathbb{F}_{128}$ peut s'appliquer avec n'importe quel corps du même type. Si le corps possède 2^n éléments, on envoie des messages M constitués de $2^n - n - 1$ bits. Ceux–ci sont complétés par n bits. Le choix de 2^{128} est astucieux, car il permet de coder 15 octets par un octet supplémentaire.

Voici des exemples plus élémentaires et abordables manuellement :

❑ Dans $\mathbb{F}_4$, avec $\alpha^2 = \alpha + 1$.

On souhaite transmettre le message $M = a_0$. Or $a_0 \alpha^2 = a_0(\alpha + 1)$. D'où :

$S = a_0\alpha^2 + a_0\alpha + a_0 = 0$

On envoie donc le message $a_0a_0a_0$. αinsi :

0 est codé 000

1 est codé 111

S'il y a une erreur, elle est facile à corriger. Ce code est peu performant, il multiplie les messages par 3.

❑ Dans $\mathbb{F}_8$ avec $\alpha^3 = \alpha + 1$

On souhaite transmettre le message $M = a_0a_1a_2a_3$. Il correspond au polynôme :

$a_0\alpha^6 + a_1\alpha^5 + a_2\alpha^4 + a_3\alpha^3 = \alpha^2(a_0+a_1+a_2) + \alpha(a_1+a_2+a_3) + (a_0+a_1+a_3)$

On envoie donc le message : $a_0a_1a_2a_3[a_0+a_1+a_2][a_1+a_2+a_3][a_0+a_1+a_3]$

Par exemple, on veut envoyer 0110. On envoie effectivement 0110001.

On reçoit $0111001 = \alpha^5 + \alpha^4 + \alpha^3 + 1 = \alpha^3$ $\Rightarrow$ erreur sur a_3

On reçoit $0110101 = \alpha^5 + \alpha^4 + \alpha^2 + 1 = \alpha^2$ $\Rightarrow$ erreur sur a_4

On reçoit $0100011 = \alpha^5 + \alpha + 1 = \alpha^2$ $\Rightarrow$ erreur sur a_4 (Il y a en fait deux erreurs)

On reçoit $0010001 = \alpha^4 + 1 = \alpha^2 + \alpha + 1 = \alpha^5$ $\Rightarrow$ erreur sur a_1.

Dans le cas de $\mathbb{F}_8$ qui n'est pas très gros, on peut comprendre à la main pourquoi la recherche d'une erreur sera possible. Notons :

$A = a_0$, $B = a_1$, $C = a_2$, $D = a_3$, $E = a_0 + a_1 + a_2$, $F = a_1 + a_2 + a_3$, $G = a_0 + a_1 + a_3$

Le message est constitué de ABCD, le code correcteur de EFG. On voit que celui-ci a été construit de façon que :

(i) $A + B + C + E = 0$

(ii) $B + C + D + F = 0$

(iii) $A + B + D + G = 0$

Si ces trois égalités sont en défaut, cela signifie qu'une erreur porte sur B

Si les égalités (i) et (ii) sont en défaut, l'erreur porte sur C
Si les égalités (i) et (iii) sont en défaut, l'erreur porte sur A
Si les égalités (ii) et (iii) sont en défaut, l'erreur porte sur D
Si l'égalité (i) seule est en défaut, l'erreur porte sur E
Si l'égalité (ii) seule est en défaut, l'erreur porte sur F
Si l'égalité (iii) seule est en défaut, l'erreur porte sur G

Plus généralement, l'utilisation de k bits de corrections conduit à la mise au point de k telles égalités. Si les k égalités sont vérifiées, le message est considéré comme correct. Si une combinaison de p lignes est en défaut, pour $1 \leq p \leq k$, cela permettra de corriger un bit du message. Le nombre de bits pouvant être utilisés est donc $\sum_{p=1}^{k} \binom{k}{p} = 2^k - 1$. Sur ces $2^k - 1$ bits, k serviront de bits correcteurs, les $2^k - k - 1$ autres servant à transmettre le message. On peut ajouter 1 bit de parité à la fin afin d'obtenir un mot de longueur 2^k. Cela permet de détecter la présence de deux erreurs (mais sans qu'on puisse les corriger). Ci-dessous, on indique, pour diverses valeurs de k, le nombre de bits signifiants du message ($2^k - k - 1$), le nombre de bits correcteurs (k), le nombre de bits d'un mot ($2^k - 1$). Le minitel utilisait $k = 7$. Bien entendu, comme $k << 2^k$, plus k est grand, plus le rapport $\frac{\text{Nombre de bits correcteurs}}{\text{Longueur du message}}$ est faible. On peut alors être tenté de prendre k arbitrairement grand, mais on n'oubliera pas que la méthode précédente suppose qu'il y a au plus une erreur par mot, et que le mot ne doit pas être trop grand pour que cette propriété soit vérifiée. La valeur de k sera donc choisie en fonction de la qualité du canal de transmission.

Nombre de bits correcteurs k	Nombre de bits signifiants $2^k - k - 1$	Longueur du mot 2^k
2	1	3
3	4	7
4	11	15
5	26	31
6	57	63
7	120	127

Ci-dessous, une méthode encore plus performante : la correction d'erreurs dans les disques compacts.

Annexe III : Utilisation d'un corps fini dans les disques compacts

Les octets sont l'unité de mémoire. Il s'agit d'une suite de huit chiffres binaires (ou bits) 0 ou 1. Il y a donc 256 octets différents qu'on peut représenter par les nombres 0 à 255 ou par les éléments de $\mathbb{F}_{256}$, corps fini à 256 éléments. La construction de tels corps finis est expliquée dans l'annexe précédente. En ce qui concerne $\mathbb{F}_{256}$, on introduit un symbole α vérifiant :

$$\alpha^8 + \alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1 = 0$$

et on calcule modulo 2. Les éléments de $\mathbb{F}_{256}$ sont de la forme $a_0 + a_1\alpha + ... + a_7\alpha^7$, avec a_i valant 0 ou 1. Il y a bien $2^8 = 256$ éléments possibles. On peut également vérifier qu'on obtient tous les éléments de $\mathbb{F}_{256}$ sous la forme α^k, $0 \leq k \leq 254$, auxquels on adjoint le 0. On a $\alpha^{255} = 1$. On a par exemple $\alpha^{20} = \alpha^7 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$.

Considérons un mot M constitué de r octets, où r est inférieur ou égal à 251. En adjoignant 4 octets

formant un code C, on obtient un mot MC de $r + 4$ octets. C est défini de façon que, si, lors de la transmission ou de la lecture de MC, on commet deux erreurs, on est capable de les localiser et de les rectifier. Si quatre octets de MC sont illisibles, on sait également les reconstituer. Comment s'y prend-on ? Supposons que M soit de la forme $[a_0, a_1, ..., a_{r-1}]$, avec a_i élément de $\mathbb{F}_{256}$ (chaque a_i est un octet). On considère M comme un polynôme $a_0 + a_1X + ... + a_{r-1}X^{r-1}$. On multiplie ce polynôme par $(X + \alpha)(X + \alpha^2)(X + \alpha^3)(X + \alpha^4)$ ce qui donne un polynôme de degré $r+3$ possédant $r + 4$ coefficients. Ces coefficients forment les composantes de MC. MC peut donc être vu ou bien comme une suite de $r + 4$ octets (ou éléments de $\mathbb{F}_{256}$), ou bien comme un polynôme MC(X) de degré $r + 3$ à coefficients dans $\mathbb{F}_{256}$ possédant les racines α, α^2, α^3 et α^4.

Supposons que deux erreurs au plus se produisent dans la transmission de MC, cela signifie qu'on reçoit ou qu'on lit non le polynôme MC(X), mais $MC(X) + kX^i + lX^j$, où $0 \le i \le j \le r + 3$ et k ou l non nul. Si on calcule la valeur de ce polynôme en α, α^2, α^3 et α^4, on obtient alors le système :

$$\begin{cases} k\alpha^i + l\alpha^j = MC(\alpha) = b_1 \\ k\alpha^{2i} + l\alpha^{2j} = MC(\alpha^2) = b_2 \\ k\alpha^{3i} + l\alpha^{3j} = MC(\alpha^3) = b_3 \\ k\alpha^{4i} + l\alpha^{4j} = MC(\alpha^4) = b_4 \end{cases}$$

On vérifiera que :

$$\begin{cases} (\alpha^i + \alpha^j)b_2 + \alpha^{i+j}b_1 = b_3 \\ (\alpha^i + \alpha^j)b_3 + \alpha^{i+j}b_2 = b_4 \end{cases}$$

Il peut arriver que le déterminant de ce dernier système soit nul. Ce déterminant vaut $b_2^2 + b_1b_3$ (on rappelle qu'on calcule modulo 2) qui est égal à $kl\alpha^i\alpha^j(\alpha^{2i} + \alpha^{2j})$. Il est nul si k ou $l = 0$ ou si $\alpha^{2i} = \alpha^{2j}$, soit $\alpha^{2i-2j} = 1$ ou $2i - 2j$ multiple de 255 (car $\alpha^{255} = 1$) donc $i - j$ multiple de 255 et donc $i = j$ (compte tenu du fait que $|i - j| \le r + 3 < 255$). Dans tous les cas, cela signifie qu'il n'y a qu'une seule erreur de commise. Dans ce cas, on peut supposer par exemple que $l = 0$, on utilise alors seulement les deux premières équations $\begin{cases} k\alpha^i = b_1 \\ k\alpha^{2i} = b_2 \end{cases}$ pour en déduire que $k = \frac{b_1^2}{b_2}$ et que $\alpha^i = \frac{b_2}{b_1}$ d'où on tire i.

Si le déterminant est non nul, on déduit du système les valeurs de $S = \alpha^i + \alpha^j$ et $P = \alpha^i\alpha^j$. α^i et α^j sont racines de $X^2 + SX + P$. On en tire α^i et α^j et donc i et j. Il est facile ensuite d'avoir k et l. On est donc capable de détecter deux erreurs et de les corriger.

Supposons maintenant que quatre octets quelconques de MC soient illisibles. Ils sont localisés en i_1, i_2, i_3 et i_4. Attribuons à ces octets provisoirement la valeur 0. Il s'agit alors de déterminer k_1, k_2, k_3 et k_4 tels que

$$\begin{cases} k_1\alpha^{i_1} + k_2\alpha^{i_2} + k_3\alpha^{i_3} + k_4\alpha^{i_4} = MC(\alpha) \\ k_1\alpha^{2i_1} + k_2\alpha^{2i_2} + k_3\alpha^{2i_3} + k_4\alpha^{2i_4} = MC(\alpha^2) \\ k_1\alpha^{3i_1} + k_2\alpha^{3i_2} + k_3\alpha^{3i_3} + k_4\alpha^{3i_4} = MC(\alpha^3) \\ k_1\alpha^{4i_1} + k_2\alpha^{4i_2} + k_3\alpha^{4i_3} + k_4\alpha^{4i_4} = MC(\alpha^4) \end{cases}$$

A la différence du cas précédent, les valeurs i_1, ..., i_4 sont connues. Il suffit alors de résoudre le système pour déterminer k_1, ..., k_4. On est donc capable de remédier à quatre effacements.

Voyons maintenant comment cet outil est utilisé pour corriger les incidents de lecture de disques compacts. Les informations musicales sont codées par paquets de 24 octets. On leur adjoint 4 octets

comme précédemment pour pouvoir corriger deux erreurs ou quatre effacements. On obtient ainsi des mots de 28 octets, le $i^{ème}$ mot étant noté MC[i]. Le $k^{ème}$ octet de ce mot ($1 \le k \le 28$) sera noté MC[i,k]. Ces mots sont entrelacés de la façon suivante. Nous notons les octets ligne par ligne. Chaque ligne est constituée de 28 octets. La $i^{ème}$ ligne contient les octets suivants :

MC[i,1] MC[i – 4,2] MC[i – 8,3] ... MC[i – 108,28]

On peut encore exprimer cela en disant que le mot MC[i] est reconstitué en considérant les octets suivants (où L[i,k] désigne le $k^{ème}$ octet de la ligne i) :

L[i,1] L[i + 4,2] L[i + 8,3] ... L[i + 108,28]

Chaque ligne de 28 octets se trouve renforcée par 4 octets permettant là aussi de corriger deux erreurs ou quatre effacements, donnant en fait des lignes de 32 octets.

Supposons que seize lignes successives soient complètement effacées (ce qui représente $16 \times 32 = 512$ octets successifs effacés). Les mots MC[i] ne faisant intervenir les lignes que tous les quatre rangs, la reconstitution de MC[i] ne laissera que quatre octets effacés. On est capable alors de reconstituer chaque mot MC. Ainsi, on est capable de réparer l'effacement de 512 octets successifs. La densité d'information sur un CD étant de l'ordre de 2 ko par cm de piste, on peut donc se permettre des rayures transversales de 2 mm de large.

Annexe IV : Cryptographie

Vous souhaitez vous faire adresser un message confidentiel. Un seul moyen, faire coder le message. Il est apparu depuis quelques années des codages dits à clef révélée. De quoi s'agit–il ?

Une personne I veut recevoir un message confidentiel M d'une personne J. La personne I rend public (dans un annuaire spécialisé, par exemple) un procédé de codage C_i. Ce procédé est donc connu de tous. La personne I est la seule à posséder le procédé de décodage D_i. La personne J, expéditrice du message M, envoie le message C_i(M). La personne I, destinataire du message n'a plus qu'à appliquer son décodage : $D_i[C_i(M)] = M$. Autrement dit, $D_i \circ C_i = Id$.

Le point fondamental est le suivant : comment est–il possible que le procédé de décodage D_i reste secret, et uniquement connu de la personne I, alors que le procédé de codage C_i est public ? Cela est possible car la connaissance d'une fonction f bijective ne suffit pas toujours pour calculer simplement sa réciproque. Une telle fonction est appelée fonction trappe. On en connaît plusieurs. Il n'est pas exclu que des fonctions trappes aujourd'hui cessent de le devenir demain, la difficulté de calculer f^{-1} étant essentiellement due à notre ignorance. Mais il n'est pas exclu non plus que l'on puisse prouver qu'une fonction est par nature une fonction trappe, le calcul de f^{-1} étant alors intrinsèquement difficile. Une fonction trappe actuelle est le calcul du logarithme discret. Etant donné trois nombres a, b et p, on sait facilement calculer a^b mod p (le temps de calcul est de l'ordre de ln(b), cf ALGRTHME.PDF). Mais connaissant a, a^b et p, on ne connaît pas de méthode rapide de calculer b. Lorsque les nombres en question possèdent plusieurs dizaines de chiffres, la méthode consistant à essayer toutes les valeurs possibles de b prend trop de temps (il est de l'ordre de b). Il existe cependant des algorithmes efficaces si p–1 possède de petits facteurs premiers. Le choix de p pour définir une bonne fonction trappe est donc crucial.

❑ Le premier exemple est le système de ElGamal. La personne I souhaitant recevoir des messages choisit un nombre premier q et choisit secrètement un nombre a. Tous les nombres sont calculés modulo q. Il publie g élément de {0, ..., q–1}, q et g^a mod q. Pour envoyer un message M à I, on choisit un entier k au hasard et on envoie le couple (g^k, Mg^{ak}). Connaissant a, I peut calculer facilement g^{ak} et donc déduire la valeur de M. Par contre, on ne connait pas actuellement de moyen efficace de calculer a connaissant g^k et g^a modulo q.

❑ Voici un autre exemple classique de cryptographie, le système RSA (Rivest–Shamir–Adleman) :
La personne I choisit en secret deux nombres premiers p et q, ainsi qu'un nombre d, premier avec $(p-1)(q-1)$. Il rend public $n = pq$, et m tel que md soit de la forme $1 + k(p-1)(q-1)$.

Procédé de codage C_i :

Découper le message en groupe de lettres et remplacer chaque lettre par un nombre (par exemple, son rang dans l'alphabet), de façon que le message à transmettre soit une suite de nombres M inférieurs à n. Transmettre les nombres $M' = M^m \bmod n$.

Procédé de décodage D_i : Calculer $M'^d \bmod n$. On peut montrer que le résultat est M. (C'est une variante un peu plus sophistiquée du petit théorème de Fermat).

Voyons pourquoi il est si difficile de déchiffrer D_i. On travaille avec des nombres p et q d'une cinquantaine de chiffres. On sait déterminer sur ordinateur en quelques minutes si un nombre est premier ou pas. Le choix de p et q ne pose donc pas de problèmes. On sait également déterminer en quelques minutes le PGCD de deux nombres. Il en découle un choix facile de d. Les coefficients du théorème de Bézout se calcule aussi rapidement, d'où la découverte rapide de m.

Par contre, le produit n étant donné, on ne connaît pas d'algorithme rapide de factorisation de n. Si n compte une centaine de chiffres, on estime que le temps nécessaire à la découverte de p et q est actuellement de l'ordre de plusieurs milliard d'années. La connaissance de C_i, et donc de n ne suffit pas, et de loin, pour déterminer p et q, et donc D_i.

Cette méthode permet également d'identifier de façon certaine l'auteur d'un message. Il suffit que l'expéditeur J envoie le message $C_i[D_j(M)]$, qu'il est seul à pouvoir envoyer, puisqu'il est seul à connaître son propre procédé de décodage D_j. Le récepteur I applique alors sur le message reçu $C_j \circ D_i$. En effet, il est facile de voir que les procédés de codage C et de décodage D commutent, et que l'on a donc :

$$C_j \circ D_i \circ C_i \circ D_j(M) = C_j \circ D_j(M) = D_j \circ C_j(M) = M.$$

Prenons des exemples avec des petits nombres :

$p = 5$
$q = 7$
$n = 35$
$d = 17$
$m = 5$

$n = 35$ et $m = 5$ sont rendus publics. On veut envoyer le message M = 23.
On expédie $M' \equiv M^5 \bmod 35 = 18$
On décode $M'^{17} \bmod 35$. On retrouve bien M = 23.

On peut prendre également :

$p = 11$
$q = 7$
$n = 77$
$d = 13$
$m = 37$

$n = 77$ et $m = 37$ sont rendus publics. On veut envoyer le message M = 18.
On expédie $M' \equiv M^{37} \bmod 77 = 39$

On décode M'^{13} mod 77. On retrouve bien M = 18.
En ce qui concerne le calcul de puissance modulo un entier, il est maladroit de calculer la puissance d'abord avant de faire la réduction modulo l'entier. Les deux doivent se faire conjointement.

Ces méthodes de cryptage sont tellement efficaces que les gouvernements ont promulgués des lois visant à limiter la taille des nombres *p* et *q*.

Voici également quelques problèmes de transmission confidentielles :

❑ Deux personnes A et B, éloignées l'une de l'autre, veulent convenir d'un nombre commun, qui pourra par exemple leur servir ultérieurement pour s'envoyer des messages codés. Ils peuvent se téléphoner ou s'écrire, mais rien ne garantit la confidentialité de leurs échanges. Comment faire ? Là aussi, on utilise des fonctions trappes au moyen du protocole de Diffie et Hellman. Diffie et Hellman ont en effet présumé qu'il était infaisable, avec les connaissances actuelles, de calculer un nombre de la forme g^{ab} mod *q*, connaissant g^a mod *q* et g^b mod *q*, lorsque *g*, *a* et *b* sont grands. Ceci est une variante du problème du logarithme discret.

Il suffit donc à A et à B de se communiquer (éventuellement publiquement) les nombres *g* et *q*. A choisit secrètement un nombre *a* et envoie à B le nombre g^a. De même, B choisit secrètement un nombre *b* et envoie à A le nombre g^b. A et B peuvent alors tous deux calculer facilement g^{ab}, mais personne d'autre ne le peut.

❑ Dans un pays fictif, les postiers sont particulièrement malhonnêtes et pillent les colis qui leur sont confiés. Les usagers disposent de colis rigides susceptibles d'être munis de cadenas. Seuls ces derniers colis arrivent intacts à leur destinataire. Comment l'usager A peut–il transmettre à l'usager B un objet précieux, sans déplacement de l'un ou de l'autre ? Il va de soi que, si A place un cadenas sur son colis, B ne dispose pas de la clef du cadenas !

Voici la réponse. A place son cadenas sur le colis et l'envoie à B. B pose lui aussi son cadenas sur le colis et le renvoie à A. A enlève son cadenas et renvoie le colis à B. Il suffit alors à B de retirer son cadenas. Ce procédé est utilisé en cryptographie dans le système de Massey-Omura. Le colis est un message à transmettre, le cadenas représente un procédé de codage confidentiel propre à chaque personne. A et B conviennent de travailler modulo *q*, *q* étant un nombre premier (éventuellement public). A veut envoyer confidentiellement un message à B, représenté par un nombre P non nul ; il choisit un nombre *a* premier avec $q - 1$ et envoie P^a mod *q*. L'algorithme d'Euclide lui permet de trouver *a*' tel que $aa' \equiv 1 \bmod q - 1$. B choisit de même un nombre *b* et son inverse *b*' modulo *q*, et renvoie $(P^a)^b = P^{ab}$ mod *q*. A calcule alors $(P^{ab})^{a'} \equiv P^b$ mod *q* en vertu du théorème de Fermat ($P^{q-1} \equiv 1 \bmod q$) et le renvoie à B. B calcule alors $(P^b)^{b'} \equiv P \bmod q$. Il faut cependant également prévoir un système d'authentification de signatures pour éviter que quelqu'un se fasse passer pour A auprès de B. Ce système d'authentification est décrit ci–dessous.

❑ Le système d'authentification de signature DSS (Digital Signature Standard).
Alice veut envoyer à Bob un message, accompagnée d'une procédure de certification de sa signature. Elle procède comme suit :
i) Choisir un nombre premier *q* d'une cinquantaine de chiffres. Il suffit de disposer d'un générateur de nombre aléatoire (*random*) et d'un test de nombres premiers (*isprime* et *nextprime* en MAPLE).
ii) Choisir un nombre premier *p* d'environ 140 chiffres tel que $p \equiv 1 \bmod q$. (On teste la primalité de nombres de la forme $1 + rq$, en faisant varier *r*).
iii) Choisir un nombre *g* pour lequel *q* est la plus petite puissance vérifiant $g^q \equiv 1 \bmod p$.

iv) Choisir un entier x aléatoire entre 0 et q, et calculer $y = g^x \bmod q$. x est gardé secret, mais g, y, p et q sont publics par Alice.

Pour signer un message H, nombre entier entre 0 et $q - 1$, Alice calcule ce qui suit :
v) Elle choisit un entier K entre 0 et $q - 1$, et calcule $R_1 = g^K \bmod p$, puis $R_2 = R_1 \bmod q$.
vi) Elle calcule enfin s tel que $sK \equiv H + xR_2 \bmod q$.
La signature est donnée par (R_2, s).

Pour vérifier la signature, Bob opère ainsi.
a) Il calcule $X_1 = s^{-1}H \bmod q$
b) Il calcule $u_2 = s^{-1}R_2 \bmod q$
c) Il calcule $g^{X_1} y^{u_2} \bmod p$ (qui n'est autre que $g^{(H+xR_2)/s \bmod q} = g^{K \bmod q} = g^K \bmod p = R_1$ compte tenu du fait que $g^q \equiv 1 \bmod p$)
d) Il calcule $R_1 \bmod q$ et il doit retrouver R_2.

Cette procédure est basée sur la difficulté de calculer x connaissant $y = g^x \bmod p$. Seule la personne connaissant x est supposée capable de créer la paire (R_2, s).

❑ Abel veut convaincre Caïn qu'il a réussi à résoudre une équation du type logarithme discret, autrement dit, étant donné y, il a découvert x tel que $b^x = y$. Cependant, Abel ne veut pas dévoiler à Caïn la valeur de x. Voilà comment procéder.
i) Abel choisit un nombre e quelconque et envoie à Caïn le nombre $b' = b^e$.
ii) Caïn tire alors à pile ou face
- Si la pièce tombe sur pile, il demande à Abel la valeur de e et vérifie que b' est bien égal à b^e.
- Si la pièce tombe sur face, il demande à Abel la valeur de $e + x$, et Caïn vérifie que $yb' = b^{x+e}$.

iii) Recommencer au i) jusqu'à ce que Caïn soit convaincu qu'Abel connaît bien la valeur de x. Si Abel ignore cette valeur, il ne peut répondre qu'à un seul des deux tirages, mais il ne peut prévoir lequel. Par ailleurs, Caïn ne peut déterminer ce que vaut x, puisqu'il ignore la valeur de e dans le cas d'un tirage sur face.

❑ Indiquons enfin un problème curieux. Caïn peut envoyer à Abel deux messages codés. Abel peut en décoder alors un et un seul, mais Caïn ne peut savoir lequel. On utilise là aussi la supposition de Diffie–Hellmann. On travaille modulo un nombre premier q et on suppose donné un nombre C dont ni Caïn ni Abel ne connaisse le logarithme en base b. Voici comment procéder :

i) Abel choisit un nombre x au hasard et envoie à Caïn l'un des deux couples $(b_1, b_2) = (b^x, \frac{C}{b^x})$ ou $(b_1, b_2) = (\frac{C}{b^x}, b^x)$. Caïn ignore lesquel de ces deux couples il reçoit.

ii) Caïn choisit deux entiers y_1 et y_2. Si les deux messages sont m_1 et m_2 codés en binaires, Caïn envoie les nombres b^{y_1}, b^{y_2}, m_1 xor $b_1^{y_1}$, m_2 xor $b_2^{y_2}$, les deux premiers étant donnés modulo q, les deux derniers codés en binaires. L'opérateur xor est le *ou exclusif* qui agit sur les chiffres binaires correspondant des deux nombres de la façon suivante : 0 xor 1 = 1 xor 0 = 1, 0 xor 0 = 1 xor 1 = 0.
iii) Abel peut calculer $(b^x)^{y_i} = (b^{y_i})^x$ car il connaît x, et il sait si $b^x = b_1$ ou b_2 donc il peut calculer $b_1^{y_1}$ ou $b_2^{y_2}$. Il pourra donc décoder le message m_i correspondant. Mais il ne peut pas décoder l'autre, car il aurait besoin de calculer $(\frac{C}{b^x})^{y_i}$, et pour cela il a besoin de connaître C exprimé comme puissance de b.

Précisons que la plupart des tests qui précèdent peuvent être appliqués dans des groupes, par exemple le groupe des courbes elliptiques sur des corps finis.

Annexe V : La recherche des grands nombres premiers, le test de Lucas

Nous avons vu que les plus grands nombres premiers connus sont de la forme $2^q - 1$. Ces nombres sont appelés les nombres de Mersenne. D'une part, leur forme est adaptée au calcul sur ordinateur, d'autre part, on dispose du test de Lucas qui permet de déterminer s'ils sont premiers ou non.

On remarque d'abord qu'il faut que q soit premier. En effet, si $q = q_1q_2$, avec $1 < q_1 < q$ et $1 < q_2 < q$, alors $2^q - 1$ est divisible par $2^{q_1} - 1$ et par $2^{q_2} - 1$. En effet, si on calcule modulo $2^{q_1} - 1$, on a :

$$2^{q_1} \equiv 1 \bmod 2^{q_1} - 1$$
$$\Rightarrow \quad 2^{q_1q_2} \equiv 1^{q_2} = 1 \bmod 2^{q_1} - 1$$
$$\Rightarrow \quad 2^q - 1 \equiv 0 \bmod 2^{q_1} - 1$$

De même avec $2^{q_2} - 1$.
Cette condition n'est pas suffisante. 11 est premier, mais $2^{11} - 1 = 2047 = 23 \times 89$.

Dans la suite, on suppose q premier supérieur ou égal à 3. On pose $p = 2^q - 1$. On va établir un test permettant de savoir si p est premier ou non. On définit la suite $(L_n)_{n\in \mathbf{N}}$ par :

$$L_0 = 4 \text{ et } L_{n+1} = L_n^{\,2} - 2$$

Le test de Lucas énonce que p est premier si et seulement si L_{q-2} est divisible par p. Pour cela, on effectue les calculs modulo p en utilisant la relation de récurrence.

EXEMPLE :
❑ Pour $q = 7$, les valeurs successives de la suite sont 4, 14, 67, 42, 111, 0. Donc $2^7 - 1$ est premier.
❑ Pour $q = 11$, les valeurs successives de la suite sont 4, 14, 194, 788, 701, 119, 1877, 240, 282, 1736 et $2^{11} - 1$ n'est pas premier.

Nous nous contenterons de montrer que la condition énoncée par Lucas est nécessaire. On suppose donc p et q premiers. Montrons que le test est valide. On a une expression explicite de L_n, à savoir : $\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^{2^{n+1}} + \left(\frac{\sqrt{2}-\sqrt{6}}{2}\right)^{2^{n+1}}$, comme on pourra le vérifier par récurrence. C'est cette expression que nous utiliserons pour L_{q-1}.

Notons que le petit théorème de Fermat énonce que $2^{q-1} \equiv 1\ [q]$, autrement dit, il existe m tel que $2^{q-1} - 1 = qm$. On a également $2^q = p + 1 \equiv 1\ [p]$. Il en résulte que :

$$2^{(p-1)/2} = 2^{2^{q-1}-1} = 2^{qm} \equiv 1^m\ [p] \equiv 1\ [p]$$

Admettons par ailleurs provisoirement que $3^{(p-1)/2} \equiv -1\ [p]$ et considérons L_{q-1} :

$$L_{q-1} = \left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^{2^q} + \left(\frac{\sqrt{2}-\sqrt{6}}{2}\right)^{2^q} = \left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^{p+1} + \left(\frac{\sqrt{2}-\sqrt{6}}{2}\right)^{p+1}$$

Développons cette expression. On obtient :

$$L_{q-1} = \frac{1}{2^{p+1}} \sum_{k=0}^{p+1} \binom{p+1}{k} \sqrt{2}^{\,p+1-k} \sqrt{6}^{k} + \frac{1}{2^{p+1}} \sum_{k=0}^{p+1} \binom{p+1}{k} \sqrt{2}^{\,p+1-k} \sqrt{6}^{k} (-1)^k$$

$$= \frac{1}{2^p} \sum_{k \text{ pair}} \binom{p+1}{k} \sqrt{2}^{\,p+1-k} \sqrt{6}^{k}$$

$$= \frac{1}{2^p} \sum_{m=0}^{(p+1)/2} \binom{p+1}{2m} 2^{(p+1)/2-m}\, 6^m \qquad \text{en posant } k = 2m$$

$$= \frac{1}{2^{(p-1)/2}} \sum_{m=0}^{(p+1)/2} \binom{p+1}{2m} 3^m$$

$$\Rightarrow \qquad 2^{(p-1)/2}\, L_{q-1} = \sum_{m=0}^{(p+1)/2} \binom{p+1}{2m} 3^m$$

Or on montrera que, pour $2 \le k \le p-1$, on a $\binom{p+1}{k} \equiv 0\ [p]$.(Utiliser le fait que p est premier et apparaît au numérateur du coefficient binomial).

$\Rightarrow \qquad 2^{(p-1)/2}\, L_{q-1} \equiv 1 + 3^{(p+1)/2}\ [p]$

$\equiv 1 - 3\ [p]$ puisque nous avons admis que $3^{(p-1)/2} \equiv -1\ [p]$

$\equiv -2\ [p]$

$\Rightarrow \qquad L_{q-1} \equiv -2\ [p]$ puisqu'au début de cette étude, nous avons vu que $2^{(p-1)/2} \equiv 1\ [p]$.

Or $L_{q-1} = {L_{q-2}}^2 - 2$, donc ${L_{q-2}}^2 = L_{q-1} + 2 \equiv 0\ [p]$ donc $L_{q-2} \equiv 0\ [p]$ (utiliser le fait que p est premier). Nous avons donc montré que le test de Lucas est vérifié.

Pour cela, nous avons admis que $3^{(p-1)/2} \equiv -1\ [p]$. Montrons cette propriété. Remarquons que $p - 1$ est divisible par 3. En effet :

$p - 1 = 2^q - 2 \equiv (-1)^q - 2\ [3] \equiv (-1)^q + 1\ [3]$ or q est impair car premier supérieur à 3 donc

$p - 1 \equiv 0\ [3]$

Nous pouvons donc considérer le polynôme $X^{(p-1)/3} - 1$. Lorsqu'on effectue les calculs sur les entiers modulo p, avec p premier, on obtient un corps dont les éléments (modulo p) sont $\{0,1,..., p-1\}$. Ce corps est noté $\mathbb{Z}/p\mathbb{Z}$ et fait l'objet d'une étude plus approfondie en deuxième année MP. Par exemple, le fait que a non nul admet un inverse résulte de l'identité de Bezout. En effet, a non nul modulo p signifie que a n'est pas divisible par p et donc que, p étant premier, a est premier avec p. Il existe donc b et m tel que $ab + pm = 1$ soit $ab \equiv 1$ modulo p. a possède donc un inverse modulo p.

Dans ce corps, le polynôme $X^{(p-1)/3} - 1$ étant de degré $\frac{p-1}{3}$ admet au plus $\frac{p-1}{3}$ racines. Il reste donc $p - 1 - \frac{p-1}{3}$ éléments a en dehors de ces racines et du 0, vérifiant :

$a \not\equiv 0\ [p]$ et $a^{(p-1)/3} \not\equiv 1 [p]$

Posons $b = a^{(p-1)/3}$. On a :

$b^3 = a^{p-1} \equiv 1\ [p]$ encore d'après le petit théorème de Fermat.

$\Rightarrow \qquad (b-1)(b^2 + b + 1) \equiv 0\ [p]$

$\Rightarrow \qquad b^2 + b + 1 \equiv 0\ [p]$ (utiliser le théorème de Gauss et le fait que p est premier et $b \not\equiv 1\ [p]$)

$\Rightarrow \qquad (2b + 1)^2 \equiv -3\ [p]$ (il suffit de développer le membre de gauche)

$\Rightarrow \quad -1 \equiv 3^{(p-1)/2}\ [p]$ (il suffit d'élever à la puissance impaire $\frac{p-1}{2}$ et d'utiliser à nouveau le petit théorème de Fermat pour conclure que $(2b+1)^{p-1} \equiv 1\ [p]$, sachant que $2b+1 \not\equiv 0\ [p]$ puisque $3 \not\equiv 0\ [p]$). CQFD

Annexe VI : Les nombres parfaits

On appelle nombre parfait tout entier positif égal à la somme de ses diviseurs positifs autre que lui-même. Par exemple, 6 est parfait car 6 = 1 + 2 + 3. Le but de cet annexe est de décrire la forme générale des nombres parfaits pairs. Pour tout entier n positif, on note $\sigma(n)$ la somme de tous ses diviseurs positifs. Ainsi, $\sigma(6)$ est égal à 12. Un nombre n est donc parfait si et seulement si $\sigma(n) = 2n$.

On peut vérifier que 28, 496 et 8128 sont d'autres nombres parfaits, et que 6, 28, 496 et 8128 peuvent tous s'écrire sous la forme $2^n(2^{n+1} - 1)$, avec $2^{n+1} - 1$ premier. A titre de curiosité, nous indiquons que le cinquième nombre parfait (découvert en 1456) est 33 550 336, et est également de la forme précédente. Il n'est pas difficile de montrer qu'un tel nombre est parfait. Ses diviseurs sont en effet de la forme 2^k, $0 \le k \le n$, ou bien $2^k(2^{n+1} - 1)$, $0 \le k \le n$. Il n'y en a pas d'autres si $2^{n+1} - 1$ est premier. La somme de ces diviseurs vaut :

$$\begin{aligned}\sigma(2^n(2^{n+1} - 1)) &= 1 + 2 + ... + 2^n + (2^{n+1} - 1) + 2(2^{n+1} - 1) + ... + 2^n(2^{n+1} - 1)\\ &= (1 + 2 + ... + 2^n)(1 + 2^{n+1} - 1)\\ &= (2^{n+1} - 1)2^{n+1}\\ &= 2 \times 2^n(2^{n+1}-1)\end{aligned}$$

donc $2^n(2^{n+1}-1)$ est parfait. Ce résultat, ainsi que la valeur des quatre premiers nombres parfaits, est connu depuis Euclide.

Il a cependant fallu attendre Euler au XVIIIème pour voir établir la réciproque. Tous les nombres parfaits pairs sont de cette forme. Il n'y en a pas d'autres. Nous devons pour cela faire plusieurs remarques préliminaires :

(i) $\sigma(2^n) = 1 + 2 + ... + 2^n = 2^{n+1} - 1$

(ii) $\sigma(p) = p + 1$ si et seulement si p est premier

(iii) Si m et n sont deux entiers premiers entre eux, alors $\sigma(mn) = \sigma(m)\sigma(n)$. En effet, les diviseurs de mn sont de la forme uv avec u diviseur de m et v diviseur de n, de sorte que :

$$\sigma(mn) = \sum_{d|mn} d = \sum_{u|m \text{ et } v|n} uv = \sum_{u|m} u \times \sum_{v|n} v = \sigma(m)\sigma(n)$$

Considérons alors $m = 2^n k$ un nombre parfait, avec k impair. Notre but est de montrer que $k = 2^{n+1} - 1$ et que k est premier. k étant impair est premier avec 2^n de sorte que :

$$\sigma(m) = \sigma(k)\sigma(2^n) = \sigma(k)(2^{n+1} - 1)$$

Comme m est premier, $\sigma(m) = 2m$ de sorte que $\sigma(k)(2^{n+1} - 1) = 2^{n+1}k$.
2^{n+1} divise $\sigma(k)(2^{n+1} - 1)$ et est premier avec $2^{n+1} - 1$ donc divise $\sigma(k)$. Il existe donc un entier t tel que :

$$\sigma(k) = 2^{n+1}t \qquad \text{(a)}$$
$$k = t(2^{n+1} - 1) \qquad \text{(b)}$$

Supposons t strictement supérieur à 1. k admet donc comme diviseurs au moins 1, t et lui-même, de sorte que $\sigma(k)$ est au moins égal à $1 + t + t(2^{n+1} - 1) = t2^{n+1} + 1$ qui est strictement supérieur à $2^{n+1}t$ contredisant le (a).

Donc nécessairement, $t = 1$, $k = 2^{n+1} - 1$, $m = 2^n(2^{n+1}-1)$. Enfin $\sigma(k) = 2^{n+1} = k + 1$, donc k est premier. CDFD

Si l'on connaît parfaitement la forme des nombres parfaits pairs, on ignore actuellement si les nombres parfaits pairs sont en nombre fini ou non. On ignore également s'il existe des nombres parfaits impairs. On a démontré en 1976 qu'il n'existe aucun parfait impair inférieur à 10^{100}. Cette limite a été portée à 10^{160} en 1989, à 10^{300} en 1991, ..., et à 10^{15000} en 2010. S'il existe un nombre parfait impair m, on sait qu'il se décompose en facteurs premiers comme produit de p^k où les facteurs p sont au moins au nombre de 9, et où tous les exposants k sont pairs sauf un qui est congru à 1 modulo 4 (i.e. de la forme $1 + 4n$). Le nombre de facteurs, distincts ou non, est au moins égal à 75. Le plus grand facteur premier est supérieur à 10^8. L'une des puissances p^k est supérieure à 10^{20}. Si m possède n facteurs premiers distincts, m est majoré par 2^{4^n}.

Annexe VII : Curiosités

1- Problèmes de la factorisation des entiers

On ne connaît pas d'algorithme efficace pour décomposer un entier n en facteurs premiers. La recherche naïve de diviseurs est un algorithme en $O(\sqrt{n})$, qui est exponentiel en le nombre r de chiffres de n puisque n est de l'ordre de 10^r et $O(\sqrt{n}) = O(10^{r/2})$. Un tel algorithme prend plusieurs milliards d'années dès que n atteint une centaine de chiffres. Certains algorithmes très astucieux ont été développés. Citons par exemple la méthode **rho de Pollard** pour déterminer un diviseur de n : on considère une fonction f définie sur les entiers modulo n. On part de x_0, et l'on calcule les itérés $x_{j+1} = f(x_j)$, jusqu'à ce que le PGCD de $x_j - x_i$ et de n soit non trivial. Cette méthode donne en général un diviseur p de n en un temps $O(\sqrt{p})$ (et non $O(\sqrt{n})$. Au pire, pour un nombre non premier, l'algorithme est en $O(\sqrt[4]{n})$. On connaît des algorithmes en $O(\exp(C\sqrt{r \ln r}))$ pour un nombre n de r chiffres.

A titre d'exemple, on sait que le nombre suivant (RSA-210) est facteur de deux nombres premiers, mais on ignore lesquels :

24524664490027821197651766357308801846702678767833275974341445171506160083003858721695220839933207154910362682719167986407977672324300560059203563124656121846581790410013185929961993381701214933503487587055106 7

En 2009, on a réussi à factoriser RSA-768 :

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 9

à savoir :

33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489 × 367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089177

(cf **http://en.wikipedia.org/wiki/RSA_Factoring_Challenge** pour plus de précisions)

Dans les années 1980, on estimait qu'il fallait des milliards d'années pour factoriser un tel nombre. Mais les ordinateurs, et surtout les algorithmes ont largement progressé. Pendant combien de temps les systèmes de protection actuels par cryptographie utilisant de grands nombres premiers resteront-ils hors d'atteinte ?

Par contre vérifier qu'inversement le produit des deux entiers ci-dessus redonne bien le nombre initial ne demande qu'une fraction de seconde avec un logiciel tel que Python. Ainsi, prouver qu'un nombre n est composé (i.e. non premier) ne demande qu'une multiplication. Il suffit de donner deux nombres d_1 et d_2 supérieurs à 1 tels que $d_1 d_2 = n$. Mais on ne dispose d'aucune procédure efficace pour trouver deux tels nombres. On se trouve donc devant la siuation suivante :

Si on se donne un entier n de plusieurs dizaines de chiffres, on est incapable en général d'en donner un diviseur en un temps raisonnable. On ne connaît pas d'algorithme qui donnerait un tel diviseur en un temps qui serait une fonction polynomiale du nombre de chiffres de n. On ignore si un tel algorithme existe.

Si on se donne n ainsi qu'un nombre d, il suffit d'une fraction de seconde pour tester si d divise n. On peut montrer que le temps de calcul de la division est une fonction polynomiale du nombre de chiffre de n.

On dit que le problème de la factorisation de n est un problème algorithmique de type NP (pour non déterministe polynomial), ce qui signifie qu'un tirage au hasard chanceux du nombre d permettrait de tester que n est composé en un temps polynomial (i.e. qui soit une fonction polynomiale du nombre de chiffre de n). Mais il n'existe aucune procédure efficace de déterminer un tel d et l'on ignore si ce problème algorithmique est de type P (pour déterministe polynomial), ce qui signifie qu'on ne connaît pas à ce jour d'algorithme en temps polynomial permettant de déterminer un tel d. La question de savoir si les problèmes de type NP sont en fait de type P est un problème central de l'algorithmique et la réponse à cette question est dotée d'une récompense d'un million de dollars par la fondation Clay (**http://www.claymath.org/millennium/Rules_etc/**).

Un dernier exemple : le nombre de Fermat $2^{2^8} + 1$ n'est pas premier puisqu'on pourra vérifier en une fraction de seconde que :

$$2^{2^8} + 1 = 1238926361552897 \times$$
$$93461639715357977769163558199606896584051237541638188580280321$$

Cependant, la décomposition précédente n'a été trouvée qu'un 1981.

Voici un aperçu de l'évolution de nos capacités de calcul :

- En 1874, on pensait impossible de factoriser les nombres d'une dizaine de chiffres, par exemple 8 616 460 799. Ce n'est qu'en 1925 qu'on le factorisa (96079×89681). Cette factorisation est aujourd'hui instantanée sur un modeste ordinateur de bureau.
- Dans les années 1960, la factorisation des nombres de 25 chiffres semblait hors de portée. On factorisa en 1970 un nombre de 39 chiffres.
- A la fin des années 1970, on s'attaque à des nombres de 80 chiffres. Le cap des 100 chiffres est atteint en 1990. Le défi RSA-129, lancé en 1977 consistait à factoriser un nombre de 129 chiffres. Le temps de calcul était alors évalué à quelques millions d'années. Les progrès algorithmique permirent d'atteindre le but en 1994. Nous avons vu ci-dessus que le défi RSA-768 a été remporté en 2009.
- On sait que le nombre de Fermat $F_{20} = 2^{2^{20}} + 1$ est composé, mais on ne connaît aucun de ses facteurs. Il est possible qu'on n'en connaîtra jamais aucun.

Le lecteur intéressé pourra se reporter au livre de Jean-Paul Delahaye, *Merveilleux nombres premiers*, Belin (2000).

2- Un test probabiliste de primalité

Bien que ne sachant que difficilement factoriser un nombre d'une centaine de chiffres, on possède des algorithmes permettant de déterminer la primalité de nombres d'un millier de chiffres. Bien entendu, ces tests de primalité n'utilise pas la recherche de diviseurs, mais d'autres moyens plus détournés. Il existe également des tests probabilistes permettant de tester de manière quasi-certaine la primalité des nombres de quelques dizaines de milliers de chiffres. La plupart utilise le petit théorème de Fermat. Malheureusement, le théorème de Fermat ne permet pas de tester si n est premier, car certains nombres n vérifient la conclusion du théorème de Fermat sans être premier. Il s'agit des nombres de Carmichael dont le plus petit est 561. On a donc affiné le théorème de Fermat de façon à obtenir une condition nécessaire et suffisante sur la primalité de n et pas seulement une condition nécessaire. En voici un exemple :

Le test de Miller–Rabin :
Soit n un nombre impair. Posons $n–1 = 2^s t$, avec t impair. Soit b premier avec n. On dit que b et n passent le test si $b^t \equiv 1 \bmod n$ ou si il existe r, $0 \leq r < s$ tel que $b^{t.2^r} \equiv -1 \bmod n$. (Le théorème de Fermat énonce seulement que $b^{n-1} = b^{t.2^s} \equiv 1 \bmod n$)

On prouve que, si n est premier, le test réussit pour tout b premier avec n, mais si n n'est pas premier, le test échoue pour au moins $\frac{3}{4}$ des nombres b. On choisit donc k nombres b au hasard. Si l'un des tests échoue, on est certain que n est composé. Si le test réussit, alors n est premier avec une probabilité d'erreur inférieure à $\frac{1}{4^k}$, soit $\frac{1}{10^{18}}$ si $k = 30$. La probabilité d'erreur est en fait certainement encore plus faible. Pour $b = 2$, 3, 5 ou 7 seulement, le seul nombre composé n inférieur à 10^{11} qui passe le test est 3215031751. En outre, il a été prouvé que le test précédent serait déterministe (et non plus probabiliste) en un temps de calcul $O(\ln^2 n)$, à condition que la conjecture dite de Riemann soit vérifiée.

La fonction *isprime* du logiciel MAPLE est un test probabiliste comparable à celui qui vient d'être exposé. Une réponse *false* assure que le nombre proposé n'est pas premier, mais l'aide de MAPLE précise qu'une réponse *true* assure seulement que "*n is very probably prime [...]. No counter example is known and it has been conjectured that such a counter example must be hundreds of digits long*".

3- Les certificats de primalité

Un certificat de primalité est une donnée permettant d'assurer qu'un entier n est premier en temps de calcul polynomial en le nombre de chiffres de n. Ce certificat est la donnée d'une liste (a, q_1, a_1, q_2, a_2, ..., q_k, a_k) telle que les trois conditions suivantes soient vérifiées :

$$\begin{cases} n - 1 = q_1^{a_1} q_2^{a_2} \dots q_k^{a_k}, \text{ les } q_k \text{ étant premiers} \\ a^{n-1} \equiv 1 \bmod n \\ \forall\, i \in \{1, \dots, k\},\ a^{(n-1)/q_i} \neq 1 \bmod n \end{cases}$$

Pratt a montré en 1975 que ces conditions sont équivalentes à dire que n est premier. (Les q_k peuvent également être accompagné de leur certificat s'il n'apparaît pas de façon évidente qu'ils sont premiers).

Ainsi, le nombre 2801196269419097900390625 1 est premier de façon certaine, son certificat étant (2, 2, 1, 3, 24, 5, 18, 13, 1). En effet :

$$2801196269419097900390625 1 - 1 = 2 \times 3^{24} \times 5^{18} \times 13$$

$2^{n-1} \equiv 1 \bmod n$
$2^{(n-1)/2} \equiv 280119626941909790039062 50 \bmod n \neq 1$
$2^{(n-1)/3} \equiv 114091892404576104880784 53 \bmod n \neq 1$
$2^{(n-1)/5} \equiv 191498652216316279684816 81 \bmod n \neq 1$
$2^{(n-1)/13} \equiv 190331129945142881395380 07 \bmod n \neq 1$

Mais tout le problème est de trouver la bonne liste. *n* étant donné, on tombe en effet sur le problème de décomposer $n - 1$ en facteurs premiers, problème dont nous avons souligné la difficulté plus haut.

Un pas théorique extrêmement important a été franchi en août 2002 par trois mathématiciens Indiens, Agrawal, Kayal et Saxena qui ont mis au point un test de primalité déterministe dont le temps de calcul est polynomial en le nombre de chiffres de *n*. Cette découverte a fait le tour de la planète en peu de temps. Ce test est encore trop lent pour pouvoir être mis efficacement en pratique par rapport aux tests probabilistes, mais on peut espérer que des tests déterministes rapides seront bientôt mis au point.

4- Le polynôme de Jones

En 1976, Jones a explicité un polynôme des 26 variables entières positives ou nulles *a*, *b*, ..., *z*, dont l'ensemble des valeurs positives coïncide avec l'ensemble des nombres premiers. Le voici :

$(k+2)[1 - (wz+h+j-q)^2 - [(gk+2g+k+1)(h+j) + h - z]^2$
$- (2n+p+q+z-e)^2 - [16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2$
$- [e^3(e+2)(a+1)^2 + 1 - o^2]^2 - [(a^2-1)y^2 + 1 - x^2]^2$
$- [16r^2y^4(a^2-1) + 1 - u^2]^2$
$- [((a+u^2(u^2-a))^2-1)(n+4dy)^2 + 1 - (x+cu)^2]^2 - [n+l+v-y]^2$
$- [(a^2-1)l^2 + 1 - m^2]^2 - [ai+k+1-l-i]^2$
$- [p + l(a-n-1) + b(2an+2a-n^2-2n-2) - m]^2$
$- [q+ y(a-p-1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2$
$- [z + pl(a-p) + t(2ap - p^2 - 1) - pm]^2]$

Pour prouver qu'un nombre est premier, il suffit de donner les "bonnes" valeurs entières aux 26 variables, et de faire le calcul pour voir si on trouve bien le nombre premier en question. (James P. Jones, Daihachiro Sato, Hideo Wada, Douglas Wien, *Diophantine representation of the set of prime numbers*, American Mathematical Monthly, 83/6 (1976), p.449-464). Malheureusement, ce résultat, trouvé en corollaire d'un problème plus fondamental (le 10ème problème de Hilbert) n'a qu'un intérêt théorique et nullement pratique, car le polynôme de Jones n'est en fait qu'un codage extrêment astucieux d'un critère fort peu efficace de primalité à savoir : $k + 2$ est premier si et seulement si $(k + 1)! + 1 \equiv 0 \bmod k+2$ (théorème de Wilson). Les nombres intervenant dans ce polynôme sont gigantesques. Ainsi, les valeurs des variables permettant d'obtenir le nombre premier 2 sont-elles :

$a = 79016903580988961616855568797499491863263807134092 90912$
$b = 0$
$e = 32,$
$f = 17$
$g = 0$
$h = 2$
$i = 0$
$j = 5$
$k = 0$
$l = 1$
$m = 79016903580988961616855568797499491863263807134092 90912$
$n = 2$

o = 834035301564579468329946270481226888212608613465610836377 7

p = 3

q = 16

s = 1

t = 0

v = 158033807161977923233711137594998983726527614268185818 21,

w = 1

x = 124873421030546123716955456199915227363498042625369404787663046 0688618240305377713493375059050669591252915834 87

y = 158033807161977923233711137594998983726527614268185818 24

z = 9

u et r sont trop grand pour être affichés (et peut-être même calculés). Ils sont solutions de l'équation :

623103237477467837531548712748569488106977789848995186243400722213058 5
819467692530519441368990697501076667981494902945038290563249052108414 1
729062190213501628290192909949095484073533946150864915984334572822465 2
061515542425077120390471654182964600840783563926683798305093390159899 2
235543308075700053356528676291900536077836446649548 8r^2 + 1 – u^2 = 0

c et d sont solutions d'une équation comparable. ☹ ☹ ☹

5- Les fractions de Conway et Guy

Dans le même genre d'exploit loufoque, J.H. Conway et R.K. Guy, dans le livre *The Book of Numbers*, (Springer-Verlag 1996), donne la curiosité suivante ("*our best effort along these lines*" selon les auteurs). Considérons la suite de fractions qui suit :

$\frac{17}{91}$	$\frac{78}{85}$	$\frac{19}{51}$	$\frac{23}{38}$	$\frac{29}{33}$	$\frac{77}{29}$	$\frac{95}{23}$	$\frac{77}{19}$	$\frac{1}{17}$	$\frac{11}{13}$	$\frac{13}{11}$	$\frac{15}{14}$	$\frac{15}{2}$	$\frac{55}{1}$
A	B	C	D	E	F	G	H	I	J	K	L	M	N

Démarrez avec une puissance de 2 de la forme 2^p, où p est premier, puis multipliez de façon répétée par la première fraction (en commençant par la gauche) qui fournira un résultat entier. Alors la prochaine puissance de 2 que l'on obtiendra sera de la forme 2^q où q est le nombre premier immédiat supérieur à p. Par exemple, en partant de 2, on obtient ainsi, en multipliant successivement par les fractions M, N, E, F, K, A, etc... les nombres suivants :

2 → 15 → 825 → 725 → 1925 → 2275 → 425 → 390 → 330 → 290 → 770 → 910 → 170 → 156 → 132 → 116 → 308 → 364 → 68 → 4

jusqu'à parvenir à $4 = 2^2$. Si on continue, on obtiendra ensuite 2^3, puis 2^5 (sans jamais passer par 2^4), etc...(Ne pas partir de p trop grand car le programme est assez long à se terminer). Nous ne résistons pas à l'envie de donner la suite des valeurs qui suivent $32 = 2^5$. On notera que l'on parvient à $128 = 2^7$ sans jamais être passé par $64 = 2^6$!! Le calcul analogue nous faisant passer de 2^7 à 2^{11} prendrait six pages !! ☺ ☺ ☺

32 → 240 → 1800 → 13500 → 101250 → 759375 → 41765625 → 36703125 → 97453125 → 85640625 → 227390625 → 199828125 → 530578125 → 466265625 → 1238015625 → 1087953125 → 2888703125 → 3413921875 → 637765625 → 585243750 → 109331250 → 100327500 → 18742500 → 17199000 → 3213000 → 2948400 → 550800 → 505440 → 427680 → 375840 → 997920 → 876960 → 2328480 → 2046240 → 5433120 → 4774560 → 12677280 → 11140640 → 29580320 → 34958560 → 6530720 → 5992896 → 1119552 → 417088 → 252448 → 1042720 → 631120 → 2606800 → 1577800 → 6517000 → 3944500 → 16292500 → 9861250 → 40731250 → 24653125 → 101828125 → 412671875 → 487703125 → 91109375 → 83606250

→ 15618750 → 14332500 → 2677500 → 2457000 → 459000 → 421200 → 356400 → 313200 → 831600 → 730800 → 1940400 → 1705200 → 4527600 → 3978800 → 10564400 → 12485200 → 2332400 → 2140320 → 399840 → 366912 → 68544 → 25536 → 15456 → 63840 → 38640 → 159600 → 96600 → 399000 → 241500 → 997500 → 603750 → 2493750 → 1509375 → 6234375 → 25265625 → 22203125 → 58953125 → 69671875 → 13015625 → 11943750 → 2231250 → 2047500 → 382500 → 351000 → 297000 → 261000 → 693000 → 609000 → 1617000 → 1421000 → 3773000 → 4459000 → 833000 → 764400 → 142800 → 131040 → 24480 → 22464 → 19008 → 16704 → 44352 → 38976 → 103488 → 90944 → 241472 → 285376 → 53312 → 3136 → 3360 → 3600 → 27000 → 202500 → 1518750 → 11390625 → 626484375 → 550546875 → 1461796875 → 1284609375 → 3410859375 → 2997421875 → 7958671875 → 6993984375 → 18570234375 → 16319296875 → 43330546875 → 38078359375 → 101104609375 → 119487265625 → 22321796875 → 20483531250 → 3826593750 → 3511462500 → 655987500 → 601965000 → 112455000 → 103194000 → 19278000 → 17690400 → 3304800 → 3032640 → 2566080 → 2255040 → 5987520 → 5261760 → 13970880 → 12277440 → 32598720 → 28647360 → 76063680 → 66843840 → 177481920 → 155968960 → 414124480 → 489419840 → 91430080 → 83900544 → 15673728 → 5839232 → 3534272 → 14598080 → 8835680 → 36495200 → 22089200 → 91238000 → 55223000 → 228095000 → 138057500 → 570237500 → 345143750 → 1425593750 → 862859375 → 3563984375 → 14443515625 → 17069609375 → 3188828125 → 2926218750 → 546656250 → 501637500 → 93712500 → 85995000 → 16065000 → 14742000 → 2754000 → 2527200 → 2138400 → 1879200 → 4989600 → 4384800 → 11642400 → 10231200 → 27165600 → 23872800 → 63386400 → 55703200 → 147901600 → 174792800 → 32653600 → 29964480 → 5597760 → 5136768 → 959616 → 357504 → 216384 → 893760 → 540960 → 2234400 → 1352400 → 5586000 → 3381000 → 13965000 → 8452500 → 34912500 → 21131250 → 87281250 → 52828125 → 218203125 → 884296875 → 777109375 → 2063359375 → 2438515625 → 455546875 → 418031250 → 78093750 → 71662500 → 13387500 → 12285000 → 2295000 → 2106000 → 1782000 → 1566000 → 4158000 → 3654000 → 9702000 → 8526000 → 22638000 → 19894000 → 52822000 → 62426000 → 11662000 → 10701600 → 1999200 → 1834560 → 342720 → 314496 → 58752 → 21888 → 13248 → 54720 → 33120 → 136800 → 82800 → 342000 → 207000 → 855000 → 517500 → 2137500 → 1293750 → 5343750 → 3234375 → 13359375 → 54140625 → 47578125 → 126328125 → 111015625 → 294765625 → 348359375 → 65078125 → 59718750 → 11156250 → 10237500 → 1912500 → 1755000 → 1485000 → 1305000 → 3465000 → 3045000 → 8085000 → 7105000 → 18865000 → 22295000 → 4165000 → 3822000 → 714000 → 655200 → 122400 → 112320 → 95040 → 83520 → 221760 → 194880 → 517440 → 454720 → 1207360 → 1426880 → 266560 → 244608 → 45696 → 17024 → 10304 → 42560 → 25760 → 106400 → 64400 → 266000 → 161000 → 665000 → 402500 → 1662500 → 1006250 → 4156250 → 2515625 → 10390625 → 42109375 → 49765625 → 9296875 → 8531250 → 1593750 → 1462500 → 1237500 → 1087500 → 2887500 → 2537500 → 6737500 → 7962500 → 1487500 → 1365000 → 255000 → 234000 → 198000 → 174000 → 462000 → 406000 → 1078000 → 1274000 → 238000 → 218400 → 40800 → 37440 → 31680 → 27840 → 73920 → 64960 → 172480 → 203840 → 38080 → 34944 → 6528 → 2432 → 1472 → 6080 → 3680 → 15200 → 9200 → 38000 → 23000 → 95000 → 57500 → 237500 → 143750 → 593750 → 359375 → 1484375 → 6015625 → 7109375 → 1328125 → 1218750 → 1031250 → 906250 → 2406250 → 2843750 → 531250 → 487500 → 412500 → 362500 → 962500 → 1137500 → 212500 → 195000 → 165000 → 145000 → 385000 → 455000 → 85000 → 78000 → 66000 → 58000 → 154000 → 182000 → 34000 → 31200 → 26400 →

23200 → 61600 → 72800 → 13600 → 12480 → 10560 → 9280 → 24640 → 29120 → 5440 → 4992 → 4224 → 3712 → 9856 → 11648 → 2176 → 128

◆