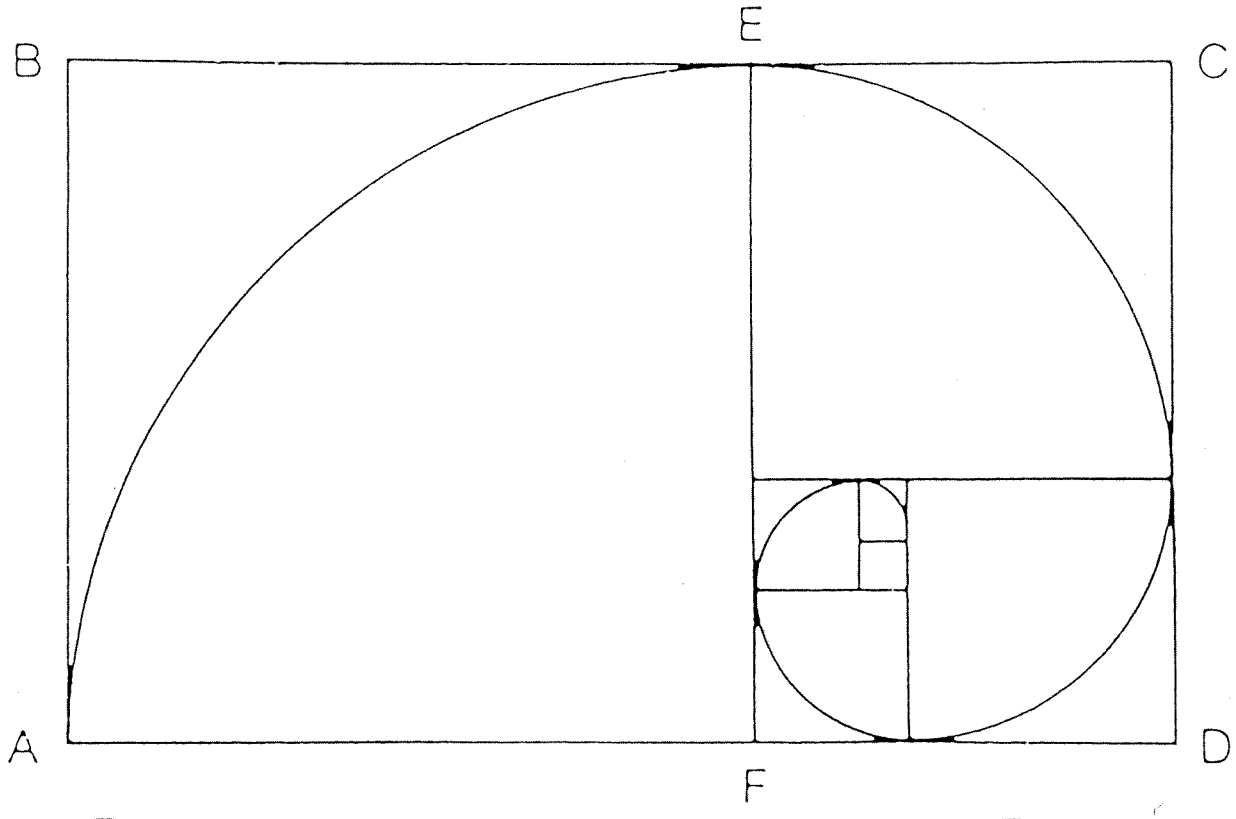
Jacques Faraut
Elisabeth Khalili

ARITHMÉTIQUE



Université Louis Pasteur
IREM de Strasbourg
1989

Jacques Faraut
Elisabeth Khalili

ARITHMÉTIQUE

Université Louis Pasteur
IREM de Strasbourg
10 rue du général Zimmer
67084 Strasbourg Cedex
1989

Un cours d'arithmétique a été introduit en première année du premier cycle de mathématiques de l'université Louis Pasteur en 1986. Cet enseignement comprend des travaux pratiques sur microordinateur qui donnent aux étudiants l'occasion d'analyser des algorithmes, comme le crible d'Eratosthène, de faire des expérimentations, sur la répartition des nombres premiers par exemple, ou de se faire une idée des applications de l'arithmétique, comme la cryptographie.

Un chapitre du cours est consacré aux fractions continues. C'est un sujet qui habituellement ne fait pas partie d'un cours d'arithmétique élémentaire, mais il a l'avantage de permettre un point de rencontre avec le cours d'analyse. De plus ce sujet ancien connait de nouveaux développements.

Nous avons rassemblé les notes de cours, les énoncés d'exercices et de travaux pratiques préparés par les personnes qui ont assuré cet enseignement pendant ces trois dernières années. Nous les publions principalement pour les travaux pratiques qui seuls présentent un caractère original.

Le texte a été saisi en TEX par madame Evelyne Le Guyader.

SOMMAIRE

Chapitre IV Polynômes

Chapitre I

DIVISIBILITÉ

1. Plus grand commun diviseur. — Rappelons que, étant donnés deux entiers relatifs a et b ($b > 0$), il existe un couple unique d'entiers (q, r) tel que

$$a = bq + r \text{ et } 0 \leq r < b.$$

On nomme a le *dividende*, b le *diviseur*, q le *quotient*, et r le *reste* de la division de a par b, et on note

$$q = a \text{ div } b$$
$$r = a \bmod b.$$

Exemple. — Les égalités de la division de 8 (resp. -8) par 3 s'écrivent :

$$\begin{array}{lll} 8 = 3 \times 2 + 2 & \text{quotient : } 2 & \text{reste : } 2 \\ -8 = 3 \times (-3) + 1 & \text{quotient : } -3 & \text{reste : } 1\ . \end{array}$$

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, et

$$a = bq + r\ ,\ 0 \leq r < b$$

l'égalité de la division de a par b. Si $r = 0$, on dit que b *divise* a, b est un *diviseur* de a, a est *divisible* par b, et a est un *multiple* de b, et on écrit $b|a$. On note $a\mathbb{Z}$ l'ensemble des multiples de a. Le nombre 1 est *diviseur impropre* de tout entier a.

PROPOSITION 1.1. — *Les sous-groupes additifs de $\mathbb{Z}$ sont les ensembles $a\mathbb{Z}$ ($a \in \mathbb{N}$).*

Démonstration.

1) Pour tout entier a, $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

2) Réciproquement, montrons que tout sous-groupe H de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$, avec $a \geq 0$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Supposons $H \neq \{0\}$ et soit a un élément non nul de H tel que $|a|$ soit minimum. Comme $-a$ est aussi un élément de H, on peut supposer $a > 0$. Pour un élément x quelconque de H, la division de x par a s'écrit

$$x = aq + r\ ,\ 0 \leq r < a.$$

Comme H est un sous-groupe de $\mathbb{Z}$, les nombres aq et $r = x - aq$ sont éléments de H. La définition de a implique que $r = 0$, donc $x = aq$ et H s'écrit de manière *unique* sous la forme $H = a\mathbb{Z}$ (avec $a \geq 0$). □

THÉORÈME 1.2. — *Soient a et b deux entiers, non tous deux nuls. Il existe un entier $d > 0$ tel que tout diviseur commun à a et b divise d. Un tel entier d est unique. Il divise a et b, et est appelé le plus grand commun diviseur (PGCD) de a et b. De plus, il existe des entiers u et v tels que*

$$d = au + bv.$$

L'égalité $d = au + bv$ est appelée égalité de Bézout.

Démonstration. — Si a et b sont deux entiers, posons

$$H = \{am + bn \mid m, n \in \mathbb{Z}\}.$$

Alors H est un sous-groupe de $\mathbb{Z}$, il existe donc un entier $d > 0$ unique tel que $H = d\mathbb{Z}$. Pour l'élément d de H, il existe u et v dans $\mathbb{Z}$ tels que

$$d = au + bv.$$

Les nombres a et b appartiennent à H, donc a et b sont de la forme

$$a = da' \text{ et } b = db' \qquad (a', b' \in \mathbb{Z})$$

et d *est un diviseur commun à a et b.*

Par ailleurs, si c est un diviseur commun à a et b ($c \in \mathbb{Z}$),

$$a = ca' \ , \ b = cb' \qquad (a', b' \in \mathbb{Z})$$

alors

$$d = au + bv = c(a'u + b'v)$$

donc c divise d, et $d \geq c$. Le nombre d est donc le *plus grand commun diviseur* de a et b. □

Dans l'égalité de BÉZOUT, le couple (u, v) n'est pas unique. Par exemple, si $a = 8, b = 6, d = 2$,

$$8 \times 1 - 6 \times 1 = 2$$
$$8 \times (-2) + 6 \times 3 = 2$$
$$8 \times 4 + 6(-5) = 2 \ , \ etc.$$

Ce théorème ne fournit pas de procédé pour déterminer le PGCD de deux nombres. C'est en revanche l'objet de l'algorithme suivant, appelé *algorithme d'Euclide* :

1. Plus grand commun diviseur

Soient a et b deux entiers strictement positifs. Supposons $a > b$. La division de a par b, de quotient q, de reste r, s'écrit

$$a = bq + r \ , \ 0 \leq r < b.$$

On remarque que les diviseurs communs à a et b sont les diviseurs communs à b et r, et qu'en particulier le PGCD de a et b est le PGCD de b et r. L'algorithme d'EUCLIDE consiste en la répétition de divisions dans lesquelles dividende, diviseur et reste ont même PGCD :

$$\begin{array}{lll}
(k=1) & a = bq_1 + r_1 & 0 < r_1 < b \\
(k=2) & b = r_1 q_2 + r_2 & 0 < r_2 < r_1 \\
(k=3) & r_1 = r_2 q_3 + r_3 & 0 < r_3 < r_2 \\
 & \cdots & \cdots \\
 & r_{k-2} = r_{k-1} q_k + r_k & 0 < r_k < r_{k-1} \\
 & \cdots & \cdots \\
(k=n-1) & r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} & 0 < r_{n-1} < r_{n-2} \\
(k=n) & r_{n-2} = r_{n-1} q_n & r_n = 0
\end{array}$$

La suite des restes $r_1, r_2, \ldots, r_k, \ldots$ est une suite d'entiers positifs ou nuls strictement décroissante, donc nécessairement il existe un entier n tel que $r_n = 0$. Le PGCD de a et b est le PGCD de b et r_1, de r_1 et r_2, ...,de r_{n-2} et r_{n-1}, de r_{n-1} et 0. C'est donc r_{n-1} : *le* PGCD *de a et b est le dernier reste non nul.*

L'algorithme d'EUCLIDE peut être résumé comme suit :

Répéter

$$\begin{aligned}
q &:= a \text{ div } b \\
r &:= a \bmod b \\
a &:= b \\
b &:= r
\end{aligned}$$

jusqu'à ce que $r = 0$.

Le PGCD est alors a.

Exemple. — $a = 44$, $b = 18$.

$$\begin{array}{llllll}
(1) & q = 2 & r = 8 & a = 18 & b = 8 \\
(2) & q = 2 & r = 2 & a = 8 & b = 2 \\
(3) & q = 4 & r = 0 & a = 2 & b = 2
\end{array}$$

Le PGCD est 2.

Programme. — Ceci donne en langage PASCAL :

```
program Euclide1;
var a, b, q, r : integer ;
BEGIN
write ('a =?'); readln(a);
write ('b =?'); readln(b);
repeat
        q := a div b;
        r := a mod b;
        a := b;
        b := r
until r = 0;
write ('le PGCD de a et b est ', a,' .');
END.
```

L'algorithme suivant, que nous appelerons *algorithme d'Euclide-Bézout*, fournit des coefficients u et v de l'égalité de Bézout $au + bv = d$.

Le sous-groupe de $\mathbb{Z}$

$$H = \{am + bn \mid m, n \in \mathbb{Z}\}$$

contient les nombres $r_1 = a - bq_1, r_2 = b - r_1 q_2, \ldots$ Si $r_1, \ldots, r_{k-1}, r_k$ sont des éléments de H, de la forme

$$r_k = au_k + bv_k \qquad (k \geq 1)$$

alors, de la relation

$$r_{k+1} = r_{k-1} - q_{k+1} r_k \qquad (k \geq 2)$$

on déduit

$$\begin{aligned} r_{k+1} &= au_{k-1} + bv_{k-1} - q_{k+1}(au_k + bv_k) \\ &= a(u_{k-1} - q_{k+1}u_k) + b(v_{k-1} - q_{k+1}v_k), \end{aligned}$$

d'où les relations de récurrence

$$\begin{aligned} u_{k+1} &= u_{k-1} - q_{k+1}u_k \\ v_{k+1} &= v_{k-1} - q_{k+1}v_k. \end{aligned} \qquad (k \geq 2)$$

Les coefficients u et v cherchés sont u_{n-1} et v_{n-1}.

Les suites (r_k), (u_k), (v_k) $(k \in \mathbb{N}^*)$ sont définies par les mêmes relations de récurrence, avec des conditions initiales différentes. En complétant l'algorithme d'EUCLIDE par les égalités

$$a = b \times 0 + a \qquad (k = -1)$$
$$b = a \times 0 + b \qquad (k = 0)$$

et en posant

$$\begin{array}{lll} r_{-1} = a & u_{-1} = 1 & v_{-1} = 0 \\ r_0 = b & u_0 = 0 & v_0 = 1, \end{array}$$

les relations de récurrence entre les r_k (resp. u_k, v_k) sont valables pour $k \geq 0$.

L'algorithme d'EUCLIDE-BEZOUT peut être résumé comme suit :

$$r_1 = a, \quad u_1 = 1, \quad v_1 = 0$$
$$r_2 = b, \quad u_2 = 0, \quad v_2 = 1$$

répéter

$$q = r_1 \text{ div } r_2$$
$$r = r_1 - q\, r_2$$
$$u = u_1 - q\, r_2$$
$$v = v_1 - q\, v_2$$
$$r_1 := r_2,\ r_2 := r$$
$$u_1 := u_2,\ u_2 := u$$
$$v_1 := v_2,\ v_2 := v$$

juqu'à ce que $r = 0$.

Le PGCD est alors $d = r_1$, et les coefficients de l'égalité de BÉZOUT sont u_1 et v_1.

Exemple. — $a = 3129$, $b = 546$.

k	r	u	v	q
-1	3129	1	0	
0	546	0	1	
1	399	1	-5	5
2	147	-1	6	1
3	105	3	-17	2
4	42	-4	23	1
5	21	11	-63	2
6	0	-26	149	2

Le PGCD de 3129 et 546 est 21 et

$$21 = 3129 \times 11 + 546 \times (-63).$$

Programme. — Ceci donne en langage PASCAL :

```
program Euclide2;
var a,b,q,r,r1,r2,u,u1,u2,v,v1,v2:integer;
BEGIN
write ('a =?'); readln (a);
write ('b =?'); readln (b);
r1 := a; u1 := 1; v1 := 0;
r2 := b; u2 := 0; v2 := 1;
repeat
        q := r1 div r2;
        r := r1 - q * r2;
        u := u1 - q * u2;
        v := v1 - q * v2;
        r1 := r2; u1 := u2; v1 := v2;
        r2 := r; u2 := u; v2 := v;
        writeln (r : 4,'      ', u : 4,'      ', v : 4,'      ', q : 4)
until r = 0;
writeln ('Le PGCD de ', a,' et ',b,' est ',r1,' .');
writeln (r1,' =',u1,'*',a,'+',v1,'*',b,' .');
END.
```

On dit que deux entiers sont *premiers entre eux* si leur PGCD est égal à 1.

THÉORÈME 1.3 (BÉZOUT). — *Pour que deux entiers a et b soient premiers entre eux il faut et il suffit qu'il existe un couple d'entiers (u, v) tel que*

$$au + bv = 1.$$

Démonstration. — Le théorème 1.2 prouve que la condition est nécessaire. La condition est aussi suffisante : si $au + bv = 1$, tout diviseur commun à a et b divise 1. □

Remarque. — Etant donnés deux entiers a et b premiers entre eux, le couple (u, v) vérifiant l'égalité de BÉZOUT n'est pas unique.

THÉORÈME 1.4 (GAUSS). — *Soient a, b et c des entiers. Si a divise bc, et si a est premier avec b, alors a divise c.*

Démonstration. — Si les entiers a et b sont premiers entre eux, d'après le théorème de BÉZOUT il existe un couple d'entiers (u, v) tel que

$$au + bv = 1,$$

et alors

$$acu + bcv = c.$$

L'entier a, divisant ac et bc, divise c.

Le PGCD possède les propriétés suivantes,

1. — *Si d est le PGCD des entiers a et b, et m est un entier, alors le PGCD de ma et mb est égal à md.*

2. — *Si d est le PGCD de a et b, alors $a = da'$ et $b = db'$, où a' et b' sont deux entiers premiers entre eux.*

C'est une conséquence immédiate du théorème 1.2 et du théorème de Bézout.

3. — *Soient a, b, c des entiers, m le PGCD de a et b, et p le PGCD de b et c. Alors le PGCD de m et c est le PGCD de a et p.*

Ce nombre est appelé le PGCD de a, b et c. Tout diviseur de a et p, et en particulier leur PGCD, divise a, b et c, donc m et c, et leur PGCD. De même, le PGCD de m et c divise le PGCD de a et p.

Plus généralement le PGCD de n entiers $a_1, \ldots, a_n$ est défini par récurrence : c'est le PGCD de a_n et du PGCD de $a_1, \ldots, a_{n-1}$. On dit que plusieurs entiers sont *premiers entre eux* si leur PGCD est égal à 1.

2. Equation diophantienne $ax + by = c$. — Etant donnés des entiers a, b, c, on cherche s'il existe des entiers x et y tels que

$$ax + by = c \tag{1}$$

D'après le théorème 1.2, si d est le PGCD de a et b, on a

$$\{ax + by, x, y \in \mathbb{Z}\} = d\mathbb{Z}.$$

Donc, pour que de tels entiers existent, il faut et il suffit que d divise c.

En divisant les deux membres de l'équation (1) par d, on se ramène au cas où a et b sont premiers entre eux. D'après le théorème de BÉZOUT, il existe alors deux entiers u et v tels que

$$au + bv = 1.$$

Les nombres u et v sont fournis, par exemple, par l'algorithme d'EUCLIDE-BÉZOUT. Les nombres $x_0 = uc$ et, $y_0 = vc$ sont solutions de (1). Posons

$$x = x_0 + X \ , \ y = y_0 + Y.$$

Alors x et y sont solutions de l'équation (1) si et seulement si

$$aX + bY = 0,$$

ou

$$aX = -bY. \tag{2}$$

L'entier a divise aX, donc bY. Il est premier avec b, il divise donc Y d'après le théorème de GAUSS, et l'on peut poser

$$Y = -ka, \ k \in \mathbb{Z}.$$

On déduit de (2) que $X = kb$, d'où la solution générale

$$x = x_0 + kb \ , \ y = y_0 - ka, \ k \in \mathbb{Z}.$$

Exemple. — Soit à résoudre dans $\mathbb{Z}$ l'équation

$$5x + 4y = 3.$$

Les nombres 5 et 4 sont premiers entre eux, l'équation a donc des solutions. En posant

$$x = 3u, \quad y = 3v$$

on se ramène à l'équation

$$5u + 4v = 1,$$

qui a pour solution évidente $u = 1$, $v = -1$. L'équation initiale a donc pour solution particulière $x_0 = 3$, $y_0 = -3$. Les nombres x et y de la forme

$$x = 3 + 4k\ ,\ y = -3 - 5k,\ k \in \mathbb{Z},$$

sont les solutions de l'équation donnée.

Remarque. — Géométriquement, la résolution de (1) consiste à rechercher les points de coordonnées entières situés sur la droite d'équation

$$ax + by = c.$$

Nous avons montré que ces points, s'ils existent, constituent une suite (M_k), $k \in \mathbb{Z}$, définie par

$$\overrightarrow{OM}_k = \overrightarrow{OM}_0 + k\overrightarrow{V},\ \overrightarrow{V} = \begin{pmatrix} b \\ -a \end{pmatrix}.$$

3. Bases de numération. — Le développement d'un entier dans une base b s'obtient à l'aide d'une suite de divisions euclidiennes.

PROPOSITION 3.1. — *Soit b un entier ($b \geq 2$). Tout entier naturel $x \neq 0$ s'écrit d'une manière unique sous la forme*

$$x = x_p b^p + \cdots + x_1 b + x_0$$

avec $0 \leq x_i < b$, $0 \leq i \leq p$ et $x_p \neq 0$ ($p \in \mathbb{N}$).

Dans le système de numération en base b on convient d'écrire

$$x = \overline{x_p \ldots x_1 x_0}\ (b) \quad ou \quad x = x_p \ldots x_1 x_0\ (b).$$

Cette écriture de x s'appelle le *développement du nombre x en base b.*

Démonstration. — Soit x un entier non nul. Si $x < b$, on pose $x_0 = x$ et $x = \overline{x_0}(b)$ $(p = 0)$. Si $x \geq b$, la division de x par b s'écrit

$$x = bq_1 + x_0 \quad \text{avec} \quad 0 \leq x_0 < b.$$

Si $q_1 < b$, on pose $x_1 = q_1$ et $x = x_1 b + x_0 = \overline{x_1 x_0}\ (b)$. Si $q_1 \geq b$, la division de q_1 par b s'écrit

$$q_1 = bq_2 + x_1 \quad \text{avec} \quad 0 \leq x_1 < b,$$

et ainsi de suite. La division de q_k par b s'écrit

$$q_k = bq_{k+1} + x_k \quad \text{avec} \quad 0 \leq x_k < b,\ k \geq 1.$$

La suite des quotients $q_1, q_2, \ldots, q_k$ est une suite d'entiers positifs strictement décroissante :

$$0 \leq q_{k+1} < q_k < \ldots < q_2 < q_1 < x.$$

Il existe donc un entier p pour lequel on a

$$\begin{aligned} &q_{p-1} = bq_p + x_{p-1}\ ,\ 0 \leq x_{p-1} < b, \\ &0 < q_p < a \leq q_{p-1} \\ &q_p = b.0 + x_p\ ,\ 0 < x_p = q_p < b \\ &q_{p+1} = 0. \end{aligned}$$

Le nombre x_p est alors le dernier quotient non nul et dans ce cas

$$x = x_p b^p + \cdots + x_1 b + x_0,$$

qui se note en base b :

$$x = \overline{x_p \ldots x_1 x_0}.$$

L'unicité de la décomposition se démontre par l'absurde. □

Remarques.

— Le nombre de chiffres de l'écriture de x en base a est égal au nombre de divisions nécessaires pour obtenir un quotient nul.

— La décomposition d'un entier x non nul suivant les puissances de b peut s'étendre à $x = 0$; pour tout $b \geq 2$:

$$0 = \bar{0}\ (b).$$

Exemple. — En base 12, on utilise les chiffres $0, 1, \ldots, 9$ et les symboles α (pour 10) et β (pour 11) :

$$\overline{\alpha\beta}\ (12) = \alpha \times 12 + \beta = 10 \times 12 + 11 = 131\ (10).$$

L'algorithme d'écriture d'un entier en base b peut être résumé comme suit,

Répéter
$\quad r = x \bmod a$
$\quad q = x \operatorname{div} a$
$\quad x := q$
jusqu'à ce que $q = 0$.

Les valeurs successives de r sont les chiffres de x en base b, obtenus dans l'ordre d'écriture de droite à gauche, $x_0, x_1, x_2, \ldots, x_l$. Il faudra les écrire ensuite dans l'ordre inverse, $x_l, \ldots, x_1, x_0$.

Exemple. — $x = 25 \quad b = 2$.

(1)	$25 = 2 \times 12 + 1$	$r = 1$	$q = 12$	$x = 12$
(2)	$12 = 2 \times 6 + 0$	$r = 0$	$q = 6$	$x = 6$
(3)	$6 = 2 \times 3 + 0$	$r = 0$	$q = 3$	$x = 3$
(4)	$3 = 2 \times 1 + 1$	$r = 1$	$q = 1$	$x = 1$
(5)	$1 = 2 \times 0 + 1$	$r = 1$	$q = 0$	$x = 0$

$$25 = \overline{11001}\ (2)$$

Programme. — Ceci donne en langage PASCAL :

```
program chbase;
var b, j, l, r, x, integer;
    U:array [1..100] of integer;
BEGIN
write ('Donner l''entier x à écrire en base b :');
readln(x);
write ('Donner la base b   (b > 1) :');
readln(b);
j := 1; r := x;
repeat
        U[j] := r mod b;
        r := r div b;
        j := j + 1;
until r = 0;
l := j - 1;
writeln ('Ecriture de ',x,' en base ',b,' :');
for j := l downto 1 do write (U[j],'      ')
END.
```

4. Nombres premiers. — Un nombre $n \geq 2$ est dit *premier* si ses seuls diviseurs sont 1 et lui-même. Un nombre entier $n \geq 2$ est dit *composé* s'il n'est pas premier.

On note $\tau(n)$ le nombre des diviseurs de n qui sont inférieurs à n, 1 et n compris.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2

Un nombre n est premier si et seulement si $\tau(n) = 2$. Ceci constitue un premier test pour reconnaître si un entier n est premier.

Le *crible d'Eratosthène* permet d'établir la liste des nombres premiers. Il consiste à éliminer successivement les multiples de 2, puis ceux de $3, \ldots,$ de $k, \ldots$ $(k \leq N)$. Les entiers qui n'ont pas été éliminés sont premiers.

Exemple. — Nombres premiers ≤ 100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

L'algorithme utilisé pour dresser le tableau précédent peut être résumé comme suit,

pour $k = 2, \ldots, n$ poser $c_k =$ vrai ;
poser $k := 2$;
répéter
    si c_k est vrai, pour $m = k^2, k^2 + k, \ldots, k^2 + \ell k$
    et tant que $m \leq n$, poser $c_m =$ faux ;
    $k := k + 1$;
tant que $k^2 < n$.

Les nombres premiers compris entre 2 et n sont les entiers k pour lesquels le booléen c_k a gardé la valeur *vrai*.

Programme. — Ceci donne en langage PASCAL :

```
program Eratosthene;
const n = 1000;
var k, m:integer;
    c:array [1..n] of boolean;
    p:boolean;
BEGIN
p:=true;
c[1]:=not p;
for k:=2 to n do c[k] := p;
k := 2;
while k * k < n do
      begin
      if c[k] = p then
            begin
            m := k * k;
            while m <= n do
                  begin
                  c[m]:=not p;
                  m:=m + k;
                  end;
            end;
      k:=k + 1;
      end;
for k:=1 to n do
      begin
      if c[k]=p then write (k : 3, '    ') else write ('///    ');
      if k mod 10=0 then writeln;
      end;
END.
```

PROPOSITION 4.1. — *Tout nombre entier $n \geq 2$ admet au moins un diviseur premier.*

Démonstration. — Soit $n \geq 2$. Son plus petit diviseur est un nombre premier. □

Voici le *premier théorème d'Euclide*

THÉORÈME 4.2 (EUCLIDE). — *La suite des nombres premiers est illimitée.*

Démonstration. — Elle se fait par l'absurde : Supposons qu'il n'existe qu'un nombre fini de nombres premiers $p_1, p_2, \ldots, p_m$. Posons

$$n = p_1 p_2 \ldots p_m + 1.$$

Le nombre n admet au moins un diviseur premier, que l'on note p, et $n = pn', \quad n' \in \mathbb{N}$. L'égalité

$$pn' - p_1 p_2 \ldots p_m = 1$$

montre que le nombre premier p ne peut être l'un des $p_i \quad (i = 1, \ldots, m)$, d'où la contradiction. □

Le théorème suivant est appelé *théorème fondamental de l'arithmétique.*

THÉORÈME 4.3. — *Tout nombre entier supérieur ou égal à 2 est égal à un produit de facteurs premiers. A l'ordre des facteurs près, cette décomposition est unique.*

Démonstration. — Montrons d'abord l'existence de la factorisation. Soit $n \geq 2$ un entier, et p_1 son plus petit diviseur. Alors p_1 est premier, et $n = p_1 n_1$, avec $1 \leq n_1 < n$. Si $n_1 \geq 2$, on répète le même raisonnement avec n_1. La suite des quotients $n_1, \ldots$ étant décroissante, le processus s'arrête lorsque le quotient est 1. L'entier n s'écrit finalement sous la forme

$$n = p_1^{a_1} \ldots p_r^{a_r}$$

où les p_i sont des nombres premiers distincts, et $a_i \geq 1 \quad (i = 1, \ldots, r)$.

Pour démontrer l'unicité on utilise le lemme suivant :

LEMME 4.4. — *Si p et q sont deux entiers premiers entre eux, alors, pour des entiers a et b, a et $b > 0$, les entiers p^a et q^b sont premiers entre eux.*

Si p et q sont premiers entre eux, il existe deux entiers u et v tels que

$$up + vq = 1$$

donc aussi

$$(up + vq)^{a+b} = 1.$$

On développe le premier membre en utilisant la formule du binôme de Newton, et on regroupe d'une part les termes contenant le facteur q^b, et d'autre part les termes contenant le facteur p^a. On obtient une expression de la forme

$$v'q^b + u'p^a = 1$$

où u' et v' sont des entiers, ce qui montre que p^a et q^b sont premiers entre eux.

Montrons maintenant l'unicité de la factorisation. Supposons que l'on ait

$$p_1^{a_1} \dots p_r^{a_r} = q_1^{b_1} \dots q_s^{b_s}$$

où les a_i et b_j sont ≥ 1, les p_i sont des nombres premiers distincts, de même que les q_j. On doit montrer qu'à l'ordre près ce sont les mêmes nombres premiers élevés aux mêmes puissances. Raisonnons par l'absurde. Après simplification on arrive à une situation où, par exemple, p_1 ne figure pas parmi les q_j : p_1 divise $q_1^{b_1}(q_2^{b_2} \dots q_s^{b_s})$, et est premier avec $q_1^{b_1}$, donc, d'après le théorème de GAUSS, p_1 divise $(q_2^{b_2} \dots q_s^{b_s})$. En recommençant on arrive à la conclusion que p_1 divise $q_s^{b_s}$, d'où la contradiction. □

COROLLAIRE 4.5. — *Si les décompositions en facteurs premiers de deux entiers m et n s'écrivent*

$$m = p_1^{a_1} \dots p_r^{a_r}$$
$$n = p_1^{b_1} \dots p_r^{b_r},$$

alors le PGCD de m et n est égal à $d = p_1^{c_1} \dots p_r^{c_r}$, où $c_i = min(a_i, b_i)$.

EXERCICES

(*Exercices sur la section 1*)

1 . — On divise deux entiers a et b par leur différence $a-b$. Comparer les quotients et les restes obtenus.

2 . — Pour diviser un entier a par un produit d'entiers $b_1 b_2$, suffit-il de diviser par b_2 le quotient entier de a par b_1 ?

3 . — Dans $\mathbb{Z}$, on définit la relation $\mathfrak{R}$ par

$$a \mathfrak{R} b \Longleftrightarrow a \text{ divise } b.$$

Vérifier que $\mathfrak{R}$ est une relation d'ordre.

4 . — Ecrire l'algorithme d'EUCLIDE-BÉZOUT pour $a = 70$, $b = 42$; pour $a = 2431$, $b = 1342$.

5 . — Vérifier que les diviseurs communs à plusieurs nombres sont les diviseurs de leur PGCD.

6 . — Soient a et b deux entiers premiers entre eux. On pose

$$s = a + b, \quad p = ab.$$

Déterminer le PGCD de a et s, de s et p.

7 . — Soient a et b deux entiers. Les diviseurs communs à a et b sont les diviseurs de a et $a - b$. En déduire une méthode de calcul du PGCD de 70 et 42 par différences successives. Ecrire un algorithme, puis un programme PASCAL affichant le PGCD de deux entiers donnés, calculé par différences successives.

8 . — Si n et m sont deux entiers strictement positifs, déterminer le PGCD de $2^n - 1$ et $2^m - 1$.

9 . — Montrer que, si l'entier a est premier avec les entiers $b_1, b_2, \ldots, b_p$, alors a est premier avec $\prod_{i=1}^{p} b_i$.

10 . — (Nombres pythagoriciens) Le but de cet exercice est de déterminer tous les triplets (x, y, z) d'entiers relatifs vérifiant l'équation :

$$\text{(E)}. \qquad x^2 + y^2 = z^2$$

Soit (x', y', z') une solution de (E).

a) Démontrer que les couples $(x', y'), (y', z')$ et (x', z') ont même PGCD. En déduire qu'il existe un entier d et trois entiers x, y, z premiers deux à deux tels que (x, y, z) est une solution de l'équation (E) et $x' = dx, y' = dy, z' = dz$.

b) Soit (x, y, z) une solution de l'équation (E) telle que x, y, z soient premiers deux à deux. Démontrer que x et y sont de parités différentes.

α) Supposons x pair et y impair. En remarquant que $z - y$ et $z + y$ sont pairs, démontrer qu'il existe deux entiers u et v tels que $y = u - v$ et $z = u + v$, et u et v sont premiers entre eux.

β) Démontrer que u et v sont les carrés de deux entiers premiers entre eux (ie. $u = a^2$ et $v = b^2$).

γ) En déduire que $x = 2ab, y = a^2 - b^2$ et $z = a^2 + b^2$.

c) En déduire toutes les solutions de l'équation (E).

11 . — (Plus petit commun multiple) L'entier c est appelé *multiple commun* de deux entiers s'il est multiple de chacun de ces entiers. On appelle *plus petit commun multiple* (PPCM) de deux entiers a et b un tel multiple commun qui divise tout multiple commun de a et b.

a) Montrer que dans $\mathbb{Z}$, deux plus petits communs multiples de deux entiers a et b ne diffèrent que du signe. On notera $[a, b]$ le plus petit commun multiple positif.

b) En considérant l'intersection $(a) \cap (b)$ des deux sous-groupes engendrés par a (resp. par b), montrer qu'il existe un plus petit commun multiple de a et b.

c) Montrer, que pour tous entiers a, b et c non nuls avec $c > 0$, on a $[ac, bc] = c[a, b]$.

d) Montrer que, si a et b sont deux entiers premiers entre eux, ab est alors un plus petit commun multiple de a et b.

e) Montrer que si a et b sont deux entiers positifs,

$$ab = \text{PGCD } (a, b).[a, b].$$

12 . — a) Soit u_n la suite définie par

$$u_n = \sum_{j=1}^{n} \frac{1}{j}.$$

La suite u_n prend-elle des valeurs entières ? (Indication : Soit k le plus grand entier tel que $2^k \leq n$, et soit d le PGCD des nombres $2, 3, \ldots, n$. Montrer que

$$d = 2^k a$$

où a est un nombre impair, et que $d\, u_n$ est un nombre impair.)

b) Soit v_n la suite définie par

$$v_n = \sum_{j=1}^{n} \frac{1}{2j-1}.$$

La suite v_n prend-elle des valeurs entières ? (Indication : Considérer les puissances de 3.)

Pour un prolongement de cet exercice on peut consulter American Math. Monthly 67 (1960)p.290 et pp. 924—925.

(*Exercices sur la section 2*)

13 . — Résoudre dans $\mathbb{Z}$:
a) $7x - 19y = 5$;
b) $12x - 7y = 15$;
c) $120x + 252y = 48$.

14 . — Donner les solutions entières positives des équations :
a) $6x + 15y = 83$;
b) $20x + 50y = 510$.

15 . — Ecrire un programme PASCAL qui donne, lorsque c'est possible, des solutions de l'équation diophantienne $ax + by = c$. (On modifiera, par exemple, le programme de l'algorithme d'Euclide-Bézout.)

(*Exercices sur la section 3*)

16 . — Ecrire
1000 (10) en base 2,
10011001 (2) en base 10.
1 101 111 010 100 011 (2) en base 8. Déterminer a et b sachant que 23 (10) = 27 (a) et 136 (10) = 253 (b).

17 . — Ecrire, en base n, un nombre a de trois chiffres, tous différents. Ecrire le nombre b obtenu en lisant les trois chiffres de a de droite à gauche. On note d la différence de a et b.

Ecrire le nombre c obtenu en lisant les chiffres de d de droite à gauche. Montrer que $s = d + c$ est indépendant de a.

18 . — Par combien de zéros se termine l'écriture (en base 10) de 100! ?

19 . — Etudier le programme suivant et donner, sous forme d'un tableau, le contenu des variables n, p, x à l'intérieur de la boucle "repeat ... until" si les valeurs initiales de n et x valent respectivement 19 et a. Quelle fonction ce programme assure-t-il ? Mettre ce programme sous forme procédurale, (odd(n) est un booléen qui est vrai si n est impair).

```
program X;
var i, n, p, x:integer;
BEGIN
read(x);read(n);
p:=1;
repeat
        while not odd(n) do
        begin
                x := x * x;
                n := n div 2;
        end;
        p := p * x;
        n := n - 1;
until n = 0;
write(p);
END.
```

(*Exercices sur la section 4*)

20 . — On suppose que le PGCD des entiers a et b est un nombre premier p. Quelles sont les valeurs possibles du PGCD de a^2 et b, a^3 et b, a^2 et b^3 ?

21 . — Soit p un nombre premier. On suppose que le PGCD de a et p^2 est p, et que le PGCD de b et p^3 est p^2. Déterminer le PGCD de ab et p^4, et le PGCD de $a + b$ et p^4.

22 . — a) Démontrer que tout nombre premier $a \geq 5$ est de la forme $a = 4n + 1$ ou $a = 4n + 3 \quad (n \in \mathbb{N})$.

b) Si p est un nombre premier, on note $p!!$ le produit des nombres premiers inférieurs ou égaux à p. On pose $q = 2(p!!) - 1$. Montrer que q est de la forme $q = 4n + 3$, puis montrer que q est soit premier, soit divisible par un entier a_1 premier, avec $a_1 > p$. Le nombre a_1 est-il de la forme $a_1 = 4n + 3$?

En déduire que la progression arithmétique $3+4n$ comprend une infinité de nombres premiers.

c) Démontrer que tout nombre premier $a \geq 5$ est de la forme $a = 6n+1$ ou $a = 6n+5$. En déduire que la progression arithmétique $6n+5$ comprend une infinité de nombres premiers.

23 . — Ecrire un programme PASCAL pour le test de primarité suivant : un entier n est premier si et seulement si $\tau(n) = 2$ (cf. § 4).

24 . — Si n est un nombre premier, on note $n!!$ le produit des nombres premiers inférieurs ou égaux à n.

a) Si n est un nombre premier, les nombres $n!! + 2, n!! + 3, \ldots$ sont-ils premiers ?

b) Démontrer que, dans $\mathbb{Z}$, on peut trouver des intervalles $[a, b]$ de longueur $b - a$ arbitrairement grande ne contenant pas de nombres premiers.

c) A l'aide d'un programme PASCAL, trouver la décomposition en facteurs premiers des nombres 30030, 30031, ..., 30043, ...jusqu'au premier nombre premier que l'on rencontrera.

d) Si n est un nombre premier, $n!! + 1$ est-il premier ?

25 . — (Théorème de WILSON) a) Soit p un nombre premier, $p \geq 5$. On pose

$$A_p = \{2, 3, \ldots, p-2\}.$$

Montrer que pour tout nombre a de A_p, il existe un nombre b de A_p tel que

$$ab \equiv 1 \pmod{p}.$$

Le nombre b est-il unique ? Est-il possible que $a = b$?

b) Pour $p = 7$ remplir le tableau suivant

a	2	3	4	5	6	7
b						

Faire de même pour $p = 11$.

c) Montrer que, si p est un nombre premier, le nombre $(p-1)! + 1$ est divisible par p.

d) Soit p un nombre tel que $(p-1)! + 1$ soit divisible par p. Le nombre p est-il premier ?

26 . — On note $\tau(n)$ le nombre de diviseurs de n. Par exemple, les diviseurs de $n = 10$ sont 1, 2, 5 et 10 : $\tau(10) = 4$.

a) Montrer que si m et n sont premiers entre eux

$$\tau(mn) = \tau(m)\tau(n).$$

b) Si p est premier et α un entier > 0, montrer que

$$\tau(p^\alpha) = \alpha + 1.$$

c) Exprimer $\tau(n)$ à l'aide de la décomposition en facteurs premiers de n, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Calculer $\tau(720)$.

d) Quel est le plus petit entier n tel que $\tau(n) = 100$?

e) Ecrire une procédure pour le calcul de la fonction $\tau(n)$. Etudier la suite définie par

$$n_0 = a$$
$$n_{k+1} = \tau(n_k).$$

f) Montrer que, pour $s > 1$,

$$\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \Big(\sum_{n=1}^{\infty} \frac{1}{n^s}\Big)^2.$$

Pour cela on utilisera la partition suivante de $\mathbb{N}^* \times \mathbb{N}^*$:

$$\mathbb{N}^* \times \mathbb{N}^* = \cup_{n=1}^{\infty} A_n,$$

avec

$$A_n = \{(u, v) | uv = n\}.$$

En particulier

$$\sum_{n=1}^{\infty} \frac{\tau(n)}{n^2} = (\frac{\pi^2}{6})^2.$$

27 . — On note $\sigma(n)$ la somme des diviseurs de n. Par exemple

$$\sigma(10) = 1 + 2 + 5 + 10 = 18.$$

a)Montrer que si m et n sont premiers entre eux

$$\sigma(mn) = \sigma(m)\sigma(n).$$

b) Si p est premier et α un entier > 0, montrer que

$$\sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}.$$

c) Exprimer $\sigma(n)$ à l'aide de la décomposition en facteurs premiers de n, $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Calculer $\sigma(200)$.

d) Montrer que, pour $s > 2$,

$$\sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} = \Big(\sum_{n=1}^{\infty} \frac{1}{n^s}\Big)\Big(\sum_{n=1}^{\infty} \frac{1}{n^{s-1}}\Big).$$

TRAVAUX PRATIQUES

1. Longueur de l'algorithme d'Euclide. — Le calcul du PGCD de deux nombres entiers $x > y > 0$ par l'algorithme d'EUCLIDE consiste en des divisions successives. Le nombre n de divisions dépend des nombres x et y : $n = f(x, y)$.

Calculons par exemple le PGCD de 44 et 18 :

$$44 = 2 \times 18 + 8 \tag{1}$$
$$18 = 2 \times 8 + 2 \tag{2}$$
$$8 = 4 \times 2 + 0 \tag{3}$$

Le PGCD est égal à 2, l'algorithme a nécessité 3 divisions :

$$f(44, 18) = 3.$$

1. — Etude de la fonction f. a) Ecrire une procédure pour le calcul de cette fonction f.

b) Soit g la fonction définie par

$$g(x) = \max\{f(x, y) | 1 \leq y \leq x\}.$$

Ecrire un programme permettant de tabuler la fonction g pour les valeurs de x comprises entre 50 et 100. Pour quelles valeurs de x atteint-elle son maximum ?

c) On propose de comparer $g(x)$ à $\ln(x)$. Montrer à l'aide d'un programme que, pour $2 \leq x \leq 250$, le rapport $g(x)/\ln(x)$ est borné. Quel est son maximum ? Quels sont les nombres x, $1 \leq x \leq 250$, pour lesquels $g(x)/\ln(x) \geq 1,9$?

2. — On note $r_1, r_2, \ldots, r_{n-1}, r_n = 0$ les restes des divisions successives. On pose $r_0 = b, r_{-1} = a$.

a) Montrer que, pour $1 \leq k \leq n - 1$,

$$r_{k-2} \geq r_{k-1} + r_k.$$

b) Soit (F_n) la suite de FIBONACCI. Les nombres F_n sont définis par

$$F_0 = 1, \quad F_1 = 1,$$
$$F_n = F_{n-1} + F_{n-2}, \quad n \geq 2.$$

Montrer que, pour $0 \leq k \leq n$,

$$r_{n-k-1} \geq F_k.$$

c) Démontrer que, pour $n \geq 0$,

$$F_n \geq \alpha^{n-1}, \quad \alpha = \frac{1+\sqrt{5}}{2},$$

et en déduire une majoration du type

$$n \leq A \ln(a) + B.$$

d) Commenter les résultats numériques obtenus en 1.

2. Quelle est la probabilité pour que deux nombres soient premiers entre eux ?. — Si u et v sont deux entiers tirés au hasard, quelle est la probabilité pour que u et v soient premiers entre eux ? Mais que signifie "*tirés au hasard*" ? Pour donner un sens à cette question, notons q_n le nombre de couples (u, v) d'entiers premiers entre eux de l'intervalle $[1, n]$, et posons $p_n = \frac{1}{n^2} q_n$. Les couples (u, v) étant supposés équiprobables, p_n est la probabilité pour que deux nombres de l'intervalle $[1, n]$ soient premiers entre eux. On propose dans ce T.P. d'étudier la suite p_n.

1. — a) Tout d'abord, simuler à l'aide de l'ordinateur le tirage au hasard d'un couple d'entiers (u, v). Pour cela utiliser la fonction random. Ecrire le programme suivant :

```
program hasard;
var k, n:integer;
BEGIN
for k := 1 to 20 do
      begin
      n :=random(1000);
      writeln(k : 2,'      ', n : 4);

END.
```

Exécuter ce programme. Les nombres de la deuxième colonne semblent tirés au hasard parmi les nombres compris entre 0 et 1000. En fait ces nombres sont calculés à l'aide d'une formule. Cette formule est choisie de telle sorte que ces nombres paraissent distribués au hasard. Ce sont des nombres pseudo-aléatoires.

b) Ecrire une procédure calculant le PGCD de deux nombres entiers. A l'aide de la fonction random écrire un programme permettant de simuler une suite de m tirages au hasard de couples d'entiers de l'intervalle $[1, 10000]$, et qui calcule pour une telle suite la fréquence relative f_m des couples d'entiers premiers entre eux : si dans la suite choisie il y a q_m couples d'entiers premiers entre eux, q_m est la fréquence, $f_m = \frac{q_m}{m}$ est la fréquence relative. Qu'observe-t-on ?

c) α) Ecrire une procédure calculant le nombre de diviseurs d'un entier.

β) Ecrire un programme calculant, pour une suite de m tirages de couples d'entiers, le nombre moyen de diviseurs communs de deux entiers de l'intervalle $[1, 10000]$ en utilisant les procédures de b) et c) α).

d) Calculer à l'aide d'un programme les probabilités p_n pour $n = 50, 100, 150, 200$.

2. — a) Pour n fixé, soit Ω l'ensemble des couples d'entiers (u, v), $1 \leq u, v \leq n$. On suppose que tous les couples sont équiprobables. On note P la probabilité ainsi définie sur Ω : la probabilité d'une partie A de Ω (évènement) est le nombre

$$P(A) = \frac{1}{n^2}(\sharp A),$$

où $\sharp A$ désigne le nombre d'éléments de A. On note p la probabilité pour que u et v soient premiers entre eux. Soit d un entier, $1 \leq d \leq n$. Quelle est la probabilité $a(d)$ pour que d soit diviseur commun à u et v ?

b) Soient $\alpha_1, \ldots, \alpha_k$ les nombres premiers $\leq n$. Soit A_j l'événement suivant : α_j est un diviseur commun à u et v. Soit $A = A_1 \cup \ldots \cup A_k$. Montrer que

$$p = 1 - P(A),$$

et que

$$P(A_1 \cap \ldots \cap A_j) = a(\alpha_1 \alpha_2 \ldots \alpha_j).$$

c) La fonction de Möbius est définie sur $\mathbb{N}^*$ par

$\mu(1) = 1$,
$\mu(d) = 0$ si d est divisible par un carré autre que 1,
$\mu(d) = (-1)^l$ si $d = \alpha_1 \alpha_2 \ldots \alpha_l$
où les α_i, $1 \leq i \leq l$, sont des nombres premiers distincts.

En utilisant la formule

$$P(A) = \sum_j P(Aj) - \sum_{j_1 < j_2} P(Aj_1 \cap Aj_2) + \cdots + (-1)^{k-1} P(A_1 \cap \ldots \cap A_k)$$

montrer que

$$p = \sum_{d=1}^{n} \mu(d)\, \frac{1}{n^2} \left[\frac{n}{d}\right]^2$$

où $[x]$ désigne la partie entière de x.

d) Ecrire un programme permettant le calcul de la fonction de Möbius. Comparer les valeurs de $p = p_n$ trouvées en 1.d) et les valeurs calculées à l'aide de la formule précédente.

3. — Cette dernière partie utilise les séries numériques.

a) Montrer que la suite p_n a une limite q quand n tend vers l'infini.

b) On note $p_n(d)$ la probabilité pour que d soit le PGCD de u et v (en particulier $p_n(1) = p_n$). Montrer que

$$\lim_{n \to \infty} p_n(d) = \frac{q}{d^2}.$$

Sachant que

$$\sum_{d=1}^{\infty} \frac{1}{d^2} = \frac{\pi^2}{6},$$

calculer q. Comparer cette valeur aux valeurs expérimentales obtenues en *1.*

c) Montrer que le nombre moyen M_n de diviseurs communs à u et v est égal à

$$M_n = \sum_{d=1}^{n} \tau(d) p_n(d),$$

où $\tau(d)$ désigne le nombre de diviseurs de d.

Démontrer que

$$M = \lim_{n \to \infty} M_n = \sum_{d=1}^{\infty} \tau(d) \frac{q}{d^2}.$$

En utilisant la formule

$$\sum_{d=1}^{\infty} \tau(d) \frac{1}{d^2} = \left(\frac{\pi^2}{6}\right)^2,$$

comparer la valeur de M aux résultats expérimentaux obtenus en *1.*

3. Bases de numération. — Si n est entier positif, on désigne par long(n) le nombre de chiffres de son écriture en base 2.

1. — Ecrire un programme en langage PASCAL qui réalise les tâches suivantes :

a) lecture au clavier de l'entier n ;

b) conversion de n en base 2 ;

c) affichage de l'écriture binaire de n ;

d) affichage de la valeur long(n).

On pourra utiliser une procédure dont le paramètre d'entrée sera n et dont les paramètres de sortie seront le tableau-ligne des chiffres de l'écriture binaire de n et l'entier long(n). Autrement dit n sera transmis par valeur tandis que la variable "tableau" et la variable long(n) seront transmises par référence.

2. — Quelle est la plus grande valeur de n dont votre programme effectue la conversion ? Expliquer.

3. — Tabuler les valeurs de la fonction long(m) + long(n) - long(mn) lorsque m et n varient indépendamment de 0 à 100 ; décrire ce que l'on obtient ; quelle est la valeur maximale de cette fonction sur ce domaine ?

4. — Montrer, en se servant éventuellement du programme, qu'il existe une valeur réelle positive du paramètre réel C pour laquelle

$$\sup_{m\in[1,1000]} |\mathrm{long}(m) - \frac{\ln(m)}{C}|$$

est la plus petite possible ($\ln(m)$ désigne le logarithme népérien de m). Pour cette valeur C_0 particulière de C, quelle est la borne supérieure obtenue et en quelles valeurs de m est-elle atteinte ?

5. — En utilisant la fonction partie entière et $\ln(\mathrm{m})/C_0$, montrer que l'on peut exprimer facilement long(m) sur l'intervalle $[2, 1000]$.

6. — Application à l'évaluation des puissances entières d'un nombre réel : si a est un nombre réel positif, quel est le nombre minimal de multiplications nécessaires pour élever a à la puissance 2^i (i entier ≥ 0) ?

7. — Le calcul d'une puissance a^n peut être accéléré si l'on procède de la façon suivante :

a) décomposer n en base 2 : $n = c_k c_{k-1} \ldots c_0$;

b) effectuer le produit des $a^{(2^i)}$ correspondant aux c_i valant 1.

Expliquer en détail les calculs donnés par cet algorithme dans l'évaluation de 3^{19}.

8. — Ecrire une fonction en langage PASCAL, fondée sur le procédé décrit ci-dessus, pour déterminer, avec le minimum de multiplications, a^n (où a est réel > 0 et n entier ≥ 0) ; utiliser cette fonction dans un programme qui détermine a^n si a et n sont entrés par l'utilisateur. Comment comparer le gain de temps gagné sur le procédé ordinaire d'évaluation de a^n ?

4. Répartition des nombres premiers. — Si n est un entier ($n \geq 2$), on note $\pi(n)$ le nombre d'entiers premiers inférieurs ou égaux à n.

1. — A l'aide d'un programme en langage PASCAL affichant $\pi(n)$ et la proportion $\frac{\pi(n)}{n}$ de nombres premiers compris entre 1 et n, observer les variations de $\pi(n)$ lorsque n varie. Vers quelle limite semble tendre le rapport $\frac{\pi(n)}{n/ln(n)}$ lorsque n tend vers l'infini ?

2. — Pour un entier $k \geq 1$, on note p_k le k-ième nombre premier dans la suite des nombres premiers rangés par ordre croissant. A l'aide d'un programme en langage PASCAL observer les variations de $\frac{p_k}{kln(k)}$ lorsque k varie ($k \geq 2$). En donnant des valeurs suffisamment grandes à k, préciser vers quelle limite semble tendre ce rapport lorsque k tend vers l'infini.

3. — Dans le système de numération décimal, quel peut être le chiffre des unités d'un entier premier ? Par quels chiffres de dizaine et d'unité peut se terminer un nombre premier ? Préciser le nombre de possibilités. Pour un entier $n \geq 1$ on note $N_i(n)$ le nombre d'apparitions du i ($1 \leq i \leq 9$) comme chiffre des unités dans les entiers premiers inférieurs ou égaux à n, et $f_i(n) = \frac{N_i(n)}{\pi(n)}$ la fréquence relative d'apparition du i. On note $N_{ji}(n)$ le nombre d'apparitions du $j (0 \leq j \leq 9)$ comme chiffre des dizaines, avec i ($1 \leq i \leq 9$) comme chiffre des unités dans les entiers premiers inférieurs ou égaux à n, et $f_{ji}(n) = \frac{N_{ji}(n)}{\pi(n)}$. Si tous les entiers i possibles, et tous les couples (j, i) sont également fréquents parmi les nombres premiers de $\mathbb{N}$, vers quelles valeurs tendent $f_i(n)$ et $f_{ji}(n)$ lorsque n tend vers l'infini ? Cette conjecture semble-t-elle confirmée par l'expérience ?

5. Conjecture de Goldbach. — *"Tout nombre entier pair supérieur à 3 peut s'écrire comme somme de deux nombres premiers."*

1. — A l'aide d'un programme en langage PASCAL, *vérifier* cette conjecture pour les entiers inférieurs à 100. Combien y a-t-il de décompositions possibles pour 10, 100, 200 ?

2. — Démontrer que tout entier supérieur à 12 est la somme de deux entiers composés.

6. Les nombres parfaits. — Un entier n positif est dit *parfait* si la somme des diviseurs de n, n non compris, est égale à n. Par exemple 28 est parfait :

$$1 + 2 + 4 + 7 + 14 = 28.$$

1. — On note $\sigma(n)$ la somme des diviseurs de n, par exemple

$$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$$

Ainsi n est parfait si $\sigma(n) = 2n$.

a) A l'aide d'un programme déterminer les nombres parfaits compris entre 1 et 1.000.

b) Déterminer la décomposition en facteurs premiers des nombres parfaits trouvés.

2. — On pose $u_n = 2^n - 1$.

a) Montrer que si u_n est premier, alors n est premier. Pour cela raisonner par l'absurde et utiliser l'identité : pour $k \geq 1$,

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + 1).$$

b) Pour étudier la réciproque on utilisera un programme qui déterminera, pour $2 \leq n \leq 15$, si le nombre u_n est premier.

c) Montrer que si u_n est premier alors $2^{n-1}u_n$ est parfait. Quels sont les nombres parfaits qui sont obtenus de cette façon ? $(2 \leq n \leq 15)$.

Remarque. — Les nombres premiers de la forme $u_n = 2^n - 1$ sont appelés *nombres premiers de Mersenne*. Il est démontré que tout nombre parfait pair s'obtient à partir d'un nombre premier de Mersenne comme en *2.c.* Mais on ne sait pas s'il existe une infinité de nombres premiers de Mersenne, s'il existe une infinité de nombres parfaits, s'il existe un nombre parfait impair.

3. — Deux nombres m et n sont dits *amis* si la somme des diviseurs de m, m non compris, est égale à n et si la somme des diviseurs de n, n non compris, est égale à m, c'est-à-dire si $\sigma(m) = m + n = \sigma(n)$. A l'aide d'un programme déterminer les nombres amis compris entre 1 et 1000.

Chapitre II

CONGRUENCES

1. Le théorème de Lagrange. — Soit H un sous-groupe d'un groupe G. La relation $\mathcal{R}$ définie sur G par

$$x\mathcal{R}y \iff x^{-1}y \in H$$

est une relation d'équivalence. En effet cette relation est

— réflexive : $\forall x \in G, x^{-1}x \in H$.

— symétrique : $\forall x, y \in G$, si $x^{-1}y \in H$ alors $y^{-1}x \in H$,

— transitive : $\forall x, y, z \in G$, si $x^{-1}y \in H$ et $y^{-1}z \in H$ alors $x^{-1}z \in H$.

La classe d'équivalence d'un élément a de G est, par définition, l'ensemble des éléments y de G tels que $a^{-1}y$ soit élément de H :

$$a^{-1}y = h \quad (h \in H).$$

C'est donc l'ensemble

$$aH = \{ah, \quad h \in H\}$$

appelé *classe à droite modulo* H. L'ensemble quotient est l'ensemble des classes à droite modulo H. Il est noté G/H.

Si E est un ensemble fini on note $\sharp E$ le nombre d'éléments de E. Supposons le groupe G fini, alors H est fini. Pour a fixé dans G, l'application

$$H \to aH$$
$$h \mapsto ah$$

est une bijection, donc $\sharp(aH) = \sharp H$: le nombre d'éléments de chacune des classes est égal au nombre d'éléments de H.

On appelle *ordre* de G le nombre $\sharp G$ d'éléments de G, *ordre* de H le nombre $\sharp H$ d'éléments de H, *indice de* H *dans* G le nombre de classes à droite modulo H, c'est à dire le nombre d'éléments de l'ensemble quotient G/H. On le note $G : H$, ainsi $G : H = \sharp(G/H)$.

Comme les classes définissent une partition de G, l'ordre de G est égal au produit de l'ordre de H par l'indice de H dans G.

$$\sharp G = (G : H)(\sharp H).$$

En conséquence nous pouvons énoncer :

THÉORÈME 1.1. — *Dans un groupe fini, l'ordre d'un sous-groupe divise l'ordre du groupe.*

Soient G et G' deux groupes dont les lois sont notées multiplicativement. Si f est une application de G dans G' telle que

$$\forall x, y \in G \qquad f(xy) = f(x)f(y),$$

on dit que f est un *homomorphisme* de G dans G'. On a alors

$$f(1_G) = 1_{G'}$$
$$f(x^{-1}) = f(x)^{-1}, \ \forall x \in G.$$

Par exemple les applications

$$\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times)$$
$$\ln : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$$

sont des homomorphismes.

Soit f un homomorphisme de groupes de G dans G'. L'ensemble $\operatorname{Ker} f = f^{-1}\{1_{G'}\}$, appelé *noyau* de f, est un sous-groupe de G. De même l'ensemble image $f(G)$ est un sous-groupe de G'. En effet, si $x, y \in \operatorname{Ker} f$, on vérifie qu'alors $xy^{-1} \in \operatorname{Ker} f$:

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)\Big(f(y)^{-1}\Big) = 1_{G'}.$$

Soit G un groupe, a un élément fixé dans G et soit f l'application de $\mathbb{Z}$ dans G et définie par $f(n) = a^n$. L'application f est un homomorphisme du groupe $(\mathbb{Z}, +)$ dans le groupe $(G, \times)$. Son noyau est un sous-groupe de $\mathbb{Z}$. Il est donc de la forme $m\mathbb{Z}$, où $m \in \mathbb{N}$. Supposons $m = 0$. On a alors

$$\operatorname{Ker} f = \{0\}$$

et f est une application injective. Ceci n'est possible que si G est infini. Si G est un groupe fini, on a nécessairement $m > 0$, et, pour un entier k,

$$a^k = 1_G \Longleftrightarrow k \in m\mathbb{Z}.$$

L'entier m est le plus petit entier strictement positif tel que $a^m = 1$; m est appelé l'*ordre* de a. Le sous-groupe image est le sous-groupe H engendré par a. Il est de la forme

$$H = \{1, a, a^2, \ldots, a^{m-1}\}.$$

L'ordre de H est m, et c'est aussi l'ordre de a. Ainsi on déduit du théorème précédent que m divise l'ordre de G. Ce résultat s'énonce:

Théorème 1.2 (Lagrange). — *Dans un groupe fini, l'ordre d'un élément divise l'ordre du groupe.*

Exemple. — L'ensemble $\mathfrak{S}_3$ des permutations de $\{1,2,3\}$ est un groupe pour la composition des permutations et $\sharp\mathfrak{S}_3 = 6$. Les valeurs possibles de l'ordre d'une permutation de $\mathfrak{S}_3$ sont 1.2.3 ou 6. Par exemple :

$$\text{ordre de } Id = 1 \ , \ \text{ordre de } \begin{pmatrix} 123 \\ 132 \end{pmatrix} = 2 \ , \ \text{ordre de } \begin{pmatrix} 123 \\ 231 \end{pmatrix} = 3.$$

2. Congruences. — Soit n un entier, $n \geq 2$. La relation $\mathcal{R}$ définie dans $\mathbb{Z}$ par

$$a\mathcal{R}b \Longleftrightarrow n \text{ divise } a-b$$

est une relation d'équivalence. On dit que a et b sont *congrus modulo* n et on écrit

$$a \equiv b \pmod{n}.$$

Cette relation d'équivalence est associée au sous-groupe $H = n\mathbb{Z}$ de $G = \mathbb{Z}$. L'ensemble quotient est noté $\mathbb{Z}/n\mathbb{Z}$. La classe d'un entier a est notée $\overline{a}$:

$$\overline{a} = \{b \in \mathbb{Z} \quad | \quad b \equiv a \ (\mathrm{mod} n)\}$$

et nous avons

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}, \ \sharp\, \mathbb{Z}/n\mathbb{Z} = n.$$

Par exemple l'heure est comptée dans $\mathbb{Z}/24\mathbb{Z}$ ou dans $\mathbb{Z}/12\mathbb{Z}$.

Proposition 2.1. — *Soit n un entier ≥ 2 et soient a, b, c, d des entiers tels que*

$$a \equiv b \pmod{n}, \ c \equiv d \pmod{n},$$

alors

$$a + c \equiv b + d \pmod{n}, \ ac \equiv bd \pmod{n}.$$

En effet si n divise $a-b$ et $c-d$, il divise leur somme $(a-b)+(c-d) = (a+c)-(b+d)$. De même n divise $(a-b)c$ et $b(c-d)$ et donc leur somme $ac-bd$. □

Cette proposition signifie que la relation d'équivalence $\mathcal{R}$ est compatible avec la structure d'anneau de $\mathbb{Z}$. Par suite en posant

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\overline{a}\ \overline{b} = \overline{ab}$$

on définit dans $\mathbb{Z}/n\mathbb{Z}$ une structure d'anneau. Cet anneau est commutatif et fini. De plus,

— $\overline{0}$ est élément neutre de l'addition,

— $(-\overline{a}) = \overline{-a}$,

— $\overline{1}$ est l'élément neutre pour la multiplication.

Voici les tables d'addition et de multiplication dans $\mathbb{Z}/n\mathbb{Z}$ pour $n = 6$ et $n = 5$:

Table d'addition de $\mathbb{Z}/6\mathbb{Z}$:

$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Table de multiplication de $\mathbb{Z}/6\mathbb{Z}$:

$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Table d'addition dans $\mathbb{Z}/5\mathbb{Z}$:

$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Table de multiplication dans $\mathbb{Z}/5\mathbb{Z}$:

$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

PROPOSITION 2.2. — *Soit n un entier ≥ 2. L'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour la multiplication, noté $(\mathbb{Z}/n\mathbb{Z})^*$.*

Par exemple les éléments inversibles de $\mathbb{Z}/6\mathbb{Z}$ sont $\overline{1}$ et $\overline{5}$: $(\mathbb{Z}/6\mathbb{Z})^* = \{\overline{1}, \overline{5}\}$, les éléments inversibles de $\mathbb{Z}/5\mathbb{Z}$ sont $\overline{1}, \overline{2}, \overline{3}$ et $\overline{4}$: $(\mathbb{Z}/5\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Pour démontrer la proposition 2.2 il suffit de remarquer que :

a) si $\overline{a}$ est inversible, alors son inverse $\overline{a}^{-1}$ est aussi inversible, d'inverse $\overline{a}$,

b) si $\overline{a}$ et $\overline{b}$ sont inversibles, d'inverses $\overline{a}^{-1}$ et $\overline{b}^{-1}$, alors $\overline{ab}$ est inversible, d'inverse $\overline{a}^{-1}\overline{b}^{-1}$. □

PROPOSITION 2.3. — *Dans $\mathbb{Z}/n\mathbb{Z}$, pour que $\overline{a}$ soit inversible, il faut et il suffit que a soit premier avec n.*

a) Si $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, il existe b dans $\mathbb{Z}$ tel que

$$\begin{aligned} ab &\equiv 1 (\text{mod } n) \\ ab &= 1 + kn \quad , \text{ où } k \in \mathbb{Z}, \\ ab - kn &= 1. \end{aligned}$$

D'après le théorème de Bézout, a et n sont alors premiers entre eux.

b) Réciproquement, si a et n sont premiers entre eux, il existe des entiers u et v tels que

$$\begin{aligned} au + nv &= 1. \\ au &\equiv 1 \ (\text{mod } n), \end{aligned}$$

et $\overline{u}$ est alors l'inverse de $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$. □

PROPOSITION 2.4. — *Si p est un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps.*

En effet, tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est alors inversible, et $(\mathbb{Z}/p\mathbb{Z})^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$. □

3. Systèmes de congruences. — Un système de congruence est un système d'équations de la forme

$$(S) \qquad \begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

THÉORÈME 3.1 (THÉORÈME DU RESTE CHINOIS). — *Soient m et n deux entiers premiers entre eux $(m, n \geq 2)$. Pour tout couple (a, b) d'entiers, le système (S) admet des solutions entières. Deux solutions quelconques diffèrent d'un multiple de mn.*

Nous donnons deux démonstrations de ce théorème.

Première démonstration. — Soit f l'application naturelle de $\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, telle que

$$f(x) = (\overline{a}, \overline{b})$$

si et seulement si

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

L'application f est un homomorphisme d'anneaux. Son noyau $f^{-1}\{(\overline{0}, \overline{0})\}$ est l'ensemble des entiers à la fois multiples de m et de n, c'est donc $mn\mathbb{Z}$. Soit g l'application naturelle de $\mathbb{Z}$ dans $\mathbb{Z}/mn\mathbb{Z}$, telle que

$$g(x) = \overline{c} \text{ si et seulement si } x \equiv c \pmod{mn}.$$

L'application g est un homomorphisme d'anneaux. Elle est surjective. De plus, pour deux entiers x et x' quelconques,

$$f(x) = f(x') \text{ si et seulement si } g(x) = g(x').$$

On peut donc définir une application $h : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, telle que, pour $\overline{c}$ dans $\mathbb{Z}/mn\mathbb{Z}$, $h(\overline{c}) = (\overline{a}, \overline{b})$ si et seulement si $\overline{c} = g(x)$ et $(\overline{a}, \overline{b}) = f(x)$, $x \in \mathbb{Z}$, c'est à dire que $f = h \circ g$. L'application h est un homomorphisme d'anneau, elle est injective. Puisque les ensembles $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ont le même nombre d'éléments, à savoir mn, cette application h est bijective. Il en résulte que l'application f est surjective. Le théorème du reste chinois est ainsi démontré.

Deuxième démonstration. — La démonstration précédente n'est pas constructive. Par contre la démonstration qui suit fournit un algorithme pour le calcul des solutions.

3. Systèmes de congruences

a) Etant donnés des entiers m et n premiers entre eux, il existe, d'après le théorème de BÉZOUT, des entiers u et v tels que

$$mu + nv = 1.$$

Alors

$$mu(a-b) + nv(a-b) = a - b$$

et

$$b + nv(a-b) = a + mu(b-a).$$

En posant

$$v(a-b) = k, \quad u(b-a) = h \quad \text{et} \quad x = a + hm = b + kn,$$

on peut écrire

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

b) Soient x et x' deux solutions du système de congruence (S).

$$\begin{aligned} x \equiv & a \pmod{m}, \quad x' \equiv a \pmod{m} \\ x \equiv & b \pmod{n}, \quad x' \equiv b \pmod{n} \end{aligned}$$

Alors

$$x - x' = 0 \pmod{m} \text{ et } x - x' \equiv 0 \pmod{n}$$

Le théorème de GAUSS montre qu'alors

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

c) *Les solutions du système de congruence* (S) *sont donc de la forme*

$$x = x_0 + kmn$$

où x_0 *est une solution particulière et* k *un entier quelconque.*

On peut remarquer que, si u et v sont des entiers tels que

$$mu + nv = 1.$$

alors le nombre

$$x_0 = bmu + anv$$

est une solution particulière du système, car

$$nv \equiv 1 \pmod{m},$$
$$x_0 \equiv avn \pmod{m} \equiv a \pmod{m}.$$

De même

$$x_0 \equiv b \pmod{n}.$$

Remarque. — A l'origine la résolution de systèmes de congruences est liée à des problèmes de calendrier du type suivant : à supposer que les mois aient tous 30 jours et sachant que le 1$^{\text{er}}$ janvier est un lundi, quels sont les vendredi 13 ?

Exemple. — Résolution du système de congruence :

$$(S) \qquad \begin{aligned} x &\equiv 1 \pmod{9} \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

Les entiers 9 et 7 sont premiers entre eux, le système admet donc des solutions entières. De plus, l'identité de Bézout

$$9u + 7v = 1$$

est vérifiée pour $u = -3$ et $v = 4$. Le nombre

$$x_0 = 2 \times 9 \times (-3) + 7 \times 4 = -26$$

est donc une solution particulière du système. Les solutions de (S) sont de la forme

$$x = 63k - 26, \quad \text{où } k \in \mathbb{Z}.$$

4. Indicatrice d'Euler. — Soit n un entier ($n \geq 2$). On appelle *indicatrice d'Euler*, et on note $\varphi(n)$, le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$:

$$\varphi(n) = \sharp(\mathbb{Z}/n\mathbb{Z})^*.$$

Par convention, on pose $\varphi(1) = 1$. Par exemple, $\varphi(6) = 2$, $\varphi(5) = 4$. Lorsque p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps,

$$(\mathbb{Z}/p\mathbb{Z})^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\},$$

donc $\varphi(p) \equiv p - 1$.

THÉORÈME 4.1 (EULER). — *Soient n un entier $n \geq 2$ et a un entier premier avec n. Alors*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Il suffit d'appliquer le théorème de LAGRANGE au groupe $G(\mathbb{Z}/n\mathbb{Z})^*$: l'entier a étant premier avec n, $\overline{a}$ est élément de $(\mathbb{Z}/n\mathbb{Z})^*$, et son ordre d divise $\varphi(n)$, ordre de $(\mathbb{Z}/n\mathbb{Z})^*$.

$$\varphi(n) = dk, \quad \text{avec} \quad k \in \mathbb{N}^*.$$

D'où

$$a^{\varphi(n)} = (a^d)^k \equiv 1 \pmod{n}.$$

THÉORÈME 4.2 (FERMAT). — *Soit p un nombre premier, et a un entier quelconque. Alors*

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

a) Supposons que a ne soit pas divisible par p. Alors a est premier avec p et, d'après le théorème d'EULER,

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

D'où

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

b) Supposons que a soit divisible par p. Alors

$$a^p \equiv a \equiv 0 \pmod{p}.$$

L'énoncé est donc vérifié pour tout a entier.

THÉORÈME 4.3. — *L'indicatrice d'Euler est multiplicative dans le sens suivant : si m et n sont deux entiers premiers entre eux, $(m, n \geq 2)$, alors*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

En effet, dans la première démonstration du théorème chinois nous avons défini un isomorphisme d'anneau h de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Par restriction on en déduit un isomorphisme de groupe $\overline{h}$ de $(\mathbb{Z}/mn\mathbb{Z})^*$ sur $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. Par conséquent les groupes $(\mathbb{Z}/mn\mathbb{Z})^*$ et $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ ont le même nombre d'éléments :

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Proposition 4.4. — *Si p est un nombre premier, et α un entier ($\alpha \geq 1$),*

$$\varphi(p^\alpha) = (p-1)p^{\alpha-1}.$$

Soit p un nombre premier. Si $\alpha = 1$, on sait que $\mathbb{Z}/p\mathbb{Z}$ est un corps et $\varphi(p) = p - 1$. Si $\alpha \geq 2$,

$$\mathbb{Z}/p^\alpha\mathbb{Z} = \{\overline{1}, \overline{2}, \ldots, \overline{p}, \overline{p+1}, \ldots, \overline{2p}, \overline{2p+1}, \ldots, \overline{p^\alpha - p}, \ldots, \overline{p^\alpha - 1}\}$$

. Les éléments non inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$ sont les multiples de $\overline{p}$:

$$\overline{0}, \overline{p}, \overline{2p}, \ldots, \overline{p^\alpha - p} = \overline{p(p^{\alpha-1} - 1)}.$$

Leur nombre est $p^{\alpha-1}$. Donc

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}.$$

□

Corollaire 4.5. — *Si la décomposition en facteurs premiers d'un entier n s'écrit*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

alors

$$\begin{aligned}\varphi(n) &= (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} \ldots (p_k - 1)p_k^{a_k - 1}, \\ &= n \prod_{p|n} (1 - \frac{1}{p})\end{aligned}$$

D'après le théorème

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \ldots \varphi(p_k^{a_k}),$$

et, d'après la proposition,

$$\varphi(p_i^{\alpha_i}) = (p_i - 1)p_i^{\alpha_i - 1} \qquad i \in [1, k]$$

d'où le résultat :

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1)p_i^{a_i - 1} = \prod_{i=1}^{k} p_i^{\alpha_i}(1 - \frac{1}{p_i}) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

□

Exemples. —
— Si $n \in \mathbb{N}^*$, $\varphi(2^n) = 2^{n-1}$.
— $816 = 2^4 \times 3 \times 17$ d'où $\varphi(816) = 2^3 \times 2 \times 16 = 256$.

EXERCICES

(Exercices sur la section 1)

1 . — On rappelle qu'un groupe fini G est *cyclique* s'il existe un élément x pour lequel

$$G = \{1, x, x^2, \ldots, x^{n-1}\};$$

x est *générateur* de G et n est son *ordre*. Soient G un groupe cyclique d'ordre n, et K un groupe cyclique d'ordre m, les entiers m et n étant premiers entre eux. Montrer que $G \times K$ est un groupe cyclique d'ordre mn.

2 . — On pose $G_n = \{z \in \mathbb{C}, z^n = 1\}$. Muni de la multiplication, l'ensemble G_n est un groupe isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$. Les éléments de G_n s'écrivent :

$$z_k = e^{i2\pi\frac{k}{n}} = \cos 2\pi\frac{k}{n} + i \sin 2\pi\frac{k}{n}, \quad k = 0, 1, \ldots n-1.$$

Les nombres z_k sont appelés *racines n-ièmes de l'unité.*

a) On suppose que $n = 12$. Quels sont les ordres des éléments z_8, z_9, z_{10} ?

b) Expliquer comment, en général, on détermine l'ordre de z_k, élément de G_n. On suppose que $n = 255$. Quel est l'ordre de z_{105} ?

c) Une racine n-ième de l'unité est dite *primitive* si son ordre est égal à n. Supposons que $n = 12$. Quelles sont les racines primitives ?

d) Soient m et n deux entiers positifs premiers entre eux. Soient α une racine primitive, élément du groupe G_m,et β une racine primitive, élément du groupe G_n. Montrer que le produit $\gamma = \alpha\beta$ est une racine primitive, élément du groupe G_{mn}. (On montrera par exemple que, si $\gamma^k = 1$, alors α^k appartient à G_n, et ensuite que m divise k.)

(Exercices sur la section 2)

3 . — Démontrer les propriétés suivantes des congruences où a, b, c, d, m, n sont des entiers $(m, n \geq 2)$.

a) Si $a \equiv b \pmod{m}$ et $c \equiv d \pmod{m}$ alors $a + c \equiv b + d \pmod{m}$.

b) Si $a \equiv b \pmod{m}$ et $c \equiv d \pmod{m}$ alors $ac \equiv bd \pmod{m}$.

c) Si $ac \equiv bc \pmod{m}$ et $(m, c) = 1$ alors $a \equiv b \pmod{m}$.

d) Si $ac \equiv bc \pmod{mc}$ alors $a \equiv b \pmod{m}$ $(c \neq 0)$.

e) Si m divise n et $a \equiv b \pmod{n}$ alors $a \equiv b \pmod{m}$.

f) Si $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$ et $(m, n) = 1$ alors $a \equiv b \pmod{mn}$.

4 . — Déterminer le reste de la division de 247^{349} par 7.

5 . — Déterminer le reste de la division de 2^{1137} par 17, le reste de la division de 2^{1137} par 13, et en déduire le reste de la division de 2^{1137} par 221.

6 . — Déterminer les inverses de 4 et 9 dans le groupe multiplicatif $(\mathbb{Z}/13\mathbb{Z})^*$, puis montrer que $2^{70} + 3^{70}$ est divisible par 13.

7 . — Démontrer que :
a) $5^4 \times 2^{28} \equiv 1 \pmod{641}$.
b) $5^4 \equiv -2^4 \pmod{641}$.
c) 641 divise $2^{32} + 1$.

8 . — Pour un entier $n \geq 0$ on note F_n le nombre $2^{2^n} + 1$.
a) Montrer que si un entier q divise F_n, l'ordre de 2 dans le groupe $(\mathbb{Z}/q\mathbb{Z})^*$ est égal à 2^{n+1}.
b) Montrer que tout diviseur premier de F_n est congru à 1 modulo 2^{n+1}.

9 . — Le but de cet exercice est de montrer que le seul entier n impair qui divise $3^n + 1$ est égal à 1. Soit n un entier impair strictement supérieur à 1 tel que n divise $3^n + 1$.
a) Montrer que n ne peut pas être premier.
b) Soit p le plus petit diviseur premier de n.
(i) Montrer que $p > 3$.
(ii) Soit δ l'ordre de 3 dans dans $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer que δ divise $p - 1$ et $2n$. Montrer que si δ est impair il est égal à 1, et que si δ est pair il est égal à 2. En déduire une impossibilité et conclure.

10 . — Soit G un groupe commutatif fini. Soit x un élément de G d'ordre m et y un élément de G d'ordre n.
a) Montrer que l'ordre de xy divise le PPCM de m et n.
b) On suppose que $(m, n) = 1$. Montrer que xy est d'ordre mn et que le sous-groupe engendré par xy contient x et y.
c) Montrer que dans le groupe additif $\mathbb{Z}/24\mathbb{Z}$ on peut trouver des éléments x et y d'ordre 12 tels que $x + y$ soit d'ordre 2, 3 ou 6.

11 . — Soit p un nombre premier. Montrer que pour tout entier q, $1 \leq q \leq p - 1$, l'entier C_p^q est un multiple de p. En déduire que, pour des entiers a et b quelconques,

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Montrer que, si $b^p \equiv b \pmod{p}$, alors $(b+1)^p \equiv b+1 \pmod{p}$. En déduire le théorème de FERMAT, énoncé p. 37. Montrer que, pour tout entier k positif et $p > 2$,

$$(1 + p)^{(p^k)} \equiv 1 + p^{k+1} \pmod{p^{k+2}}.$$

12 . — a) A quelle condition l'équation $ax + b = 0$ admet-elle des solutions dans $\mathbb{Z}/n\mathbb{Z}$? Comment obtient-on toutes les solutions ?

b) Résoudre l'équation $120x - 48 = 0$ dans $\mathbb{Z}/252\mathbb{Z}$.

c) Donner une condition nécessaire et suffisante sur m $(m \in \mathbb{N}^*)$, a et b $(a, b \in \mathbb{Z})$ pour que l'application $x \mapsto ax + b$ soit une bijection de $\mathbb{Z}/m\mathbb{Z}$ dans lui-même.

13 . — 1) Soit n un entier ≥ 1. Prouver que

$$n^5 \equiv n \pmod{10}.$$

Montrer que, pour tout $k \geq 1$,

$$n^{k+4} \equiv n^k \pmod{10}. \tag{1}$$

On désigne par x_k le chiffre des unités de n^k. Déduire de la relation (1) que la suite $(x_k)_{k\geq 1}$ est périodique et que sa période p divise 4. Déterminer les valeurs de p et les suites $(x_k)_{k\geq 1}$ pour $n = 1, 2, 3, \ldots, 9$. Les résultats devront être présentés dans un tableau comme ci-dessous :

M	p	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
1									
2									
3									
4									
5									
6									
7									
8									
9									

2) Pour $k \geq 1$, entier, vérifier la congruence

$$(k + 20)^{k+20} \equiv k^k \pmod{10}. \tag{2}$$

a) En déduire que la suite $(y_k)_{k\geq 1}$ des chiffres des unités de k^k est périodique et que sa période divise 20.

b) Déterminer, en détaillant les calculs, y_{12}, y_{13}, y_{18}.

c) Calculer les y_k pour $1 \leq k \leq 20$; rassembler les résultats dans un tableau. Qu'en concluez-vous ?

3) On note z_k le chiffre des unités de $(k^k)^k$.

a) Montrer que la suite $(z_k)_{k\geq 1}$ est également périodique, de période divisant 20.

b) En utilisant les résultats du **2)** déterminer z_{12}, z_{13}, z_{18} et z_{19}.

c) Calculer tous les z_k pour $1 \leq k \leq 20$. Quelle est la période de la suite $(z_k)_{k\geq 1}$?

(Exercices sur la section 3)

14 . — Trouver toutes les solutions x dans $\mathbb{Z}$ des systèmes :

a) $x \equiv 4 \pmod 7$
$x \equiv 9 \pmod{11}$

b) $x \equiv 5 \pmod{12}$
$x \equiv 8 \pmod{15}$

15 . — Déterminer le plus petit multiple de 7 qui est égal à 1 modulo 2, 3, 4, 5 et 6.

16 . — Considérons les équations

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3}, \end{aligned}$$

où $(m_1, m_2) = (m_1, m_3) = (m_2, m_3) = 1$. Posons $M = m_1 m_2 m_3$. Montrer que l'entier $\frac{M}{m_i}$ est inversible modulo m_i pour $i = 1, 2, 3$. Soit alors

$$c_i = \left(\frac{M}{m_i}\right)^{-1} \pmod{m_i}, \quad i = 1, 2, 3.$$

Montrer que la somme à trois termes

$$x = \sum a_i \frac{M}{m_i} c_i$$

est une solution de (1). Montrer que deux solutions quelconques diffèrent d'un multiple de M. Trouver le plus petit entier $n > 0$ vérifiant $n \equiv 2 \pmod 3$, $n \equiv 3 \pmod 5$ et $n \equiv 2 \pmod 7$.

17 . — a) Résoudre dans $\mathbb{Z}$ les deux équations suivantes,

$$\begin{aligned} 7x &= 13 \pmod{16}, \\ 4x &= 5 \pmod{16}. \end{aligned}$$

b) Soit f l'application de $\mathbb{Z}$ dans $\mathbb{Z}/17\mathbb{Z}$ définie par

$$f(n) \equiv 3^n \pmod{17}.$$

Montrer que f est périodique. Quelle est sa période ?

c) Soit m, $1 \leq m \leq 16$. Montrer qu'il existe un entier unique n, $0 \leq n \leq 15$, vérifiant

$$3^n \equiv m \pmod{17}.$$

On notera g l'application qui à l'entier $m, 1 \leq m \leq 16$, fait correspondre l'entier n, $0 \leq n \leq 15$. Dresser le tableau des valeurs de g :

m	1	2	3	4	5	...	16
$g(m)$	0		1				

d) Démontrer les propriétés suivantes :

(i) Si $m = m_1 m_2 \pmod{17}$ alors $g(m) = g(m_1) + g(m_2) \pmod{16}$.

(ii) Soit $k \in \mathbb{Z}$, si $m' = m^k \pmod{17}$ alors $g(m') = kg(m) \pmod{16}$.

e) En utilisant la fonction g

calculer $15^{10} \pmod{17}$,

résoudre $X^7 = 12 \pmod{17}$,

résoudre $X^4 = 5 \pmod{17}$.

(Exercices sur la section 4)

18 . — On désigne par φ l'indicatrice d'Euler. Montrer que tout entier n est égal à la somme des $\varphi(d)$ où d parcourt l'ensemble des diviseurs de n.

19 . — Soient a et b deux entiers positifs premiers entre eux, u et v des entiers tels que $au + bv = 1$. Montrer que

$$u \equiv a^{\varphi(b)-1} \pmod{b}$$
$$v \equiv b^{\varphi(a)-1} \pmod{a}.$$

20 . — Soit p un nombre premier. Montrer que pour tout entier q, $1 \leq q \leq p-1$, l'entier C_p^q est un multiple de p. En déduire que, pour des entiers a et b quelconques,

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Montrer que, si $b^p \equiv b \pmod{p}$, alors $(b+1)^p \equiv b+1 \pmod{p}$. En déduire le théorème de FERMAT, énoncé p. 37. Montrer que, pour tout entier k positif et $p > 2$,

$$(1+p)^{(p^k)} \equiv 1 + p^{k+1} \pmod{p^{k+2}}.$$

21 . — a) Montrer que l'équation $ax+b = 0$ admet au plus une solution dans $\mathbb{Z}/p\mathbb{Z}$ si p est premier.

b) Montrer que l'équation $x^2 = a$ admet au plus deux solutions dans $\mathbb{Z}/p\mathbb{Z}$ si p est premier.

c) Résoudre les équations suivantes :

$$x^2 \equiv -1 \pmod{65},$$
$$x^2 \equiv -2, \pmod{33}.$$

d) Soit p un nombre premier. Montrer par récurrence sur n que l'équation

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0,$$

dont les coefficients sont des éléments de $\mathbb{Z}/p\mathbb{Z}$, admet au plus n solutions dans $\mathbb{Z}/p\mathbb{Z}$.

e) On suppose que p est premier et que d divise $p-1$. Montrer que l'équation

$$x^d = 1$$

admet exactement d solutions dans $\mathbb{Z}/p\mathbb{Z}$. (Utiliser le théorème d'EULER.) Que se passe-t-il si d ne divise pas $p-1$?

22 . — Soit p un nombre premier.

a) Soit a un élément d'ordre d dans le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ Montrer que l'ensemble

$$M = \{1, a, \ldots, a^{d-1}\}$$

contient tous les éléments d'ordre d de $(\mathbb{Z}/p\mathbb{Z})^*$. (Utiliser la partie d) de l'exercice précédent.) En déduire qu'il y a au plus $\varphi(d)$ éléments d'ordre d dans $(\mathbb{Z}/p\mathbb{Z})^*$.

b) Déduire de l'exercice 18 que si d divise $p-1$, il y a exactement $\varphi(d)$ éléments d'ordre d dans $(\mathbb{Z}/p\mathbb{Z})^*$.

TRAVAUX PRATIQUES

1. Racines carrées de l'unité. — On dit qu'un élément a de $\mathbb{Z}/n\mathbb{Z}$ est une *racine carrée* de 1 si

$$a^2 = 1 \text{ dans } \mathbb{Z}/n\mathbb{Z},$$

et on note R_n l'ensemble des racines carrées de 1 dans $\mathbb{Z}/n\mathbb{Z}$.

1. — Démontrer que R_n est un sous-groupe du groupe $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

2. — Ecrire un programme qui calcule le nombre d'éléments de R_n et qui affiche les éléments de R_n (on demande que ce programme soit exécutable pour n assez grand, pour $n = 1000$ par exemple).

3. — On suppose n premier.

a) Conjecturer à l'aide de *2.*- la liste des éléments de R_n.

b) Démontrer cette conjecture et préciser le groupe bien connu isomorphe à R_n.

4. — On suppose que $n = p^m$, avec p premier et $p \neq 2$, m entier et $m \geq 2$.

a) Conjecturer la liste des éléments de R_n à l'aide de *2.*-.

b) Démontrer cette conjecture par récurrence sur m, en utilisant la remarque :

$$x^2 \equiv 1 (\text{mod } p^m) \Longrightarrow x^2 \equiv 1 (\text{mod } p^{m-1}).$$

Préciser le groupe bien connu isomorphe à R_n.

5. — On suppose que $n = 2^m$. m entier et $m \geq 2$.

a) Conjecturer à l'aide de *2.*- le nombre d'éléments de R_n.

b) Démontrer la conjecture pour $n = 4$. Préciser le groupe bien connu isomorphe à R_4.

c) Vérifier que :

$$(2^m - 1) \equiv 1 (\text{mod } 2^{m+1}) \text{ et } (2^m + 1)^2 \equiv 1 (\text{mod } 2^{m+1}).$$

d) Démontrer la conjecture pour $n = 8$, puis par récurrence sur m pour $n = 2^m$. (On utilisera la remarque de *4* b.)

e) Ecrire la table de multiplication du groupe R_{2^m} $(m > 2)$ et celle du groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Les comparer.

6. — Soient n et m deux entiers premiers entre eux.

a) Conjecturer une relation entre le nombre d'éléments de R_n, R_m et R_{nm}.

b) Soit f l'application de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ qui à x associe le couple (a, b) où a est la classe de x dans $\mathbb{Z}/n\mathbb{Z}$ et b est la classe de x dans $\mathbb{Z}/m\mathbb{Z}$.

Montrer que si $x^2 \equiv 1 (\mathrm{mod}\ mn)$ alors a appartient à R_n et b appartient à R_m.

Si (a, b) appartient à $R_n \times R_m$, déterminer l'ensemble des $x \in \mathbb{Z}$ tels que $f(x) = (a, b)$.

En déduire une bijection de R_{nm} sur $R_n \times R_m$. Montrer que cette bijection est un isomorphisme de groupes.

La conjecture est-elle démontrée ?

c) Exemple : Soit $n = 5^{10}$ et $m = 3$. Déterminer les éléments de R_{nm}. (On les exprimera à l'aide des puissances de 5.)

7. — Soit n un entier quelconque ($n \geq 2$).

a) Calculer le nombre d'éléments de R_n en fonction du nombre de facteurs premiers et de la puissance de 2 intervenant dans la décomposition en facteurs premiers de n.

b) Vérifier ce résultat en utilisant le programme écrit en *2.-* et une procédure calculant les éléments de la décomposition en facteurs premiers de n intervenant dans la formule ci-dessus.

c) Démontrer que R_n est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^{\alpha(n)}$ où l'on précisera la valeur de l'entier $\alpha(n)$.

2. Cryptographie. — La cryptographie (du grec *kruptos*, caché, et *graphein*, écriture) est la science du codage et du déchiffrement des messages codés. L'arithmétique de l'anneau $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo n fournit des systèmes de codage.

1. Codage par multiplication. — La méthode de codage utilise la multiplication modulo 26 par un entier inversible modulo 26. Il y a $\varphi(26) = 12$ entiers inversibles modulo 26.

Par exemple, soit à coder le message BONJOUR.

a) On remplace chaque lettre par son rang dans l'alphabet :

2 15 14 10 15 21 18.

b) On multiplie chacun des nombres par 7 modulo 26. Comme 7 est inversible modulo 26, la multiplication par 7 modulo 26 est une bijection de $\mathbb{Z}/26\mathbb{Z}$. On obtient

14 1 20 18 1 17 22.

Le nombre 7 est la clé de codage.

c) Pour décoder ce message on multiplie chacun des nombres par 15 qui est l'inverse de 7 modulo 26. Le nombre 15 est la clé de décodage.

Ecrire un programme qui vous dira si un entier h est inversible modulo n et qui calculera son inverse modulo n. Il s'agit essentiellement de l'algorithme d'Euclide.

2. Les chaînes de caractères. — Pour écrire un programme effectuant le codage et le décodage, on utilisera des variables de type STRING (chaîne de caractères), et certaines fonctions opérant sur ce type de variable : LENGTH, CONCAT, POS, COPY.

La déclaration d'une variable de type STRING se fait comme suit

var phrase:string[40];

Le nombre 40 indique le nombre maximum de caractères que la chaîne de caractères affectée à la variable dans le programme peut contenir. Ce nombre est limité à 80.

a) Ecrire le programme suivant

```
program western;
var phrase:string[40];
    l:integer;
BEGIN
phrase:='le train sifflera trois fois';
l:=length(phrase);
writeln(phrase);
write(L);
END.
```

Exécuter ce programme. LENGTH est une fonction d'une variable de type STRING à valeur de type INTEGER.

b) Modifier le programme comme suit

```
program western;
var phrase1,phrase2,phrase:string[40];
BEGIN
phrase1:='le train sifflera ';
phrase2:='trois fois';
phrase:=concat(phrase1,phrase2);
writeln(phrase1);
writeln(phrase2);
write(phrase);
END.
```

Exécuter ce programme. La fonction CONCAT assemble ou concatène deux, ou plus de deux chaînes de caractères, pour en faire une chaîne unique.

c) Modifier le programme comme suit

```
program western:
var phrase:string[40];
    p:integer;
BEGIN
phrase:='le train sifflera trois fois';
p:=pos('trois',phrase);
writeln(phrase);
write(p);
END.
```

Exécuter ce programme. La valeur retournée par POS est un entier qui indique la position de la première occurence de la chaîne 'TROIS' dans la chaîne PHRASE.

d) Modifier le programme comme suit

```
program western;
var phrase,partie:string[40];
BEGIN
phrase:='le train sifflera trois fois';
partie:=copy(phrase,10,8);
writeln(phrase);
write(partie);
END.
```

Exécuter ce programme. La valeur retournée par COPY est la sous-chaîne de la chaîne PHRASE commençant au 10^e caractère et de longueur 8 caractères.

Voici deux exemples de programmes qui seront utiles dans la suite

```
program alphanum;
const alpha='abcdefghijklmnopqrstuvwxyz';
var L:string[1];
    j:integer;
BEGIN
writeln('taper une lettre');
readln(L);
j:=pos(L,alpha);
write(j);
END.
```

```
program numalpha:
const alpha='abcdefghijklmnopqrstuvwxyz';
var j:integer;
    L:string[1];
BEGIN
writeln ('donner un nombre compris entre 1 et 26');
readln(j);
L:=copy(alpha,j,1);
write(L);
END.
```

3. Programme de codage par multiplication. — a) Ecrire un programme de codage par multiplication.

Entrées : la clé de codage (entier inversible modulo 26)
le message en clair (une chaîne de caractères, constituée d'un seul mot)
Sorties : le message chiffré (un tableau d'entiers, de 20 entiers par exemple)

b) Ecrire un programme de décodage.

Entrées : la clé de décodage,
le message chiffré
Sortie : le message en clair

c) Décoder le message suivant :

13 17 19 10 17 23 11 11 17 4 15

sachant que la clé de codage est 17.

Décoder le message suivant

14 3 24 3 12 16 3 1 23 16 7 9 23 16

sachant que la clé de codage est 11.

4. Codage par élévation à une puissance. — La méthode utilise l'élévation à une puissance modulo n.

Soit $\varphi(n)$ l'indicatrice d'Euler de n, et soit h un entier premier avec $\varphi(n)$. Il existe un entier k tel que

$$hk \equiv 1 \pmod{\varphi(n)}.$$

D'après le théorème d'Euler, si a est un entier premier avec n,

$$(a^h)^k \equiv a \pmod{n}.$$

Par exemple, soit à coder le message LA DIAGONALE DU FOU.

a) On remplace chaque lettre par son rang dans l'alphabet augmenté d'une unité de façon à réserver le chiffre 1 pour les espaces entre les mots. On obtient :

13 2 1 5 10 2 8 16 15 2 13 6 1 5 22 1 7 16 22.

b) Choisissons $n = 43$. Nous avons $\varphi(n) = 42$. Elevons chacun des nombres à la puissance $h = 5$ modulo 43. On obtient

31 32 1 29 25 32 2 21 38 32 31 36 1 29 39 1 37 21 39

Le nombre 43 est la première clé de codage, le nombre 5 est la seconde clé de codage.

c) Pour décoder ce message, on élève chacun des nombres à la puissance 17 modulo 43. En effet $5 \times 17 \equiv 1 \pmod{42}$. Les clés de décodage sont $n = 43$ et $k = 17$.

Ecrire un programme qui élève un entier a à la puissance h modulo n. On utilisera un développement binaire de h.

5. Programme de codage par élévation à une puissance. — a) Ecrire un programme de codage et un programme de décodage.

b) Décoder le message suivant :

62 41 1 3 41 24 71 54 41 24 1 42 41 21 24 25

sachant que les clés de codage sont 77 et 17.

Décoder le message suivant :

8 51 1 39 52 31 26 20 1 23 51 39 21

sachant que les clés de codage sont 55 et 33.

Décoder le message suivant :

5 61 59 54 1 48 26 1 13 32 59

sachant que les clés de codage sont 65 et 5.

Décoder le message suivant

29 20 29 6 19 6 23 11 1 5 20 19 4 23 16 10 6

sachant que les clés de codage sont 31 et 7.

On peut consulter

H. Lehning – D. Jakubowicz – *Mathématiques par l'informatique individuelle* - Masson, 1982. Tome 1.

M. Mignotte – *Cryptographie et arithmétique* – Revue du Palais de la Découverte – vol. 11, nov. 1982, p. 64-71.

3. Développement décimal des rationnels. — Le rationnel $\frac{13}{5}$ est un nombre décimal qui peut s'écrire 2,6. Le rationnel $\frac{31}{11}$ n'est pas un décimal, il peut s'écrire 2.818181...ou $2,\overline{81}$ pour exprimer que le développement illimité est périodique. De même, $\frac{21}{55} = 0,3\overline{81}$.

L'irrationnel π admet un développement décimal illimité non périodique

dont seulement quelques milliers de décimales sont connues.

1. Développements décimaux. — On dit qu'un nombre réel x est un *nombre décimal* s'il est égal au quotient d'un entier par une puissance de 10.

Démontrer qu'un nombre rationnel $\frac{p}{q}$, où p et q sont des entiers premiers entre eux, est un nombre décimal si et seulement si la décomposition en facteurs premiers de q ne comporte que des puissances de 2 et de 5.

On dit que le nombre réel x admet pour *développement décimal*

$$c_n \dots c_0, b_1 \dots b_j \dots,$$

si $c_n, \dots c_0, b_1, \dots, b_j \dots$ sont des chiffres du système décimal, c'est à dire $0, 1, 2, \dots 9$, et si la suite des nombres décimaux

$$x_m = \sum_{k=0}^{n} c_k 10^k + \sum_{j=1}^{m} b_j 10^{-j},$$

que l'on note $x_m = c_n \dots c_0, b_1 . b_m$ converge vers x quand m tend vers l'infini. Si les chiffres b_j ne sont pas tous nuls à partir d'un certain rang le développement décimal est dit *illimité.*

Montrer que tout nombre réel x admet un développement décimal.

Montrer que le nombre 1 admet deux développements décimaux distincts. Déterminer d'autres rationnels pour lesquels c'est le cas. Montrer que le développement décimal $c_n \dots c_0, b_1 \dots b_j \dots$ d'un nombre réel est déterminé de manière unique si on suppose de plus que tous les chiffres b_j ne sont pas égaux à 9 à partir d'un certain rang. Quels sont les nombres réels dont le développement décimal est déterminé de manière unique ?

2. Développements décimaux périodiques. — En effectuant les calculs "à la main" déterminer les développements décimaux des nombres rationnels ci-dessous

$$\frac{1}{7}, \frac{5}{7}, \frac{22}{7}, \frac{100}{7}, \frac{1}{70}, \frac{1}{14}, \frac{11}{35}, \frac{10}{7}$$

Soit $c_n \dots c_0, b_1 \dots b_j \dots$ le développement décimal du nombre réel x. S'il existe des entiers $\lambda \geq 1$ et $\mu \geq 0$ tels que

$$b_j = b_{j+\lambda},$$

pour $j \geq \mu + 1$, le développement décimal est dit *périodique.* Dans ce cas, après avoir posé $a_1 = b_{\mu+1}, \dots, a_\lambda = b_{\mu+\lambda}$, on note

$$x = c_n \dots c_0, b_1 \dots b_\mu \overline{a_1 \dots a_\lambda}.$$

Si λ est le plus petit entier possédant cette propriété on l'appelle la *longueur de la période*, et si $\mu = 0$, ou si $b_\mu = b_{\mu+\lambda}$, l'entier μ est la longueur de la *prépériode*. Par exemple l'écriture $0,38\overline{18} = 0,\overline{381}$ représente un développement décimal illimité dont la prépériode a pour longueur 1 et la période 2.

Soit $\frac{p}{q}$ un rationnel, où p et q sont des entiers premiers entre eux. Montrer que si $\frac{p}{q}$ n'est pas décimal il admet un développement décimal périodique illimité, qui s'obtient par une suite de divisions, et que la longueur λ de la période est strictement inférieure à q. Quelle la valeur de 10^λ modulo q ?

Ecrire une procédure *"développement"* qui, étant donné un nombre rationnel, décimal ou non, en donne un développement décimal sous la forme

$$c_n \dots c_0, b_1 \dots b_\mu \overline{a1 \dots a_\lambda},$$

et affiche les longueurs de la période et de la prépériode.

Soit $c_n \dots c_0, b_1 \dots b_\mu \overline{a_1 \dots a_\lambda}$ un développement décimal illimité périodique d'un nombre réel x. Démontrer que x est rationnel et s'écrit sous la forme

$$(*) \qquad x = C + \frac{B}{10^\mu} + \frac{A}{10^\mu(10^\lambda - 1)},$$

où A, B, C sont des entiers ≥ 0 vérifiant

$$0 < A < 10^\lambda - 1, \ B < 10^\mu.$$

Réciproquement montrer que si x est un nombre réel s'écrivant sous la forme $(*)$, il admet un développement périodique illimité qui a une période dont la longueur divise λ et une prépériode dont la longueur est inférieure ou égale à μ. Donner un exemple où la période (resp. la prépériode) a une longueur inférieure à λ (resp. μ).

Ecrire une procédure *"réduction"* qui affiche sous forme d'une fraction irréductible le rationnel dont le développement décimal périodique (illimité ou non) est donné.

3. Propriétés de la période et de la prépériode d'un développement décimal périodique. — En utilisant l'écriture $(*)$ montrer que si $\frac{p}{q}$ est une fraction irréductible représentant un nombre rationnel dont le développement décimal est de la forme $c_n \dots c_0, \overline{a_1 \dots a_\lambda}$, alors

$$10^\lambda \equiv 1 \pmod{q}$$

Soient q un entier > 1, premier avec 10, et λ l'ordre de 10 dans le groupe $(\mathbb{Z}/q\mathbb{Z})^*$. Montrer que toute fraction irréductible $\frac{p}{q}$ admet un

développement décimal périodique dont la période a pour longueur λ et dont la prépériode est de longueur 0.

On décompose l'entier $q > 1$ sous la forme $q = 2^a 5^b q_1$, où $q_1 > 1$ et est premier avec 10. Montrer que toute fraction irréductible $\frac{p}{q}$ admet un développement décimal périodique pour lequel on peut préciser en fonction des nombres q_1, a et b la longueur de la période et un majorant de la longueur de la prépériode.

Ecrire une procédure *"longueur"* qui, étant donné un entier q, affiche la longueur de la période d'un développement décimal d'une fraction irréductible $\frac{p}{q}$.

En employant, par exemple, l'instruction CASE OF et un *menu* écrire un programme permettant d'exécuter au choix l'une des trois procédures ci-dessus. L'exécuter dans un nombre suffisamment varié de cas pour, en particulier, vérifier la cohérence des longueurs obtenues par les procédures *"développement"* et *"longueur"*.

Chapitre III

FRACTIONS CONTINUES

1. Développement en fraction continue d'un nombre rationnel. Considérons à nouveau l'algorithme d'EUCLIDE que nous avons étudié dans la section 1 du chapitre I. Cet algorithme, qui permet le calcul du PGCD de deux nombres a et b, consiste en une suite de divisions euclidiennes. Par exemple, pour $a = 39$, $b = 14$.

$$\begin{aligned} 39 &= 2 \times 14 + 11 \\ 14 &= 1 \times 11 + 3 \\ 11 &= 3 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1 \end{aligned}$$

Ainsi nous pouvons écrire :

$$\begin{aligned} \frac{39}{14} &= 2 + \frac{11}{14} = 2 + \frac{1}{\frac{14}{11}} \\ &= 2 + \frac{1}{1 + \frac{3}{11}} = 2 + \frac{1}{1 + \frac{1}{\frac{11}{3}}} \\ &= 2 + \frac{1}{1 + \frac{1}{3 + \frac{2}{3}}} = 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{\frac{3}{2}}}} \end{aligned}$$

Finalement

$$\frac{39}{14} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{2}}}}$$

Cette formule permet de reconstituer la fraction $\frac{39}{14}$ à partir de la suite des quotients successifs 2,1,3,1,2.

Etudions les fractions obtenues à partir des suites $\{2\}$, $\{2,1\}$, $\{2,1,3\}$, $\{2,1,3,1\}$ et $\{2,1,3,1,2\}$:

$$\begin{aligned}
x_0 &= 2 && = 2\\
x_1 &= 2+\frac{1}{1} && = 3\\
x_2 &= 2+\cfrac{1}{1+\frac{1}{3}} && = \frac{11}{4} = 2,75\\
x_3 &= 2+\cfrac{1}{1+\cfrac{1}{3+1}} && = \frac{14}{5} = 2,8\\
x_4 &= \cdots && = \frac{39}{14} = 2,785\ldots
\end{aligned}$$

Nous observons que

$$x_0 < x_2 < x_4 < x_3 < x_1.$$

Un *développement en fraction continue* est une expression de la forme

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}$$

où a_0 est un entier relatif, $a_0 \in \mathbb{Z}$, et $a_1, \ldots, a_n$ sont des entiers positifs, $a_1, \ldots a_n \in \mathbb{N}^*$. On note $x = [a_0; a_1, \ldots, a_n]$. Deux questions se posent :

1) Etant donné un nombre rationnel $x = \frac{p}{q}$, comment développer ce nombre en fraction continue ? La question est de décrire un algorithme permettant le calcul de la fraction $\frac{p}{q}$.

2) Etant donnée la suite des nombres $a_0, \ldots a_n$, comment calculer le nombre rationnel x ? La question est de décrire un algorithme permettant le calcul de la fraction $\frac{p}{q}$.

La première question est résolue par l'algorithme d' EUCLIDE, *Algorithme (1)* :

$$\begin{aligned}
p &= a_0 q + r_0, && 0 < r_0 < q,\\
q &= a_1 r_0 + r_1, && 0 < r_1 < r_0,\\
&\cdots\\
r_{n-3} &= a_{n-1} r_{n-2} + r_{n-1}, && 0 < r_{n-1} < r_{n-2},\\
r_{n-2} &= a_n r_{n-1}. && r_n = 0.
\end{aligned}$$

Les nombres $a_0, a_1, \ldots, a_n$ sont les quotients successifs, appelés *quotients partiels*.

Programme. — Ceci donne en langage PASCAL :

```
program Fraction1;
var p,p1,p2,q,q1,q2,r,r1,r2,a :integer;
BEGIN
write('p=? '); readln(p);
write('q=? '); readln(q);
p1:=0; q1:=1; r1:=p;
p2:=1; q2:=0; r2:=q;
repeat
        a:=r1 div r2;
        p:=a*p2+p1;
        q:=a*q2+q1;
        r:=-a*r2+r1;
        p1:=p2; q1:=q2; r1:=r2;
        p2:=p; q2:=q; r2:=r;
        writeln(a:4,' ',p:4,' ',p/q:6:4);
until r=0;
END.
```

Si on entre les nombres $p = 789$ et $q = 543$, l'exécution de ce programme donne

a_k	p_k	q_k	x_k
1	1	1	1.0000
2	3	2	1.5000
4	13	9	1.4444
1	16	11	1.4545
4	77	53	1.4528
1	93	64	1.4531
2	263	181	1.4530

Pour répondre à la deuxième question considérons les nombres rationnels x_k, $0 \leq k \leq n$, définis par

$$x_0 = a_0,$$
$$x_1 = [a_0; a_1] = a_0 + \frac{1}{a_1},$$
$$x_2 = [a_0; a1, a2] = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}},$$
$$\dots$$
$$x_k = [a_0; a_1, \dots, a_k],$$
$$\dots$$
$$x_n = x = [a_0; a_1, \dots, a_n].$$

Nous avons

$$x_1 = \frac{a_1 a_0 + 1}{a_1},$$
$$x_2 = \frac{a_2(a_1 a_0 + 1) + a_0}{a_2 a_1 + 1}.$$

Algorithme (2) : Définissons les suites d'entiers p_k et q_k, $-2 \leq k \leq n$, par les données initiales

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

et les relations de récurrence, si $k \geq 0$,

$$p_k = a_k p_{k-1} + p_{k-2},$$
$$q_k = a_k q_{k-1} + q_{k-2}.$$

PROPOSITION 1.1. — *Pour* $0 \leq k \leq n$,

$$x_k = \frac{p_k}{q_k}.$$

Ces nombres s'appellent *fractions réduites* ou *réduites*.

Démonstration. — Démontrons la proposition par récurrence sur k. Nous venons de voir que la relation est vérifiée pour $k = 0, 1, 2$. Supposons qu'elle soit vraie pour k et montrons qu'elle est vraie pour $k+1$.

Remarquons que, si nous admettons que les nombres $a_0, \dots, a_n$ puissent prendre des valeurs rationnelles, nous pouvons écrire,

$$x_{k+1} = [a_0; a_1, \dots, a_{k-1}, a_k + \frac{1}{a_{k+1}}],$$
$$= [a_0; a_1, \dots, a_{k-1}, a'_k],$$

de telle sorte que, d'après l'hypothèse de récurrence,

$$x_{k+1} = \frac{p'_k}{q'_k}.$$

avec

$$p'_k = a'_k p_{k-1} + p_{k-2},$$
$$q'_k = a'_k q_{k-1} + q_{k-2}.$$

Ainsi

$$\begin{aligned} x_{k+1} &= \frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}}, \\ &= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}}, \\ &= \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}. \end{aligned}$$

La proposition est bien démontrée. □

Puisque $x = \frac{p_n}{q_n}$, l'algorithme (2) permet le calcul des réduites d'un nombre rationnel dont on connaît le développement en fraction continue.

Programme. — Ceci donne en langage PASCAL :

```
program Fraction2;
const n = 9;
var k, p, p1, p2, q, q1, q2 : integer;
    x : real;
    a : array[0..n] of integer;
BEGIN
writeln('entrer 10 nombres entiers');
for k := 0 to n do
        read(a[k]);
writeln;
p1 := 0; q1 := 1;
p2 := 1; q2 := 0;
for k := 0 to n do
begin
        p := a[k] * p2 + p1;
        p1 := p2; p2 := p;
        q := a[k] * q2 + q1;
        q1 := q2; q2 := q;
        x := p/q;
        writeln(k : 4,' ',p : 4,' ',q : 4,' ',x : 6 : 4);
end;
END.
```

Si on entre les nombres 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, l'exécution de ce programme donne

k	p_k	q_k	x_k
0	1	1	1.0000
1	2	1	2.0000
2	3	2	1.5000
3	5	3	1.6667
4	8	5	1.6000
5	13	8	1.6250
6	21	13	1.6154
7	34	21	1.6190
8	55	34	1.6176
9	89	55	1.6182

Dans la suite de cette section nous allons étudier quelques propriétés des réduites du développement en fraction continue d'un nombre rationnel.

PROPOSITION 1.2. — *Pour* $-1 \leq k \leq n$,

$$q_k p_{k-1} - p_k q_{k-1} = (-1)^k.$$

Démonstration. — Partons des relations, pour $0 \leq k \leq n$,

$$p_k = a_k p_{k-1} + p_{k-2},$$
$$q_k = a_k q_{k-1} + q_{k-2}.$$

Multiplions les deux membres de la première égalité par q_{k-1}, et ceux de la deuxième par p_{k-1}. Par soustraction nous obtenons

$$q_k p_{k-1} - p_k q_{k-1} = -(q_{k-1} p_{k-2} - p_{k-1} q_{k-2}).$$

Puisque $q_0 p_{-1} - p_0 q_{-1} = 1$, la proposition est ainsi démontrée par récurrence. □

COROLLAIRE 1.3. — *Les fractions réduites* $\frac{p_k}{q_k}$ *sont irréductibles.*

Remarque. — Soient p et q des entiers, $q \geq 1$. Considérons le développement en fraction continue de $x = \frac{p}{q}$. Alors

$$p = d p_n, \quad q = d q_n.$$

où d est le PGCD de p et q.

PROPOSITION 1.4. — *La suite $x_0, x_2, x_4, \ldots$ des réduites de rang pair est croissante, la suite $x_1, x_3, x_5, \ldots$ des réduites de rang impair est décroissante. De plus pour tout k, x_k est situé entre x_{k-2} et x_{k-1}.*

Cette proposition est une conséquence du lemme suivant :

LEMME 1.5. —

$$x_{k-1} - x_k = \frac{(-1)^k}{q_k q_{k-1}}. \tag{1}$$

$$x_k - x_{k-2} = (-1)^k \frac{a_k}{q_k q_{k-2}}. \tag{2}$$

Démonstration. — Nous avons déjà vu que

$$q_k p_{k-1} - p_k q_{k-1} = (-1)^k.$$

En divisant cette relation par $q_k q_{k-1}$ nous obtenons (1).
Nous avons

$$\begin{aligned} x_k - x_{k-2} &= \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - q_k p_{k-2}}{q_k q_{k-2}} \\ &= \frac{(a_k p_{k-1} + p_{k-2}) q_{k-2} - (a_k q_{k-1} + q_{k-2}) p_{k-2}}{q_k q_{k-2}} \\ &= (-1)^k \frac{a_k}{q_k q_{k-2}}. \end{aligned}$$

ce qui démontre (2). □

2. Développement en fraction continue d'un nombre réel. — Commençons par observer que la division euclidienne de deux entiers p et q

$$p = aq + r, 0 \leq r < q,$$

peut s'écrire

$$\begin{aligned} a &= [\frac{p}{q}] \\ \frac{r}{q} &= \{\frac{p}{q}\} = \frac{p}{q} - a. \end{aligned}$$

où, pour un nombre réel x, $[x]$ désigne la partie entière de x, et $\{x\}$ la partie "fractionnaire" :

$$x = [x] + \{x\}, [x] \in \mathbb{Z}, 0 \leq \{x\} < 1.$$

Nous pouvons récrire l'algorithme d'EUCLIDE en calculant le PGCD de p et q comme suit :

Etant donnés deux entiers p et q, $q \geq 1$, l'algorithme construit une suite $\alpha_0, \alpha_1, \ldots, \alpha_n$ de nombres rationnels et une suite $a_0, a_1, \ldots a_n$ de nombres entiers ; on pose

$$\alpha_0 = \frac{p}{q},$$

puis, pour $k = 0, 1, 2, \ldots$ on répète les opérations

$$a_k = [\alpha_k]$$
$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$$

tant que α_k n'est pas un entier:

Nous remarquons que, sous cette forme, l'algorithme se généralise au cas où le rationnel $\frac{p}{q}$ est remplacé par un nombre réel x.

Algorithme (3): on pose

$$\alpha_0 = x$$

puis, pour $k = 0, 1, 2, \ldots,$ on répète les opérations

$$a_k = [\alpha_k]$$
$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$$

tant que α_k n'est pas un entier.

PROPOSITION 2.1. — *L'algorithme précédent s'arrête au bout d'un nombre fini d'étapes si et seulement si le nombre x est rationnel.*

En effet si $x = \frac{p}{q}$ est un rationnel, nous avons vu que l'algorithme précédent n'est autre que l'algorithme d'EUCLIDE pour le calcul du PGCD de p et q. Réciproquement, si l'algorithme s'arrête au bout de n étapes,

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}$$

donc x est un nombre rationnel. □

Ainsi, si x est irrationnel, l'algorithme (3) construit une suite infinie d'entiers $a_0, a_1, \ldots, a_n, \ldots$, avec $a_n \geq 1$ si $n \geq 1$.

Exemple. — Prenons $x = \sqrt{3}$. alors

$$\begin{aligned}
a_0 &= [x] = 1 \\
\alpha_1 &= \frac{1}{x - [x]} = \frac{\sqrt{3}+1}{2} \\
a_1 &= [\alpha_1] = 1 \\
\alpha_2 &= \frac{1}{\alpha_1 - [\alpha_1]} = \frac{2}{\sqrt{3}-1} = \sqrt{3}+1 \\
a_2 &= [\alpha_2] = 2 \\
\alpha_3 &= \frac{1}{\alpha_3 - [\alpha_3]} = \frac{1}{\sqrt{3}-1} = \alpha_1.
\end{aligned}$$

Puisque $\alpha_3 = \alpha_1$, nous avons

$$a_3 = a_1,\ a_4 = a_2, \ldots,\ a_{k+2} = a_k.$$

La suite a_n est périodique de période 2 à partir de $n = 1$, c'est la suite suivante

$$1, 1, 2, 1, 2, 1, 2, 1, \ldots$$

Nous pouvons maintenant transposer dans le cadre des nombres réels les questions que nous nous sommes posées au sujet du développement en fractions continues des nombres rationnels.

Soit $a_0, a_1, \ldots, a_n, \ldots$ une suite d'entiers telle que $a_n \geq 1$ si $n \geq 1$. Nous lui associons la suite x_k des nombres rationnels définis par

$$x_k = [a_0; a_1, \ldots, a_k].$$

THÉROÈME 2.2. — *La suite x_k est convergente. Sa limite est un nombre irrationnel. Si la suite a_n est celle qui est construite par l'algorithme* (3) *à partir d'un nombre irrationnel x, alors*

$$\lim_{k \to \infty} x_k = x.$$

D'après la relation (2) du lemme 1.4 la suite x_{2k} est croissante, et la suite $x_{2\ell+1}$ est décroissante. On déduit de plus de la relation (1) de ce lemme que pour tous k et ℓ

$$x_{2k} < x_{2\ell+1}.$$

Ainsi la suite x_{2k} est croissante et majorée donc convergente, de même la suite $x_{2\ell+1}$ est décroissante et minorée donc converge aussi. Montrons

que ces deux suites ont même limite. D'après la relation (1) du lemme 1.4,

$$x_{2k+1} - x_{2k} = \frac{1}{q_{2k}q_{2k+1}}.$$

Des relations

$$q_0 = 1\ , q_1 = a_1,\ q_k = a_k q_{k-1} + q_{k-2},$$

on déduit que $q_k > k$. Par suite

$$\lim_{k-\infty}(x_{2k+1} - x_{2k}) = 0,$$

ce qui montre bien que les deux suites ont même limite.

Pour montrer que x est irrationnel raisonnons par l'absurde : supposons que $x = \frac{p}{q}$, p et q entiers, $q \geq 1$. Nous avons

$$x - x_{2k} < \frac{1}{q_{2k}q_{2k+1}},$$

d'où

$$pq_{2k} - qp_{2k} < \frac{q}{q_{2k+1}}.$$

Le premier nombre est un entier > 0, et pour k assez grand le deuxième membre est < 1, d'où la contradiction.

Soit x un nombre irrationnel et soient a_n et α_n les suites construites par l'algorithme (3) à partir de x. Si nous autorisons que les quotients partiels puissent prendre des valeurs réelles, nous pouvons écrire

$$x = [a_0; a_1, \ldots, a_n, \alpha_{n+1}],$$

si bien que

$$x = \frac{p_n\alpha_{n+1} + q_{n-1}}{q_n\alpha_{n+1} + q_{n-1}},$$

donc

$$\begin{aligned} x - x_n &= \frac{p_n\alpha_{n+1} + p_{n-1}}{q_n\alpha_{n+1} + q_{n-1}} - \frac{p_n}{q_n} \\ &= \frac{p_{n-1}q_n - q_{n-1}p_n}{(q_n\alpha_{n+1} + q_{n-1})q_n} = \frac{(-1)^n}{(q_n\alpha_{n+1} + q_{n-1})q_n} \end{aligned}$$

et

$$|x - x_n| < \frac{1}{q_{n+1}q_n},$$

puisque $\alpha_n > a_n$. □

Nous noterons

$$x = [a_0; a_1, \ldots, a_n, \ldots]$$

PROPOSITION 2.3. — *Soient deux suites* $(a_0, a_1, \ldots)$ *et* $(b_0, b_1, \ldots b_n, \ldots)$ *telles que*

$$[a_0; a_1, \ldots a_n, \ldots] = [b_0; b_1, \ldots b_n, \ldots].$$

Alors, pour tout $n, a_n = b_n$.

Démonstration. — Posons

$$x = [a_0; a_1, \ldots, a_n, \ldots] = [b_2; b_1, \ldots b_n, \ldots].$$

Nous allons démontrer la proposition par récurrence :

$$x_0 = a_0, \ x_1 = a_0 + \frac{1}{a_1},$$

donc

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

et a_0 est la partie entière de x, donc $a_0 = b_0$. Supposons que $a_0 = b_0$, $a_1 = b_1, \ldots, a_n = b_n$. Nous avons

$$x = \frac{p_n \alpha_{n+1} + p_{n-1}}{q_n \alpha_{n+1} + q_{n-1}} = \frac{p_n \beta_{n+1} + p_{n-1}}{q_n \beta_{n+1} + q_{n-1}},$$

avec $\alpha_{n+1} = [a_{n+1}; a_{n+2}, \ldots]$, $\beta_{n+1} = [b_{n+1}; b_{n+2}, \ldots]$, donc $\alpha_{n+1} = \beta_{n+1}$, et par suite $a_{n+1} = b_{n+1}$. □

Programme. — Le programme suivant exécute l'algorithme (3).

```
program Fraction3;
const eps = 0.00001;
var a, p, p1, p2, q, q1, q2 : integer;
    x, y, z : real;
BEGIN
write('x =?'); readln(x);
p1 := 0; q1 := 1;
p2 := 1; q2 := 0;
y := x;
repeat
        a := trunc(y);
        p := a * p2 + p1;
        p1 := p2; p2 := p;
        q := a * q2 + q1;
        q1 := q2; q2 := q;
        z := p/q;
        writeln(a : 4,' ',p : 4,' ',q : 4,' ',z : 6 : 4);
        if y <> a then y := 1/(y - a);
until abs(x - z) <= eps;
END.
```

Si on entre le nombre $x = 2.7182818$. l'exécution de ce programme donne

a_k	p_k	q_k	x_k
2	2	1	2.0000
1	3	1	3.0000
2	8	3	2.6667
1	11	4	2.7500
1	19	7	27143
4	87	32	2.7188
1	106	39	2.7179
1	193	71	2.7183
6	1264	465	2.7183

En conclusion nous avons montré que l'application qui à une suite d'entiers $(a_0, a_1, \ldots, a_n, \ldots)$, associe le nombre $x = [a_0; a_1, \ldots, a_n, \ldots]$ est une bijection des suites d'entiers a_n telles que $a_n \geq 1$ si $n \geq 1$ sur l'ensemble des nombres irrationnels.

3. Fractions continues périodiques. — Nous avons déjà remarqué que le développement en fraction continue de $\sqrt{3}$ est périodique,

$$\sqrt{3} = [1; 1, 2, 1, 2, \ldots]$$

Il en est de même du développement en fraction continue du nombre d'or,

$$\frac{1+\sqrt{5}}{2} = [1; 1, 1, 1, \ldots].$$

Nous dirons que la suite a_n est périodique s'il existe des entiers m et k tels que, pour $n \geq m$,

$$a_{n+k} = a_n.$$

Nous noterons

$$[a_0; a_1, a_2, \ldots, a_{m-1}, \overline{a_m, \ldots, a_{m+k-1}}]$$

Par exemple

$$\sqrt{7} = [2; \overline{1, 1, 1, 4}].$$

Le théorème suivant, dû à Lagrange, nous dit quels sont les nombres qui ont un développement en fraction continue périodique.

THÉORÈME 3.1. — *Le développement en fraction continue d'un nombre irrationnel α est périodique si et seulement si α est un irrationnel quadratique, c'est-à-dire si et seulement si α est irrationnel et est racine d'une équation du second degré à coefficients entiers,*

$$A\alpha^2 + B\alpha + C = 0. \quad A, B, C \in \mathbb{Z}.$$

Démonstration.

(a) Soit α un nombre irrationnel dont le développement en fraction continue est périodique,

$$\alpha = [a_0; a_1, \ldots, a_{m-1}, \overline{a_m, \ldots, a_{m+k-1}}]$$

Posons

$$\alpha_n = [a_n; a_{n+1}, \ldots],$$

et rappelons que

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$$

avec les notations des sections précédentes. Supposons d'abord que $m = 0$, alors $\alpha_k = \alpha$, et donc

$$\alpha = \frac{\alpha p_{k-1} + p_{k-2}}{\alpha q_{k-1} + q_{k-2}},$$

par suite α est racine de l'équation

$$q_{k-1}\alpha^2 + (q_{k-2} - p_{k-1})\alpha - p_{k-2} = 0,$$

Supposons maintenant $m > 0$. D'après ce qui précède α_m est racine d'une équation du second degré à coefficients entiers,

$$A\alpha_m^2 + B\alpha_m + C = 0, \quad A, B, C \in \mathbb{Z}.$$

Or

$$\alpha = \frac{\alpha_m p_{m-1} + p_{m-2}}{\alpha_m q_{m-1} + q_{m-2}},$$

ou

$$\alpha_m = \frac{\alpha q_{m-1} - p_{m-1}}{-\alpha q_{m-2} + p_{m-2}}.$$

Il en résulte que α est aussi racine d'une équation du second degré à coefficients entiers.

(b) Supposons que α soit racine d'une équation du second degré à coefficients entiers,

$$f(\alpha) = 0$$

avec

$$f(x) = Ax^2 + Bx + C,$$

où A, B, C sont des entiers, $A > 0$, $\Delta = B^2 - 4AC$ est positif et n'est pas un carré parfait.

Nous supposons d'abord que $C < 0$. L'équation $f(x) = 0$ admet deux racines de signes contraires. Nous supposons aussi que α est positif. Construisons le développement en fraction continue de α à l'aide de l'algorithme (3). Nous avons $a_0 = [\alpha]$, c'est-à-dire

$$a_0 = \sup\{u \in \mathbb{N} |\ f(u) < 0\},$$
$$\alpha_1 = \frac{1}{\alpha - a_0}.$$

donc $f(a_0 + \frac{1}{\alpha_1}) = 0$, c'est-à-dire que α_1 est racine de l'équation

$$(Aa_0^2 + Ba_0 + C)x^2 + (2Aa_0 + B)x + A = 0.$$

Posons

$$\begin{aligned} A_1 &= -(Aa_0^2 + Ba_0 + C), \\ B_1 &= -(2Aa_0 + B), \\ C_1 &= -A, \\ f_1(x) &= A_1x^2 + B_1x + C_1. \end{aligned}$$

Nous avons $A_1 > 0, C_1 < 0$, et α_1 est la racine positive de l'équation $f_1(x) = 0$, par suite

$$a_1 = [\alpha_1] = \sup\{u \in \mathbb{N} | f_1(u) < 0\}.$$

Calculons le discriminant de f_1 :

$$\begin{aligned} \Delta_1 &= B_1^2 - 4A_1C_1 \\ &= (2Aa_0 + B)^2 - 4(Aa_0^2 + Ba_0 + C)A \\ &= B^2 - 4AC = \Delta. \end{aligned}$$

En itérant la construction précédente nous obtenons une suite f_n de trinômes du second degré,

$$f_n(x) = A_nx^2 + B_nx + C_n,$$

vérifiant $A_n > 0$, $C_n < 0$, $\Delta_n = \Delta$.

Le nombre α_n est la racine positive de $f_n(x) = 0$, et

$$a_n = \sup\{u \in \mathbb{N} |\ f_n(u) < 0\}.$$

De plus, de l'égalité

$$B_n^2 - 4A_nC_n = \Delta$$

on déduit que

$$|B_n| \leq \sqrt{\Delta},\ 0 \leq A_n \leq \frac{1}{4}\Delta,\ -\frac{1}{4}\Delta \leq C_n \leq 0.$$

Les valeurs possibles des entiers A_n, B_n, C_n sont donc en nombre fini. Par suite, il existe des entiers m et k tels que pour $n \geq m$,

$$f_{n+k} = f_n.$$

et donc aussi

$$a_{n+k} = a_n.$$

(c) Il nous reste à montrer qu'on peut se ramener au cas où $\alpha > 0$ et $C < 0$. Considérons l'ensemble $\mathbb{Q}[\sqrt{\Delta}]$ des nombres réels de la forme $a + b\sqrt{\Delta}$, où a et b sont des rationnels. $\mathbb{Q}[\sqrt{\Delta}]$ est un sous-corps de $\mathbb{R}$. Le conjugué d'un nombre $x = a + b\sqrt{\Delta}$ est le nombre $x^* = a - b\sqrt{\Delta}$. Pour deux nombres x et y de $\mathbb{Q}[\sqrt{\Delta}]$ nous avons

$$(x+y)^* = x^* + y^*,$$
$$(xy)^* = x^* y^*,$$

et, si $x \neq 0$,

$$(\frac{1}{x})^* = \frac{1}{x^*}.$$

Nous avons

$$\alpha_n = \frac{\alpha q_{n-1} - p_{n-1}}{-\alpha q_{n-2} + p_{n-2}},$$

si bien que, pour tout n, α_n est un élément de $\mathbb{Q}[\sqrt{\Delta}]$, et

$$\begin{aligned} \alpha_n^* &= \frac{\alpha^* q_{n-1} - p_{n-1}}{-\alpha^* q_{n-2} + p_{n-2}} \\ &= -\frac{q_{n-1}}{q_{n-2}} \frac{\alpha^* - x_{n-1}}{\alpha^* - x_{n-2}}, \end{aligned}$$

où x_n désigne la n-ième réduite de α, et puisque la limite de x_n est α,

$$\lim_{n \to \infty} \alpha_n^* \frac{q_{n-2}}{q_{n-1}} = -1.$$

Il existe donc un entier N à partir duquel $\alpha_n^* < 0$. Pour un tel $n \geq 1$, $\alpha_n > 0$, et, les racines de l'équation $f_n(x) = 0$ étant α_n et α_n^*,

$$C = \alpha_n \alpha_n^* < 0.$$

Ainsi nous pouvons appliquer les résultats du (b) à α_n : le développement en fraction continue de α_n est périodique. Or

$$\alpha_n = [a_n; a_{n+1}, \ldots],$$

donc le développement en fraction continue de α est également périodique.

4. Approximations rationnelles des nombres réels. — Les fractions réduites x_m d'un nombre irrationnel x sont de bonnes approximations rationnelles du nombre réel x. Précisons d'abord ce que nous

entendons par bonne approximation. Un nombre rationnel $\frac{p}{q}, q \geq 1$, est appelé *bonne approximation rationnelle* du nombre réel x si

$$\forall \frac{a}{b} \in \mathbb{Q}, 1 \leq b \leq q, |x - \frac{p}{q}| \leq |x - \frac{a}{b}|.$$

Avant de montrer que les fractions réduites sont de bonnes approximations rationnelles nous allons établir quelques propriétés d'approximation de ces réduites.

PROPOSITIONS 4.1. — *Soit $x_n = \frac{p_n}{q_n}$ la suite des réduites d'un nombre réel x, alors*

(i) $$|x - x_n| < |x - x_{n-1}|$$

(ii) $$\frac{1}{q_n(q_{n+1} + q_n)} < |x - x_n| < \frac{1}{q_n q_{n+1}}$$

Démonstration. — Soit $x = [a_0; a_1, a_2, \ldots]$ le développement en fraction continue du nombre x. Posons $\alpha_{n+1} = [a_{n+1}; a_{n+2}, \ldots]$. Nous pouvons écrire $x = [a_0; a_1, \ldots, a_n, \alpha_{n+1}]$, et par suite

$$x = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}.$$

De cette égalité on déduit

$$x - \frac{p_n}{q_n} = \left(-\frac{q_{n-1}}{\alpha_{n+1} q_n}\right)\left(x - \frac{p_{n-1}}{q_{n-1}}\right).$$

Puisque $\alpha_{n+1} > 1$, $q_n > q_{n-1}$, l'inégalité (i) s'ensuit.
On en déduit aussi que

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(q_n \alpha_{n+1} + q_{n-1})}$$

car $p_{n-1} q_n - q_{n-1} p_n = (-1)^n$ (Proposition 1.2). Puisque

$$a_n < \alpha_{n+1} < a_{n+1},$$

nous avons

$$q_{n+1} < q_n \alpha_{n+1} + q_{n-1} < q_n + q_{n+1},$$

et l'inégalité (ii) s'ensuit. □

THÉORÈME 4.2. — *Soit x un nombre réel. Les fractions réduites de x sont de bonnes approximations rationnelles de x.*

LEMME 4.3. — *Soit* $\frac{a}{b}, b \geq 1$, *un rationnel compris entre* x_{n-1} *et* x_n, *alors* $b \geq q_n + q_{n-1}$.

Démonstration. — Supposons n impair (pour n pair la démonstration est analogue), nous avons alors

$$\frac{p_{n-1}}{q_{n-1}} < \frac{a}{b} < \frac{p_n}{q_n}.$$

Par suite $aq_{n-1} - bp_{n-1} > 0$, et puisque c'est un entier,

$$aq_{n-1} - bp_{n-1} \geq 1. \tag{1}$$

Pour la même raison,

$$bp_n - aq_n \geq 1. \tag{2}$$

Multiplions (1) par q_n et (2) par q_{n-1}. En ajoutant les inégalités obtenues,

$$b(p_n q_{n-1} - q_n p_{n-1}) \geq q_n + q_{n-1},$$

et, puisque $p_n q_{n-1} - q_n p_{n-1} = 1$ (Proposition 1.2), $b \geq q_n + q_{n-1}$. □

Démontrons maintenant le théorème 4.2. Montrons que $x_n = \frac{p_n}{q_n}$ est une bonne approximation rationnelle de x. Soit en effet $y = \frac{a}{b}, b \geq 1$, un rationnel tel que

$$|x - y| < |x - x_n|.$$

D'après l'inégalité (i) de la proposition 4.1, y est compris entre x_{n-1} et x_n, et, d'après le lemme 4.3, $b \geq q_n + q_{n-1}$, donc $b > q_n$. □

Exemples. — Pour $x = \pi$, nous avons

$$\pi = [3; 7, 15, 1, \ldots],$$
$$\frac{p_1}{q_1} = \frac{22}{7}, \frac{p_2}{q_2} = \frac{333}{106},$$

donc $\frac{22}{7}$ et $\frac{333}{106}$ sont de bonnes approximations rationnelles de π.

La réciproque du théorème 4.2 est fausse. En effet $\frac{13}{4}$ est une bonne approximation de π mais n'est pas une réduite. On peut cependant énoncer une réciproque à condition de modifier la définition de bonne approximation. Nous dirons qu'un nombre rationnel $\frac{p}{q}, q \geq 1$, est une *approximation économique* (ou bonne approximation de deuxième espèce) du nombre réel x si,

$$\forall \frac{a}{b} \in \mathbb{Q}, 1 \leq b \leq q, |qx - p| \leq |bx - a|.$$

On vérifie qu'une approximation économique de x est une bonne approximation de x.

THÉORÈME 4.4. — *Les approximations économiques d'un nombre irrationnel x sont les fractions réduites de x.*

Démonstration.

(a) Soit $\frac{p}{q}$ une approximation économique du nombre irrationnel x. Soit $x = [a_0; a_1, a_2, \ldots]$ le développement en fraction continue de x. En prenant $a = a_0, b = 1$, nous obtenons

$$|qx - p| \leq |x - a_0|,$$

et par suite

$$|x - \frac{p}{q}| \leq |x - a_0|,$$

dont on déduit que $\frac{p}{q} \geq a_0 = x_0$.

Supposons $\frac{p}{q} \neq \frac{p_1}{q_1}$. Puisque $x - a_0 < \frac{1}{a_1}$, et $q_1 = a_1$, nous avons $|pq_1 - qp_1| \geq 1$ et

$$|qx - p| < \frac{1}{a_1} \leq \frac{|pq_1 - qp_1|}{q_1},$$
$$|x - \frac{p}{q}| < |\frac{p}{q} - \frac{p_1}{q_1}|$$

donc $\frac{p}{q} \leq x_1$. Finalement nous avons montré

$$x_0 \leq \frac{p}{q} \leq x_1.$$

Raisonnons maintenant par l'absurde : supposons que pour tout entier $n \geq 0$, $\frac{p}{q} \neq \frac{p_n}{q_n}$. Il existe alors un entier n tel que $\frac{p}{q}$ soit compris entre x_{n-1} et x_{n+1}, et d'après le lemme 4.3, $q > q_n$. Comme nous avons ou bien $x_{n-1} < \frac{p}{q} < x_{n+1} < x < x_n$, ou bien $x_n < x < x_{n+1} < \frac{p}{q} < x_{n-1}$, alors

$$|x - \frac{p}{q}| \geq |\frac{p_{n+1}}{q_{n+1}} - \frac{p}{q}| \geq \frac{1}{q\, q_{n+1}}$$

et

$$|qx - p| \geq \frac{1}{q_{n+1}}.$$

D'autre part, d'après l'inégalité (ii) de la proposition 4.1,

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

On en déduit que

$$|q_n x - p_n| < |qx - p|,$$

et comme $q_n < q$, ceci contredit le fait que $\frac{p}{q}$ est une approximation économique de x.

(b) Fixons n et considérons le minimum de $|qx - p|$, pour $p \in \mathbb{Z}$, et $1 \leq q \leq q_n$. Ce minimum existe (et est unique car x est irrationnel). Il est atteint en (a, b) et $\frac{a}{b}$ est donc une approximation économique de x. D'après (a) c'est une réduite : $\frac{a}{b} = \frac{p_k}{q_k}$, avec $k \leq n$. Nous voulons montrer que $k = n$. D'après l'inégalité (ii) de la proposition 4.1,

$$|q_k x - p_k| > \frac{1}{q_k + q_{k+1}},$$
$$|q_n x - p_n| < \frac{1}{q_{n+1}},$$

donc $q_k + q_{k+1} > q_{n+1}$, ce qui implique que $k = n$. □

EXERCICES

(exercices sur la section 1)

1 . — Déterminer le développement en fraction continue de $\frac{163}{59}$, et en calculer les réduites.

2 . — Calculer le nombre rationnel $x = [3; 6, 1, 7]$.

3 . — Soit $x = [a_0; a_1, \ldots, a_n]$, $a_0 \geq 1$, le développement en fraction continue du nombre rationnel x. On note $x_k = \frac{p_k}{q_k}$ les fractions réduites. Quel est le développement en fraction continue de $\frac{p_n}{p_{n-1}}$? (Utiliser la relation

$$\frac{p_n}{p_{n-1}} = a_n + \frac{1}{\frac{p_{n-1}}{p_{n-2}}} \; .)$$

(exercices sur la section 2)

4 . — Calculer le développement en fraction continue de $x = \sqrt{2}$, $x = \sqrt{5}$.

5 . — Calculer les 4 premiers termes du développement en fraction continue de π, et calculer les réduites x_0, x_1, x_2, x_3.

6 . — On démontre que

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots].$$

Calculer les réduites x_0, x_1, x_2, x_3. Comparer les valeurs obtenues aux premiers termes de la suite

$$y_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}.$$

7 . — Soit $x = [a_0; a_1, \ldots, a_n \ldots]$ le développement en fraction continue d'un nombre irrationnel $x \neq 0$.

a) Quel est le développement en fraction continue de $\frac{1}{x}$? Quelle relation existe-t-il entre les réduites de x et celles de $\frac{1}{x}$?

b) Quel est le développement en fraction continue de $-x$? (On distinguera deux cas suivant que $a_1 > 1$ ou $a_1 = 1$.)

(exercises sur la section 3)

8 . — Calculer les développements en fraction continue des nombres suivants

$$\sqrt{7},\ \sqrt{11},\ \sqrt{23},\ \sqrt{47},\ \sqrt{59},\ \sqrt{94},$$
$$\frac{1+\sqrt{3}}{2},\ \frac{14+\sqrt{37}}{3},\ \frac{13-\sqrt{2}}{7}.$$

9 . — Quels sont les nombres dont les développements en fraction continue sont

$$[2;1,\overline{5}],\ [2;\overline{1,5}],\ [\overline{2;1,5}]\ ?$$

10 . — Soit a un entier positif. Déterminer le développement en fraction continue de $\sqrt{a^2+1}$.

11 . — Quels sont les nombres dont le développement en fraction continue est périodique de période 1 ?

TRAVAUX PRATIQUES

1. Approximations rationnelles des nombres réels. — Soit x un nombre réel. Un nombre rationnel $\frac{p}{q}$, $q \geq 1$, est appelé *bonne approximation rationnelle* de x si

$$\forall \frac{a}{b} \in \mathbb{Q},\ 1 \leq b \leq q,\ |x - \frac{p}{q}| \leq |x - \frac{a}{b}|.$$

1. — Ecrire un programme fournissant les bonnes approximations rationnelles $\frac{p}{q}$ d'un nombre réel x, pour $q \leq 200$. Les résultats devront s'aficher dans un tableau à 4 colonnes correspondant à $p, q, \frac{p}{q}, |x - \frac{p}{q}|$.

Exécuter le programme pour $x = \frac{\sqrt{5}-1}{2}$, $x = \sqrt{7}$, $x = \pi$. Observer la suite des nombres p, et la suite des nombres q obtenus.

2. — Ecrire un programme produisant les réduites $\frac{p_k}{q_k}$ du développement en fraction continue du nombre réel x jusqu'au rang n, le plus petit entier tel que

$$|x - \frac{p_n}{q_n}| \leq 10^{-4}.$$

Exécuter le programme pour $x = \frac{\sqrt{5}-1}{2}$, $x = \sqrt{7}$, et $x = \pi$.

Utiliser les programmes précédents pour conjecturer les réponses aux questions suivantes :

(a) Les réduites sont-elles de bonnes approximations rationnelles ?

(b) Les bonnes approximations rationnelles sont-elles des réduites ?

3. — Quelles sont les bonnes approximations rationnelles $\frac{p}{q}$ du nombre π vérifiant

$$3 < \frac{p}{q} < \frac{333}{106} \ ?$$

On vérifiera que les points correspondants de coordonnées $(p;q)$ sont alignés, situés sur le segment de droite d'extrémités (3;1) et (333;106) et que l'on passe d'un point au suivant par une translation de vecteur (22;7).

4. — On propose de montrer que si $\frac{p}{q}$ est une bonne approximation rationnelle du nombre x compris entre les fractions réduites $\frac{p_n}{q_n}$ et $\frac{p_{n+2}}{p_{n+2}}$, alors

$$\frac{p}{q} = \frac{ap_{n+1} + p_n}{aq_{n+1} + q_n}.$$

où a est un entier vérifiant $0 < a < a_{n+2}$. Supposons n pair et soit $y = \frac{p}{q}$ une bonne approximation rationnelle de x située entre les fractions

réduites x_n et x_{n+2}. Soit f la fonction définie pour $t \geq 0$ par

$$f(t) = \frac{tp_{n+1} + p_n}{tq_{n+1} + q_n}.$$

On pose $y_k = f(k)$, $k \in \mathbb{N}$. Montrer que f est croissante et qu'il existe un nombre réel t, $0 < t < a_{n+2}$, tel que $f(t) = y$. Si t n'est pas un entier on pose $r = [t]$ (partie entière de t). Montrer alors que

$$x_n < y_r < y < y_{r+1} < x_{n+2} \leq x.$$

De l'inégalité

$$y - y_r < y_{r+1} - y_r,$$

déduire que $q > (r+1)q_{n+1} + q_n$, et montrer que cela contredit le fait que y est une bonne approximation rationnelle de x.

5. — Un nombre rationnel $\frac{p}{q}$, $q \geq 1$, est une *approximation rationnelle économique* d'un nombre réel x si

$$\forall \frac{a}{b} \in \mathbb{Q},\ 1 \leq b \leq q,\ |qx - p| \geq |bx - a|.$$

Ecrire un programme produisant les approximations économiques d'un nombre réel x, pour $q \leq 200$.

Observer les résultats sur plusieurs exemples. Enoncer une conjecture.

2. Développement en fraction continue de la racine d'une équation du troisième degré. — Soit P un polynôme du troisième degré à coefficients entiers. On suppose que

(i) $P(0) > 0$,

(ii) la fonction polynôme associée à P est strictement croissante sur $\mathbb{R}$.

L'équation

$$P(x) = 0$$

admet une racine unique α qui est strictement positive. On note a_0 la partie entière de α, c'est le plus grand entier tel que $P(a_0) \leq 0$.

1. — Ecrire une procédure (1) qui, étant donnés les quatre coefficients de P, détermine a_0.

2. — Montrer que $\alpha_1 = \frac{1}{\alpha - a_0}$ est racine du polynôme P_1 défini par

$$P_1(x) = -x^3 P(a_0 + \frac{1}{x}),$$

et que le polynôme P_1 vérifie aussi les propriétés (i) et (ii). Ecrire une procédure (2) qui calcule les coefficients du polynôme P_1 à partir de ceux du polynôme P.

3. — On construit ainsi une suite de polynômes P_1, P_2,...,P_n,... vérifiant (i) et (ii). Montrer que la procédure (1) appliquée au polynôme P_n détermine le n-ième coefficient a_n du développement en fraction continue de la racine α de P.

4. — Ecrire un programme qui calcule avec une précision donnée la racine d'un polynôme du troisième degré vérifiant (i) et (ii), et qui affiche les coefficients a_n du développement en fraction continue de cette racine, ainsi que les réduites correspondantes.

Calculer les dix premiers termes du développement en fraction continue de $\sqrt[3]{2}$.

3. Développement en fraction continue de $\sqrt{d}$. — Soit

$$ax^2 + bx + c = 0$$

une équation du second degré à coefficients entiers. On suppose que $\Delta = b^2 - 4ac$ est positif, n'est pas un carré parfait et que c est négatif. On note α la racine positive de cette équation.

1. — En utilisant l'algorithme décrit dans la section 3, écrire un programme qui calcule le développement en fraction continue de α.

Compléter ce programme de façon à obtenir la prépériode et la période de ce développement,

$$\alpha = [a_0; a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+p-1}}].$$

2. — Soit d un entier positif qui n'est pas un carré parfait. Utiliser le programme précédent pour le calcul du développement en fraction continue de $\sqrt{d}$. Exécuter ce calcul pour $200 \leq d \leq 250$. Observer les résultats. Comparer a_{k-1} et $a_{k+p-1-j}$ pour $j = 1, \ldots, [\frac{p}{2}]$. Enoncer des conjectures.

Chapitre IV

POLYNÔMES

1. L'anneau $K[X]$. — Soit K un corps commutatif (par exemple $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ avec p premier). Un polynôme à coefficients dans K est une expression

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n,$$

c'est à dire la donnée d'une suite d'éléments de K, nuls à partir d'un certain rang :

$$P = (a_0, a_1, \ldots, a_n, 0, 0, \ldots).$$

L'ensemble $K[X]$ des polynômes à coefficients dans K est muni des opérations suivantes :

a) *Addition* : si P et Q sont deux polynômes,

$$P(X) = a_0 + a_1 X + \cdots + a_p X^p,$$
$$Q(X) = b_0 + b_1 X + \cdots + b_q X^q,$$

leur somme $P + Q$ est égale à

$$(P + Q)(X) = c_0 + c_1 X + \cdots + c_m X^m,$$

avec $c_k = a_k + b_k$, $m = \max(p, q)$.

b) *Multiplication* : le produit des polynômes P et Q est égal à

$$PQ(X) = d_0 + d_1 X + \cdots + d_m X^n,$$

avec

$$d_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i},$$

et $n = pq$.

L'ensemble $K[X]$ est ainsi muni d'une structure d'anneau commutatif. Cet anneau est de plus unitaire (la constante 1 est l'élément neutre pour la multiplication), et intègre (si le produit PQ de deux polynômes P et Q est nul, $PQ = 0$, soit $P = 0$, soit $Q = 0$). On dit aussi que l'anneau $K[X]$ n'a pas de diviseur de zéro.

Si

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n,$$

avec $a_n \neq 0$, alors n est appelé le *degré* de P, on note $\deg P = n$. Le degré du polynôme nul n'est pas défini. L'expression "$\deg P \leq n$" signifie soit que $P \neq 0$ et $\deg P \leq n$, soit que $P = 0$. Avec cette convention

$$\deg(P + Q) \leq \max(\deg P, \deg Q),$$

et si P et Q ne sont pas nuls

$$\deg(PQ) = \deg P + \deg Q.$$

Les éléments inversibles de l'anneau $K[X]$ sont les polynômes de degré 0, c'est à dire les constantes non nulles.

A un polynôme P,

$$P(X) = a_0 + a_1 + \cdots + a_n X^n,$$

on associe une *fonction polynôme* : c'est l'application de K dans K définie par

$$x \mapsto P(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

Nous avons

$$(P + Q)(x) = P(x) + Q(x),$$
$$(PQ)(x) = P(x)Q(x).$$

Supposons que le corps K soit infini ($K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, par exemple). Si pour tout x de K, $P(x) = 0$, nous verrons qu'alors $P = 0$, c'est à dire que tous les coefficients de P sont nuls. Ce n'est pas vrai en général si K est fini. En effet, si $K = \mathbb{Z}/p\mathbb{Z}$ avec p premier, et si $P(X) = X^p - X$, alors, pour tout x de K, $P(x) = 0$. C'est précisément le théorème de FERMAT (cf. Ch. II, théorème 4.2) :

$$\forall x \in \mathbb{Z},\ x^p \equiv x \pmod{p}.$$

Etudions comment calculer la valeur numérique d'un polynôme à l'aide de l'*algorithme de Horner*. Soit à calculer

$$P(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

Le calcul brutal de cette expression nécessite

$$1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2}$$

multiplications et n additions. Cette expression peut être transformée comme suit

$$P(x) = a_0 + x\Big(a_1 + x\big(\cdots + x(a_{n-1} + xa_n)\cdots\big)\Big).$$

Sous cette forme son calcul nécessite n multiplications et n additions. De plus cette méthode de calcul évite, lorsque n et x sont grands, $P(x)$ petit, des sommes algébriques de termes très grands. L'algorithme de HORNER peut être exécuté comme suit : on pose

$$\begin{aligned} b_n &= a_n, \\ b_{n-1} &= b_n x + a_{n-1}, \\ &\vdots \\ b_k &= b_{k+1}x + a_k, \\ &\vdots \\ b_0 &= b_1 x + a_0, \end{aligned}$$

et alors $P(x) = b_0$.

2. Division des polynômes, plus grand commun diviseur. Soit K un corps commutatif, et soit $K[X]$ l'anneau des polynômes à coefficients dans K. Il existe dans $K[X]$ une *division* appelée *division euclidienne*, ou *division suivant les puissances croissantes.*

THÉORÈME 2.1. — *Soient A et B deux polynômes de $K[X]$, B étant non nul. Il existe deux polynômes Q et R uniques tels que*

$$A = BQ + R, \ \deg R < \deg B.$$

Q est le quotient, R le reste de la division de A par B.

Démonstration.
a) Démontrons d'abord l'unicité. Supposons que

$$A = BQ_1 + R_1 = BQ_2 + R_2,$$

avec $\deg R_1 < \deg B$, $\deg B_2 < \deg B$. Si $Q = Q_2 - Q_1$, $R = R_1 - R_2$, nous avons

$$BQ = R.$$

Si $Q \neq 0$, $\deg BQ \geq \deg B$, or $\deg R < \deg B$, donc $Q = 0$ et $R = 0$.

b) Montrons maintenant l'existence. Posons

$$A(X) = a_0 + a_1 X + \cdots + a_n X^n,$$
$$B(X) = b_0 + b_1 X + \cdots + b_p X^p,$$

avec $b_p \neq 0$. Si $\deg A < \deg B$, alors $Q = 0$ et $R = A$ conviennent. Supposons $\deg A \geq \deg B$ $(n \geq p)$, et posons

$$A_1(X) = A(X) - \frac{a_n}{b_p} X^{n-p} B(X) = A(X) - Q_1(X)B(X).$$

Si $\deg A_1 < \deg B$, alors $Q = Q_1$ et $R = A_1$ conviennent. Sinon on recommence avec A_1 à la place de A,

$$A_2 = A_1 - Q_2 B, \ \deg A_2 < \deg A_1.$$

A chaque opération le degré de A_k diminue au moins d'une unité. On s'arrête lorsque $\deg A_k < \deg B$. Alors

$$Q = Q_1 + Q_2 + \cdots + Q_k, \ R = A_k,$$

conviennent. □

Remarque. — Lorsqu'on divise un polynôme P par le polynôme $X - \alpha$, $\alpha \in K$, le reste est la constante $R = P(\alpha)$. La division euclidienne de P par $X - \alpha$ fournit un algorithme pour le calcul de $P(\alpha)$ qui n'est autre que l'algorithme de HORNER.

Programme. — Le programme suivant exécute la division euclidienne.

```
program Division-polynomes;
const  n=5;
type   polynome=record
          deg:integer;
          coef:array[0..n] of real;
       end;
var    d,e,j,k,p:integer;
       a,b,q:polynome;

procedure lecture(var s:polynome);
var d,j:integer;
begin
       write('quel est le degré ?');
       readln(d); s.deg:=d;
       writeln('quels sont les coefficients ?');
       for j:=0 to d do
       begin
              write('coef',j:2,'=?');
              readln(s.coef[j]);
       end;
end;
BEGIN
writeln('saisie du dividende'); lecture(a);
writeln('saisie du diviseur'); lecture(b);
d := b.deg; e := a.deg−b.deg; q.deg:= e;
for k:=e downto 0 do
begin
       q.coef[k] := a.coef[d + k]/b.coef[d];
       for j := n downto k do
       a.coef[j] := a.coef[j] − q.coef[k] * b.coef[j − k];
end;
for j := 0 to (d − 1) do
       writeln('r[', j : 1,'] =', a.coef[j] : 4 : 2,' ');
writeln;
for j := 0 to e do
       writeln('q[', j : 1,'] =', q.coef[j] : 4 : 2,' ');
END.
```

Exemple.

$$\begin{aligned} A(X) &= X^6 + 2X^5 + 5X^4 + 7X^3 + X^2 + 3X + 5, \\ B(X) &= X^3 + 5X + 3, \\ Q(X) &= X^3 + 2X^2 - 6, \\ R(X) &= -5X^2 + 33X + 23. \end{aligned}$$

Soient P et Q deux polynômes non nuls. *le polynôme Q divise le polynôme P* ou *Q est un diviseur de P* signifie qu'il existe un polynôme A tel que $P = AQ$. Remarquons que les constantes non nulles divisent tout polynôme. Si Q divise P, alors $\deg Q \leq \deg P$. Si Q divise P et si P divise Q, alors A est une constante non nulle λ et $Q = \lambda P$.

Nous allons maintenant déterminer l'ensemble des diviseurs communs à deux polynômes.

THÉORÈME 2.2. — *Soient P et Q deux polynômes non nuls. Il existe un polynôme D tel que les diviseurs communs à P et Q soient exactement les diviseurs de D Le polynôme D est déterminé de façon unique à la multiplication près par une constante non nulle.*

Le polynôme D est un *plus grand commun diviseur* de P et Q.

Démonstration. — Supposons $\deg Q \leq \deg P$ et effectuons la division de P par Q,

$$P = AQ + R, \ \deg R < \deg Q.$$

Un polynôme C divise P et Q si et seulement si C divise Q et R. Le polynôme D est obtenu par une suite de divisions, c'est l'*algorithme d'Euclide* :

$$\begin{aligned} P &= A_0 Q + R_0, && \deg R_0 < \deg Q, \\ Q &= A_1 R_0 + R_1, && \deg R_1 < \deg R_0, \\ R_0 &= A_2 R_1 + R_2, && \deg R_2 < \deg R_1, \\ &\cdots \\ R_{n-3} &= A_{n-1} R_{n-2} + R_{n-1}, && \deg R_{n-1} < \deg R_{n-2}, \\ R_{n-2} &= A_n R_{n-1}. \end{aligned}$$

On effectue les divisions jusqu'à trouver un reste nul, $R_n = 0$, ce qui se produit certainement puisque les degrés des restes forment une suite d'entiers ≥ 0 strictement décroissante. Finalement C divise P et Q si et seulement C divise R_{n-1} : R_{n-1} est un PGCD de P et Q. □

Deux polynômes sont dits *premiers entre eux* si leurs seuls diviseurs communs sont les constantes non nulles.

Exactement comme dans le cas de l'anneau $\mathbb{Z}$ des entiers on démontre les énoncés suivants :

THÉORÈME 2.3 (BEZOUT). — *Soit D un PGCD des polynômes A et B. Il existe deux polynômes U et V tels que*

$$D = AU + BV.$$

Pour que A et B soient premiers entre eux, il faut et suffit qu'il existe deux polynômes U et V tels que

$$AU + BV = 1$$

L'algorithme d'EUCLIDE le montre et l'algorithme d'EUCLIDE-BÉZOUT fournit les polynômes U et V.

Exemple. — Les polynômes $A(X) = X^2 + 1$, et $B(X) = X - 1$ sont premiers entre eux,

$$X^2 + 1 - (X + 1)(X - 1) = 2.$$

THÉORÈME 2.4 (GAUSS). — *Soient A, B et C des polynômes. Si A divise BC et est premier avec B, alors A divise C.*

La propriété suivante s'en déduit :

COROLLAIRE 2.5. — *Si le polynôme A est premier avec chacun des polynômes $B_1, B_2, \ldots, B_n$, alors A est premier avec le produit $B_1 B_2 \ldots B_n$.*

De plus le PGCD possède les propriétés suivantes :

1. — *Si D est un PGCD de A et B, et si P est un polynôme, alors DP est un PGCD de AP et BP.*

2. — *Soit D un diviseur commun à deux polynômes A et B, $A = DA'$, $B = DB'$. Pour que D soit un PGCD de A et B il faut et suffit que A' et B' soient premiers entre eux.*

3. Racines d'un polynôme. — Soit K un corps commutatif. Une *racine* d'un polynôme P de $K[X]$ est un élément α de K tel que $P(\alpha) = 0$. Pour que α soit racine de P il faut et suffit que P soit divisible par $(X - \alpha)$. Un élément α de K est une *racine d'ordre k* du polynôme P si P est divisible par $(X - \alpha)^k$ et n'est pas divisible par $(X - \alpha)^{k+1}$. Pour que α soit racine d'ordre k de P il faut et suffit que

$$P(X) = (X - \alpha)^k Q(X),$$

où Q est un polynôme tel que $Q(\alpha) \neq 0$.

La *dérivée* du polynôme

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n$$

est le polynôme

$$P'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1},$$

et la *dérivée k-ième* de P est le polynôme

$$P^{(k)}(X) = \sum_{j=k}^{n} \frac{j!}{(j-k)!} a_j X^{j-k}.$$

Si α est une racine de P d'ordre $k \geq 2$, alors α est racine de P' d'ordre $k-1$. Si P et P' sont premiers entre eux, alors les racines de P sont toutes simples.

PROPOSITION 3.1 (FORMULE DE TAYLOR). — *Soit P un polynôme de degré n. Si α est un élément de K,*

$$P(X) = \sum_{k=0}^{n} \frac{(X-\alpha)^k}{k!} P^{(k)}(\alpha).$$

Démonstration. — La formule du binôme peut s'écrire

$$X^j = ((X-\alpha)+\alpha)^j = \sum_{k=0}^{j} \binom{j}{k} (X-\alpha)^k \alpha^{j-k}.$$

Si

$$P(X) = \sum_{j=0}^{n} a_j X^j,$$

il en résulte que

$$\begin{aligned} P(X) &= \sum_{j=0}^{n} a_j \Big(\sum_{k=0}^{j} \binom{j}{k} (X-\alpha)^k \alpha^{j-k} \Big) \\ &= \sum_{k=0}^{n} \frac{(X-\alpha)^k}{k!} \sum_{j=k}^{n} \frac{j!}{(j-k)!} a_j \alpha^{j-k} \\ &= \sum_{k=0}^{n} \frac{(X-\alpha)^k}{k!} P^{(k)}(\alpha). \end{aligned}$$

□

De la formule de TAYLOR on déduit la caractérisation suivante des racines d'ordre k d'un polynôme :

PROPOSITION 3.2. — *Pour que α soit racine d'ordre k du polynôme P il faut et suffit que*

$$P(\alpha) = 0,\ P'(\alpha) = 0, \ldots, P^{(k-1)}(\alpha) = 0,\ P^{(k)}(\alpha) \neq 0.$$

PROPOSITION 3.3. — *Si $\alpha_1, \alpha_2, \ldots, \alpha_p$ sont les racines d'un polynôme P, et si k_j est l'ordre de la racine α_j, alors*

$$P(X) = (X - \alpha_1)^{k_1}(X - \alpha_2)^{k_2} \ldots (X - \alpha_p)^{k_p} Q(X),$$

où Q est un polynôme sans racine (dans K).

Démonstration. — Le polynôme P est divisible par chacun des polynômes $(X - \alpha_j)^{k_j}$. Puisque ceux-ci sont premiers entre eux, P est divisible par leur produit.

$$P(X) = (X - \alpha_1)^{k_1} \ldots (X - \alpha_p)^{k_p} Q(X).$$

Si le polynôme Q avait une racine, ce serait l'un des éléments α_j, et ceci contredirait le fait que α_j est une racine d'ordre k_j. □

Par suite un polynôme de degré n a au plus n racines, chacune étant comptée un nombre de fois égal à son ordre. Si K est un corps infini deux polynômes dont les fonctions polynômes associées sont égales pour tout élément x de K sont égaux (c'est à dire qu'ils ont les mêmes coefficients).

Lorsque le corps K est le corps des nombres complexes, $K = \mathbb{C}$, la situation est particulièrement simple grâce au théorème de D'ALEMBERT-GAUSS :

THÉORÈME 3.4 (D'ALEMBERT-GAUSS). — *Tout polynôme à coefficients complexes de degré ≥ 1 admet au moins une racine complexe.*

La démonstration de ce théorème est difficile et nous ne la donnerons pas ici.

COROLLAIRE 3.5. — *Soit P un polynôme à coefficients complexes de degré n. Soient $\alpha_1, \ldots, \alpha_p$, les racines de P, $k_1, \ldots, k_p$ leurs ordres. Alors*

$$P(X) = \lambda(X - \alpha_1)^{k_1} \ldots (X - \alpha_p)^{k_p},$$

où λ est le coefficient de X^n et $k_1 + \cdots + k_p = n$.

Démonstration. — Cela résulte de la proposition 3.3 et du théorème de D'ALEMBERT-GAUSS puisque d'après celui-ci un polynôme de $\mathbb{C}[X]$ qui n'admet pas de racine est une constante. □

Soit f une fonction de n variables notées $\alpha_1, \alpha_2, \ldots, \alpha_n$. La fonction f est dite *symétrique* si sa valeur ne change pas lorsqu'on permute les

variables, c'est à dire que pour toute permutation s du groupe symétrique $\mathfrak{S}_n$,

$$f(\alpha_{s(1)}, \alpha_{s(2)}, \ldots, \alpha_{s(n)}) = f(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Les fonctions symétriques suivantes sont appellées *fonctions symétriques élémentaires*,

$$\begin{aligned}
\sigma_1 &= \alpha_1 + \alpha_2 + \cdots + \alpha_n, \\
\sigma_2 &= \sum_{i<j} \alpha_i \alpha_j, \\
\sigma_3 &= \sum_{i<j<k} \alpha_i \alpha_j \alpha_k, \\
&\cdots \\
\sigma_n &= \alpha_1 \alpha_2 \ldots \alpha_n.
\end{aligned}$$

Soit P un polynôme de degré n à coefficients complexes,

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n.$$

Proposition 3.6. — *Soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ les racines de P. Dans cette suite chaque racine est répétée un nombre de fois égal à son ordre. Soient σ_1, σ_2,...,σ_n, les fonctions symétriques élémentaires des racines, alors*

$$\sigma_1 = -\frac{a_{n-1}}{a_n}, \ \sigma_2 = \frac{a_{n-2}}{a_n}, \ldots, \ \sigma_n = (-1)^n \frac{a_0}{a_n}.$$

Démonstration. — Ces formules s'obtiennent par identification à partir de la relation

$$\begin{aligned}
P(X) &= a_0 + a_1 X + \cdots + a_n X^n \\
&= a_n (X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n).
\end{aligned}$$

□

Pour $n = 2$, $P(X) = a_0 + a_1 X + a_2 X^2$,

$$\begin{aligned}
\sigma_1 &= \alpha_1 + \alpha_2 = -\frac{a_1}{a_2}, \\
\sigma_2 &= \alpha_1 \alpha_2 = \frac{a_0}{a_2}.
\end{aligned}$$

Pour $n = 3$, $P(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3$,

$$\begin{aligned}
\sigma_1 &= \alpha_1 + \alpha_2 + \alpha_3 = -\frac{a_2}{a_3}, \\
\sigma_2 &= \alpha_1 \alpha_2 + \alpha_2 \alpha_3 + \alpha_3 \alpha_1 = \frac{a1}{a_3}, \\
\sigma_3 &= \alpha_1 \alpha_2 \alpha_3 = -\frac{a_0}{a_3}.
\end{aligned}$$

4. Polynômes irréductibles. Décomposition en facteurs irréductibles. — Soit K un corps commutatif. Un polynôme P de $K[X]$ est dit *irréductible* si $\deg P \geq 1$ et s'il n'admet pas de diviseur Q tel que

$$0 < \deg Q < \deg P$$

Il résulte de cette définition que les polynômes de degré 1 sont irréductibles.

Exemples.

a) Si $K = \mathbb{Q}$, $P(X) = X^2 - 2$ est irréductible.

b) Si $K = \mathbb{R}$, $P(X) = X^2 - 2$ n'est pas irréductible, en effet

$$P(X) = (X - \sqrt{2})(X + \sqrt{2}).$$

Par contre $P(X) = X^2 + 2$ est irréductible.

c) Si $K = \mathbb{C}$, $P(X) = X^2 + 2$ n'est pas irréductible,

$$X^2 + 2 = (X - i\sqrt{2})(X + i\sqrt{2}).$$

PROPOSITION 4.1. — *Soient P et Q deux polynômes de $K[X]$. Si P est irréductible, alors soit P divise Q, soit P et Q sont premiers entre eux.*

Démonstration. — Soit D un PGCD de P et Q. Puisque D divise P, soit D est une constante non nulle et alors P et Q sont premiers entre eux, soit $D = \lambda P$, où λ est une constante non nulle, et alors P divise Q. □

PROPOSITION 4.2. — *Si P est irréductible et divise le produit $Q_1 Q_2 \dots Q_n$, alors P divise au moins un des facteurs Q_i.*

Démonstration. — Si P ne divise pas Q_1, alors d'après la proposition précédente, P est premier avec Q_1, et d'après le théorème 2.4, P divise $Q_2 \dots Q_n$. □

THÉORÈME 4.3. — *Tout polynôme A est un produit de polynômes irréductibles. Plus précisément*

$$A = \lambda P_1^{\alpha_1} \dots P_m^{\alpha_m}$$

où λ est une constante non nulle, et les polynômes P_i sont irréductibles et unitaires. La décomposition est unique à l'ordre près des facteurs.

Un polynôme P est dit *unitaire* si le coefficient du terme de plus haut degré de P est égal à 1.

Démonstration.

a) L'existence de la décomposition se démontre par récurrence sur le degré de A. Si $\deg A > 1$, soit A est irréductible, soit $A = A_1 A_2$ avec

$0 < \deg A_i < \deg A$, $i = 1, 2$. Par hypothèse de récurrence les polynômes A_1 et A_2 sont produits de polynômes irréductibles.

b) Montrons l'unicité. Supposons qu'il existe deux décompositions

$$\begin{aligned} A &= \lambda P_1^{\alpha_1} \dots P_m^{\alpha_m} \\ &= \mu Q_1^{\beta_1} \dots Q_n^{\beta_n}. \end{aligned}$$

En comparant les termes de plus haut degré on trouve que $\lambda = \mu$. Le polynôme P_1 divise $Q_1^{\beta_1} \dots Q_n^{\beta_n}$, donc divise l'un des facteurs d'après la proposition 4.2. Il existe donc j_1 tel que $P_1 = Q_{j_1}$. On simplifie l'égalité par P_1, et on recommence. On en déduit que tout facteur du premier membre se trouve dans le second membre avec le même exposant. □

Du théorème de D'ALEMBERT-GAUSS (théorème 3.3) on déduit,

THÉORÈME 4.4.

a) Dans l'anneau $\mathbb{C}[X]$ des polynômes à coefficients complexes, les polynômes irréductibles sont les polynômes de degré 1.

b) La décomposition en facteurs irréductibles d'un polynôme P de degré n s'écrit

$$P(X) = \lambda(X - \alpha_1)^{k_1} \dots (X - \alpha_p)^{k_p},$$

où $\alpha_1, \dots, \alpha_p$ sont les racines de P, $k_1, \dots k_p$ sont leurs ordres, λ est le coefficient de X^n, et

$$k_1 + \dots + k_p = n.$$

Si P est un polynôme à coefficients complexes,

$$P(X) = a_0 + a_1 + \dots + a_n X^n,$$

on note $\bar{P}$ le polynôme

$$\bar{P}(X) = \bar{a}_0 + \bar{a}_1 X + \dots + \bar{a}_n X^n.$$

Si P et Q sont deux polynômes à coefficients complexes,

$$\overline{P+Q} = \bar{P} + \bar{Q}, \ \overline{PQ} = \bar{P}\bar{Q},$$

et si α est un nombre complexe,

$$\overline{P(\alpha)} = \bar{P}(\bar{\alpha}).$$

Pour qu'un nombre complexe α soit racine d'ordre k d'un polynôme P, il faut et suffit que $\bar{\alpha}$ soit racine d'ordre k de $\bar{P}$.

Soit P un polynôme à coefficients réels. Il peut être considéré comme un élément de $\mathbb{C}[X]$. Si α est racine de P, alors $\bar{\alpha}$ est aussi racine de P avec le même ordre.

PROPOSITION 4.5. — *Dans l'anneau $\mathbb{R}[X]$ des polynômes à coefficients réels, les polynômes irréductibles sont les polynômes de degré 1, et les polynômes de degré 2 de discriminant négatif, c'est à dire sans racine réelle.*

Démonstration. — Il est clair qu'un polynôme de degré 2 sans racine réelle est irréductible.

Soit P un polynôme irréductible. D'après le théorème de D'ALEMBERT-GAUSS (théorème 3.3), P admet au moins une racine complexe α. Si α est réelle, alors

$$P(X) = \lambda(X - \alpha),\ \lambda \in \mathbb{R}.$$

Si α n'est pas réelle, $\bar{\alpha}$ est aussi racine, et

$$P(X) = \lambda(X - \alpha)(X - \bar{\alpha}) = \lambda(X^2 + \beta X + \gamma),$$

où β, γ et λ sont réels, $\beta^2 - 4\gamma < 0$. □

PROPOSITION 4.6. — *Soit P un polynôme à coefficients réels de degré n. Soient $\alpha_1, \ldots, \alpha_p$ les racines réelles de P, $k_1, \ldots, k_p$ leurs ordres, $\xi_1, \bar{\xi}_1, \ldots, \xi_q, \bar{\xi}_q$ les racines non réelles, $\ell_1, \ldots, \ell_q$ leurs ordres. Posons*

$$(X - \xi_j)(X - \bar{\xi}_j) = X^2 + \beta_j X + \gamma_j.$$

Alors

$$\begin{aligned} P(X) =& \lambda(X - \alpha_1)^{k_1} \ldots (X - \alpha_p)^{k_p} \\ & (X^2 + \beta_1 X + \gamma_1)^{\ell_1} \ldots (X^2 + \beta_q X + \gamma_q)^{\ell_q}, \end{aligned}$$

où λ est le coefficient de X^n, et

$$k_1 + \cdots + k_p + 2\ell_1 + \cdots + 2\ell_q = n.$$

C'est la décomposition en facteurs irréductibles dans l'anneau $\mathbb{R}[X]$. Cette proposition se déduit facilement du théorème 4.4.

Exemple. — Soit $P(X) = X^6 - 1$. Les racines complexes de P sont les nombres

$$\alpha_k = e^{ik\frac{\pi}{3}} = \cos k\frac{\pi}{3} + i \sin k\frac{\pi}{3},\ k = 0, 1, \ldots, 5.$$

La décomposition de P en facteurs irréductibles de $\mathbb{C}[X]$ est

$$P(X) = (X - 1)(X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4)(X - \alpha_5),$$

et la décomposition de P en facteurs irréductibles de $\mathbb{R}[X]$ est

$$P(X) = (X-1)(X+1)(X^2-X+1)(X^2+X+1).$$

5. Anneau des polynômes à coefficients entiers. — Si A est un anneau commutatif (par exemple $A = \mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$), un polynôme à coefficients dans A est une expression de la forme

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n,$$

où les coeficients $a_0, \ldots, a_n$ sont des éléments de A. L'ensemble $A[X]$ des polynômes à coefficients dans A est muni d'une addition et d'une multiplication qui en font un anneau commutatif. Si A est intègre alors $A[X]$ l'est aussi. Si A est unitaire, $A[X]$ l'est aussi et les éléments inversibles de $A[X]$ sont les constantes inversibles.

Dans cette section nous allons étudier quelques propriétés de l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}$. Puisque $\mathbb{Z}$ est intègre, il en est de même de $\mathbb{Z}[X]$. Les éléments inversibles de $\mathbb{Z}[X]$ sont les constantes $+1$ et -1.

Soient A et B deux polynômes de $\mathbb{Z}[X]$, $\deg B = p$. Lorsqu'on effectue la division euclidienne de A par B, dans le cours des opérations on doit diviser par le coefficient b_p du terme de plus haut degré de B. Si $b_p = \pm 1$, on peut donc effectuer la division euclidienne dans $\mathbb{Z}[X]$:

$$A = BQ + R, \ \deg R < \deg B,$$

et les polynômes Q et R appartiennent à $\mathbb{Z}[X]$.

Si $P \in \mathbb{Z}[X]$, on appelle *contenu* de P le PGCD des coefficients de P, et on le note $c(P)$. Un polynôme P est dit *primitif* si ses coefficients sont premiers entre eux, c'est à dire si $c(P) = 1$.

THÉORÈME 5.1 (GAUSS). — *Soient B et C deux polynômes de $\mathbb{Z}[X]$, alors*

$$c(AB) = c(A)\,c(B).$$

Démonstration. — On peut écrire

$$A = \alpha A_1$$

avec $\alpha = c(A)$ et où A_1 est un polynôme primitif. De même

$$B = \beta B_1, \ \beta = c(B).$$

Ainsi

$$AB = \alpha\beta A_1 B_1.$$

Il suffit donc de montrer que le produit de deux polynômes primitifs est primitif. Soient donc A et B deux polynômes primitifs,

$$A(X) = a_0 + a_1 X + \cdots + a_m X^m,$$
$$B(X) = b_0 + b_1 X + \cdots + b_n X^n.$$

Soit p un nombre premier. Puisque A est primitif, l'un de ses coefficients n'est pas divisible par p. Notons k le plus petit entier tel que a_k ne soit pas divisible par p. De même soit ℓ le plus petit entier tel que b_ℓ ne soit pas divisible par p. Le coefficient $c_{k+\ell}$ du polynôme $C = AB$ est donné par

$$\begin{aligned} c_{k+\ell} &= \sum_{i+j=k+\ell} a_i b_j \\ &= a_0 b_{k+\ell} + \cdots + a_k b_\ell + \cdots a_{k+\ell} b_0. \end{aligned}$$

Chacun des termes de cette somme est divisible par p sauf $a_k b_\ell$. Donc $c_{k+\ell}$ n'est pas divisible par p. Ceci montre que le polynôme C est primitif. □

COROLLAIRE 5.2. — *Soit Q un polynôme primitif de $\mathbb{Z}[X]$, et soit P un polynôme de $\mathbb{Q}[X]$. Si le produit PQ appartient à $\mathbb{Z}[X]$, alors P appartient à $\mathbb{Z}[X]$.*

Démonstration. — En réduisant au même dénominateur les coefficients de P nous pouvons écrire

$$P = \frac{1}{d} P_1,$$

où $P_1 \in \mathbb{Z}[X]$. Ainsi, puisque $dPQ = P_1 Q$, d divise $c(P_1 Q)$ qui est égal à $c(P_1)c(Q) = c(P_1)$ d'après le théorème 5.1, donc les coefficients de P sont des nombres entiers. □

COROLLAIRE 5.3. — *Soient A et B deux polynômes unitaires de $\mathbb{Q}[X]$ tels que $C = AB$ appartienne à $\mathbb{Z}[X]$, alors A et B appartiennent à $\mathbb{Z}[X]$.*

Démonstration. — En réduisant au même dénominateur les coefficients de A nous pouvons écrire

$$A(X) = \frac{1}{p}(a'_0 + a'_1 X + \cdots + a'_{m-1} + pX^m) = \frac{1}{p} A_1(X),$$

où les nombres $a'_0, \ldots, a'_{m-1}, p$ sont des entiers premiers entre eux, c'est à dire que A_1 est un polynôme primitif. De même

$$B(X) = \frac{1}{q} B_1(X),$$

où B_1 est un polynôme primitif de $\mathbb{Z}[X]$. D'après le théorème 5.1 le polynôme $A_1 B_1$ est primitif. D'autre part $pqAB = A_1 B_1$, donc $p = 1$ et $q = 1$. □

Un polynôme Q de $\mathbb{Z}[X]$ est dit *irréductible* si $Q \neq 0$, $Q \neq \pm 1$, et si les seuls diviseurs de Q sont ± 1 et $\pm Q$.

Exemple. — Les polynômes $X^2 + 1$, $X^2 - 2$ sont irréductibles.

PROPOSITION 5.4. — *Les polynômes irréductibles de $\mathbb{Z}[X]$ sont*
(i) *les constantes $\pm p$, où p est un nombre premier,*
(ii) *les polynômes primitifs de degré ≥ 1 qui sont irréductibles dans $\mathbb{Q}[X]$.*

Démonstration. — Soit Q un polynôme primitif de degré ≥ 1 qui est irréductible dans $\mathbb{Q}[X]$. Si $Q = AB$ où A et B sont deux polynômes de $\mathbb{Z}[X]$, alors l'un des polynômes A et B est une constante λ qui divise 1, donc $\lambda = \pm 1$. □

THÉORÈME 5.5 (CRITÈRE D'EISENSTEIN). — *Soit Q un polynôme de $\mathbb{Z}[X]$ de degré $n > 1$,*

$$Q(X) = c_0 + c_1 X + \cdots + c_n X^n.$$

S'il existe un nombre premier p tel que
(i) *p divise $c_0, c_1, \ldots, c_{n-1}$,*
(ii) *p ne divise pas c_n,*
(iii) *p^2 ne divise pas c_0,*
alors Q est irréductible.

Démonstration. — Supposons que le polynôme Q vérifie les propriétés (i) et (ii), et soit $Q = AB$ une factorisation de Q (A et $B \neq 1$),

$$A(X) = a_0 + a_1 X + \cdots + a_k X^k,$$
$$B(X) = b_0 + b_1 X + \cdots + b_\ell X^\ell.$$

Puisque $c_0 = a_0 b_0$, et que c_0 est divisible par p, l'un des nombres a_0 et b_0 est divisible par p. Supposons que p divise a_0. Puisque $c_n = a_k b_\ell$ n'est pas divisible par p, a_k n'est pas non plus divisible par p. Soit j le plus petit entier tel que p ne divise pas a_j. Nous avons

$$c_j = a_0 b_j + a_1 b_{j-1} + \cdots + a_{j-1} b_1 + a_j b_0.$$

Puisque p divise $c_j, a_0, a_1, \ldots, a_{j-1}$, mais ne divise pas a_j, il divise b_0. Ainsi $c_0 = a_0 b_0$ est divisible par p^2.

Par suite si p^2 ne divise pas c_0, une telle factorisation ne peut pas exister et Q est irréductible. □

Exemples.

a) Le polynôme

$$Q(X) = 2X^5 + 3X^4 - 9X^2 + 6X + 15$$

est irréductible.

b) Pour tout nombre premier p et tout entier n, le polynôme $Q(X) = X^n - p$ est irréductible.

PROPOSITION 5.6. — *Soit Q un polynôme irréductible de $\mathbb{Z}[X]$. Si Q divise le produit $A_1 A_2 \ldots A_n$, $A_i \in \mathbb{Z}[X]$, alors Q divise l'un des facteurs A_i.*

Démonstration. — Si Q est une constante, $Q = \pm p$, où p est un nombre premier, p divise le produit $c(A_1) \ldots c(A_n)$ des contenus des polynômes A_i, donc divise l'un d'eux.

Soit Q un polynôme primitif de $\mathbb{Z}[X]$, irréductible dans $\mathbb{Q}[X]$. D'après la prosition 4.2, il divise l'un des polynômes A_i dans l'anneau $\mathbb{Q}[X]$, c'est à dire que

$$A_i = QB,$$

où $B \in \mathbb{Q}[X]$. Puisque Q est primitif, $B \in \mathbb{Q}[X]$ d'après le corollaire 5.2. □

THÉORÈME 5.7. — *Tout polynôme A de $\mathbb{Z}[X]$ est un produit de facteurs irréductibles.*

$$A(X) = p_1^{\alpha_1} \ldots p_k^{\alpha_k} Q_1(X)^{\beta_1} \ldots Q_\ell^{\beta_\ell}(X),$$

où $p_1, \ldots, p_k$ sont des nombres premiers, $Q_1, \ldots, Q_\ell$ des polynômes primitifs irréductibles dans $\mathbb{Q}[X]$. La décomposition est unique à l'ordre près des facteurs, et au signe près des facteurs Q_i.

Le produit $p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ est la décomposition en facteurs premiers du contenu de A. La démonstration est semblable à celle du théorème 4.3.

EXERCICES

(Exercices sur la section 1)

1 . — Soit K un corps commutatif, P un polynôme à coefficients dans K. Montrer que $P(P(X)) - X$ est divisible par $P(X) - X$. Déterminer le quotient.

2 . — Pour deux entiers positifs n et p, soient P et Q les polynômes,

$$P(X) = (X^n + X^{n-1} + \cdots + X^2 + X + 1)^p - X^n$$
$$Q(X) = X^{n-1} + X^{n-2} + \cdots + X^2 + X + 1.$$

Montrer que P est divisible par Q.

3 . — Trouver un polynôme P, de degré minimum, tel que P soit divisible par $X^2 + 1$ et $P - 1$ soit divisible par $X^4 + 1$.

(Exercices sur la section 2)

4 . — Soit A le polynôme

$$A(X) = X^2 + X + 1$$

et, pour tout entier $n \geq 2$,

$$P_n(X) = X^n + X + 1.$$

a) Montrer que, pour tout $n \geq 2$, le polynôme $P_{n+3} - P_n$ est divisible par A.

b) Pour quelles valeurs de n le polynôme P_n est-il divisible par A ?

c) Soit R_n le reste de la division de P_n par A,

$$P_n = AQ_n + R_n, \ \deg R_n < \deg A.$$

Déterminer la suite des polynômes R_n.

5 . — Soit U le polynôme

$$U(X) = X^3 - 2X^2 - 3X + 1.$$

a) Déterminer les restes de la division par $U(X)$ des polynômes $1, X, X^2, X^3$ et X^4.

b) Déterminer le reste de la division par U du polynôme $X^3 + pX + q$.

c) On note

$$R_k(X) = a_k X^2 + b_k X + c_k,\ k \geq 0,$$

le reste de la division de X^k par U. En divisant $X\ R_k$ par U établir une relation de récurrence entre R_{k+1} et R_k du type :

$$\begin{aligned} a_{k+1} &= \ell_1 a_k + m_1 b_k + n_1 c_k, \\ b_{k+1} &= \ell_2 a_k + m_2 b_k + n_2 c_k, \\ c_{k+1} &= \ell_3 a_k + m_3 b_k + n_3 c_k, \end{aligned}$$

où les ℓ_i, m_i, n_i sont des coefficients à déterminer.

d) Ecrire un programme PASCAL permettant d'afficher sur 3 colonnes les coefficients a_k, b_k, c_k pour k allant de 0 à 20.

e) Déterminer R_5 et R_6 puis le reste de la division du polynôme

$$P(X) = X^6 + aX^5 + aX^4 + (a+2)X^3 + (a-3)X^2 + aX + 1$$

par U. Pour quelles valeurs du paramètre a le polynôme P est-il divisible par U ?

6 . — Déterminer le P.G.C.D. des polynômes suivants :

$$\begin{aligned} a)\quad & A(X) = X^6 - 2X^5 + 3X^4 - 4X^3 + 3X^2 - 2X + 1, \\ & B(X) = 3X^5 - 5X^4 + 6X^3 - 6X^2 + 3X - 1. \\ b)\quad & A(X) = X^5 + X^4 + 2X^3 - 2X + 3, \\ & B(X) = X^4 + 3X^3 + 7X^2 + 8X + 6. \end{aligned}$$

7 . — Dans les calculs des P.G.C.D. de l'exercice précédent, déterminer la suite des restes R_n, ainsi que les suites de polynômes U_n et V_n tels que $R_n = U_n A + V_n B$.

8 . — Soit K un corps commutatif, A, B, U, V des polynômes de $K[X]$ tels que

$$AU + BV = Q.$$

Q étant le P.G.C.D. des polynômes A et B. Quel est le P.G.C.D. de U et V ?

9 . — Déterminer des polynômes A et B à coeffificients réels tels que

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

a) en utilisant l'algorithme d'EUCLIDE.

b) en développant par la formule du binôme de NEWTON $(X+(1-X))^4$.

10 . — Etant donnés deux entiers m et n $(n > m > 0)$, on se propose de déterminer le P.G.C.D. de $X^n - 1$ et $X^m - 1$.

a) Montrer que, si l'entier k divise n, $X^k - 1$ divise $X^n - 1$.

b) Soit d le P.G.C.D. de m et n, il existe alors deux entiers u et v tels que $vm - un = d$. Montrer que

$$X^{un}(X^d - 1) = (X^{vm} - 1) - (X^{un} - 1).$$

Conclure.

c) Quel est le P.G.C.D. de $X^{n-1} + \cdots + X + 1$ et $X^{m-1} + \cdots + X + 1$?

11 . — Soit K un corps commutatif.

a) Soient $A, B, C \in K[X]$. Montrer que si A et B sont premiers entre eux, et si A et C sont premiers entre eux, alors A et BC sont premiers entre eux.

b) En déduire que si A et B sont premiers entre eux et si p, q sont des entiers supérieurs ou égaux à 1, A^p et B sont premiers entre eux, A et B^q sont premiers entre eux, A^p et B^q sont premiers entre eux.

c) Montrer que si A et B sont premiers entre eux, $A + B$ et AB sont aussi premiers entre eux. (On pourra raisonner par l'absurde et utiliser b).)

d) On considère les polynômes A et B de $\mathbb{R}[X]$,

$$\begin{aligned} A =& X^4 - 2X^3 - 7X^2 + 20X - 12 \\ B =& X^2 + 3X + 2. \end{aligned}$$

Quel est le P.G.C.D. de $A + B$ et AB ?

(Exercices sur la section 3)

12 . — Soit P un polynôme à coefficients réels vérifiant $P(1) = 1$ et $P(2) = 4$. On pose $B(X) = X^2 - 3X + 2$. Déterminer le reste de la division de P par B.

13 . — Les racines du polynôme $P(X) = X^n - 1$ étant notées $1, x_2, \ldots, x_n$, calculer en fonction de n le produit

$$\prod_{i=2}^{n}(1 - x_i).$$

14 . — Soient x_1, x_2, x_3 les trois racines, non nulles, du polynôme

$$P(X) = aX^3 + 3bX^2 + 3cX + d,$$

à coefficients complexes. A quelle condition a-t-on

$$\frac{2}{x_1} = \frac{1}{x_2} + \frac{1}{x_3} \ ?$$

15 . — Quelles sont les racines du polynôme

$$P_n(X) = 1 - \frac{1}{1!}X + \frac{1}{2!}X(X-1) + \cdots + (-1)^n \frac{1}{n!}X(X-1)\ldots(X-n+1)?$$

16 . — Un polynôme peut-il être divisible par sa dérivée ?

17 . — Montrer que, dans $\mathbb{Z}/p\mathbb{Z}[X]$ avec p premier,

$$X^{p-1} - 1 = \Pi_{i=1}^{p-1}(X - ai)$$

où $a_1, a_2, \ldots, a_{p-1}$ sont les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$.

En déduire que pour tout nombre premier p, $(p-1)! + 1$ est divisible par p (c'est la partie directe du théorème de Wilson, cf. ex. 25 du ch. I).

18 . — Dans $\mathbb{R}[X]$, montrer qu'il existe un polynôme P unique, de degré inférieur à 7, tel que $P(X)+1$ soit divisible par $(X-1)^4$ et $P(X)-1$ soit divisible par $(X+1)^4$. Le déterminer en utilisant :

a) le polynôme dérivé de P,

b) l'algorithme d'EUCLIDE.

c) la formule du binôme de NEWTON.

19 . — On considère, dans $\mathbb{C}[X]$, les polynômes

$$P_n(X) = 1 + X + \frac{1}{2!}X^2 + \cdots + \frac{1}{n!}X^n, \ n > 0.$$

a) Démontrer que, dans $\mathbb{C}$, le polynôme P_n admet n racines distinctes.

b) Démontrer que, si n est impair, $P_n(X)$ a une seule racine réelle, et si n est pair, $P_n(x) > 0$ pour tout x réel.

20 . — Soit K un corps commutatif et P un polynôme de $K[X]$. Soit $\alpha \in K$ une racine de P. On pose

$$Q(X) = \frac{1}{2}(X-\alpha)(P'(X) + P'(\alpha)) = P(X) + P(\alpha).$$

Montrer que α est racine du polynôme Q. Quel est son ordre ?

21 . — (Formules de CARDAN) Considérons l'équation du troisième degré,

$$x^3 + ax^2 + bx + c = 0,$$

à coefficients complexes. En posant $y = x + \frac{a}{3}$, on obtient une équation de la forme

$$y^3 + py + q = 0.$$

Considérons donc maintenant l'équation

$$x^3 + px + q = 0,$$

et notons α_1, α_2, α_3, ses racines (complexes, distinctes ou non). On pose

$$u = \alpha_1 + j\alpha_2 + j^2\alpha_3,$$
$$v = \alpha_1 + j^2\alpha_2 + j\alpha_3,$$

$(j = \exp(2i\frac{\pi}{3}) = -\frac{1}{2} + i\frac{\sqrt{3}}{2})$.

a) En utilisant les relations entre les coefficients et les racines (proposition 3.6), exprimer uv et $u^3 + v^3$ en fonction de p et q. En déduire que u^3 et v^3 sont racines de l'équation

$$z^2 + 27qz - 27p^3 = 0.$$

On pose $\Delta' = (\frac{p}{3})^3 + (\frac{q}{2})^2$, et on note $\sqrt{\Delta'}$ une racine carrée du nombre complexe Δ', si bien que

$$(\frac{u}{3})^3 = -\frac{q}{2} + \sqrt{\Delta'},$$
$$(\frac{v}{3})^3 = -\frac{q}{2} - \sqrt{\Delta'}.$$

b) En résolvant le système

$$\alpha_1 + \alpha_2 + \alpha_3 = 0,$$
$$\alpha_1 + j\alpha_2 + j^2\alpha_3 = u,$$
$$\alpha_1 + j^2\alpha_2 + j\alpha_3 = v,$$

montrer que

$$\begin{aligned}
\alpha_1 &= \quad \sqrt[3]{-\tfrac{q}{2} + \sqrt{\Delta'}} + \quad \sqrt[3]{-\tfrac{q}{2} - \sqrt{\Delta'}}, \\
\alpha_2 &= j^2 \sqrt[3]{-\tfrac{q}{2} + \sqrt{\Delta'}} + j \quad \sqrt[3]{-\tfrac{q}{2} - \sqrt{\Delta'}}, \\
\alpha_3 &= \quad j \sqrt[3]{-\tfrac{q}{2} + \sqrt{\Delta'}} + j^2 \sqrt[3]{-\tfrac{q}{2} - \sqrt{\Delta'}},
\end{aligned}$$

les racines cubiques étant choisies de telle sorte que $uv = -3p$.

c) On suppose que p et q sont réels. Discuter la réalité des racines suivant le signe de Δ'.

d) Résoudre les équations

$$x^3 + 6x + 2 = 0,$$
$$x^3 - 3x - 1 = 0.$$

22 . — Soient x_1, x_2, x_3 les racines du plynôme

$$P(X) = X^3 + pX + q.$$

Calculer en fonction de p et q le produit

$$(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2,$$

a) en utilisant les formules de CARDAN,

b) en utilisant les relations entre coefficients et racines du plynôme P.

On pourra remarquer que

$$(x_1 - x_2)^2 = -4p - 3x_3^2.$$

(Exercices sur la section 4)

23 . — Décomposer les polynômes $A(X) = X^5 - 1$ et $B(X) = X^5 + 1$ en facteurs irréductibles dans $\mathbb{R}[X]$, puis $\mathbb{C}[X]$. En déduire $\cos\frac{2\pi}{5}$ et $\sin\frac{2\pi}{5}$.

24 . — Décomposer en produit de facteurs irréductibles dans $\mathbb{C}[X]$, $\mathbb{R}[X]$ et$\mathbb{Z}/5\mathbb{Z}[X]$ les polynômes

$$A(X) = X^4 + 2X^2 + 1$$
$$B(X) = X^4 - X^2 + 1.$$

(Exercices sur la section 5)

25 . — Démontrer que si $\frac{p}{q}$ est une fraction irréductible représentant l'un des zéros du polynôme

$$P(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n$$

à coefficients entiers, alors

a) q est un diviseur de a_0.

b) p est un diviseur de a_n.

c) pour tout entier $m, p - m\ q$ est un diviseur de $P(m)$.

Déterminer les zéros rationnels du polynôme suivant :

$$P(X) = X^4 - 2X^3 - 8X^2 + 13X - 24.$$

26 . — Soit n un entier positif.

a) Démontrer que, dans $\mathbb{Q}[X]$, il existe un couple unique (A, B) de polynômes tel que

$$(1 - X)^n\ A(X) + X^n B(X) = 1,\ \deg A < n,\ \deg B < n.$$

b) Comparer $B(X)$ et $A(X - 1)$.

c) Démontrer qu'il existe une constante $\lambda \in \mathbb{Q}$ telle que

$$(1 - X)A'(X) - nA(X) = \lambda X^{n-1}.$$

d) Calculer les coefficients de A et la constante λ.

e) Retrouver le résultat de d) en développant $((1 - X) + X)^{2n-1}$ par la formule du binôme de Newton.

27 . — Montrer que, si p est premier, le polynôme

$$P(X) = 1 + X + \cdots + X^{p-1},$$

est irréductible dans l'anneau $\mathbb{Z}[X]$. On utilisera le critère d'Eisenstein (théorème 5.5), après avoir fait le changement de variable défini par $X = Y + 1$.

28 . — (Polynômes cyclotomiques) Pour tout entier $n \geq 1$ on note R_n l'ensemble des nombres complexes $\alpha = \exp(2i\pi\frac{k}{n})$, où $1 \leq k < n$, k et n étant premiers entre eux. Par exemple

$$R_3 = \{\exp(2i\pi\frac{1}{3}), \exp(2i\pi\frac{2}{3})\}.$$

Soit Φ_n le polynôme défini par

$$\Phi_n(X) = \Pi_{\alpha \in R_n}(X - \alpha).$$

Par exemple

$$\Phi_3(X) = X^2 + X + 1.$$

On remarquera que le degré de Φ_n est égal à $\varphi(n)$.

a) Déterminer les polynômes Φ_n, pour $n = 4, 5, 6, 7, 8$.

b) Montrer que si p est premier,

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

c) Montrer que si d divise n, alors le polynôme Φ_d divise le polynôme $X^n - 1$, et que

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

En déduire que

$$\sum_{d|n} \varphi(d) = n.$$

d) Montrer que Φ_d est un polynôme à coefficients entiers.

e) Déterminer la décomposition de $X^{12} - 1$ en facteurs irréductibles dans l'anneau $\mathbb{Z}[X]$.

(On pourra consulter A. Warusfel, Structures algébriques finies, Hachette.)

TRAVAUX PRATIQUES

Fonctions génératrices

I

Ecrire des procédures PASCAL pour
— la lecture d'un polynôme par ses coefficients,
— l'affichage des coefficients d'un polynôme,
— le calcul du produit d'un polynôme par un scalaire,
— le calcul de la somme de deux polynômes,
— le calcul du produit de deux polynômes,
— l'éléva tion à une puissance entière d'un polynôme,
— le calcul du composé de deux polynômes.

II

1) Définition de la fonction génératrice.

Soit Y une variable aléatoire (v.a.) ne prenant qu'un nombre fini k de valeurs entières, de loi

$$P(Y = i) = p_i,\ 0 \leq i \leq k,\ \text{avec}\ \Sigma_{i=1}^{k} p_i = 1.$$

On associe à la v.a. Y et à sa distribution de probabilités $\{p_i,\ 0 \leq i \leq k\}$ un polynôme f_Y, nommé *fonction génératrice* (f.g.) de la v.a. Y, par la relation

$$f_Y(X) = \Sigma_{i=0}^{n} p_i X^i.$$

On remarque que $f_Y(X) = E(X^Y)$.

a) Quelle est la f.g. de la v.a. représentant le nombre de points apparus sur un dé au cours d'un lancer ?

b) Déterminer la f.g. d'une v.a. suivant une loi binomiale $\mathcal{B}(k; p, q)$.

c) Donner, dans le cas général, une expression simple de $f_Y(0)$, $f_Y(1)$, $f'_X(0)$, $f'_X(1)$, $f_X^{(j)}(0)$, pour $1 \leq j$, entier.

Exprimer la variance de Y en fonction des dérivées de la f.g. f_Y.

d) Considérons la v.a. Y représentant le nombre de fils d'un couple, avec

$$P(Y = 0) = 0,4828$$
$$P(Y = i) = pq^{i-1}$$

où $p = 0,2126, q = 0,5893$, si $1 \leq i \leq 12$ (résultats approchés du recensement américain de 1920). Ecrire un programme PASCAL affichant la loi de Y.

A l'aide d'une procédure pour le calcul de la moyenne $E(Y)$, donner une valeur approchée à 1/100 près du nombre moyen de fils des couples américains en 1920.

2) Somme de variables aléatoires indépendantes.

a) On suppose que deux v.a. indépendantes, Y_1 et Y_2, ont pour lois

$$P(Y_1 = i) = p_i \text{ pour } 0 \leq i \leq k_1,$$
$$P(Y_2 = j) = q_j \text{ pour } 0 \leq j \leq k_2,$$

et pour f.g. respectivement f_1 et f_2. Quelle est la f.g. de $Y_1 + Y_2$?

b) Déterminer la loi de la v.a. Y représentant le nombre de petits-fils d'un couple américain ayant deux fils dans les conditions de 1-d). Préciser la valeur de $E(Y)$.

3) Somme en nombre aléatoire de v.a. indépendantes.

a) Soit $\{Y_\ell,\ \ell \in \mathbb{N}\}$ une suite de v.a. indépendantes, de même loi, la f.g. commune des variables Y_ℓ étant le polynôme f_Y.

On considère la somme $S = Y_1 + Y_2 + \cdots + Y_N$ où N est une v.a. à valeurs entières, dont la f.g. est le polynôme g_N. On suppose de plus que la v.a. N est indépendante des v.a. Y_ℓ . Montrer que la f.g. de S est alors le polynôme $g_N o f_Y$, défini par $g_N o f_Y(X) = g_N(f_Y(X))$.

b) Quelle est la loi de la v.a. Z représentant le nombre de petits-fils d'un couple dans la société américaine de 1920 ? Préciser la valeur de $E(Z)$.

c) Comparer l'évolution des trois familles suivantes, dans lesquelles la loi de procréation est supposée fixée au cours du temps (Y représente le nombre d'enfants) :

$$\alpha)\ P(Y = 0) = 1/2, \quad P(Y = 1) = P(Y = 2) = 1/4,$$
$$\beta)\ P(Y = 0) = 1/4, \quad P(Y = 1) = 1/2 \quad P(Y = 2) = 1/4,$$
$$\gamma)\ P(Y = 0) = 1/4, \quad P(Y = 1) = 1/4, \quad P(Y = 2) = 1/2.$$

d) Si l'on note Z_n le nombre de descendants d'un couple à la n-ième génération, la probabilité d'extinction de la famille est :

$$e = P(Z_1 = 0 \text{ ou } Z_2 = 0 \text{ ou } \ldots\ Z_n = 0 \text{ ou} \ldots)$$
$$= \lim_{n \to \infty} P(Z_n = 0).$$

Montrer qu'elle vérifie $e = f_Y(e)$.

Quelles sont les probabilités d'extinction de chacune des trois familles étudiées ci-dessus ?

INDEX

Index des noms propres

Titre
Arithmétique

Auteurs
Jacques Faraut, Elisabeth Khalili

Date
1989

Editeur
IREM de Strasbourg

Brochure S 135

Mots-clé
Arithmétique, Polynômes, Pascal

Résumé
Ce cours d'arithmétique s'adresse aux étudiants de mathématiques en première année de premier cycle. Deux chapitres d'arithmétique élémentaire sont suivis d'un troisième sur les fractions continues et d'un quatrième sur les polynômes. Pour chacun des chapitres des travaux pratiques sur microordinateur sont proposés.