7
Arithmétique

I
Arithmétique euclidienne

1. Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ sont tous deux munis d'une **division euclidienne**. L'arithmétique de ces anneaux est l'étude des propriétés qui se déduisent de la division euclidienne.
Dans ce qui suit, A désignera aussi bien $\mathbb{Z}$ que $\mathbb{K}[X]$.
L'idéal de $\mathbb{Z}$ engendré par un entier x_0 sera noté $x_0\mathbb{Z}$ ou $\langle x_0\rangle$.
De même, l'idéal de $\mathbb{K}[X]$ engendré par un polynôme P_0 sera noté $\langle P_0\rangle$.

2. Lemme fondamental

2.1 ➔ *Un élément $x \neq 0$ de A divise $y \in A$ si, et seulement si, le reste de la division euclidienne de y par x est nul.*

2.2 Applications

1. L'ensemble des solutions $x \in \mathbb{Z}$ de $x+1 \mid x+3$ est égal à $\{-3,-2,0,1\}$.
2. Un entier $x \in \mathbb{Z}$ est solution de $x+2 \mid x^2+2$ si, et seulement si, $x+2$ divise 6.
3. Le polynôme $X^4+X^3+aX^2+bX+2$ est divisible par X^2+2 dans $\mathbb{R}[X]$ si, et seulement si, $(a,b)=(3,2)$.
4. Soit $n \geqslant 1$. Le polynôme $aX^{n+1}+bX^n+1$ est divisible par $(X-1)^2$ dans $\mathbb{R}[X]$ si, et seulement si, $a=n$ et $b=-(n+1)$. Dans ce cas, le quotient de la division euclidienne est égal à

$$nX^{n-1}+(n-1)X^{n-2}+\cdots+3X^2+2X+1.$$

5. Un polynôme $P \in \mathbb{K}[X]$ est divisible par son polynôme dérivé P' si, et seulement si, il existe deux scalaires α, β et un entier $n \geqslant 1$ tels que $P=\alpha(X-\beta)^n$.

I.1 PGCD

3.1 ✍ *Soient a et b, deux éléments de A. Un élément d de A est **un plus grand commun diviseur (pgcd)** de a et b lorsque*

$$dA = aA+bA.$$

3.2 Quels que soient a et b dans A, il existe au moins un pgcd $d \in A$ de a et b et si $(a,b) \neq (0,0)$, alors il existe un, et un seul, pgcd normalisé.

3.3 Pour tout pgcd d de a et b, il existe u et v dans A tels que $au+bv=d$.

3.4 ✍ **PGCD normalisé**

*Soit $(a,b) \neq (0,0)$, un couple d'éléments de A. **Le pgcd** de a et de b est l'unique élément normalisé d_0 de A tel que*

$$d_0A = aA+bA.$$

Ce pgcd est noté $a \wedge b$.

3.5 Cas particuliers

1. Si a ou b est inversible, alors $a \wedge b = 1$.
2. Si $a=0$, alors b est un pgcd de a et b.
3. Le pgcd de a et b est nul si, et seulement si, $a=b=0$.

4. ➔ **Caractérisation des PGCD**

Soient a, b et d, trois éléments de A. Alors d est un pgcd de a et b si, et seulement si,

1. *l'élément d divise a et b et*
2. *tout élément δ qui divise a et b divise également d.*

5. Éléments premiers entre eux

Le cas particulier où deux éléments sont *premiers entre eux* n'est en fait pas loin d'être le cas général. →[10.3]

5.1 ✍ *Deux éléments a et b sont **premiers entre eux** lorsque leur pgcd $a \wedge b$ est égal à 1, c'est-à-dire*

$$aA+bA = A.$$

5.2 Soient a et b, deux éléments premiers entre eux. Si $x \mid a$ et si $y \mid b$, alors x et y sont premiers entre eux.

5.3 ➔ *Deux éléments a et b sont premiers entre eux si, et seulement si, tout diviseur commun à a et à b est inversible.*

5.4 Soient a et b, deux éléments normalisés. Si d est le pgcd normalisé de a et b, alors il existe deux éléments normalisés α et β tels que $a=d\alpha$ et $b=d\beta$.

5.5 ➔ *Deux éléments irréductibles normalisés sont égaux ou premiers entre eux.*

5.6 Si a est irréductible et si a ne divise pas b, alors

$$aA \subsetneq aA+bA = A$$

donc a et b sont premiers entre eux. →[6.69.6]

6. PGCD d'une famille finie

6.1 ✍ *On appelle **pgcd** d'une famille finie $(a_i)_{1\leqslant i\leqslant n}$ d'éléments de A tout élément $d \in A$ tel que*

$$\sum_{i=1}^{n} a_iA = dA.$$

6.2 Toute une famille finie admet au moins un pgcd et si elle n'est pas la famille nulle, alors elle admet un, et un seul, pgcd normalisé.

6.3 Un élément d_0 de A est un pgcd de $(a_i)_{1\leqslant i\leqslant n}$ si, et seulement si,

$$\begin{cases} \forall\, 1 \leqslant i \leqslant n, \quad d_0 \mid a_i, \\ \forall\, D \in A, \quad \big(\forall\, 1 \leqslant i \leqslant n, \quad D \mid a_i\big) \implies D \mid d_0. \end{cases}$$

6.4 Pour tout $1 \leqslant k < n$, un pgcd de $pgcd(a_1,\ldots,a_k)$ et de $pgcd(a_{k+1},\ldots,a_n)$ est un pgcd de $(a_1,\ldots,a_n)$.

6.5 Un pgcd de $(a_i)_{1\leqslant i\leqslant n}$ est inversible si, et seulement si,

$$\sum_{i=1}^{n} a_iA = A.$$

6.6 ✍ *Les éléments $(a_i)_{1\leqslant i\leqslant n}$ sont **premiers dans leur ensemble**, ou **globalement premiers entre eux**, lorsqu'ils admettent 1 pour pgcd.*

6.7 Si deux des éléments $(a_i)_{1\leqslant i\leqslant n}$ sont premiers entre eux, alors les $(a_i)_{1\leqslant i\leqslant n}$ sont premiers dans leur ensemble.

6.8 Des éléments peuvent être premiers dans leur ensemble sans être deux à deux premiers entre eux. →[20.2]

I.2 PPCM

7.1 ✍ *Soient a et b dans A. Un élément m de A est **un plus petit commun multiple (ppcm)** de a et b lorsque*

$$mA = aA \cap bA.$$

7.2 Quels que soient a et b dans A, il existe au moins un ppcm de a et b. Si a et b sont non nuls, alors il existe un, et un seul, ppcm normalisé.

7.3 Pour tout ppcm m de a et de b, il existe deux éléments u et v de A, premiers entre eux, tels que

$$m = au = bv.$$

7.4 ✍ **PPCM normalisé**

*Soient a et b dans A, non nuls. **Le ppcm** de a et b est l'unique élément normalisé m_0 de A tel que*

$$m_0A = aA \cap bA.$$

Ce ppcm est noté $a \vee b$.

I.5

Théorèm

20. Dans
considère des é
eux.

20.1 On pose

et

$$\forall\, 1 \leqslant k \leqslant$$

de telle sorte que

$$\forall\, 1 \leqslant k \leqslant n, \quad x = x_k y_k \quad \text{et}$$

20.2 ➔ *Les éléments $y_1, \ldots, y_n$ sont premiers a*
existe des éléments $a_1, a_2, \ldots, a_n$ de A tels que

$$\sum_{k=1}^{n} a_k y_k = 1.$$

21. Applications dans $\mathbb{K}[X]$

21.1 Si λ et μ sont deux scalaires distincts, alors les polynôme
$X - \lambda$ et $X - \mu$ sont premiers entre eux :

$$\frac{1}{\lambda - \mu}(X - \mu) + \frac{-1}{\lambda - \mu}(X - \lambda) = 1.$$

21.2 Si le polynôme P est scindé :

$$P = \prod_{i=1}^{n} (X - \lambda_i)^{m_i}$$

(où les racines λ_i sont deux à deux distinctes et les multiplicités

29.2 Les produits md et ab sont associés.
29.3 ➔ *Le produit ab est un ppcm de a et b si, et seulement si, a et b sont premiers entre eux.*
29.4 Le produit des a_i est un ppcm de $(a_i)_{1\leqslant i\leqslant n}$ si, et seulement si, les a_i sont deux à deux premiers entre eux.

30. On pose $u_n = n^2 + (n+1)^2 + (n+3)^2$ pour tout $n \in \mathbb{N}$.
1. On a $u_n = n(3n-2) \pmod{10}$.
2. Les propositions suivantes sont équivalentes :
2.a L'entier u_n est un multiple de 10.
2.b L'un des entiers n ou $3n-2$ est un multiple de 10.
2.c L'entier n est congru à 0 ou à 4 modulo 10.

31. Soient $I = \mathbb{N}^* \times \mathbb{N}^*$ et

$$\forall\, n \in \mathbb{N}^*, \quad I_n = \big\{(p,q) \in I \,:\, p \wedge q = n\big\}.$$

Alors $(I_n)_{n\geqslant 1}$ est une partition de I et comme l'application

$$[(\alpha,\beta) \mapsto (n\alpha, n\beta)]$$

est une bijection de I_1 sur I_n, alors

$$\sum_{(p,q)\in I} \frac{1}{p^2q^2} = \Big(\sum_{(p,q)\in I_1} \frac{1}{p^2q^2}\Big)\Big(\sum_{n=1}^{+\infty} \frac{1}{n^4}\Big).$$

32. Soient A et B, deux polynômes à coefficients dans $\mathbb{Z}$. S'il existe un nombre premier p qui divise tous les coefficients du produit AB, alors p divise tous les coefficients de A ou tous les coefficients de B.

33. Si A et B sont deux polynômes premiers entre eux, alors

$$\forall\, C \in \mathbb{K}[X], \quad A \wedge (BC) = A \wedge C.$$

II

Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

34. L'*arithmétique modulaire* est une initiation, limitée ici à l'anneau des entiers $\mathbb{Z}$, à la structure d'**anneau quotient**. →**[100]**

35.1 ✍ *Soit $n \in \mathbb{N}^*$. Un entier $a \in \mathbb{Z}$ est **congru modulo** n à $b \in \mathbb{Z}$ lorsqu'il existe $k \in \mathbb{Z}$ tel que $b = a + kn$. On note alors :*

$$a = b \pmod{n}$$

ou encore $a \equiv b\ [n]$.
35.2

$$a = b \pmod{n} \iff n \mid (b-a) \iff b = a \pmod{n}$$

35.3 **Exemples**
1. Pour tout entier n,

$$n(n+1) = 0 \pmod 2 \quad \text{et} \quad (n-1)n(n+1) = 0 \pmod 3.$$

2. Si $p > 3$ est premier, alors $p^2 = 1 \pmod{24}$.

II.1 Classes de congruence modulo n

36.1 ➔ *La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.*
36.2 ✍ *La **classe modulo** n de $a \in \mathbb{Z}$ est l'ensemble des entiers congrus à a modulo n.*

$$\mathscr{C}(a) = \big\{a + kn,\ k \in \mathbb{Z}\big\}$$

Elle est aussi notée $a + n\mathbb{Z}$, $\overline{a}$, $\dot{a}$, ou même a (quand aucune ambiguïté n'est possible).
36.3

$$\mathscr{C}(a) = \mathscr{C}(b) \iff b \in \mathscr{C}(a)$$

36.4 Si $\mathscr{C}(a) \cap \mathscr{C}(b) \neq \varnothing$, alors $\mathscr{C}(a) = \mathscr{C}(b)$.
36.5 Si $r \in \mathbb{N}$ est le reste de la division euclidienne de a par n, alors $\mathscr{C}(a) = \mathscr{C}(r)$.

37.1 ✍ *Pour tout $n \in \mathbb{N}^*$, on note $\mathbb{Z}/n\mathbb{Z}$, l'ensemble des classes de congruence modulo n des éléments de $\mathbb{Z}$.*

$$\mathbb{Z}/n\mathbb{Z} = \big\{\mathscr{C}(a),\ a \in \mathbb{Z}\big\}$$

37.2 L'application $\mathscr{C}$ est une surjection de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.
37.3 ✍ *Un entier $k \in \mathbb{Z}$ est un **représentant** de la classe $C \in \mathbb{Z}/n\mathbb{Z}$ lorsque $C = \mathscr{C}(k)$.*

38. ➔ *Le cardinal de l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est égal à n et*

$$\mathbb{Z}/n\mathbb{Z} = \big\{\mathscr{C}(r),\ 0 \leqslant r < n\big\}.$$

39. L'ensemble $\mathbb{Z}/2\mathbb{Z}$ est constitué d'une part de l'ensemble $\mathscr{C}(0)$ des entiers pairs et de l'ensemble $\mathscr{C}(1)$ des entiers impairs.

II.2 Opérations modulo n

Addition

40.1 Quels que soient $\alpha \in \mathscr{C}(a)$ et $\beta \in \mathscr{C}(b)$,

$$\mathscr{C}(\alpha+\beta) = \mathscr{C}(a+b).$$

40.2 ✍ *Soient C_1 et C_2 dans $\mathbb{Z}/n\mathbb{Z}$: il existe a et b dans $\mathbb{Z}$ tels que $C_1 = \mathscr{C}(a)$ et $C_2 = \mathscr{C}(b)$ et la **somme** de C_1 et de C_2 est définie par*

$$C_1 \oplus C_2 = \mathscr{C}(a+b).$$

40.3 ➔ *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de $\oplus$ est un groupe cyclique.*
40.4 ➔ *Tout groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, \oplus)$.*

41. **Exemples de morphismes de groupes**
1. Le seul morphisme de groupes de $\mathbb{Z}/5\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$ est le morphisme trivial : $[x \mapsto 0]$.
2. Il existe six morphismes de groupes de $\mathbb{Z}/6\mathbb{Z}$ dans $\mathbb{U}_6$, dont seulement deux sont des isomorphismes.
3. Si f est un automorphisme de $\mathbb{Z}/4\mathbb{Z}$, alors $f(1)$ est un élément d'ordre 4. Les automorphismes de $\mathbb{Z}/4\mathbb{Z}$ sont $[x \mapsto x]$ et $[x \mapsto -x]$.
4. Il existe autant de morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ que d'éléments de $\mathbb{Z}/m\mathbb{Z}$ dont l'ordre divise n.

Multiplication modulo n

42.1 Quels que soient $\alpha \in \mathscr{C}(a)$ et $\beta \in \mathscr{C}(b)$,

$$\mathscr{C}(\alpha\beta) = \mathscr{C}(ab).$$

42.2 ✍ *Soient C_1 et C_2 dans $\mathbb{Z}/n\mathbb{Z}$: il existe a et b dans $\mathbb{Z}$ tels que $C_1 = \mathscr{C}(a)$ et $C_2 = \mathscr{C}(b)$ et le **produit** de C_1 et de C_2 est défini par*

$$C_1 \otimes C_2 = \mathscr{C}(ab).$$

42.3 ➔ *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de $\oplus$ et de $\otimes$ est un anneau commutatif.*

43. **Calculs de puissances**
43.1

$$\forall\, a \in \mathbb{Z}, \forall\, m \in \mathbb{N}^*, \quad \mathscr{C}(a^m) = \mathscr{C}(a)^{\otimes m}.$$

43.2 La suite des puissances de $\mathscr{C}(a)$ dans $\mathbb{Z}/n\mathbb{Z}$ est périodique à partir d'un certain rang :

$$\exists\, 1 \leqslant p \leqslant n,\ \exists\, 0 \leqslant n_0 < n,\ \forall\, q \geqslant n_0, \quad \big[\mathscr{C}(a)\big]^{q+p} = \big[\mathscr{C}(a)\big]^q.$$

43.3 **Exemples**
1. Le chiffre des unités de $7^{(7^7)}$ est égal à 3 et celui de $(7^7)^7$ est égal à 7.
2. Le chiffre des unités de 1789^{1515} est égal à 9.
3. $5^{2n} + 5^n = 0 \pmod{13} \iff n = 2 \pmod 4$.
4. L'équation $x^3 = x$ a trois solutions dans $\mathbb{Z}/11\mathbb{Z}$, mais elle en a 9 dans $\mathbb{Z}/12\mathbb{Z}$.

5. Pour tout $n \in \mathbb{N}$:

$$\begin{aligned} 5n^3 + n &= 0 \pmod 6 \\ 3^{2n+1} + 2^{n+2} &= 0 \pmod 7 \\ 2^{2n+1} + 3^{2n+1} &= 0 \pmod 5 \\ 5^4.3^{8n} + 7^3.5^{6n} &= 0 \pmod{11} \\ 4^n &= 3n+1 \pmod 9 \\ 16^n &= 15n+1 \pmod{225} \end{aligned}$$

Morphisme canonique

44. ✍ *L'application $\mathscr{C} : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est appelée* ***réduction modulo*** *n ou* ***projection canonique sur*** *$\mathbb{Z}/n\mathbb{Z}$.*

45. ➔ *La réduction modulo n est un morphisme surjectif de l'anneau $(\mathbb{Z}, +, \times)$ sur l'anneau $(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$ et son noyau est $n\mathbb{Z}$.*

46. Preuve par 9
Pour tout entier $a \in \mathbb{N}$, on note n_a, la somme des chiffres utilisés pour écrire a en base dix (écriture décimale habituelle) et on suppose ici que $\mathscr{C}$ désigne la réduction modulo 9.

1. $$\forall\, a \in \mathbb{N}, \quad \mathscr{C}(a) = \mathscr{C}(n_a).$$
2. Si $c = ab$, alors $\mathscr{C}(n_c) = \mathscr{C}(n_a) \otimes \mathscr{C}(n_b)$.

II.3 Groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

47. Exemples de tables de multiplication
L'élément 0 est absorbant pour la multiplication dans chaque anneau : il est inutile de le faire apparaître dans la table de multiplication.
Les anneaux considérés sont commutatifs : les tables de multiplication sont symétriques.

Table de $\mathbb{Z}/5\mathbb{Z}$

	1	2	3	4
1×	1	2	3	4
2×	2	4	1	3
3×	3	1	4	2
4×	4	3	2	1

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

	1	2	3	4	5
1×	1	2	3	4	5
2×	2	4	0	2	4
3×	3	0	3	0	3
4×	4	2	0	4	2
5×	5	4	3	2	1

Les carrés apparaissent sur la diagonale.
Un élément est inversible si, et seulement si, le nombre 1 apparaît dans sa colonne.
Un élément est un diviseur de zéro si, et seulement si, le nombre 0 apparaît dans sa colonne.

48. Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$
Soit $n \in \mathbb{N}$, non nul.
48.1 La classe $\mathscr{C}(n-1)$ est inversible et égale à son inverse.
48.2 ➔ *La classe $\mathscr{C}(a)$ est inversible pour la structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, a et n sont premiers entre eux.*
48.3 Si $1 < p < n$ divise n, alors la classe $\mathscr{C}(p)$ est un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$.

49. ➔ *L'anneau $(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$ est un corps si, et seulement si, l'entier n est un nombre premier.*

50. Soit $n \in \mathbb{N}^*$.
50.1 Le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\mathscr{C}_n(1)$.
50.2 ➔ *L'élément $\mathscr{C}_n(k)$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, il est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

51. Exemples
51.1 Il y a 24 éléments inversibles dans $\mathbb{Z}/78\mathbb{Z}$.
51.2 Dans l'anneau $\mathbb{Z}/5\mathbb{Z}$, l'élément 3 est inversible et l'équation $3x + 5 = 0$ admet $x = 0$ pour seule solution.
51.3 Dans un anneau de cardinal *fini*, on peut chercher les racines d'un polynôme en évaluant ce polynôme en chaque point. Dans un *corps fini*, on peut ainsi obtenir la forme factorisée **[25]** de ce polynôme. Ainsi, dans $\mathbb{Z}/7\mathbb{Z}$,

$$X^5 - 3X^4 - 2X^3 + 2X^2 + 3X - 1 = (X-1)(X-3)^2(X+2)^2.$$

51.4 Sur le corps $\mathbb{Z}/5\mathbb{Z}$, le système

$$\begin{cases} 3x + y = 3 \\ x + y = 1 \end{cases}$$

est un système de Cramer et admet $(1, 0)$ pour unique solution. Sur l'anneau $\mathbb{Z}/4\mathbb{Z}$, son déterminant n'est pas inversible et le système admet $(1, 0)$ et $(3, 2)$ pour solutions.
51.5 Le système

$$\begin{cases} 6x + 7y = 30 \\ 3x - 7y = 0 \end{cases}$$

admet $(28, 12)$ pour seule solution dans $\mathbb{Z}/37\mathbb{Z}$.

52. Petit théorème de Fermat
Le *petit théorème de Fermat* permet de simplifier le calcul des puissances d'un entier n modulo un nombre premier p. Ce résultat sera généralisé avec le théorème d'Euler **[63.3]**.
52.1 Si p est un nombre premier, alors pour tout $1 \leqslant k < p$, le coefficient binomial $\binom{p}{k}$ est un multiple de p.
52.2 ➔ *Soit p, un nombre premier. Pour tout $n \in \mathbb{N}$,*

$$n^p = n \pmod p$$

et si n n'est pas un multiple de p, alors

$$n^{p-1} = 1 \pmod p.$$

52.3 Applications simples
1. $2^{123} + 3^{121} = 0 \pmod{11}$
2. $1234^{4321} + 4321^{1234} = 4 \pmod 7$

52.4 Résidus quadratiques
Soient $p \geqslant 2$, un nombre premier et $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$.
On pose $q = (p-1)/2$.
1. Si le degré de $P \in \mathbb{K}[X]$ est égal à $d \in \mathbb{N}$, alors **[6.81.** 4**]** le polynôme P admet au plus d racines dans le corps $\mathbb{K}$.
2. Il y a exactement q carrés non nuls dans $\mathbb{K}$ et chaque carré $x \neq 0$ est une racine de $(X^q - 1)$.
3. Le polynôme $X^{p-1} - 1 = (X^q - 1)(X^q + 1)$ est scindé à racines simples dans $\mathbb{K}$.
4. Un élément non nul x de $\mathbb{Z}/p\mathbb{Z}$ est un carré si, et seulement si, $x^q = 1$.

II.4 Lemme chinois

53. Soient m et n, deux entiers premiers entre eux.
53.1 Il existe deux entiers e_1 et e_2 tels que

$$\begin{cases} e_1 \equiv 1 \pmod m \\ e_1 \equiv 0 \pmod n \end{cases} \quad \text{et que} \quad \begin{cases} e_2 \equiv 0 \pmod m \\ e_2 \equiv 1 \pmod n. \end{cases}$$

53.2 Si x et x' sont deux entiers tels que

$$\begin{cases} x \equiv x' \pmod m \\ x \equiv x' \pmod n, \end{cases}$$

alors $x \equiv x' \pmod{mn}$.
53.3 ➔ *Si m et n sont deux entiers premiers entre eux, alors*

$$\forall\, (a,b) \in \mathbb{Z}^2,\ \exists\, x \in \mathbb{Z}, \quad \begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n. \end{cases}$$

De plus, si x_0 est une solution particulière de ce système, alors x est une solution de ce système si, et seulement si,

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

54. Un isomorphisme canonique
Soient m et n, deux entiers naturels premiers entre eux.
54.1 L'application

$$\begin{aligned} \Phi : \mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ k &\mapsto \big(\mathscr{C}_m(k), \mathscr{C}_n(k)\big) \end{aligned}$$

est un morphisme de groupes.

54.2 Il existe un morphisme d'anneaux Ψ de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tel que →[98.3]

$$\forall\, k \in \mathbb{Z}, \quad \Psi\big(\mathscr{C}_{mn}(k)\big) = \big(\mathscr{C}_m(k), \mathscr{C}_n(k)\big).$$

54.3 ➔ *L'application Ψ est un isomorphisme d'anneaux de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

54.4 Action sur les éléments inversibles

1. L'image $\Psi(x)$ de tout élément inversible $x \in (\mathbb{Z}/mn\mathbb{Z})^\times$ appartient à $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.
2. Quels que soient $\alpha \in (\mathbb{Z}/m\mathbb{Z})^\times$ et $\beta \in (\mathbb{Z}/n\mathbb{Z})^\times$, il existe un, et un seul, $x \in (\mathbb{Z}/mn\mathbb{Z})^\times$ tel que $\Psi(x) = (\alpha, \beta)$.

L'isomorphisme Ψ induit une bijection de l'ensemble $(\mathbb{Z}/mn\mathbb{Z})^\times$ sur le produit cartésien $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. →[64.3]

55. Généralisation

55.1 Soient $m_1, m_2, \ldots, m_n$, des entiers naturels deux à deux premiers entre eux.

1. Pour tout $1 \leqslant i \leqslant n$, on pose

$$M_i = \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} m_j$$

et [**20.2**] il existe $u_i \in \mathbb{Z}$ tel que $M_i u_i \equiv 1 \pmod{m_i}$.

2. Quels que soient les entiers $a_1, a_2, \ldots, a_n$, l'entier

$$x = \sum_{i=1}^{n} a_i M_i u_i \in \mathbb{Z}$$

vérifie $x \equiv a_i \pmod{m_i}$ pour tout $1 \leqslant i \leqslant n$.

2.a Si $y \in \mathbb{Z}$ vérifie $y \equiv a_i \pmod{m_i}$ pour tout $1 \leqslant i \leqslant n$, alors la différence $x - y$ est divisible par le produit $m_1 m_2 \cdots m_n$.

55.2 Un entier x

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 1 \pmod 6 \\ x \equiv 2 \pmod 7 \end{cases}$$

si, et seulement si,

$$\exists\, k \in \mathbb{Z}, \quad x = 163 + 210k.$$

Entraînement

56. Questions pour réfléchir

1. Si $a = b \pmod n$, alors $a^n = b^n \pmod{n^2}$.
2. Soit $n \geqslant 2$, un entier.

2.a Soit $x \in \mathbb{N}^*$. Il existe $k \in \mathbb{N}$ tel que n divise x^k si, et seulement si, tout diviseur premier de n est aussi un diviseur premier de x.

2.b Il existe des éléments nilpotents dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, n est divisible par le carré d'un nombre premier.

57. Soient $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, avec p premier. Pour tout $k \in \mathbb{N}^*$, on pose

$$\sigma_k = \sum_{x \in \mathbb{K}} x^k.$$

Comme

$$\sigma_k^2 = \sum_{a \in \mathbb{K}^*} \sum_{x \in \mathbb{K}} (ax)^k = (p-1)\sigma_k,$$

alors σ_k est égal à 0 ou à -1.

58. Applications du lemme chinois [53.3]

Un entier $x \in \mathbb{N}$ est une solution du système

$$\begin{cases} x = 1 \pmod 6 \\ x = 2 \pmod 7 \end{cases}$$

si, et seulement si, il existe $k \in \mathbb{N}$ tel que $x = 37 + 42k$.

Un entier $x \in \mathbb{N}$ est une solution du système

$$\begin{cases} 3x = 2 \pmod 5 \\ 5x = 1 \pmod 6 \end{cases}$$

si, et seulement si, il existe $k \in \mathbb{N}$ tel que $x = 29 + 30k$.

59. Équations du second degré dans $\mathbb{Z}/n\mathbb{Z}$

Quel que soit l'anneau A dans lequel on calcule, on résout une équation de la forme

$$ax^2 + bx + c = 0$$

en commençant par l'écrire sous forme réduite :

$$(x - \alpha)^2 = \beta.$$

Il suffit pour cela que a soit inversible dans A puis que ba^{-1} soit divisible par 2 dans A.

Il reste alors à trouver les éléments $y \in A$ tels que $y^2 = \beta$.

59.1 Dans $\mathbb{Z}/8\mathbb{Z}$, l'équation $x^2 = 1$ admet quatre solutions : ± 1 et ± 3.

59.2 Dans $\mathbb{Z}/7\mathbb{Z}$, l'équation $x^2 + 3x + 4 = 0$ devient sous forme réduite $(x+5)^2 = 0$. Elle admet 2 pour seule solution.

59.3 Dans $\mathbb{Z}/5\mathbb{Z}$:

L'équation $x^2 + 2x + 2 = 0$ admet deux solutions : 1 et 2.

L'équation $x^2 - 3x = 1$ devient $(x+1)^2 = 2$ et n'a pas de solution.

59.4 Dans $\mathbb{Z}/9\mathbb{Z}$, l'élément $\mathscr{C}(2)$ est inversible, d'inverse $\mathscr{C}(5)$; l'image de $\big[x \mapsto x^2\big]$ est constituée des éléments $\mathscr{C}(0)$, $\mathscr{C}(1)$, $\mathscr{C}(4)$ et $\mathscr{C}(7)$.

L'équation $x^2 + bx + c = 0$ admet exactement deux solutions dans $\mathbb{Z}/9\mathbb{Z}$ si, et seulement si, son discriminant $b^2 - 4c$ est égal à 1, 4 ou 7.

59.5 Dans l'anneau $\mathbb{Z}/11\mathbb{Z}$, les solutions de l'équation

$$x^2 - 4x - 1 = 0$$

sont 6 et 9 ; les solutions du système

$$\begin{cases} x + y = 4 \\ xy = 10 \end{cases}$$

sont $(6,9)$ et $(9,6)$.

60. Nombres de Carmichael

Un entier $n \geqslant 2$ est un **nombre de Carmichael** lorsque

$$\forall\, a \in \mathbb{N}^*, \quad a^{n-1} = 1 \pmod n$$

sans être un nombre premier. →[52]

60.1 Rédiger une procédure vérifiant si un entier n donné est, ou non, un nombre de Carmichael.

60.2 On suppose qu'un nombre de Carmichael n admet un facteur carré : il existe donc deux entiers p et m tels que $n = p^2 m$. Avec $a = 1 + pm$, on obtient

$$a^n = 1 \pmod n = 1 + pm \pmod n,$$

ce qui est absurde : les nombres de Carmichael n'admettent pas de facteur carré.

61. Exemples et contre-exemples de groupes cycliques

1.a Les groupes $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ et $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \oplus)$ sont cycliques.

1.b Le groupe multiplicatif $(\mathbb{Z}/7\mathbb{Z})^\times$ est engendré par $\mathscr{C}_7(3)$.

1.c Les groupes $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{U}_6$, $(\mathbb{Z}/7\mathbb{Z})^\times$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ sont isomorphes.

2. Le groupe multiplicatif $(\mathbb{Z}/9\mathbb{Z})^\times$ est cyclique, isomorphe à $\mathbb{Z}/6\mathbb{Z}$.
3. Le groupe $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \oplus)$ n'est pas cyclique.
4. Les éléments du groupe multiplicatif $(\mathbb{Z}/8\mathbb{Z})^\times$ sont tous d'ordre inférieur à 2. Ce groupe n'est pas cyclique.
5. Le groupe multiplicatif $(\mathbb{Z}/15\mathbb{Z})^\times$ n'est pas cyclique.

III

Applications de l'arithmétique modulaire

III.1 Indicatrice d'Euler

62. ✍ *L'**indicatrice d'Euler** (ou* Euler totient function*) est l'application de $\mathbb{N}^*$ dans $\mathbb{N}$ qui, à tout entier $n \geqslant 1$, associe le nombre $\varphi(n)$ d'entiers $1 \leqslant k \leqslant n$ qui sont premiers à n.*

63.1 Pour tout $n \in \mathbb{N}^*$, l'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal à $\varphi(n)$.

63.2

$$\forall\, x \in (\mathbb{Z}/n\mathbb{Z})^\times, \quad x^{\varphi(n)} = 1$$

63.3 ➔ **Théorème d'Euler**

$$\forall\, x \in \mathbb{Z}, \quad x \wedge n = 1 \Rightarrow x^{\varphi(n)} \equiv 1 \pmod{n}$$

63.4 Le théorème d'Euler **[63.3]** est une généralisation du petit théorème de Fermat **[52]**.

64. Expression de l'indicatrice d'Euler

64.1 Si p est premier, alors $\varphi(p) = p - 1$ et

$$\forall\, x \in \mathbb{Z}/p\mathbb{Z}, \quad x^p = x$$

soit

$$\forall\, x \in \mathbb{Z}, \quad x^p \equiv x \pmod{p}.$$

64.2 Si p est premier et si α est un entier supérieur à 2, alors

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

64.3 L'indicatrice d'Euler est une **fonction multiplicative** :

$$\forall\, (m,n) \in \mathbb{Z}^2, \qquad m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n).$$

64.4 ➔ *Connaissant la décomposition en produit de facteurs premiers*

$$n = \prod_{k=1}^{q} p_k^{m_k}$$

(où les nombres premiers p_k sont deux à deux distincts et les multiplicités m_k sont strictement positives), on en déduit que :

$$\varphi(n) = \prod_{k=1}^{q} p_k^{m_k-1}(p_k - 1).$$

65. Utilisation

Pour calculer les deux dernières décimales de 3^{1789}, il suffit de savoir que $\varphi(100) = 40$, mais il vaut mieux remarquer que $3^{20} = 1 \pmod{100}$.

Pour calculer les deux dernières décimales de 4^{2016}, la connaissance de $\varphi(100)$ est inutile. On aboutit au résultat avec la relation :

$$\forall\, (k,r) \in \mathbb{N} \times \mathbb{N}^*, \quad 4^{10k+r} = 4^r \pmod{100}.$$

III.2 Éléments de cryptographie

66. *Crypter* un message M, c'est lui appliquer une transformation f pour transmettre le message $M' = f(M)$; *décrypter* le message transmis, c'est lui appliquer la bijection réciproque g de f pour obtenir $M = g(M')$.

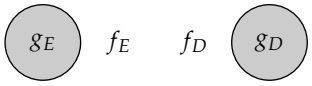
67. Les méthodes les plus anciennes de cryptage supposaient que les deux fonctions f et g étaient connues seulement de l'expéditeur et du destinataire de M. Il fallait donc pouvoir transmettre un message ultra-secret (les deux fonctions f et g) avant de transmettre des messages secrets.

La cryptographie par clé publique est assez récente (Diffie & Hellmann, 1976) et plus subtile.

Cryptographie à clés publiques

68. Tout d'abord, on doit choisir la fonction de cryptage f pour que la connaissance de f ne permette pas *dans la pratique* de trouver la fonction de décryptage g. La fonction f peut alors être publiée (sur le site internet de son possesseur) sans que personne puisse en déduire la fonction g. La fonction f est la **clé publique** *a priori* connue de tous ; la fonction g est la **clé privée** et ne reste connue que d'une seule personne.

69. Ensuite, l'expéditeur E d'un message M et son destinataire D doivent chacun disposer d'un couple de fonctions de cryptage et décryptage : (f_E, g_E) et (f_D, g_D).



Les clés privées (sur fond gris) ne sont connues que de leurs propriétaires respectifs. Les clés publiques sont connues de tous.

69.1 L'expéditeur du message M dispose alors de sa clé privée g_E et des deux clés publiques f_E et f_D, ce qui lui permet d'envoyer le message chiffré

$$M' = f_D \circ g_E(M).$$

69.2 Le destinataire du message chiffré dispose de sa clé privée g_D et des deux clés publiques f_D et f_E : il reçoit M' et peut donc en déduire le message original, puisque

$$M = f_E \circ g_D(M').$$

69.3 Seul le destinataire dispose de g_D et peut donc décoder M'. Le message ainsi transmis reste donc secret, car illisible par un tiers.

69.4 Seul l'expéditeur dispose de g_E et peut donc composer le message chiffré M'. Le message transmis est donc authentifié, car non modifiable par un tiers.

Le système RSA

70. Soient p et q, deux nombres premiers distincts. On pose

$$n = pq$$

et on choisit deux entiers r et s tels que

$$rs \equiv 1 \mod \varphi(n).$$

70.1 L'entier $\varphi(n)$ est égal à $(p-1)(q-1)$ et il existe $k \in \mathbb{N}$ tel que $rs = k(p-1)(q-1) + 1$ et

$$\begin{aligned} \forall\, x \in \mathbb{Z}, \quad x^{rs} &\equiv x \pmod{p} \\ &\equiv x \pmod{q}. \end{aligned}$$

70.2 Les applications

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \quad \text{et} \quad g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

définies par

$$\forall\, u \in \mathbb{Z}/n\mathbb{Z}, \qquad f(u) = u^r \quad \text{et} \quad g(u) = u^s$$

sont bijectives et réciproques l'une de l'autre.

71. Considérations pratiques [70]

Le couple (n,r) est public, ce qui permet à chacun de calculer facilement $f(x)$ pour tout $x \in \mathbb{Z}$.

Pour déterminer la bijection réciproque g, il faut connaître le couple (n,s) et il suffit pour cela de savoir expliciter la factorisation $n = pq$. C'est évidemment possible en théorie, mais les entiers p et q ayant chacun un très grand nombre de décimales, le calcul de la factorisation est trop long pour aboutir dans un délai raisonnable en pratique.

Ce système de cryptographie est dû à Rivest, Shamir & Adelman (1978).

IV

Résolution de l'équation de Bézout

72. L'algorithme d'Euclide permet de calculer un pgcd $d \in A$ de deux éléments a et b de A et, par définition du pgcd, l'équation de Bézout

$$au + bv = d \tag{2}$$

admet des solutions $(u, v) \in A \times A$. Comment calculer ces solutions ?

73. Réduction du problème
Il existe α et β tels que $a = d\alpha$ et $b = d\beta$ et :

$$au + bv = d \iff \alpha u + \beta v = 1.$$

Il suffit donc de savoir trouver les solutions $(u, v) \in A \times A$ de l'équation de Bézout lorsque a et b sont premiers entre eux :

$$au + bv = 1. \tag{3}$$

74. Solution générale
Le principe de superposition s'applique à l'équation de Bézout : Si (u_0, v_0) est une solution particulière de (3), alors (u, v) est une solution de (3) si, et seulement si,

$$\exists\, k \in A, \quad (u, v) = (u_0, v_0) + k(-b, a).$$

Solution minimale

75. On cherche une solution de (3) qui soit, en un certain sens, aussi petite que possible.

76. Cas de $\mathbb{K}[X]$
Soient a et b, deux polynômes de $\mathbb{K}[X]$ tels que $\deg a \geqslant 1$ et que $\deg b \geqslant 1$.

1. Si q est le quotient de la division euclidienne de u_0 par b, alors $(u_1, v_1) = (u_0 - qb, v_0 + qa)$ est une solution de (3) telle que
$$\deg a - \deg v_1 = \deg b - \deg u_1 > 0.$$
et $-q$ est le quotient de la division euclidienne de v_0 par a.
2. Pour toute autre solution (u, v) de (3),
$$\deg u > \deg u_1 \quad \text{et} \quad \deg v > \deg v_1.$$

77. Cas de $\mathbb{Z}$
Soient a et b, deux entiers naturels supérieurs à 2, qu'on suppose premiers entre eux.

1. Il existe deux solutions (u_1, v_1) et (u_2, v_2) de (3) telles que $-b < u_2 < 0 < u_1 < b$ et $-a < v_1 < 0 < v_2 < a$.
2. Il existe une solution $(u_0, v_0) \in \mathbb{Z}^2$ de l'équation (3) telle que
$$|u| + |v| \geqslant |u_0| + |v_0|$$
pour toute autre solution (u, v) de (3).

Algorithme de Blankinship

78. L'algorithme d'Euclide classique permet de calculer un pgcd de deux éléments, puis d'en déduire un ppcm et (plus laborieusement) une solution particulière de l'équation de Bézout. Nous allons exposer un algorithme qui permet de calculer *simultanément* un pgcd *et* un ppcm de deux éléments a et b de A ainsi qu'une solution particulière de l'équation de Bézout. (W.A. Blankinship, *A new version of the euclidean algorithm*, American Mathematical Monthly, 1963, pp.742–745)

78.1 Pour tout entier n compris entre 0 et un rang N à déterminer, nous allons définir une matrice

$$M_n = \begin{pmatrix} \alpha_n & \beta_n & a_n \\ \gamma_n & \delta_n & b_n \end{pmatrix}$$

à coefficients dans l'anneau A.

78.2 Initialisation
Soient a et b dans A. On pose

$$X_0 = \begin{pmatrix} a \\ b \\ -1 \end{pmatrix} \quad \text{et} \quad M_0 = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix}$$

de telle sorte que la matrice colonne $M_0 X_0$ est nulle.

78.3 Itération
Si la matrice M_n est connue, alors :

1. Ou bien $b_n = 0$, et la procédure est achevée $(N = n)$;
2. Ou bien $b_n \neq 0$ et dans ce cas,

2.a on effectue la division euclidienne de a_n par b_n :

$$a_n = q_n b_n + r_n$$

2.b on effectue sur M_n les opérations $L_1 \leftarrow L_1 - q_n L_1$ puis $L_1 \leftrightarrow L_2$, c'est-à-dire

$$M_{n+1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -q_n \\ 0 & 1 \end{pmatrix} M_n.$$

En particulier, $a_{n+1} = b_n$ et $b_{n+1} = r_n$.

78.4 Conclusion
À la fin de la procédure, la matrice M_N est de la forme

$$\begin{pmatrix} \alpha_N & \beta_N & a_N \\ \gamma_N & \delta_N & 0 \end{pmatrix}$$

où a_N est un pgcd de a et b ; où (α_N, β_N) est une solution de l'équation de Bézout :

$$\alpha_N a + \beta_N b = a_N$$

et où $a\gamma_N = -b\delta_N$ est un ppcm de a et b.

79. Terminaison de l'algorithme
La famille de terme général $|b_n|$ (pour $A = \mathbb{Z}$) ou $\deg b_n$ (pour $A = \mathbb{K}[X]$) est une famille strictement décroissante d'entiers naturels.

80. Preuve de l'algorithme

1. Pour tout $0 \leqslant n < N$,
$$a_{n+1} \wedge b_{n+1} = a_n \wedge b_n$$
et en particulier
$$a_N = a_N \wedge b_N = a_0 \wedge b_0 = a \wedge b.$$

2.a Pour tout $0 \leqslant n \leqslant N$,

$$M_n = \begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix} M_0 \quad \text{et} \quad \alpha_n \delta_n - \beta_n \gamma_n = (-1)^n$$

et la matrice colonne $M_n X_0$ est nulle.

2.b La première ligne de la relation $M_N X_0 = 0$ donne une solution particulière de l'équation de Bézout.

2.c La deuxième ligne de la relation $M_N X_0 = 0$ donne

$$(a\gamma_N)d = (-b\delta_N)d = -ab(\alpha_N \delta_N - \beta_N \gamma_N),$$

donc $m = a\gamma_N = -b\delta_N$ est un ppcm de a et b.

Questions, exercices & problèmes

Perfectionnement

81. Exemples et contre-exemples

1. Exemples d'éléments nilpotents :
1.a dans $\mathbb{Z}/15\mathbb{Z}$;
1.b dans $\mathbb{Z}/12\mathbb{Z}$.
2. Exemple de polynôme à coefficients dans $\mathbb{Z}/6\mathbb{Z}$ admettant deux factorisations différentes.

82. Méthodes

1. Comment calculer facilement $\mathscr{C}(a^m)$?
2. Comment résoudre une équation polynomiale dont l'inconnue appartient à $\mathbb{Z}/n\mathbb{Z}$?
3. Comment factoriser un polynôme dont les coefficients appartiennent à $\mathbb{Z}/n\mathbb{Z}$?
4. *Suite de* **[77]** –

4.a Comment programmer le calcul de (u_0, v_0) ?

4.b Comment vérifier expérimentalement l'unicité de la solution (u_0, v_0) ?

83. Questions pour réfléchir

1. Soient P et Q dans $\mathbb{R}[X]$. Si $D \in \mathbb{R}[X]$ est un pgcd de P et Q considérés comme des éléments de $\mathbb{R}[X]$, alors D est aussi un pgcd de P et Q considérés comme des éléments de $\mathbb{C}[X]$.
2. Discuter l'existence du pgcd d'une famille infinie d'éléments de A.
3. Discuter l'existence du ppcm d'une famille infinie d'éléments de A.
4. Relier la propriété **[20.2]** :

$$\frac{1}{P} = \sum_{k=1}^{n} \frac{A_k}{P_k}$$

à l'existence d'une **décomposition en éléments simples** pour la fraction rationnelle $1/P$.

5. Discuter l'intérêt pratique des formules **[26]**.
6. *Suite de* **[78]** – Généraliser l'algorithme pour calculer le pgcd d'une famille finie d'éléments de A.

Approfondissement

84. Soit n, un entier naturel non nul. Le nombre N de diviseurs positifs de n et le produit P des diviseurs positifs de n sont liés par l'égalité $P^2 = n^N$.

85. Factorisation dans $\mathbb{Q}[X]$

1. Soient $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ et $r \in \mathbb{Q}$, une racine de P représentée sous forme irréductible par $r = p/q$. L'entier p divise a_0 et l'entier q divise a_n. La différence $q - p$ divise $P(1)$ et la somme $q + p$ divise $P(-1)$.
2. Comment programmer le calcul de *toutes* les racines rationnelles d'un polynôme à coefficients *rationnels* ?
3. Comment obtenir la factorisation suivante ?

$$29X^3 - 175X^2 + 267X - 9 = (X-3)^3(29X-1)$$

4. Le polynôme $Q = 3X^3 - 19X^2 + 33X + 9$ est irréductible dans $\mathbb{Q}[X]$.

86. Factorisations dans $\mathbb{Z}$

On démontre qu'un entier est composé **[6.69.1]** en le factorisant sous la forme d'un produit de deux entiers supérieurs à 2.

86.1 *Suite de* **[85]** – Pour tout $n \in \mathbb{Z}$, l'entier $n^4 - n + 16$ est composé.

86.2 L'entier $4n^3 + 6n^2 + 4n + 1 = (n+1)^4 - n^4$ est composé pour tout $n \in \mathbb{N}^*$.

86.3 Série géométrique

1. Pour tout entier $a \geqslant 3$ et tout entier $n \geqslant 2$, l'entier $a^n - 1$ est composé.
2. Pour tout $n \in \mathbb{N}$, on pose

$$U_n = 1 + 10 + 10^2 + \cdots + 10^n.$$

2.a Si n est divisible par 3, alors U_{n-1} est divisible par 3.

2.b Si p est un nombre premier distinct de 2, 3 et 5, alors p divise $10^{p-1} - 1$ et U_{p-2}.

86.4 Nombres de Mersenne

Si l'entier $a^p - 1$ est premier avec $a \geqslant 2$ et $p \geqslant 2$, alors $a = 2$ et p est premier.

La réciproque est fausse, puisque $2^{11} - 1 = 23 \times 89$.

87. Triplets pythagoriciens

On étudie les solutions $(x, y, z) \in \mathbb{N}^3$ de l'équation

$$x^2 + y^2 = z^2. \tag{4}$$

87.1 Analyse

Soit $(x, y, z) \in \mathbb{N}^3$, une solution de (4).

1. Les pgcd $x \wedge y$, $y \wedge z$ et $z \wedge x$ sont égaux.
2. On suppose que x, y et z sont deux à deux premiers entre eux.

2.a Les entiers x et y sont de parités différentes : l'un est pair, l'autre est impair.

2.b On suppose que x est pair et que y est impair :

$$\exists\, (m, n, q) \in \mathbb{N}^3, \quad x = 2m, \quad y = 2n+1, \quad z = 2q+1.$$

Alors

$$m^2 = (n+q+1)(q-n)$$

et les facteurs $n+q+1$ et $q-n$ sont premiers entre eux, donc il existe deux entiers k et □, premiers entre eux, tels que

$$n + q + 1 = \pm k^2 \quad \text{et} \quad q - n = \pm □^2.$$

87.2 Synthèse

Le triplet $(x, y, z) \in \mathbb{N}^3$ est solution de (4) si, et seulement si, il existe deux entiers $0 \leqslant k < □$ premiers entre eux tels que →**[19]**

$$(x, y, z) = (2k□,\ □^2 - k^2,\ □^2 + k^2).$$

88. Soient m et n, deux entiers naturels non nuls.

1. Si la division euclidienne de m par n s'écrit $m = qn + r$ avec $q \geqslant 2$, alors

$$X^m - 1 = X^r(X^n - 1)(X^{(q-1)n} + \cdots + X^n + 1) + (X^r - 1).$$

Que devient cette relation pour $q = 1$ et $q = 0$?

2. Le pgcd de $(X^m - 1)$ et de $(X^n - 1)$ est égal au pgcd de $(X^n - 1)$ et de $(X^r - 1)$.
3. Le pgcd de $(X^m - 1)$ et de $(X^n - 1)$ est égal à $(X^{m \wedge n} - 1)$.

89. Points entiers d'une hyperbole

1. Soit p, un nombre premier.

Pour tout $n \in \mathbb{N}$, le pgcd de n et de $(n - p)$ est égal à 1 ou à p.

2. Les couples $(x, y) \in \mathbb{Z}^2$ qui appartiennent à l'hyperbole $[xy = 2x + 3y]$ sont :

$$(-3,1), (0,0), (1,-1), (2,-4), (4,8), (5,5), (6,4), (9,3).$$

3. Les couples $(x, y) \in \mathbb{Z}^2$ qui appartiennent à l'hyperbole $[xy = 5x + 5y]$ sont :

$$(-20,4), (0,0), (4,-20), (6,30), (10,10), (30,6).$$

4. Si $(x, y) \in \mathbb{Z}^2$ est un point de l'hyperbole

$$\mathscr{H} = [x^2 - y^2 - 4x - 2y = 5]$$

alors $(x + y - 1)(x - y - 3) = 10$.

Comme $(x + y - 1)$ et $(x - y - 3)$ ont même parité, l'hyperbole $\mathscr{H}$ ne rencontre pas $\mathbb{Z}^2$.

90.1 Le couple $(x, y) \in \mathbb{N}^2$ est une solution de

$$\begin{cases} x \wedge y = 5 \\ x \vee y = 60 \end{cases}$$

si, et seulement si, il existe un couple (α, β) tel que

$$(x, y) = (5\alpha, 5\beta) \quad \text{et} \quad \{\alpha, \beta\} = \{1, 12\} \quad \text{ou} \quad \{3, 4\}.$$

90.2 Le couple $(x,y) \in \mathbb{N}^2$ est une solution de

$$\begin{cases} x+y &= 100 \\ x \wedge y &= 10 \end{cases}$$

si, et seulement si, il existe un couple (α,β) tel que

$$(x,y) = (10\alpha, 10\beta) \quad \text{et} \quad \{\alpha,\beta\} = \{1,9\} \quad \text{ou} \quad \{3,7\}.$$

90.3 Le couple $(x,y) \in \mathbb{N}^2$ est une solution de

$$\begin{cases} 11x - 5y &= 10 \\ x \wedge y &= 10 \end{cases}$$

si, et seulement si, il existe un entier $k \in \mathbb{N}$ tel que

$$(x,y) = (10\alpha, 10\beta) \quad \text{où} \quad (\alpha,\beta) = (1+5k, 2+11k).$$

91. Théorème de Wilson
Le théorème de Wilson est une caractérisation, peu utile, des entiers premiers.
91.1 Soit p, un nombre premier.
1. Résoudre l'équation $x^2 = 1$ dans $\mathbb{Z}/p\mathbb{Z}$.
2. Si $p \geqslant 3$, il y a $(p-3)$ éléments inversibles et distincts de leur inverse dans $\mathbb{Z}/p\mathbb{Z}$, donc $(p-1)! \equiv -1 \pmod{p}$.

91.2 Soit n, un nombre composé. Il existe donc deux entiers p et q tels que $2 \leqslant p \leqslant q \leqslant n-1$ et que $n = pq$.
3. Si $p < q$, alors $(n-1)! = 0 \pmod{n}$.
4. Si $3 \leqslant p = q$, alors $2 \leqslant p < 2p \leqslant n-1$ et $(n-1)!$ est un multiple de n.

91.3 ➔ *Un entier $n \geqslant 2$ est premier si, et seulement si,*

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

92. Soient a, b et c, trois entiers compris entre 0 et 4, l'entier a étant non nul. On suppose qu'un entier N s'écrit $abc0$ en base 5 et abc en base 12 :

$$N = 5^3a + 5^2b + 5c = 12^2a + 12b + c.$$

Déterminer a, b, c et N en raisonnant dans $\mathbb{Z}/4\mathbb{Z}$.

93. Soit $f : \mathbb{Z} \to \mathbb{R}$, une fonction non identiquement nulle telle que

$$\forall\, p \in \mathbb{Z}, \quad f(2p) = 0 \quad \text{et} \quad f(p+4) = f(p)$$

et que

$$\forall\, (p,q) \in \mathbb{Z}^2, \quad f(pq) = f(p)f(q).$$

Que vaut $f(1)$? Que vaut $f(3)$? En déduire les valeurs de $f(k)$ pour tout $k \in \mathbb{Z}$.

94. Théorème de Lagrange [6.26.2] dans $\mathbb{Z}/n\mathbb{Z}$
Soient $n \in \mathbb{N}^*$ et $x \in \mathbb{Z}$. On note $d \in \mathbb{N}^*$, le pgcd de n et x.
1. Il existe $\delta \in \mathbb{N}^*$ et $\xi \in \mathbb{Z}$, premiers entre eux, tels que $n = d\delta$ et $x = d\xi$. L'entier n divise δx.
2. Si n divise kx, alors il existe $\square \in \mathbb{Z}$ tel que $kx = n\square$ et $k\xi = \square\delta$. L'entier δ divise k.
3. L'ordre de $\mathscr{C}(x)$ est égal à δ.

95. Si l'entier n admet $p_1^{\alpha_1} \cdots p_q^{\alpha_q}$ pour décomposition en produit de facteurs premiers, alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au produit

$$\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_q^{\alpha_q}\mathbb{Z}.$$

Relier cette factorisation au théorème [**49**].

96. Comparaison de groupes
On compare ici les groupes $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/np\mathbb{Z}$.
96.1 On pose $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Les images du morphisme $[x \mapsto 2x]$ en tant qu'application $G \to G$ et en tant qu'application $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes, donc les groupes G et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes.

96.2 L'addition dans le groupe produit $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est définie par la table suivante.

$\oplus$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$	$(1,2)$	$(0,2)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,2)$	$(0,2)$	$(1,0)$	$(0,0)$
$(0,2)$	$(0,2)$	$(1,2)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,2)$	$(1,2)$	$(0,2)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$

L'application

$$\begin{aligned} \theta : \mathbb{Z}/6\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\ \mathscr{C}_6(n) &\mapsto \big(n\mathscr{C}_2(1),\, n\mathscr{C}_3(1)\big) \end{aligned}$$

est un isomorphisme de groupes.

Pour aller plus loin

97. Questions pour réfléchir
1. Mettre au point un algorithme qui calcule les tables [**47**] et [**96**].
2. Un anneau intègre contient-il un élément nilpotent ? Et un anneau qui n'est pas intègre ?
3. *Suite de* [**14.1**] – Condition sur les entiers a, b, c et d pour que les entiers $an+b$ et $cn+d$ soient premiers entre eux pour tout $n \in \mathbb{N}$.

98. Théorèmes de factorisation
Pour un entier $n \geqslant 1$ fixé, on note $\mathscr{C}$, le morphisme canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$. [**36.2**]
98.1 Si $\psi : \mathbb{Z}/n\mathbb{Z} \to G$ est un morphisme de groupes, alors l'application $\varphi : \mathbb{Z} \to G$ définie par $\varphi = \psi \circ \mathscr{C}$ est un morphisme de groupes dont le noyau contient $n\mathbb{Z}$.
98.2 Premier théorème
Soit $\varphi : \mathbb{Z} \to G$, un morphisme de groupes.
Si $n\mathbb{Z} \subset \operatorname{Ker}\varphi$, alors il existe un, et un seul, morphisme de groupes

$$\psi : \mathbb{Z}/n\mathbb{Z} \to G$$

tel que $\varphi = \psi \circ \mathscr{C}$.
De plus, $\operatorname{Im}\varphi = \operatorname{Im}\psi$ et le morphisme ψ est injectif si, et seulement si, $\operatorname{Ker}\varphi = n\mathbb{Z}$.
98.3 Second théorème de factorisation
Soit $\varphi : \mathbb{Z} \to A$, un morphisme d'anneaux tel que $n\mathbb{Z} \subset \operatorname{Ker}\varphi$. Il existe un, et un seul, morphisme d'anneaux

$$\psi : \mathbb{Z}/n\mathbb{Z} \to A$$

tel que $\varphi = \psi \circ \mathscr{C}$.
98.4 Chercher un analogue au théorème de factorisation [**98.3**] pour les morphismes d'anneaux définis sur $\mathbb{K}[X]$.

99. Caractéristique d'un corps
Soit $(\mathbb{K}, +, \times)$, un corps.
99.1 L'application $\varphi : \mathbb{Z} \to \mathbb{K}$ définie par

$$\forall\, k \in \mathbb{Z}, \quad \varphi(k) = k \cdot 1_{\mathbb{K}}$$

est un morphisme d'anneaux.
99.2 Si $n = pq$ avec $1 < p \leqslant q < n$, alors il n'existe pas d'isomorphisme d'anneaux $\psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{K}$.
99.3 *Suite de* [**98.3**] – Si φ n'est pas injectif, alors il existe un nombre premier p tel que $\operatorname{Ker}\varphi = p\mathbb{Z}$.
99.4 ✍ *Un corps $\mathbb{K}$ est un* ***corps de caractéristique nulle*** *lorsque le morphisme $[k \mapsto k \cdot 1_{\mathbb{K}}]$ est injectif.*
99.5 ✍ *Un corps $\mathbb{K}$ est un* ***corps de caractéristique*** *p lorsque le noyau du morphisme $[k \mapsto k \cdot 1_K]$ est égal à $p\mathbb{Z}$.*
Dans ce cas, l'entier p est premier.

99.6 Exemples
Les corps $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(X)$, $\mathbb{R}(X)$, $\mathbb{C}(X)$ et

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2},\ (a,b) \in \mathbb{Q}^2\}$$

sont des corps de caractéristique nulle.
Les corps $\mathbb{Z}/2\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})(X)$ ont pour caractéristique 2.
99.7 Si $\mathbb{K}$ est un corps de caractéristique nulle, alors il existe un morphisme d'anneaux injectif de $\mathbb{Q}$ dans $\mathbb{K}$.

100. Quotients de $\mathbb{R}[X]$
On transpose ici à l'anneau $\mathbb{R}[X]$ l'étude de $\mathbb{Z}/n\mathbb{Z}$.
100.1 Exemples de calculs modulo P_0
Soient $A = X^{100} - X^4 + X - 1$ et $P_0 = X^3 + X^2 + X + 1$.

1. Il existe $P_1 \in \mathbb{R}[X]$ tel que $X^4 = 1 + P_1P_0$.
2. Il existe $P_2 \in \mathbb{R}[X]$ tel que $X^{100} = 1 + P_2P_0$.
3. Le reste de la division euclidienne du polynôme A par P_0 est égal à $(X - 1)$.

100.2 Généralisation
Soit $P_0 \in \mathbb{R}[X]$, un polynôme dont le degré est supérieur à 1. On pose

$$\forall\ P \in \mathbb{R}[X], \quad \mathscr{C}(P) = \{P + P_0Q,\ Q \in \mathbb{R}[X]\}$$

et

$$\mathbb{R}[X]/\langle P_0\rangle = \{\mathscr{C}(P),\ P \in \mathbb{R}[X]\}.$$

4. Définir une structure d'anneau sur $\mathbb{R}[X]/\langle P_0\rangle$ qui soit compatible avec la structure d'anneau de $\mathbb{R}[X]$.
5. Si $\deg P_0 = 1$, alors il existe un isomorphisme d'anneaux de $\mathbb{R}[X]/\langle P_0\rangle$ sur $\mathbb{R}$.
6. Si $P_0 = X^2 + 1$, alors il existe un isomorphisme d'anneaux de $\mathbb{R}[X]/\langle P_0\rangle$ sur $\mathbb{C}$.

101. Nombres de Fibonacci
La **suite de Fibonacci** est définie par la donnée de $F_0 = 0$, $F_1 = 1$ et par la relation de récurrence

$$\forall\ n \in \mathbb{N}, \quad F_{n+2} = F_{n+1} + F_n.$$

1. Comme

$$\forall\ n \geqslant 1, \quad F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

les entiers F_n et F_{n+1} sont premiers entre eux.
2. Soit $m \geqslant 1$.
2.a

$$\forall\ n \in \mathbb{N}, \quad F_{m+n} = F_mF_{n+1} + F_{m-1}F_n$$

2.b

$$\forall\ n \geqslant 1, \quad F_n \wedge F_{m+n} = F_n \wedge F_m$$

2.c Si r est le reste de la division euclidienne de m par n, alors

$$\forall\ n \geqslant 1, \quad F_m \wedge F_n = F_n \wedge F_r.$$

2.d

$$\forall\ m \geqslant 1,\ \forall\ n \geqslant 1, \quad F_m \wedge F_n = F_{m\wedge n}.$$

102. Critère d'Eisenstein
Soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p qui divise a_0, a_1, …, a_{n-1} mais ne divise pas a_n et que p^2 ne divise pas a_0.
1. On suppose qu'il existe

$$B = \sum_{k=0}^{m_1} b_kX^k \in \mathbb{Z}[X], \qquad C = \sum_{k=0}^{m_2} c_kX^k \in \mathbb{Z}[X]$$

tels que $A = BC$, avec $m_1 < n$ et $m_2 < n$.
1.a Comme $a_0 = b_0c_0$, alors b_0 ou c_0 est divisible par p. Est-il possible que p divise b_0 et c_0 ?
1.b Si $p \mid b_0$, alors $p \mid b_k$ pour tout $0 \leqslant k \leqslant m_1$ et, en particulier, $p \mid a_n$.
2. Le polynôme P est irréductible en tant qu'élément de l'anneau $\mathbb{Q}[X]$.
3. Le polynôme $X^5 - 12X^2 + 9X - 3 \in \mathbb{Q}[X]$ est irréductible.

103. Quotient par un idéal maximal
Soit A, un anneau commutatif. Un idéal $I \subsetneq A$ est dit **maximal** lorsque le seul idéal J de A tel que

$$I \subsetneq J \subset A$$

est l'idéal $J = A$.
103.1 Les idéaux maximaux de $A = \mathbb{K}[X]$ sont les idéaux engendrés par un polynôme irréductible.
Les idéaux maximaux de $\mathbb{Z}$ sont les idéaux engendrés par un nombre premier.
103.2 Soit I, un idéal de A. La **classe modulo** I de $x \in A$ est définie par

$$x + I = \{x + y,\ y \in I\}.$$

En particulier, l'idéal I est la classe de 0.
Le **quotient** de l'anneau A par un idéal I est l'ensemble $R = {}^A\!/_I$ des classes modulo I.

$${}^A\!/_I = \{x + I,\ x \in A\}$$

1. Étant donnés deux éléments u et v de R, il existe deux éléments x et y de A tels que

$$u = x + I \qquad \text{et} \qquad v = y + I.$$

1.a La somme $u \oplus v$ est bien définie par

$$u \oplus v = (x + y) + I.$$

L'élément I de R, classe de 0 modulo I, est neutre pour $\oplus$.
1.b Le produit $u \otimes v$ est bien défini par

$$u \otimes v = (x * y) + I.$$

L'élément $1 + I$ de R, classe de 1 modulo I, est neutre pour $\otimes$.
1.c Le quotient R est muni d'une structure d'anneau commutatif pour les opérations $\oplus$ et $\otimes$.
103.3 Soit $u = x + I \in R$, distinct de $0 + I$.
2. L'idéal de R engendré par u :

$$\begin{aligned}\langle u\rangle &= \{u \otimes v,\ v \in R\}\\ &= \{(x * y) + I,\ y \in A\}\end{aligned}$$

est un idéal de A qui contient I et $x \notin I$, donc $\langle u\rangle = A$.
3. Il existe $y \in A$ tel que la classe $y + I$ soit l'inverse de la classe u pour la multiplication $\otimes$.
4. L'anneau quotient $R = {}^A\!/_I$ est un corps. →**[49]**, **[100]**