COLLECTION ATOMATH

Préparation progressive aux Olympiades internationales de mathématiques

TOME III

ARITHMÉTIQUE

De la divisibilité aux problèmes de l'IMO

ÉDITION DÉTAILLÉE · TOUS LES THÉORÈMES DÉMONTRÉS

Ali AKIR

FORMATEUR OLYMPIQUE

Première édition

COLLECTION ATOMATH

ATOMATH

Préparation progressive aux Olympiades internationales de mathématiques

TOME III

Arithmétique

De la divisibilité aux problèmes de l'IMO

Cours complet de théorie des nombres

Ali AKIR

Formateur olympique

Première édition

ATOMATH — Tome III : Arithmétique

Collection ATOMATH, préparation aux Olympiades internationales de mathématiques.

Tous droits réservés. Toute reproduction, même partielle, par quelque procédé que ce soit, est interdite sans autorisation préalable, à l'exception des courtes citations dans le cadre d'un usage pédagogique, conformément aux dispositions légales en vigueur.

Table des matières

Introduction **1**

Mode d'emploi de ce tome **2**

À qui s'adresse ce tome 2
Le programme couvert 2
Structure d'un chapitre 2
Code de difficulté 3
Comment travailler 3
Notations utilisées 3

PARTIE I — Fondements **5**

1 Divisibilité et division euclidienne **6**

1.1 La relation de divisibilité 6
1.2 La division euclidienne 7
1.3 Identités algébriques fondamentales 9
1.4 Exercices 10
1.5 Corrigés 11

2 PGCD, PPCM, algorithme d'Euclide et théorème de Bézout **13**

2.1 PGCD et PPCM 13
2.2 L'algorithme d'Euclide 14
2.3 Le théorème de Bézout 15
2.4 Une formule très utile 17
2.5 Exercices 18
2.6 Corrigés 18

3 Nombres premiers, factorisation et valuation -adique **20**

3.1 Théorème fondamental de l'arithmétique 20
3.2 Valuation p-adique 21
3.3 La formule de Legendre 23
3.4 Il y a une infinité de nombres premiers 24
3.5 Exercices 25
3.6 Corrigés 25

4 Congruences **27**

4.1 Définition et règles de calcul 27
4.2 Comment choisir le module 28
4.3 Critères de divisibilité 29
4.4 Le théorème de Wilson 29
4.5 Systèmes de résidus 31
4.6 Exercices 31
4.7 Corrigés 31

PARTIE II — Les classiques de l'arsenal olympique **33**

5 Inverses modulaires, équations linéaires et théorème des restes chinois 34
5.1 Inverse modulaire 34
5.2 Équations linéaires modulaires 35
5.3 Le théorème des restes chinois 35
5.4 Application : structure de $\mathbb{Z}/n\mathbb{Z}^\times$ 37
5.5 Exercices 37
5.6 Corrigés 37

6 Les théorèmes de Fermat et d'Euler 39
6.1 L'indicatrice d'Euler 39
6.2 Petit théorème de Fermat 40
6.3 Exercices 42
6.4 Corrigés 43

7 Ordre multiplicatif et racines primitives 44
7.1 L'ordre multiplicatif 44
7.2 Racines primitives 45
7.3 Exercices 47
7.4 Corrigés 47

8 Résidus quadratiques 49
8.1 Le symbole de Legendre 49
8.2 Applications aux équations diophantiennes 53
8.3 Exercices 55
8.4 Corrigés 55

PARTIE III — Fonctions arithmétiques et parties entières 57

9 Fonctions arithmétiques 58
9.1 Les fonctions classiques 58
9.2 Convolution de Dirichlet 59
9.3 Problèmes de comptage de diviseurs 61
9.4 Exercices 62
9.5 Corrigés 62

10 Partie entière et partie fractionnaire 64
10.1 Propriétés de base 64
10.2 La partie entière comme outil de comptage 65
10.3 Exercices 67
10.4 Corrigés 67

PARTIE IV — Équations diophantiennes 69

11 Méthodes générales de résolution 70
11.1 L'équation linéaire 70
11.2 Méthode 1 : la factorisation 71
11.3 Méthode 2 : les congruences 72
11.4 Méthode 3 : bornes et inégalités 73
11.5 Méthode 4 : paramétrisation 73

11.6 Méthode 5 : monotonie et descente 74
11.7 Exercices 74
11.8 Corrigés 75

12 Triplets pythagoriciens et descente infinie 77
12.1 L'équation de Pythagore 77
12.2 La descente infinie 79
12.3 Exercices 80
12.4 Corrigés 80

13 L'équation de Pell 82
13.1 Existence d'une solution non triviale 82
13.2 Applications olympiques 84
13.3 Exercices 85
13.4 Corrigés 85

PARTIE V — Techniques de haut niveau et problèmes d'IMO 87

14 Le lemme LTE (Lifting the Exponent) 88
14.1 Le cas p impair 88
14.2 Le cas $p = 2$ 89
14.3 Applications 89
14.4 Exercices 91
14.5 Corrigés 91

15 Zsigmondy et polynômes cyclotomiques 93
15.1 Diviseurs primitifs 93
15.2 Polynômes cyclotomiques 94
15.3 Démonstration du théorème de Zsigmondy 97
15.4 Exercices 98
15.5 Corrigés 98

16 Le saut de Viète (Vieta jumping) 100
16.1 Le mécanisme 100
16.2 Le problème archétype 100
16.3 Exercices 103
16.4 Corrigés 103

17 Coefficients binomiaux et arithmétique 105
17.1 Valuation d'un coefficient binomial 105
17.2 Le coefficient central et Bertrand 107
17.3 Exercices 108
17.4 Corrigés 108

18 Stratégie de résolution et problèmes d'IMO 110
18.1 La méthode d'attaque en sept temps 110
18.2 Problèmes d'IMO entièrement corrigés 111
18.3 Banque d'entraînement 113

PARTIE VI — Annexes 115

A Formulaire complet 116
A.1 Divisibilité et PGCD 116
A.2 Valuations et factorisation 116
A.3 Congruences 116
A.4 Résidus quadratiques 117
A.5 Fonctions arithmétiques 117
A.6 Outils avancés 118
B Plan d'entraînement sur six mois 119
C Table des difficultés et index des méthodes 120
C.1 Index des méthodes par symptôme 120
C.2 Bibliographie 120
À propos de l'auteur 122

Introduction

La collection ATOMATH propose un parcours complet de préparation aux Olympiades internationales de mathématiques, organisé en quatre tomes indépendants mais complémentaires : Algèbre, Géométrie, Arithmétique et Combinatoire. Chaque tome couvre, de façon autonome, l'un des quatre grands domaines abordés lors des compétitions internationales, depuis les premiers automatismes jusqu'aux techniques mobilisées dans les problèmes les plus exigeants de l'épreuve.

Ce troisième tome est consacré à l'**arithmétique olympique**, c'est-à-dire à la théorie des nombres telle qu'elle apparaît en compétition : divisibilité, PGCD et PPCM, nombres premiers et valuations, congruences, théorèmes de Fermat et d'Euler, ordre multiplicatif et racines primitives, résidus quadratiques, fonctions arithmétiques, équations diophantiennes, puis les techniques de haut niveau (lemme LTE, théorème de Zsigmondy, saut de Viète, coefficients binomiaux). Il n'exige aucun prérequis au-delà du programme de lycée ; chaque notion nouvelle est introduite et démontrée avant d'être utilisée.

L'arithmétique occupe une place singulière dans les compétitions internationales : à l'IMO, un problème sur six en moyenne relève directement de cette discipline, et c'est souvent l'un des deux problèmes les plus difficiles de l'épreuve. Sa particularité est la suivante : le bagage théorique nécessaire est étonnamment restreint — une quinzaine de théorèmes suffisent — mais la distance entre *connaître* le petit théorème de Fermat et *savoir s'en servir* au bon moment est immense. C'est précisément cette distance que ce tome entend combler.

L'ouvrage suit le même principe que le reste de la collection : rien n'est admis sans démonstration, et chaque outil théorique est immédiatement mis à l'épreuve sur des exemples résolus, puis sur des exercices gradués en quatre niveaux de difficulté, dont les solutions complètes sont rédigées comme elles devraient l'être en compétition. Un lecteur qui traverse le tome dans l'ordre, en cherchant réellement chaque exercice avant de consulter sa solution, dispose à la fin d'une boîte à outils suffisante pour aborder la majorité des problèmes d'arithmétique proposés à l'Olympiade internationale de mathématiques et aux compétitions qui y préparent.

Bon travail, et bonne route vers l'IMO.

Mode d'emploi de ce tome

À qui s'adresse ce tome

Ce tome est un cours complet d'arithmétique olympique (théorie des nombres). Il est conçu pour accompagner un élève depuis le niveau junior (fin de collège, début de lycée, premières compétitions nationales) jusqu'au niveau senior : celui exigé par l'Olympiade internationale de mathématiques (IMO) et les olympiades régionales de haut niveau (Balkanique, Asie-Pacifique, Panafricaine, Méditerranéenne). Aucun prérequis n'est supposé au-delà du programme de lycée. Chaque notion nouvelle est définie avant d'être utilisée, y compris celles qui dépassent le programme scolaire (valuation p-adique, ordre multiplicatif, résidus quadratiques, lemme LTE, théorème de Zsigmondy).

Le programme couvert

L'arithmétique olympique se décompose en cinq grands blocs, qui structurent ce tome :

Bloc	Contenu	Partie
Fondements	divisibilité, Euclide, Bézout, nombres premiers, valuation p-adique, congruences	I
Les classiques	restes chinois, Fermat–Euler, ordre multiplicatif, racines primitives, résidus quadratiques	II
Fonctions arithmétiques et parties entières	τ, σ, φ, μ, convolution de Dirichlet, partie entière	III
Équations diophantiennes	méthodes générales, triplets pythagoriciens, descente infinie, équation de Pell	IV
Techniques de haut niveau	lemme LTE, Zsigmondy, saut de Viète, coefficients binomiaux, problèmes d'IMO	V

Statistiquement, sur les six problèmes d'une IMO, un problème relève en moyenne directement de l'arithmétique, et les techniques de ce tome interviennent aussi, ponctuellement, dans des problèmes de combinatoire ou d'algèbre. Les cinq blocs sont tous indispensables : les Parties I et II, même si leur contenu semble élémentaire, contiennent déjà des exercices de niveau olympique.

Structure d'un chapitre

Chaque chapitre suit le même schéma, pensé pour un travail autonome :

1. Le **cours**, avec définitions, théorèmes démontrés et méthodes encadrées. Les démonstrations ne sont pas décoratives : les techniques qu'elles contiennent sont réutilisées dans les problèmes.
2. Des **exemples résolus**, choisis pour illustrer immédiatement chaque outil, souvent tirés de compétitions réelles.
3. Une série d'**exercices** gradués en quatre niveaux.
4. Les **solutions** complètes de tous les exercices, rédigées comme elles devraient l'être en compétition, sous forme de solutions commentées qui exposent la recherche.

Code de difficulté

- ★ **Junior** : application directe du cours.
- ★★ **Intermédiaire** : exercice consistant, une idée à trouver puis une technique standard.
- ★★★ **Senior** : niveau olympiade nationale. Plusieurs idées à combiner.
- ★★★★ **IMO** : niveau IMO / listes courtes. 30 à 60 minutes de recherche sont normales.

Comment travailler

À retenir

1. Lire le cours avec un crayon et refaire chaque démonstration sur une feuille blanche, cours fermé.
2. Chercher chaque exercice au moins 45 minutes avant de regarder la solution. Un problème cherché en vain pendant une heure apprend davantage que dix corrigés lus passivement.
3. Après avoir lu une solution, la réécrire seul le lendemain. C'est cette réécriture, et non la lecture, qui installe la technique.
4. Tenir un carnet de techniques : pour chaque problème raté, noter la phrase de la solution qu'on n'aurait pas trouvée seul. C'est le meilleur programme de révision personnel.
5. Une fois une partie terminée, passer la banque d'entraînement correspondante, en temps limité, sans aucune aide.

Attention.

Un piège classique de l'entraînement autonome consiste à lire beaucoup de solutions et à en tirer l'impression de progresser. Cette impression est fausse : on ne progresse qu'en produisant soi-même une rédaction complète. Un exercice « compris » mais non rédigé n'est pas acquis.

Notations utilisées

Notation	Signification
$\mathbb{N}$	entiers naturels $0,1,2,\ldots$; $\mathbb{N}^* = \mathbb{N}\backslash\{0\}$
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	entiers relatifs, rationnels, réels, complexes
$a \mid b$	a divise b ; $a \nmid b$: a ne divise pas b
$\gcd(a,b)$, $\operatorname{ppcm}(a,b)$	plus grand commun diviseur, plus petit commun multiple
$a \equiv b \pmod{n}$	n divise $a-b$
$\lfloor x \rfloor$, $\{x\}$	partie entière et partie fractionnaire de x
$(\mathbb{Z}/n\mathbb{Z})^\times$	groupe des inversibles modulo n
$v_p(n)$, $p^k \parallel n$	valuation p-adique de n ; $p^k \parallel n$ signifie $v_p(n) = k$ exactement
$\varphi(n)$	indicatrice d'Euler
$\tau(n)$, $\sigma(n)$	nombre et somme des diviseurs de n
$\mu(n)$	fonction de Möbius
$\operatorname{ord}_n(a)$	ordre multiplicatif de a modulo n

Notation	Signification
$\left(\frac{a}{p}\right)$	symbole de Legendre

Les problèmes sont étiquetés par leur origine lorsqu'elle est connue : (IMO 1988, problème 6) désigne le problème 6 de l'IMO 1988, (ISL) un problème de la liste courte (*shortlist*) de l'IMO, (USAMO), (Baltique), (Iran TST), etc. Un problème sans étiquette est un exercice d'entraînement classique.

PARTIE I — Fondements

CHAPITRE 1

1 Divisibilité et division euclidienne

Objectifs du chapitre.

- Maîtriser la définition de la divisibilité et ses manipulations formelles.
- Utiliser la division euclidienne comme outil de classification des entiers.
- Connaître les identités algébriques fondamentales ($a^n - b^n$, $a^n + b^n$, Sophie Germain).
- Acquérir les trois réflexes de base : factoriser, majorer, distinguer des cas.

1.1 La relation de divisibilité

Définition 1.1.1 (Divisibilité)

Soient $a, b \in \mathbb{Z}$. On dit que a divise b, et on note $a \mid b$, s'il existe $c \in \mathbb{Z}$ tel que $b = ac$. On dit alors que a est un diviseur de b, et que b est un multiple de a.

Remarque.

Attention : tout entier divise 0 (car $0 = a \cdot 0$), et 0 ne divise que 0. Le cas $a = 0$ est une source d'erreurs classique dans les rédactions ; en compétition, mentionnez-le explicitement quand il peut se produire.

Proposition 1.1.2 (Règles de calcul sur la divisibilité)

Pour tous $a, b, c, x, y \in \mathbb{Z}$:

- (i) $a \mid b$ et $b \mid c \Longrightarrow a \mid c$ (transitivité) ;
- (ii) $a \mid b$ et $a \mid c \Longrightarrow a \mid bx + cy$ (combinaison linéaire) ;
- (iii) $a \mid b$ et $b \neq 0 \Longrightarrow |a| \leq |b|$ (argument de taille) ;
- (iv) $a \mid b$ et $b \mid a \Longrightarrow a = \pm b$;
- (v) $a \mid b \Longrightarrow ac \mid bc$, et réciproquement si $c \neq 0$.

Démonstration.

(i) Si $b = ak$ et $c = b\ell$, alors $c = a(k\ell)$. (ii) Si $b = ak$ et $c = a\ell$, alors $bx + cy = a(kx + \ell y)$. (iii) Si $b = ak$ avec $b \neq 0$, alors $k \neq 0$, donc $|k| \geq 1$ et $|b| = |a|\,|k| \geq |a|$. (iv) Si a ou b est nul, les deux le sont (car 0 ne divise que 0) ; sinon, cela découle de (iii) appliqué deux fois : $|a| \leq |b|$ et $|b| \leq |a|$. (v) Immédiat. ■

Les points (ii) et (iii) sont les deux chevaux de bataille de tout problème d'arithmétique élémentaire. Le point (ii) permet de fabriquer de nouveaux multiples ; le point (iii) permet de conclure en enfermant une quantité dans un intervalle fini.

Méthode 1.1.3 — Le réflexe « combinaison linéaire »

Lorsqu'un énoncé impose $d \mid A$ et $d \mid B$ avec A, B deux expressions en les inconnues, cherchez systématiquement une combinaison $xA + yB$ qui élimine les inconnues. Le nombre constant obtenu borne alors d.

Exemple 1.1.4. *Déterminer tous les entiers $n \in \mathbb{Z}$ tels que $n+3$ divise n^2+5.*

Comme $n+3 \mid n^2+5$ et $n+3 \mid (n+3)(n-3) = n^2-9$, la règle de combinaison linéaire donne

$$n+3 \mid (n^2+5) - (n^2-9) = 14.$$

Donc $n+3 \in \{\pm 1, \pm 2, \pm 7, \pm 14\}$, c'est-à-dire

$$n \in \{-2, -4, -1, -5{,}4, -10{,}11, -17\}.$$

Réciproquement, chacune de ces valeurs convient puisque le raisonnement est réversible : si $n+3 \mid 14$, alors $n+3 \mid (n^2-9)+14 = n^2+5$.

Attention.

La divisibilité n'est pas une équivalence : le raisonnement direct donne seulement des candidats. Vérifiez toujours la réciproque, ou assurez-vous que chaque implication est une équivalence. Perdre un point pour cela à l'IMO est une faute banale mais coûteuse.

1.2 La division euclidienne

Théorème 1.2.1 (Division euclidienne)

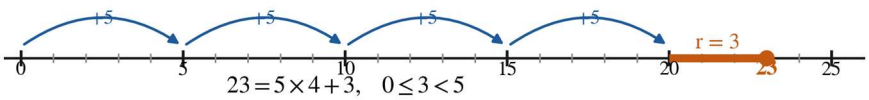
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

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

On appelle q le quotient et r le reste de la division de a par b.

Démonstration. *Existence.* L'ensemble $E = \{a - bk : k \in \mathbb{Z}\} \cap \mathbb{N}$ est non vide (prendre $k = -|a|$: alors $a - bk = a + b|a| \geq a + |a| \geq 0$). Étant une partie non vide de $\mathbb{N}$, E possède un plus petit élément $r = a - bq$. Si l'on avait $r \geq b$, alors $r - b = a - b(q+1) \geq 0$ appartiendrait à E et serait strictement plus petit que r : contradiction. Donc $0 \leq r < b$.

Unicité. Si $bq + r = bq' + r'$ avec $0 \leq r, r' < b$, alors $b(q - q') = r' - r$, donc $b \mid r' - r$. Or $|r' - r| < b$, ce qui force $r' = r$, puis $q = q'$. ■



Division euclidienne de a = 23 par b = 5 : a = 5·4 + 3 ; le reste est la distance de a au plus grand multiple de b qui ne le dépasse pas.

L'usage réellement important de ce théorème en olympiades n'est pas le calcul, mais la classification : tout entier n s'écrit sous l'une des b formes $bq, bq+1, \ldots, bq+b-1$. Cela transforme une infinité de cas en un nombre fini.

Exemple 1.2.2. *Montrer que pour tout entier n, l'entier $n(n+1)(2n+1)$ est divisible par 6.*

Divisibilité par 2. Parmi n et $n+1$, l'un est pair.

Divisibilité par 3. Écrivons $n = 3q + r$ avec $r \in \{0,1,2\}$. Si $r = 0$, $3 \mid n$. Si $r = 2$, $n + 1 = 3(q+1)$, donc $3 \mid n+1$. Si $r = 1$, $2n + 1 = 6q + 3 = 3(2q+1)$, donc $3 \mid 2n+1$.

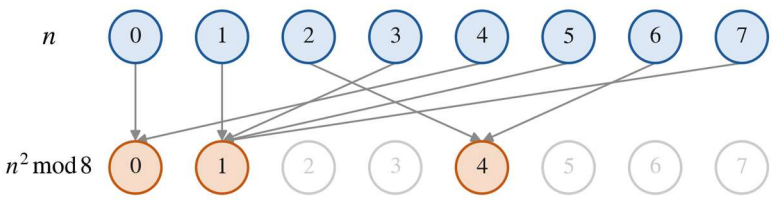
Dans tous les cas $2 \mid n(n+1)(2n+1)$ et $3 \mid n(n+1)(2n+1)$; comme $\gcd(2,3) = 1$, on conclut $6 \mid n(n+1)(2n+1)$.

Proposition 1.2.3 (Résidus des carrés, cubes et puissances quatrièmes)

- (i) Un carré parfait est congru à 0 ou 1 modulo 4 ; à 0, 1 ou 4 modulo 8.
- (ii) Un carré parfait est congru à 0 ou 1 modulo 3.
- (iii) Un cube est congru à 0, 1 ou -1 modulo 9, et à 0, 1 ou -1 modulo 7.
- (iv) Une puissance quatrième est congrue à 0 ou 1 modulo 16, et à 0 ou 1 modulo 5.

Démonstration. Le reste de n^k modulo m ne dépend que du reste de n modulo m : si $n = mq + r$, le développement de $(mq+r)^k$ par la formule du binôme montre que $n^k - r^k$ est un multiple de m. Il suffit donc de calculer r^k pour $0 \le r < m$; on peut même se limiter à $0 \le r \le \frac{m}{2}$, car $(m-r)^k \equiv (-r)^k = \pm r^k$.

- (i) Modulo 4 : $0^2, 1^2, 2^2 \equiv 0,1,0$. Modulo 8 : $0,1,4,9,16 \equiv 0,1,4,1,0$ pour $r = 0,1,2,3,4$; les carrés impairs valent tous 1 modulo 8.
- (ii) Modulo 3 : $0^2 = 0$, $1^2 = 1$ (et $2^2 \equiv 1$).
- (iii) Modulo 9 : r^3 pour $r = 0, \ldots, 4$ vaut $0,1,8,27,64 \equiv 0,1,-1,0,1$, et $(9-r)^3 \equiv -r^3$. Modulo 7 : $0,1,8,27 \equiv 0,1,1,-1$ pour $r = 0,1,2,3$, et $(7-r)^3 \equiv -r^3$.
- (iv) Modulo 16 : si n est pair, $16 \mid n^4$; si n est impair, $n^2 \equiv 1 \pmod 8$, donc $n^2 = 8k+1$ et $n^4 = 64k^2 + 16k + 1 \equiv 1 \pmod{16}$. Modulo 5 : $1^4 = 1$, $2^4 = 16 \equiv 1$, et $3^4, 4^4 \equiv 2^4, 1^4$. ■



Carrés modulo 8 : les restes de n² pour n = 0, 1, …, 7 ne prennent que les valeurs 0, 1 et 4.

À retenir (Le tableau des résidus)

Ce tableau minuscule résout à lui seul un grand nombre d'exercices : dès qu'une équation contient des carrés et une constante, testez modulo 4, 8, 3, 5 et 16. C'est le premier réflexe à avoir devant une équation diophantienne.

Exemple 1.2.4. *Montrer que l'équation $x^2 + y^2 = 4z + 3$ n'a aucune solution en entiers.*

Modulo 4, x^2 et y^2 valent chacun 0 ou 1. Leur somme vaut donc 0, 1 ou 2 modulo 4, jamais 3.

1.3 Identités algébriques fondamentales

Proposition 1.3.1 (Factorisation de $a^n - b^n$ et de $a^n + b^n$)

Pour tous a, b et tout $n \geq 1$:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}).$$

En particulier $a - b \mid a^n - b^n$. Si n est impair,

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}),$$

donc $a + b \mid a^n + b^n$.

Démonstration. Notons $S = a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1} = \sum_{k=0}^{n-1} a^{n-1-k}\, b^k$. Alors

$$(a-b)S = \sum_{k=0}^{n-1} a^{n-k}\, b^k - \sum_{k=0}^{n-1} a^{n-1-k}\, b^{k+1} = \sum_{k=0}^{n-1} a^{n-k}\, b^k - \sum_{k=1}^{n} a^{n-k}\, b^k = a^n - b^n,$$

car tous les termes d'indice $1 \leq k \leq n-1$ se simplifient (télescopage). Si a, b sont entiers, S l'est aussi, d'où $a - b \mid a^n - b^n$. Pour n impair, on applique cette identité à a et $-b$: $a^n - (-b)^n = a^n + b^n$ et $a - (-b) = a + b$; le second facteur devient $\sum a^{n-1-k}(-b)^k$, somme à signes alternés. ■

Corollaire 1.3.2

Si $d \mid n$, alors $a^d - b^d \mid a^n - b^n$. En particulier, $2^d - 1 \mid 2^n - 1$.

Démonstration. Écrire $n = dm$ et appliquer la proposition 1.3.1 à $A = a^d$, $B = b^d$: $A - B \mid A^m - B^m$. ■

Proposition 1.3.3 (Identité de Sophie Germain)

$$a^4 + 4b^4 = (a^2 + 2b^2 - 2ab)(a^2 + 2b^2 + 2ab).$$

Démonstration. $a^4 + 4b^4 = (a^2 + 2b^2)^2 - 4a^2b^2$, puis différence de deux carrés. ■

Exemple 1.3.4. *Montrer que $n^4 + 4^n$ est composé pour tout entier $n > 1$.*

Si n est pair, $n^4 + 4^n$ est pair et > 2, donc composé.

Si n est impair, $n = 2k + 1$, alors $4^n = 4 \cdot 4^{2k} = 4\left(2^k\right)^4$. En posant $b = 2^k$, l'identité de Sophie Germain donne

$$n^4 + 4b^4 = (n^2 + 2b^2 - 2nb)(n^2 + 2b^2 + 2nb).$$

Le second facteur est clairement > 1. Le premier vaut $(n-b)^2 + b^2 \geq b^2 = 4^k$, et il est > 1 dès que $k \geq 1$, c'est-à-dire $n \geq 3$. Donc $n^4 + 4^n$ est composé.

Méthode 1.3.5 — Reconnaître une factorisation cachée

Les motifs suivants doivent déclencher une factorisation immédiate :

Motif	Factorisation
$x^2 - y^2$	$(x-y)(x+y)$
$x^3 \pm y^3$	$(x \pm y)(x^2 \mp xy + y^2)$
$x^4 + 4y^4$	Sophie Germain
$xy + x + y$	$(x+1)(y+1) - 1$
$xy - ax - by$	$(x-b)(y-a) - ab$
$x^2 + y^2 + z^2 - 2xy - \cdots$	compléter des carrés

La technique « $xy + ax + by = (x+b)(y+a) - ab$ » s'appelle l'astuce de Simon (*Simon's Favorite Factoring Trick*) : elle transforme une équation en produit d'entiers, donc en un nombre fini de cas.

Exemple 1.3.6. *Résoudre en entiers strictement positifs :* $\frac{1}{x} + \frac{1}{y} = \frac{1}{3}$.

En multipliant par $3xy$: $3y + 3x = xy$, soit $xy - 3x - 3y = 0$, puis $(x-3)(y-3) = 9$. Comme $x, y > 0$, on a $x - 3 \geq -2$ et $y - 3 \geq -2$; les diviseurs négatifs sont donc exclus (leur produit devrait valoir 9 avec les deux facteurs ≥ -2, ce qui est impossible). Donc $(x-3, y-3) \in \{(1,9), (3,3), (9,1)\}$ et

$$(x, y) \in \{(4,12), (6,6), (12,4)\}.$$

1.4 Exercices

Exercice 1.1 ★. Trouver tous les entiers n tels que $n - 1 \mid n^3 + 4$.

Exercice 1.2 ★. Montrer que pour tout $n \in \mathbb{N}$, $30 \mid n^5 - n$.

Exercice 1.3 ★★. Montrer que la somme de deux carrés parfaits impairs n'est jamais un carré parfait.

Exercice 1.4 ★★. Résoudre en entiers positifs : $x^2 - y^2 = 105$.

Exercice 1.5 ★★. Montrer que si $2^n - 1$ est premier, alors n est premier. La réciproque est-elle vraie ?

Exercice 1.6 ★★. Montrer que si $2^n + 1$ est premier ($n \geq 1$), alors n est une puissance de 2.

Exercice 1.7 ★★★. Déterminer tous les entiers $n \geq 1$ tels que $n \mid 2^n - 1$.

Exercice 1.8 ★★★. Montrer que pour tout entier $n \geq 1$, le nombre formé de n chiffres « 1 », suivis de $n+1$ chiffres « 2 », puis d'un chiffre « 5 », est un carré parfait. (Exemples : $1225 = 35^2$, $112\,225 = 335^2$.)

1.5 Corrigés

Solution de l'exercice 1.1. On a $n-1 \mid n^3-1$ (identité a^n-b^n avec $a=n$, $b=1$), donc par combinaison linéaire $n-1 \mid (n^3+4)-(n^3-1)=5$. Ainsi $n-1 \in \{\pm 1, \pm 5\}$, soit $n \in \{2,0,6,-4\}$. Réciproquement, si $n-1 \mid 5$, alors $n-1 \mid (n^3-1)+5 = n^3+4$. Toutes ces valeurs conviennent.

Solution de l'exercice 1.2. $n^5-n = n(n^4-1) = n(n-1)(n+1)(n^2+1)$. Parmi les trois entiers consécutifs $n-1, n, n+1$, il y a un multiple de 2 et un multiple de 3, d'où $6 \mid n^5-n$. Pour 5 : si $n \equiv 0, \pm 1 \pmod 5$, l'un des facteurs $n, n-1, n+1$ est divisible par 5 ; si $n \equiv \pm 2$, alors $n^2 \equiv 4 \equiv -1$, donc $5 \mid n^2+1$. Comme $2,3,5$ sont des nombres premiers distincts, $30 \mid n^5-n$.

> **Remarque.**
> On verra au chapitre 6 que ce résultat est un cas particulier du petit théorème de Fermat : $n^5 \equiv n \pmod 5$.

Solution de l'exercice 1.3. Soient a, b impairs. Alors $a^2 \equiv b^2 \equiv 1 \pmod 8$, donc $a^2+b^2 \equiv 2 \pmod 8$. Or un carré parfait est $\equiv 0,1$ ou $4 \pmod 8$. Contradiction. (Travailler modulo 4 suffit d'ailleurs : $a^2+b^2 \equiv 2 \pmod 4$ alors qu'un carré vaut 0 ou 1.)

Solution de l'exercice 1.4. $(x-y)(x+y) = 105 = 3 \cdot 5 \cdot 7$. Les deux facteurs sont de même parité ; comme 105 est impair, ils sont tous deux impairs — pas de contrainte supplémentaire. Avec $0 < x-y < x+y$ et $(x-y)(x+y)=105$:

$$(x-y, x+y) \in \{(1,105), (3,35), (5,21), (7,15)\},$$

d'où

$$(x,y) \in \{(53,52), (19,16), (13,8), (11,4)\}.$$

Solution de l'exercice 1.5. Si $n = ab$ avec $1 < a < n$, le corollaire 1.3.2 donne $2^a-1 \mid 2^n-1$, avec $1 < 2^a-1 < 2^n-1$: donc 2^n-1 est composé. Par contraposée, 2^n-1 premier $\Rightarrow n$ premier.

La réciproque est fausse : $n=11$ est premier mais $2^{11}-1 = 2047 = 23 \times 89$. (Les nombres 2^p-1 premiers s'appellent nombres de Mersenne.)

Solution de l'exercice 1.6. Si n possède un diviseur impair $d > 1$, écrivons $n = dm$. Alors $2^m+1 \mid (2^m)^d+1 = 2^n+1$ (identité a^d+b^d avec d impair, $a=2^m$, $b=1$). Comme $1 < 2^m+1 < 2^n+1$, le nombre 2^n+1 est composé. Donc n n'a pas de diviseur impair > 1 : $n = 2^k$.

> **Remarque.**
> Les $F_k = 2^{2^k}+1$ sont les nombres de Fermat. $F_0, \ldots, F_4$ sont premiers, mais Euler a montré que $F_5 = 641 \times 6\,700\,417$.

Solution de l'exercice 1.7. Réponse : $n=1$ uniquement.

Supposons $n > 1$ et $n \mid 2^n-1$. Comme 2^n-1 est impair, n est impair. Soit p le plus petit facteur premier de n. On a $p \mid 2^n-1$, donc $2^n \equiv 1 \pmod p$. Par le petit théorème de Fermat, $2^{p-1} \equiv 1 \pmod p$. Notons $d = \mathrm{ord}_p(2)$ (chapitre 7) : alors $d \mid n$ et $d \mid p-1$, donc $d \mid \mathrm{pgcd}(n, p-1)$. Or tout facteur premier de $\mathrm{pgcd}(n,p-1)$ divise n et est $< p$, ce qui contredit la minimalité de p — sauf si $\mathrm{pgcd}(n,p-1)=1$. Donc $d=1$, c'est-à-dire $p \mid 2^1-1 = 1$: absurde.

À retenir (La technique du plus petit facteur premier)

Cet argument — prendre le plus petit facteur premier p de n, puis observer que $\gcd(n, p-1) = 1$ — est l'une des dix techniques les plus rentables de l'arithmétique olympique. Retenez-la : elle résout à elle seule plusieurs problèmes d'IMO.

Solution de l'exercice 1.8. Notons $R_k = \underbrace{1\cdots 1}_{k} = \frac{10^k-1}{9}$ et posons

$$t = \underbrace{3\cdots 35}_{n} = 30R_n + 5 = \frac{10(10^n-1)}{3} + 5 = \frac{10^{n+1}+5}{3}.$$

Alors

$$t^2 = \frac{10^{2n+2} + 10\cdot 10^{n+1} + 25}{9} = \frac{10^{2n+2} + 10^{n+2} + 25}{9}.$$

D'autre part, le nombre de l'énoncé vaut

$$N = R_n \cdot 10^{n+2} + 2R_{n+1}\cdot 10 + 5 = \frac{10^n-1}{9}\,10^{n+2} + \frac{20(10^{n+1}-1)}{9} + 5.$$

En réduisant au même dénominateur :

$$9N = 10^{2n+2} - 10^{n+2} + 20\cdot 10^{n+1} - 20 + 45 = 10^{2n+2} + 10^{n+2} + 25,$$

puisque $-10^{n+2} + 20\cdot 10^{n+1} = -10^{n+2} + 2\cdot 10^{n+2} = 10^{n+2}$. Donc $N = t^2$.

Remarque.

La démarche est instructive : on ne devine pas la racine, on la fait apparaître en calculant $9N$. Devant un nombre décrit par ses chiffres, le premier geste est toujours de le réécrire comme combinaison de puissances de 10.

CHAPITRE 2

2 PGCD, PPCM, algorithme d'Euclide et théorème de Bézout

Objectifs du chapitre.

- Définir rigoureusement PGCD et PPCM et connaître leurs propriétés.
- Maîtriser l'algorithme d'Euclide, y compris sous forme « symbolique ».
- Démontrer et exploiter le théorème de Bézout et le lemme de Gauss.
- Savoir calculer $\mathrm{pgcd}(a^m - 1, a^n - 1)$ et manipuler des suites récurrentes.

2.1 PGCD et PPCM

Définition 2.1.1 (PGCD, PPCM, entiers premiers entre eux)

Soient $a, b \in \mathbb{Z}$ non tous deux nuls. Le plus grand commun diviseur $\mathrm{pgcd}(a, b)$ est le plus grand entier divisant à la fois a et b. Le plus petit commun multiple $\mathrm{ppcm}(a, b)$ est le plus petit entier strictement positif multiple de a et de b (lorsque a et b sont tous deux non nuls).

On dit que a et b sont premiers entre eux si $\mathrm{pgcd}(a, b) = 1$.

Proposition 2.1.2 (Propriétés du PGCD)

Pour a, b entiers non tous deux nuls et $k \in \mathbb{N}^*$:

- (i) $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, a) = \mathrm{pgcd}(|a|, |b|)$;
- (ii) $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(a, b + ma)$ pour tout $m \in \mathbb{Z}$;
- (iii) $\mathrm{pgcd}(ka, kb) = k\mathrm{pgcd}(a, b)$;
- (iv) si $d = \mathrm{pgcd}(a, b)$, alors $\mathrm{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$;
- (v) $\mathrm{pgcd}(a, b) \cdot \mathrm{ppcm}(a, b) = |ab|$ (pour a, b non nuls).

Démonstration.

(i) Les diviseurs de a et de $-a$ sont les mêmes, et la définition est symétrique en a et b.

(ii) Tout diviseur commun de a et b divise $b + ma$; réciproquement, tout diviseur commun de a et $b + ma$ divise $(b + ma) - ma = b$. Les deux paires ont donc les mêmes diviseurs communs, donc le même plus grand.

Les trois points suivants utilisent le théorème de Bézout (théorème 2.3.1 ci-dessous, dont la démonstration n'utilise que (i) et la division euclidienne) et sa conséquence : **tout diviseur commun de a et b divise** $\mathrm{pgcd}(a, b)$ (si $e \mid a$ et $e \mid b$, alors $e \mid au + bv = d$).

(iii) Soit $d = \gcd(a,b)$. L'entier kd divise ka et kb, donc $kd \mid D := \gcd(ka,kb)$. Inversement, par Bézout, $au + bv = d$, donc $kau + kbv = kd$; comme D divise ka et kb, $D \mid kd$. Ainsi $D = kd$.

(iv) De $au + bv = d$ on tire $\frac{a}{d}u + \frac{b}{d}v = 1$; tout diviseur commun de $\frac{a}{d}$ et $\frac{b}{d}$ divise 1.

(v) On peut supposer $a, b > 0$. Écrivons $a = da'$, $b = db'$ avec $\gcd(a',b') = 1$ par (iv), et posons $m = da'b' = \frac{ab}{d}$. C'est un multiple commun de a ($m = ab'$) et de b ($m = a'b$). Soit $M > 0$ un multiple commun quelconque : $M = ak = da'k$, et $b = db' \mid da'k$ donne $b' \mid a'k$, donc $b' \mid k$ par le lemme de Gauss (théorème 2.3.3). Ainsi $M = da'k$ est un multiple de $da'b' = m$, et $M \geq m$. Donc $\operatorname{ppcm}(a,b) = m$ et $\gcd(a,b)\operatorname{ppcm}(a,b) = dm = ab$. On a montré au passage que **tout multiple commun de a et b est un multiple de $\operatorname{ppcm}(a,b)$.** ■

Le point (ii) est le moteur de tout : on peut remplacer un argument par lui-même modulo l'autre.

2.2 L'algorithme d'Euclide

Théorème 2.2.1 (Algorithme d'Euclide)

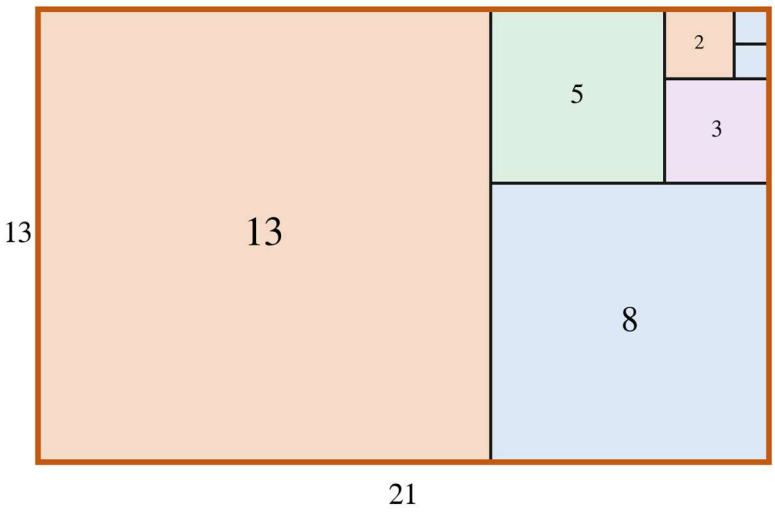
Soient $a \geq b > 0$ et r le reste de la division euclidienne de a par b. Alors

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

En itérant, la suite des restes est strictement décroissante et atteint 0 ; le dernier reste non nul est $\gcd(a,b)$.

Démonstration. Si $a = bq + r$, alors $\gcd(a,b) = \gcd(b, a - bq) = \gcd(b,r)$ par la proposition 2.1.2 (ii). La suite (r_k) des restes est strictement décroissante dans $\mathbb{N}$, donc finie ; si $r_{k+1} = 0$, alors $\gcd(r_{k-1}, r_k) = \gcd(r_k, 0) = r_k$. ■

$$21 = 1\cdot 13 + 8,\ 13 = 1\cdot 8 + 5,\ 8 = 1\cdot 5 + 3,\ 5 = 1\cdot 3 + 2,\ 3 = 1\cdot 2 + 1$$



L'algorithme d'Euclide vu géométriquement pour (21, 13) : on découpe le rectangle en carrés aussi grands que possible ; le côté du plus petit carré est le PGCD.

Exemple 2.2.2. *Calculer* $\gcd(1071,462)$.

$$1071 = 2\cdot 462 + 147, \qquad 462 = 3\cdot 147 + 21, \qquad 147 = 7\cdot 21 + 0.$$

Donc $\gcd(1071,462) = 21$.

Méthode 2.2.3 — Euclide symbolique

En compétition, on applique l'algorithme non pas à des nombres, mais à des expressions. Pour calculer $\gcd\big(f(n), g(n)\big)$ où f, g sont des polynômes, on soustrait des multiples de l'un à l'autre jusqu'à faire disparaître n.

Exemple 2.2.4. *Calculer $d_n = \gcd(n^3+1, n^2+2)$ en fonction de n.*

$$\gcd(n^3+1, n^2+2) = \gcd(n^3+1-n(n^2+2),\ n^2+2) = \gcd(1-2n,\ n^2+2).$$

Comme $\gcd(1-2n, 2) = 1$ ($1-2n$ est impair), on peut multiplier le second argument par 4 :

$$\gcd(1-2n, n^2+2) = \gcd(1-2n, 4n^2+8) = \gcd(1-2n, (2n-1)(2n+1)+9),$$

c'est-à-dire

$$\gcd(1-2n, n^2+2) = \gcd(1-2n, 9).$$

Donc $d_n = \gcd(2n-1, 9) \in \{1, 3, 9\}$: $d_n = 9$ si $n \equiv 5 \pmod 9$, $d_n = 3$ si $n \equiv 2 \pmod 3$ sans être $\equiv 5 \pmod 9$, et $d_n = 1$ sinon.

2.3 Le théorème de Bézout

Théorème 2.3.1 (Théorème de Bézout)

Soient a, b entiers non tous deux nuls et $d = \gcd(a, b)$. Alors il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = d.$$

De plus, d est le plus petit entier strictement positif de la forme $au + bv$, et l'ensemble $\{au + bv : u, v \in \mathbb{Z}\}$ est exactement l'ensemble des multiples de d.

Démonstration. Soit $E = \{au + bv : u, v \in \mathbb{Z}\} \cap \mathbb{N}^*$. Cet ensemble est non vide (il contient $|a|$ ou $|b|$), donc admet un plus petit élément $\delta = au_0 + bv_0$.

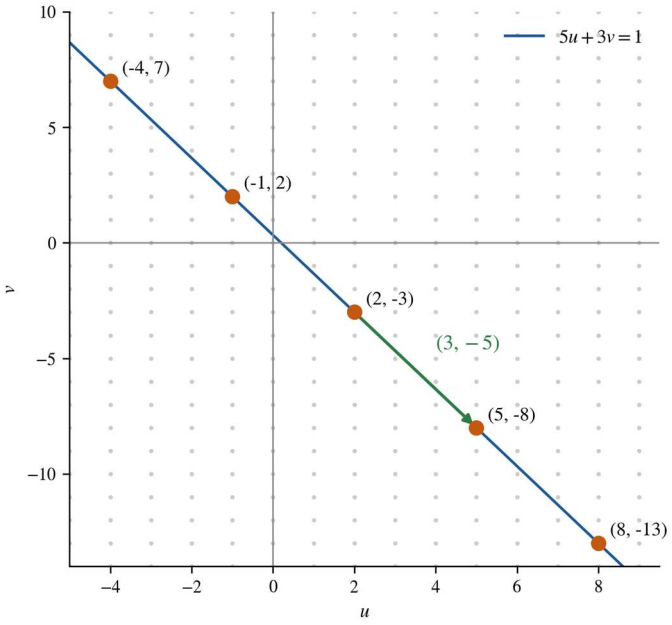
δ divise a : écrivons $a = \delta q + r$ avec $0 \le r < \delta$. Alors

$$r = a - \delta q = a(1 - u_0 q) + b(-v_0 q)$$

est de la forme $au + bv$. Comme $0 \le r < \delta$ et que δ est minimal dans E, on a $r = 0$. Donc $\delta \mid a$, et de même $\delta \mid b$: δ est un diviseur commun, donc $\delta \le d$.

Réciproquement, $d \mid a$ et $d \mid b$, donc $d \mid au_0 + bv_0 = \delta$, d'où $d \le \delta$. Conclusion : $\delta = d$.

Enfin, tout entier $au + bv$ est un multiple de d (car $d \mid a$ et $d \mid b$), et tout multiple kd s'écrit $a(ku_0) + b(kv_0)$. ∎



Les solutions de 5u + 3v = 1 sont les points entiers d'une droite, régulièrement espacés : (u, v) = (2, −3) + k(3, −5).

Corollaire 2.3.2 (Caractérisation des entiers premiers entre eux)

$\gcd(a,b) = 1$ si, et seulement si, il existe $u, v \in \mathbb{Z}$ avec $au + bv = 1$.

Démonstration. Si $\gcd(a,b) = 1$, le théorème 2.3.1 fournit u, v. Réciproquement, si $au + bv = 1$, tout diviseur commun de a et b divise 1, donc $\gcd(a,b) = 1$. ■

Théorème 2.3.3 (Lemme de Gauss)

Si $a \mid bc$ et $\gcd(a,b) = 1$, alors $a \mid c$.

Démonstration. Par Bézout, $au + bv = 1$. Multiplions par c : $acu + bcv = c$. Or $a \mid acu$ et $a \mid bc \mid bcv$, donc $a \mid c$. ■

Corollaire 2.3.4 (Conséquences du lemme de Gauss)

- (i) Si $a \mid c$, $b \mid c$ et $\gcd(a,b) = 1$, alors $ab \mid c$.
- (ii) Si $\gcd(a,b) = 1$ et $\gcd(a,c) = 1$, alors $\gcd(a,bc) = 1$.
- (iii) (Euclide) Si p est premier et $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration.

(i) $c = ak$; $b \mid ak$ avec $\gcd(a,b) = 1$ donne $b \mid k$ par Gauss, donc $k = bm$ et $c = abm$. (ii) $au + bv = 1$ et $au' + cv' = 1$; en multipliant : $a \cdot (\dots) + bc(vv') = 1$. (iii) Si $p \nmid a$, alors $\gcd(p,a) = 1$ (les seuls diviseurs positifs de p sont 1 et p), donc Gauss donne $p \mid b$. ■

Attention.
Le lemme de Gauss exige l'hypothèse de coprimalité. Sans elle, tout s'effondre : $6 \mid 4 \times 3$ mais $6 \nmid 4$ et $6 \nmid 3$. De même, (i) est fausse sans coprimalité : $4 \mid 12$ et $6 \mid 12$ mais $24 \nmid 12$.

2.4 Une formule très utile

Théorème 2.4.1 (PGCD de $a^m - 1$ et $a^n - 1$)

Soient $a \geq 2$ et $m, n \geq 1$ des entiers. Alors

$$\operatorname{pgcd}(a^m - 1, a^n - 1) = a^{\operatorname{pgcd}(m,n)} - 1.$$

Démonstration. Procédons par récurrence forte sur $m + n$, en supposant $m \geq n$ (le cas $m = n$ est clair). Posons $x_k = a^k - 1$. On a

$$x_m - a^{m-n} x_n = (a^m - 1) - a^{m-n}(a^n - 1) = a^{m-n} - 1 = x_{m-n}.$$

Donc $\operatorname{pgcd}(x_m, x_n) = \operatorname{pgcd}(x_{m-n}, x_n)$. Par hypothèse de récurrence (car $(m-n) + n < m + n$) et puisque $\operatorname{pgcd}(m-n, n) = \operatorname{pgcd}(m, n)$:

$\operatorname{pgcd}(x_m, x_n) = a^{\operatorname{pgcd}(m-n,n)} - 1 = a^{\operatorname{pgcd}(m,n)} - 1.$ ■

Exemple 2.4.2. *Calculer* $\operatorname{pgcd}(2^{2024} - 1, 2^{1000} - 1)$.

$\operatorname{pgcd}(2024, 1000) = 8$, donc le PGCD vaut $2^8 - 1 = 255$.

Proposition 2.4.3 (PGCD de deux termes de la suite de Fibonacci)

Soit (F_n) définie par $F_1 = F_2 = 1$, $F_{n+2} = F_{n+1} + F_n$. Alors

$$\operatorname{pgcd}(F_m, F_n) = F_{\operatorname{pgcd}(m,n)}.$$

Démonstration. *Étape 1 :* $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$ *pour* $m \geq 2$, $n \geq 1$ *(avec* $F_0 = 0$*, cette formule vaut aussi pour* $m = 1$*).* Récurrence sur n. Pour $n = 1$: $F_m F_2 + F_{m-1} F_1 = F_m + F_{m-1} = F_{m+1}$. Pour $n = 2$: $F_m F_3 + F_{m-1} F_2 = 2F_m + F_{m-1} = F_{m+1} + F_m = F_{m+2}$. Si la formule vaut pour n et $n+1$, en additionnant on obtient $F_{m+n} + F_{m+n+1} = F_m(F_{n+1} + F_{n+2}) + F_{m-1}(F_n + F_{n+1})$, soit $F_{m+n+2} = F_m F_{n+3} + F_{m-1} F_{n+2}$.

Étape 2 : $\operatorname{pgcd}(F_n, F_{n+1}) = 1$. Par la proposition 2.1.2 (ii), $\operatorname{pgcd}(F_{n+1}, F_{n+2}) = \operatorname{pgcd}(F_{n+1}, F_{n+2} - F_{n+1}) = \operatorname{pgcd}(F_{n+1}, F_n)$, et $\operatorname{pgcd}(F_1, F_2) = 1$; on conclut par récurrence.

Étape 3 : $\operatorname{pgcd}(F_{m+n}, F_n) = \operatorname{pgcd}(F_m, F_n)$. Par l'étape 1 et la proposition 2.1.2 (ii), $\operatorname{pgcd}(F_{m+n}, F_n) = \operatorname{pgcd}(F_m F_{n+1}, F_n)$. Comme F_{n+1} est premier avec F_n, les diviseurs communs de $F_m F_{n+1}$ et F_n sont ceux de F_m et F_n : un diviseur commun e de $F_m F_{n+1}$ et F_n est premier avec F_{n+1}, donc divise F_m par le lemme de Gauss ; la réciproque est claire.

Étape 4 : conclusion. On raisonne par récurrence forte sur $m + n$, comme pour le théorème 2.4.1 : si $m > n$, l'étape 3 donne $\operatorname{pgcd}(F_m, F_n) = \operatorname{pgcd}(F_{m-n}, F_n)$, et $\operatorname{pgcd}(m-n, n) = \operatorname{pgcd}(m, n)$; si $m = n$, c'est évident. Les pas de l'algorithme d'Euclide sur les indices se reproduisent sur les termes, et l'on aboutit à $F_{\operatorname{pgcd}(m,n)}$. ■

2.5 Exercices

Exercice 2.1 ★. Calculer $\gcd(n, n+1)$, $\gcd(2n+1, 3n+2)$ et $\gcd(n^2+n, 2n+1)$.

Exercice 2.2 ★ (IMO 1959, problème 1). Montrer que la fraction $\frac{21n+4}{14n+3}$ est irréductible pour tout $n \in \mathbb{N}$.

Exercice 2.3 ★★. Soient a, b premiers entre eux. Montrer que $\gcd(a+b, a^2-ab+b^2) \in \{1, 3\}$.

Exercice 2.4 ★★. Montrer que $\gcd(2^m+1, 2^n+1) = 1$ si $\frac{m}{\gcd(m,n)}$ et $\frac{n}{\gcd(m,n)}$ ne sont pas tous deux impairs.

Traiter en particulier le cas des nombres de Fermat $F_k = 2^{2^k}+1$: montrer qu'ils sont deux à deux premiers entre eux, et en déduire qu'il existe une infinité de nombres premiers.

Exercice 2.5 ★★★. Montrer que si $n > 1$ vérifie $n \mid 2^n+1$, alors $3 \mid n$. Montrer réciproquement que $n = 3^k$ convient pour tout $k \geq 0$.

Exercice 2.6 ★★★. Soient a, b des entiers strictement positifs tels que $\gcd(a, b) = 1$. Montrer que le plus grand entier qui n'est pas de la forme $ax + by$ avec $x, y \in \mathbb{N}$ est $ab - a - b$ (problème de Frobenius, cas de deux entiers).

2.6 Corrigés

Solution de l'exercice 2.1. $\gcd(n, n+1) = \gcd(n, 1) = 1$.

$\gcd(2n+1, 3n+2)$: $3n+2-(2n+1) = n+1$, puis $2n+1-2(n+1) = -1$. Donc le PGCD vaut 1.

$\gcd(n^2+n, 2n+1)$: $4(n^2+n) = (2n+1)^2 - 1$, donc $\gcd(4(n^2+n), 2n+1) = \gcd(1, 2n+1) = 1$; comme $2n+1$ est impair, $\gcd(n^2+n, 2n+1) = 1$.

Solution de l'exercice 2.2. $3(14n+3) - 2(21n+4) = 42n+9-42n-8 = 1$. Par Bézout, $\gcd(21n+4, 14n+3) = 1$: la fraction est irréductible.

> **Remarque.**
> C'est le tout premier problème de la toute première IMO (1959). Sa solution tient en une ligne — à condition d'avoir le réflexe Bézout.

Solution de l'exercice 2.3. Posons $d = \gcd(a+b, a^2-ab+b^2)$. Comme

$$a^2 - ab + b^2 = (a+b)^2 - 3ab,$$

on a $d \mid 3ab$. Or $\gcd(a+b, a) = \gcd(b, a) = 1$ et de même $\gcd(a+b, b) = 1$, donc $\gcd(a+b, ab) = 1$ (corollaire 2.3.4 (ii)), puis $\gcd(d, ab) = 1$ et $d \mid 3$ par Gauss. Les deux valeurs sont atteintes : $a = b = 1$ donne $d = 1$; $a = 2$, $b = 1$ donne $\gcd(3, 3) = 3$.

Solution de l'exercice 2.4. *Cas général.* Soient $g = \gcd(m, n)$ et $d = \gcd(2^m+1, 2^n+1)$; d est impair. De $2^m \equiv -1$ et $2^n \equiv -1 \pmod d$, on tire $d \mid 2^{2m}-1$ et $d \mid 2^{2n}-1$, donc $d \mid \gcd(2^{2m}-1, 2^{2n}-1) = 2^{2g}-1$ (théorème 2.4.1). Si $\frac{m}{g}$ est pair, alors $2g \mid m$, donc $2^m \equiv 1 \pmod d$; avec $2^m \equiv -1$, on obtient $d \mid 2$, d'où $d = 1$. De même si $\frac{n}{g}$ est pair.

Nombres de Fermat. Traitons-les directement. Soient $k < \ell$ et $d = \gcd(F_k, F_\ell)$. On utilise l'identité

$$F_0F_1\cdots F_{\ell-1} = 2^{2^\ell} - 1 = F_\ell - 2,$$

qui se démontre par récurrence : $F_0\cdots F_{\ell-1} = \left(2^{2^{\ell-1}} - 1\right)F_{\ell-1} = \left(2^{2^{\ell-1}} - 1\right)\left(2^{2^{\ell-1}} + 1\right) = 2^{2^\ell} - 1$. Comme $k \le \ell - 1$, F_k divise $F_\ell - 2$. Donc $d \mid F_\ell$ et $d \mid F_\ell - 2$, d'où $d \mid 2$. Mais les F_k sont impairs, donc $d = 1$.

Infinité de nombres premiers. Chaque F_k possède au moins un facteur premier p_k ; comme les F_k sont deux à deux premiers entre eux, les p_k sont deux à deux distincts. On obtient ainsi une infinité de nombres premiers (argument dû à Goldbach, popularisé par Pólya).

Solution de l'exercice 2.5. *Sens direct.* Soit $n > 1$ avec $n \mid 2^n + 1$. Comme $2^n + 1$ est impair, n est impair. Soient p le plus petit facteur premier de n et $d = \mathrm{ord}_p(2)$ (chapitre 7). De $2^n \equiv -1 \pmod p$, on tire $2^{2n} \equiv 1$, donc $d \mid 2n$, tandis que $d \nmid n$.

Par Fermat, $d \mid p - 1$, donc $d \mid \mathrm{pgcd}(2n, p-1)$. Or tout facteur premier impair de $\mathrm{pgcd}(2n, p-1)$ diviserait n tout en étant $< p$: impossible par minimalité de p. Comme n est impair, $v_2(2n) = 1$, donc $\mathrm{pgcd}(2n, p-1)$ divise 2 et $d \mid 2$. Enfin $d \neq 1$ (sinon $p \mid 2 - 1 = 1$), donc $d = 2$ et $p \mid 2^2 - 1 = 3$: ainsi $p = 3$ et $3 \mid n$.

Réciproque. Pour $n = 3^k$, le lemme LTE (chapitre 14) donne

$$v_3\left(2^{3^k} + 1\right) = v_3(2+1) + v_3\left(3^k\right) = 1 + k \ge k = v_3(n),$$

donc $3^k \mid 2^{3^k} + 1$.

> **Remarque.**
> Attention : les puissances de 3 ne sont pas les seules solutions. Ainsi $n = 171 = 9 \times 19$ convient : d'une part $v_3(2^{171} + 1) = 1 + 2 = 3 \ge 2$, d'autre part $\mathrm{ord}_{19}(2) = 18$ et $171 \equiv 9 \pmod{18}$, donc $2^{171} \equiv 2^9 \equiv -1 \pmod{19}$ et $19 \mid 2^{171} + 1$. En revanche, la condition bien plus rigide $n^2 \mid 2^n + 1$ ne laisse subsister que $n = 1$ et $n = 3$: c'est le problème 3 de l'IMO 1990.

Solution de l'exercice 2.6.

(a) $ab - a - b$ n'est pas représentable. Supposons $ab - a - b = ax + by$ avec $x, y \ge 0$. Alors $ab = a(x+1) + b(y+1)$. Comme $a \mid ab$ et $a \mid a(x+1)$, on a $a \mid b(y+1)$, donc $a \mid y + 1$ par Gauss ; ainsi $y + 1 \ge a$. Symétriquement, $x + 1 \ge b$. D'où $ab = a(x+1) + b(y+1) \ge ab + ab = 2ab$: absurde.

(b) Tout $n > ab - a - b$ est représentable. Comme $\mathrm{pgcd}(a, b) = 1$, a est inversible modulo b : choisissons $x \in \{0, 1, \ldots, b-1\}$ avec $ax \equiv n \pmod b$. Alors $n - ax = by$ pour un entier y, et

$$by = n - ax > (ab - a - b) - a(b-1) = -b,$$

donc $y > -1$, c'est-à-dire $y \ge 0$. Ainsi $n = ax + by$ avec $x, y \ge 0$.

CHAPITRE 3

3 Nombres premiers, factorisation et valuation p-adique

Objectifs du chapitre.

- Démontrer le théorème fondamental de l'arithmétique.
- Traduire divisibilité, PGCD et PPCM en langage de valuations.
- Maîtriser la formule de Legendre pour $v_p(n!)$.
- Connaître plusieurs preuves de l'infinitude des nombres premiers.

3.1 Théorème fondamental de l'arithmétique

Définition 3.1.1 (Nombre premier)

Un entier $p \geq 2$ est premier si ses seuls diviseurs positifs sont 1 et p. Un entier $n \geq 2$ non premier est composé.

Théorème 3.1.2 (Théorème fondamental de l'arithmétique)

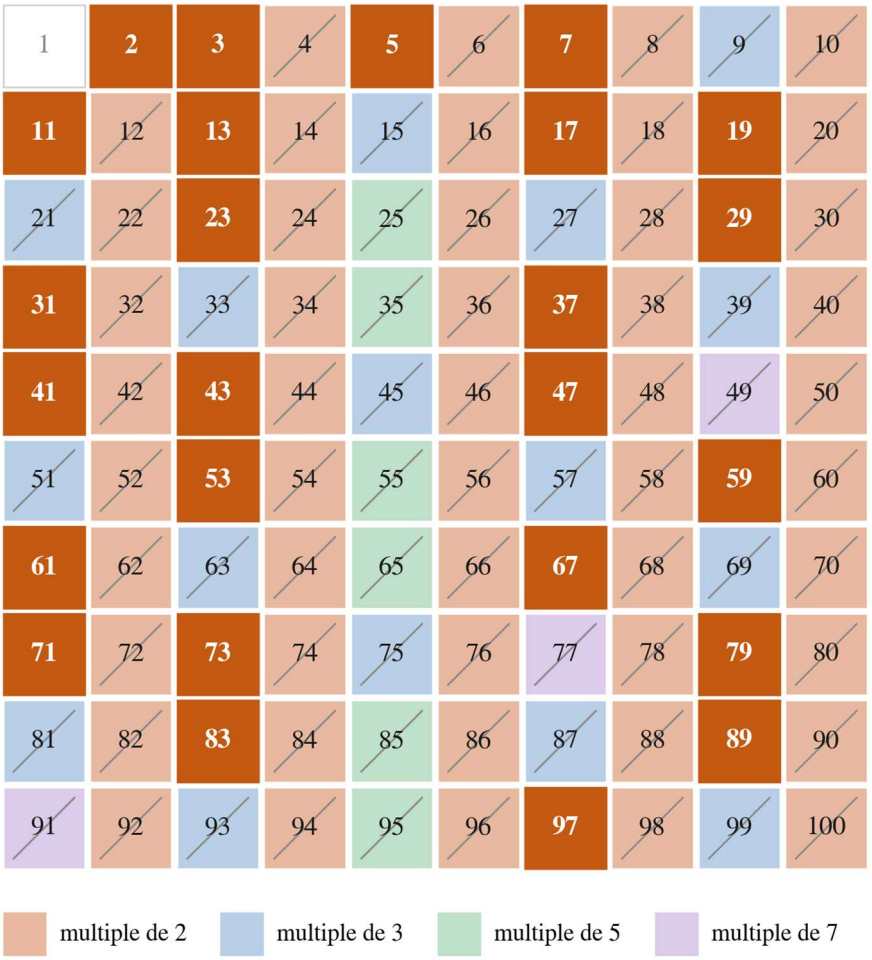
Tout entier $n \geq 2$ s'écrit de manière unique (à l'ordre près) sous la forme

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

où $p_1 < p_2 < \cdots < p_k$ sont premiers et $\alpha_i \geq 1$.

Démonstration. *Existence*, par récurrence forte sur $n \geq 2$. Si n est premier, c'est une décomposition. Sinon, n a un diviseur positif a autre que 1 et n ; alors $n = ab$ avec $1 < a, b < n$, et l'hypothèse de récurrence fournit des décompositions de a et de b, dont le produit est une décomposition de n.

Unicité. Montrons, par récurrence forte sur n, que deux écritures $n = p_1 \cdots p_r = q_1 \cdots q_s$ comme produits de nombres premiers (avec répétitions) coïncident à l'ordre près. Le premier p_1 divise $q_1 \cdots q_s$; par le lemme d'Euclide (corollaire 2.3.4 (iii)) appliqué de proche en proche, il divise l'un des q_j. Comme q_j est premier et $p_1 > 1$, on a $p_1 = q_j$. En simplifiant par p_1, on obtient deux écritures de $\frac{n}{p_1} < n$; si $\frac{n}{p_1} = 1$, les deux produits restants sont vides ; sinon l'hypothèse de récurrence s'applique. ■



Le crible d'Ératosthène jusqu'à 100 : on barre les multiples de 2, 3, 5 et 7 ; les nombres restants (en couleur) sont les 25 nombres premiers inférieurs à 100.

À retenir

L'unicité de la factorisation repose sur le lemme d'Euclide, qui repose sur Bézout, qui repose sur la division euclidienne. Ce n'est pas une évidence : dans l'anneau $\mathbb{Z}[\sqrt{-5}]$, on a $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, deux factorisations essentiellement différentes en éléments irréductibles.

3.2 Valuation p-adique

Définition 3.2.1 (Valuation p-adique)

Soit p premier et $n \in \mathbb{Z}^*$. La valuation p-adique $v_p(n)$ est l'exposant de p dans la décomposition de $|n|$; autrement dit, c'est le plus grand entier k tel que $p^k \mid n$. On note $p^k \parallel n$ pour $v_p(n) = k$. Par convention, $v_p(0) = +\infty$.

Proposition 3.2.2 (Propriétés des valuations)

Pour tous $a, b \in \mathbb{Z}^*$ et p premier :

(i) $v_p(ab) = v_p(a) + v_p(b)$;

(ii) $v_p(a+b) \geq \min\big(v_p(a), v_p(b)\big)$, avec égalité si $v_p(a) \neq v_p(b)$;

(iii) $a \mid b \Leftrightarrow \forall p,\ v_p(a) \leq v_p(b)$;

(iv) $v_p\big(\mathrm{pgcd}(a,b)\big) = \min\big(v_p(a), v_p(b)\big)$ et $v_p\big(\mathrm{ppcm}(a,b)\big) = \max\big(v_p(a), v_p(b)\big)$;

(v) a est un carré parfait si, et seulement si, $v_p(a)$ est pair pour tout p (avec $a > 0$).

Démonstration. Écrivons $|a| = \prod_p p^{v_p(a)}$ et $|b| = \prod_p p^{v_p(b)}$ (produits finis, théorème 3.1.2).

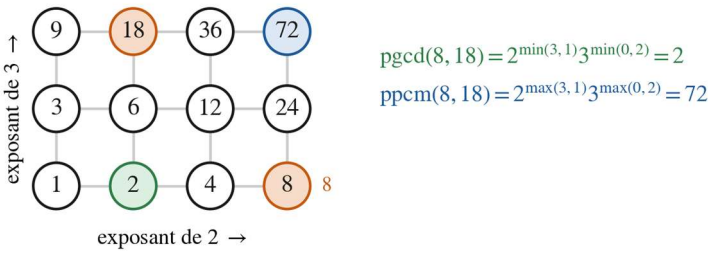
(i) En multipliant ces écritures, $|ab| = \prod_p p^{v_p(a)+v_p(b)}$; par unicité de la décomposition, $v_p(ab) = v_p(a) + v_p(b)$.

(ii) Si $v_p(a) = \alpha \leq \beta = v_p(b)$, écrivons $a = p^\alpha a'$, $b = p^\beta b'$ avec $p \nmid a'$. Alors $a + b = p^\alpha\big(a' + p^{\beta-\alpha}b'\big)$, donc $v_p(a+b) \geq \alpha$ (si $a + b \neq 0$). Si $\alpha < \beta$, la parenthèse est $\equiv a' \not\equiv 0 \pmod p$, d'où l'égalité.

(iii) Si $b = ac$, alors $v_p(b) = v_p(a) + v_p(c) \geq v_p(a)$ par (i). Réciproquement, si $v_p(a) \leq v_p(b)$ pour tout p, l'entier $c = \prod_p p^{v_p(b)-v_p(a)}$ vérifie $|b| = |a|c$, donc $a \mid b$.

(iv) Soit $m = \prod_p p^{\min\left(v_p(a),v_p(b)\right)}$. Par (iii), m divise a et b, et tout diviseur commun e vérifie $v_p(e) \leq \min\big(v_p(a), v_p(b)\big)$ pour tout p, donc $e \mid m$; ainsi m est le plus grand diviseur commun. De même, $M = \prod_p p^{\max\left(v_p(a),v_p(b)\right)}$ est un multiple commun, et tout multiple commun est un multiple de M par (iii).

(v) Si $a = c^2$, alors $v_p(a) = 2v_p(c)$. Réciproquement, si toutes les valuations de $a > 0$ sont paires, $a = \big(\prod_p p^{v_p(a)/2}\big)^2$. ■



Les diviseurs de 72 = 2³·3² : a divise b si, et seulement si, les exposants de a sont inférieurs à ceux de b ; le PGCD et le PPCM se lisent coordonnée par coordonnée.

Corollaire 3.2.3

$\mathrm{pgcd}(a,b) \cdot \mathrm{ppcm}(a,b) = |ab|$, car $\min(x,y) + \max(x,y) = x + y$.

Démonstration. Par la proposition 3.2.2 (iv) et (i), pour tout premier p, $v_p\big(\mathrm{pgcd}(a,b)\mathrm{ppcm}(a,b)\big) = \min + \max = v_p(a) + v_p(b) = v_p(ab)$; les deux entiers positifs ont les mêmes valuations, ils sont égaux. (C'est une seconde démonstration de la proposition 2.1.2 (v).) ■

Méthode 3.2.4 — Traduire en valuations

Dès qu'un problème mêle divisibilité, carrés, puissances n-ièmes ou PGCD/PPCM, fixez un nombre premier p arbitraire et traduisez tout l'énoncé en inégalités sur v_p. Une identité entre entiers devient une identité entre nombres entiers positifs, souvent triviale à analyser.

Exemple 3.2.5. *Soient a, b, c des entiers strictement positifs tels que abc soit un cube parfait et $\gcd(a,b) = \gcd(b,c) = \gcd(c,a) = 1$. Montrer que a, b, c sont des cubes parfaits.*

Soit p premier. Par coprimalité deux à deux, p divise au plus un des trois nombres. Si $p \mid a$, alors $v_p(b) = v_p(c) = 0$ et donc $v_p(a) = v_p(abc) \equiv 0 \pmod 3$. Ainsi toutes les valuations de a sont multiples de 3 : a est un cube. Idem pour b et c.

Exemple 3.2.6. *Montrer que $\sqrt{2}$ est irrationnel, puis que $\sqrt[n]{m}$ est irrationnel dès que m n'est pas une puissance n-ième.*

Si $\sqrt[n]{m} = a/b$ avec $a, b \in \mathbb{N}^*$, alors $mb^n = a^n$. Pour tout premier p : $v_p(m) + n\, v_p(b) = n\, v_p(a)$, donc $n \mid v_p(m)$. Toutes les valuations de m étant multiples de n, m est une puissance n-ième.

3.3 La formule de Legendre

Théorème 3.3.1 (Formule de Legendre)

Soient p premier et $n \in \mathbb{N}^*$. Alors

$$v_p(n!) = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - S_p(n)}{p-1},$$

où $S_p(n)$ désigne la somme des chiffres de n écrit en base p.

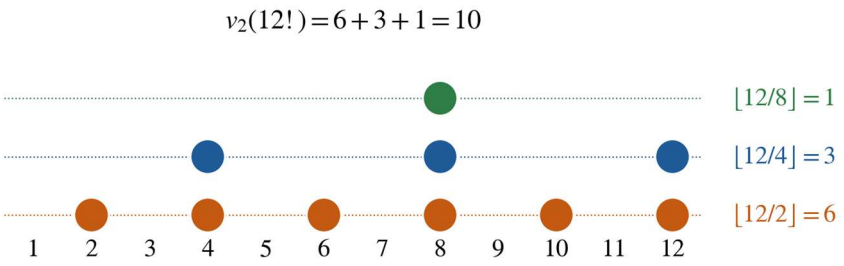
Démonstration. *Première formule.* Par la proposition 3.2.2 (i), $v_p(n!) = \sum_{k=1}^{n} v_p(k)$. Or $v_p(k)$ est le nombre d'entiers $i \geq 1$ tels que $p^i \mid k$. Donc

$$v_p(n!) = \sum_{k=1}^{n} \sum_{i \geq 1} \mathbf{1}_{p^i \mid k} = \sum_{i \geq 1} \#\{k \leq n : p^i \mid k\} = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor,$$

car les multiples de p^i dans $\{1, \dots, n\}$ sont $p^i, 2p^i, \dots, \left\lfloor \frac{n}{p^i} \right\rfloor p^i$. La somme est finie, puisque $\lfloor n/p^i \rfloor = 0$ dès que $p^i > n$. On a interverti deux sommes finies : c'est un **double comptage** des couples (k, i) tels que $p^i \mid k$ (figure ci-dessous).

Seconde formule. Écrivons $n = \sum_{j=0}^{k} a_j\, p^j$ en base p. Alors $\lfloor n/p^i \rfloor = \sum_{j \geq i} a_j\, p^{j-i}$, donc

$\sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{j \geq 1} a_j \left(p^{j-1} + \cdots + p + 1\right) = \sum_{j \geq 1} a_j \frac{p^j - 1}{p-1} = \frac{1}{p-1}\left(\sum_j a_j\, p^j - \sum_j a_j\right) = \frac{n - S_p(n)}{p-1}.$ ∎



Formule de Legendre pour $v_2(12!)$: chaque colonne k porte $v_2(k)$ jetons ; en comptant par lignes, on obtient ⌊12/2⌋ + ⌊12/4⌋ + ⌊12/8⌋ = 6 + 3 + 1 = 10.

Exemple 3.3.2. *Par combien de zéros se termine* $2026!$ *?*

Le nombre de zéros finaux est $\min(v_2, v_5) = v_5(2026!)$ (car $v_2 > v_5$ toujours). Or

$$v_5(2026!) = \left\lfloor \frac{2026}{5} \right\rfloor + \left\lfloor \frac{2026}{25} \right\rfloor + \left\lfloor \frac{2026}{125} \right\rfloor + \left\lfloor \frac{2026}{625} \right\rfloor = 405 + 81 + 16 + 3 = 505.$$

Exemple 3.3.3. *Montrer que* $\frac{(2m)!\,(2n)!}{m!\,n!\,(m+n)!}$ *est un entier pour tous* $m, n \geq 0$.

Fixons p premier. Il faut montrer que, pour tout $i \geq 1$,

$$\left\lfloor \frac{2m}{p^i} \right\rfloor + \left\lfloor \frac{2n}{p^i} \right\rfloor \geq \left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor + \left\lfloor \frac{m+n}{p^i} \right\rfloor.$$

Il suffit donc de prouver l'inégalité élémentaire, pour tous réels $x, y \geq 0$:

$$\lfloor 2x \rfloor + \lfloor 2y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor.$$

Posons $x = \lfloor x \rfloor + \{x\}$, $y = \lfloor y \rfloor + \{y\}$. L'inégalité se réduit à $\lfloor 2\{x\} \rfloor + \lfloor 2\{y\} \rfloor \geq \lfloor \{x\} + \{y\} \rfloor$. Si $\{x\} + \{y\} < 1$, le membre de droite vaut 0 et c'est clair. Sinon, l'un au moins de $\{x\}, \{y\}$ est $\geq 1/2$, donc le membre de gauche vaut au moins 1, égal au membre de droite.

À retenir

La technique « réduire à une inégalité sur les parties entières » démontre l'intégralité de la plupart des quotients factoriels, en particulier celle des coefficients binomiaux $\binom{n}{k}$ et des coefficients multinomiaux.

3.4 Il y a une infinité de nombres premiers

Théorème 3.4.1 (Euclide)

L'ensemble des nombres premiers est infini.

Démonstration (Euclide). Supposons que $p_1, \ldots, p_k$ soient les seuls nombres premiers et posons $N = p_1 \cdots p_k + 1$. Comme $N \geq 2$, N possède un facteur premier p, qui est l'un des p_i. Alors $p \mid N$ et $p \mid N - 1$, donc $p \mid 1$: absurde. ∎

Proposition 3.4.2 (Premiers de la forme 4k + 3)

Il existe une infinité de nombres premiers de la forme $4k + 3$.

Démonstration. Supposons-en un nombre fini $p_1 = 3, p_2 = 7, \dots, p_k$ et posons $N = 4p_1p_2\cdots p_k - 1$. Alors $N \equiv 3 \pmod 4$, donc N possède au moins un facteur premier $q \equiv 3 \pmod 4$: en effet, un produit de nombres $\equiv 1 \pmod 4$ est $\equiv 1 \pmod 4$, et N est impair. Ce q est l'un des p_i, donc $q \mid N$ et $q \mid N+1$: absurde. ■

Remarque.

De même, il existe une infinité de premiers $\equiv 5 \pmod 6$, $\equiv 2 \pmod 3$… Le cas général — toute progression arithmétique $an + b$ avec $\gcd(a,b) = 1$ contient une infinité de premiers — est le théorème de Dirichlet, dont la démonstration dépasse le cadre élémentaire. En compétition, on ne peut pas l'invoquer sans risque : cherchez toujours un argument *ad hoc* du type ci-dessus.

Proposition 3.4.3 (Longues suites de nombres composés)

Pour tout k, il existe k entiers consécutifs tous composés.

Démonstration. Les entiers $(k+1)!+2, (k+1)!+3, \dots, (k+1)!+(k+1)$ sont divisibles respectivement par $2,3,\dots,k+1$ et strictement supérieurs à ces diviseurs. ■

3.5 Exercices

Exercice 3.1 ★. Déterminer $v_3(100!)$ et $v_7(1000!)$.

Exercice 3.2 ★. Soit $n = 2^a 3^b 5^c$. Combien n possède-t-il de diviseurs ? Combien sont des carrés parfaits ?

Exercice 3.3 ★★. Trouver tous les n tels que $n!$ se termine par exactement 2026 zéros.

Exercice 3.4 ★★. Montrer que, pour tout $n \geq 1$, $\operatorname{ppcm}(1,2,\dots,2n) = \operatorname{ppcm}(n+1, n+2, \dots, 2n)$.

Exercice 3.5 ★★. Montrer que $\sum_{k=1}^{n} \frac{1}{k}$ n'est jamais un entier pour $n \geq 2$.

Exercice 3.6 ★★★. Soit p un premier impair. Montrer que $\binom{2p}{p} \equiv 2 \pmod{p^2}$.

Exercice 3.7 ★★★ (ISL). Déterminer tous les entiers $n \geq 1$ tels que $2^n \mid 3^n - 1$.

3.6 Corrigés

Solution de l'exercice 3.1. $v_3(100!) = 33 + 11 + 3 + 1 = 48$. $v_7(1000!) = 142 + 20 + 2 = 164$.

Solution de l'exercice 3.2. Un diviseur s'écrit $2^x 3^y 5^z$ avec $0 \leq x \leq a$, etc. : il y en a $(a+1)(b+1)(c+1)$. Les carrés correspondent à x, y, z pairs : $\left(\left\lfloor \frac{a}{2} \right\rfloor + 1\right)\left(\left\lfloor \frac{b}{2} \right\rfloor + 1\right)\left(\left\lfloor \frac{c}{2} \right\rfloor + 1\right)$.

Solution de l'exercice 3.3. On cherche $v_5(n!) = 2026$, soit $\frac{n - S_5(n)}{4} = 2026$, c'est-à-dire $n - S_5(n) = 8104$. On calcule : $v_5(8110) = 1622 + 324 + 64 + 12 + 2 = 2024$; $v_5(8115) = 1623 + 324 + 64 + 12 + 2 = 2025$; $v_5(8120) = 1624 + 324 + 64 + 12 + 2 = 2026$; $v_5(8125) = 1625 + 325 + 65 + 13 + 2 = 2030$. Comme $v_5(n!)$ ne change qu'aux multiples de 5, les solutions sont

$$n \in \{8120, 8121, 8122, 8123, 8124\}.$$

Solution de l'exercice 3.4. Notons $L = \operatorname{ppcm}(n+1, \dots, 2n)$ et $M = \operatorname{ppcm}(1, \dots, 2n)$. Comme $\{n+1, \dots, 2n\} \subset \{1, \dots, 2n\}$, on a $L \mid M$.

Réciproquement, M est le produit des puissances de premiers p^α maximales sous $2n$ (c'est-à-dire $p^\alpha \le 2n < p^{\alpha+1}$). Il suffit donc de montrer que chacune divise L. Deux cas :

- si $p^\alpha > n$, alors p^α appartient lui-même à $\{n+1, \dots, 2n\}$;
- si $p^\alpha \le n$, posons $t = \lfloor 2n/p^\alpha \rfloor$ et $m = tp^\alpha$. Alors $m \le 2n$ et $m > 2n - p^\alpha \ge 2n - n = n$, donc $m \in \{n+1, \dots, 2n\}$ et $p^\alpha \mid m \mid L$.

Dans les deux cas $p^\alpha \mid L$, donc $M \mid L$ et finalement $L = M$.

Solution de l'exercice 3.5. Soit 2^r la plus grande puissance de 2 inférieure ou égale à n. Il n'existe qu'un seul multiple de 2^r dans $\{1, \dots, n\}$, à savoir 2^r lui-même : sinon $2^{r+1} \le n$. Multiplions $H_n = \sum 1/k$ par $M = \operatorname{ppcm}(1, \dots, n)$. Tous les termes M/k sont pairs sauf $M/2^r$, qui est impair (car $v_2(M) = r$). Donc MH_n est impair, alors que M est pair : si H_n était entier, MH_n serait pair. Contradiction.

Solution de l'exercice 3.6.

$$\binom{2p}{p} = \frac{(2p)!}{(p!)^2} = 2 \cdot \frac{(2p-1)!}{p!\,(p-1)!} = 2\prod_{k=1}^{p-1} \frac{p+k}{k}.$$

Donc

$$\frac{1}{2}\binom{2p}{p} = \prod_{k=1}^{p-1}\left(1 + \frac{p}{k}\right) \equiv 1 + p\sum_{k=1}^{p-1}\frac{1}{k} \pmod{p^2},$$

au sens des inverses modulaires. Or $\sum_{k=1}^{p-1} k^{-1} \equiv \sum_{k=1}^{p-1} k = \frac{p(p-1)}{2} \equiv 0 \pmod{p}$ (les inverses parcourent le même ensemble que les k). Donc $\frac{1}{2}\binom{2p}{p} \equiv 1 \pmod{p^2}$, c'est-à-dire $\binom{2p}{p} \equiv 2 \pmod{p^2}$.

> **Remarque.**
> C'est le théorème de Wolstenholme (version faible) ; la version forte affirme $\binom{2p}{p} \equiv 2 \pmod{p^3}$ pour $p \ge 5$.

Solution de l'exercice 3.7. Par le lemme LTE, version $p = 2$ (chapitre 14) : pour n pair,

$$v_2(3^n - 1) = v_2(3-1) + v_2(3+1) + v_2(n) - 1 = 1 + 2 + v_2(n) - 1 = 2 + v_2(n).$$

Pour n impair, $3^n - 1 \equiv 2 \pmod 4$, donc $v_2(3^n - 1) = 1$.

La condition $2^n \mid 3^n - 1$ s'écrit $n \le v_2(3^n - 1)$. Si n est impair : $n \le 1$, donc $n = 1$. Si n est pair : $n \le 2 + v_2(n)$. Or $v_2(n) \le \log_2 n$, donc $n - \log_2 n \le 2$, ce qui donne $n \in \{2,4\}$. On vérifie : $n = 2 : 2^2 = 4 \mid 8$ ✓ ; $n = 4 : 2^4 = 16 \mid 80$ ✓.

Réponse : $n \in \{1,2,4\}$.

CHAPITRE 4

4 Congruences

Objectifs du chapitre.

- Manipuler les congruences comme une véritable arithmétique.
- Savoir choisir le bon module devant un problème.
- Connaître les critères de divisibilité et le théorème de Wilson.
- Utiliser les systèmes complets de résidus.

4.1 Définition et règles de calcul

Définition 4.1.1 (Congruence)

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On écrit $a \equiv b \pmod{n}$ si $n \mid a - b$.

Proposition 4.1.2 (Compatibilité avec les opérations)

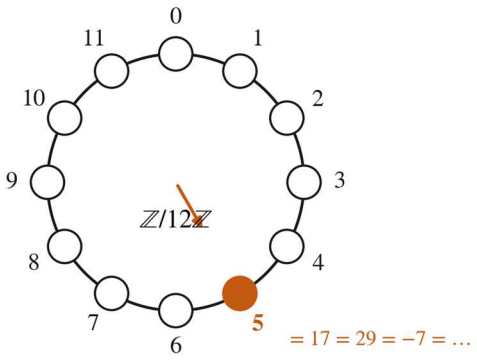
La relation $\equiv \pmod{n}$ est une relation d'équivalence compatible avec l'addition et la multiplication : si $a \equiv b$ et $c \equiv d \pmod{n}$, alors

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

et, par récurrence, $a^k \equiv b^k \pmod{n}$ pour tout $k \geq 0$.

Démonstration. *Relation d'équivalence.* $n \mid a - a = 0$ (réflexivité) ; si $n \mid a - b$, alors $n \mid b - a$ (symétrie) ; si $n \mid a - b$ et $n \mid b - c$, alors $n \mid (a - b) + (b - c) = a - c$ (transitivité).

Compatibilité. Si $n \mid a - b$ et $n \mid c - d$, alors $n \mid (a \pm c) - (b \pm d) = (a - b) \pm (c - d)$. Pour le produit : $ac - bd = c(a - b) + b(c - d)$ est une combinaison des deux multiples de n. Enfin, $a^k \equiv b^k$ s'obtient par récurrence sur k, en multipliant $a^k \equiv b^k$ par $a \equiv b$. ■



Arithmétique modulo 12 : les entiers s'enroulent sur une horloge ; 5, 17, 29 et −7 occupent la même position, car ils sont congrus modulo 12.

Attention — La division est interdite… sauf précaution.

De $ac \equiv bc \pmod{n}$, on ne peut pas déduire $a \equiv b$. Exemple : $2 \cdot 3 \equiv 2 \cdot 0 \pmod{6}$ mais $3 \not\equiv 0 \pmod{6}$. La règle correcte est

$$ac \equiv bc \pmod{n} \Leftrightarrow a \equiv b \left(\mathrm{mod}\, \frac{n}{\mathrm{pgcd}(n,c)}\right).$$

En particulier, si $\mathrm{pgcd}(c,n) = 1$, on peut simplifier librement.

Démonstration. On a $n \mid c(a-b)$. Posons $d = \mathrm{pgcd}(n,c)$, $n = dn'$, $c = dc'$ avec $\mathrm{pgcd}(n',c') = 1$. Alors $dn' \mid dc'(a-b)$, donc $n' \mid c'(a-b)$, et par Gauss $n' \mid a-b$. Réciproquement, si $n' \mid a-b$, alors $n = dn' \mid dc'(a-b) = c(a-b)$. ■

Proposition 4.1.3 (Congruences simultanées)

Si $a \equiv b \pmod{m}$ et $a \equiv b \pmod{n}$, alors $a \equiv b \pmod{\mathrm{ppcm}(m,n)}$. En particulier, si $\mathrm{pgcd}(m,n) = 1$, alors $a \equiv b \pmod{mn}$.

Démonstration. L'entier $a-b$ est un multiple commun de m et de n, donc un multiple de $\mathrm{ppcm}(m,n)$ (proposition 2.1.2 (v) et sa démonstration). Si $\mathrm{pgcd}(m,n) = 1$, alors $\mathrm{ppcm}(m,n) = mn$. ■

4.2 Comment choisir le module

C'est la compétence centrale. Voici le dictionnaire de référence.

Méthode 4.2.1 — Dictionnaire des modules

Ce que je vois dans l'énoncé	Modules à essayer
des carrés	$4,8,3,5,16$
des cubes	$9,7,13$
des puissances quatrièmes	$16,5$
x^n avec n fixé	p premier avec $n \mid p-1$
2^n, 3^n (exponentielles)	modules où l'ordre est petit
sommes de deux carrés	4 (un premier $\equiv 3 \pmod 4$ ne peut pas apparaître à une puissance impaire)
factorielles	p premier ($n! \equiv 0 \pmod p$ dès que $n \geq p$)
chiffres d'un nombre	$9,11,10^k$
équation $a^2+b^2=c^2$	$4,3,16$

Règle d'or : si l'énoncé contient x^k, cherchez un premier p tel que $k \mid p-1$; les puissances k-ièmes n'occuperont alors que $\frac{p-1}{k}+1$ classes modulo p, une petite fraction des p classes.

Exemple 4.2.2. *Montrer que $x^3+y^3 = 2003$ n'a pas de solution entière.*

Travaillons modulo 9 : les cubes valent $0,1,-1$. Donc $x^3+y^3 \in \{-2,-1,0,1,2\} \pmod 9$. Or $2003 = 9 \cdot 222 + 5$, donc $2003 \equiv 5 \equiv -4 \pmod 9$: impossible.

Exemple 4.2.3. *Montrer que n^2+n+1 n'est jamais divisible par 5.*

Modulo 5, n prend les valeurs $0,1,2,3,4$ et n^2+n+1 vaut respectivement $1,3,2,3,1$: jamais 0.

4.3 Critères de divisibilité

Proposition 4.3.1 (Critères de divisibilité)

Soit $n = \overline{a_k a_{k-1} \cdots a_1 a_0}$ l'écriture décimale de n.

- $9 \mid n \Leftrightarrow 9 \mid \sum a_i$ (et de même pour 3), car $10 \equiv 1 \pmod 9$.
- $11 \mid n \Leftrightarrow 11 \mid \sum (-1)^i a_i$, car $10 \equiv -1 \pmod{11}$.
- $2^k \mid n \Leftrightarrow 2^k$ divise le nombre formé des k derniers chiffres (idem pour 5^k).
- $7,11,13 \mid n$: regrouper par tranches de 3 chiffres avec signes alternés, car $10^3 \equiv -1 \pmod{1001}$ et $1001 = 7 \cdot 11 \cdot 13$.

Démonstration. On a $n = \sum_{i=0}^{k} a_i \, 10^i$. Par la proposition 4.1.2, on peut remplacer 10 par tout entier qui lui est congru.

- Modulo 9 (et 3) : $10 \equiv 1$, donc $n \equiv \sum a_i$.
- Modulo 11 : $10 \equiv -1$, donc $n \equiv \sum (-1)^i a_i$.
- Modulo 2^k : pour $i \geq k$, $2^k \mid 10^i$, donc $n \equiv \sum_{i<k} a_i \, 10^i$, qui est le nombre formé des k derniers chiffres. Même argument avec 5^k.
- Modulo 1001 : écrivons $n = \sum_j t_j \, 1000^j$ où les t_j sont les tranches de trois chiffres ; comme $1000 \equiv -1 \pmod{1001}$, $n \equiv \sum_j (-1)^j \, t_j \pmod{1001}$, et cette congruence reste vraie modulo chacun des diviseurs 7, 11, 13 de 1001. ■

Exemple 4.3.2. *Déterminer tous les chiffres a et b tels que $\overline{62a6b}$ soit divisible par 99.*

$99 = 9 \times 11$ avec $\gcd(9,11) = 1$: il faut et il suffit que le nombre soit divisible par 9 et par 11.

Modulo 9 (somme des chiffres) : $6+2+a+6+b = 14+a+b \equiv 0$, donc $a+b \equiv 4 \pmod 9$, soit $a+b \in \{4,13\}$.

Modulo 11 (somme alternée à partir des unités) : $b-6+a-2+6 = a+b-2 \equiv 0 \pmod{11}$, soit $a+b \in \{2,13\}$.

L'unique valeur commune est $a+b = 13$, et réciproquement toute paire de chiffres de somme 13 convient :

$$(a,b) \in \{(4,9),(5,8),(6,7),(7,6),(8,5),(9,4)\}.$$

Vérification : $62469 = 99 \times 631$ ✓.

4.4 Le théorème de Wilson

Théorème 4.4.1 (Wilson)

Soit $p \geq 2$. Alors

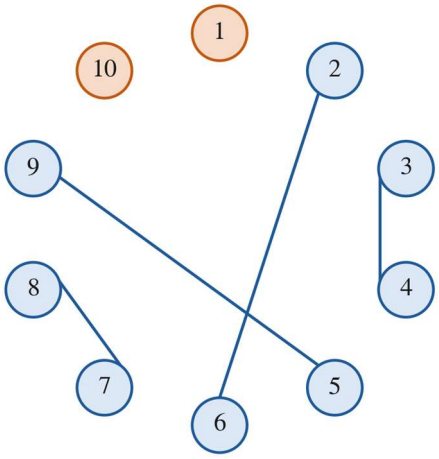
$$(p-1)! \equiv -1 \pmod p \Leftrightarrow p \text{ est premier.}$$

Démonstration. *Sens direct.* Soit p premier. Pour chaque $a \in \{1, \ldots, p-1\}$, il existe un unique a^{-1} dans cet ensemble avec $a a^{-1} \equiv 1$ (voir chapitre 5, ou Bézout). Les éléments qui sont leur propre

inverse vérifient $a^2 \equiv 1$, soit $p \mid (a-1)(a+1)$, soit $a \equiv \pm 1$: ce sont 1 et $p-1$. Les autres se regroupent par paires $\{a, a^{-1}\}$ de produit 1. Donc

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

Réciproque. Si p est composé, $p = ab$ avec $1 < a < p$. Alors a apparaît dans $(p-1)!$, donc $a \mid (p-1)!$; si l'on avait $(p-1)! \equiv -1 \pmod{p}$, alors $a \mid (p-1)! + 1$, donc $a \mid 1$: absurde. (Le cas $p = 4$ se vérifie aussi à la main : $3! = 6 \equiv 2 \pmod{4}$.) ■



Démonstration de Wilson pour p = 11 : chaque élément de {2, …, 9} est relié à son inverse modulo 11 ; seuls 1 et 10 sont leurs propres inverses.

Proposition 4.4.2 (−1 est un carré modulo p ≡ 1 (mod 4))

Si $p \equiv 1 \pmod{4}$ est premier, alors $x = \left(\frac{p-1}{2}\right)!$ vérifie $x^2 \equiv -1 \pmod{p}$. Autrement dit, -1 est un carré modulo p.

Démonstration.

$$(p-1)! = \prod_{k=1}^{(p-1)/2} k \cdot \prod_{k=1}^{(p-1)/2} (p-k) \equiv \prod_{k=1}^{(p-1)/2} k \cdot \prod_{k=1}^{(p-1)/2} (-k) = (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}.$$

Si $p \equiv 1 \pmod{4}$, $(-1)^{(p-1)/2} = 1$, et Wilson donne $x^2 \equiv -1$. ■

Exemple 4.4.3. *Montrer qu'il existe une infinité de premiers* $\equiv 1 \pmod{4}$.

Supposons-en un nombre fini $p_1, \ldots, p_k$ et posons $N = (2p_1 \cdots p_k)^2 + 1$. Soit q un facteur premier de N ; q est impair. Alors $x^2 \equiv -1 \pmod{q}$ avec $x = 2p_1 \cdots p_k$. Donc $x^4 \equiv 1$ et $\mathrm{ord}_q(x) = 4$, ce qui impose $4 \mid q-1$ par le petit théorème de Fermat et la proposition 7.1.2 (l'ordre divise $q-1$), soit $q \equiv 1 \pmod{4}$. Mais $q \neq p_i$ car $q \mid N$ et $p_i \mid N - 1$. Absurde.

4.5 Systèmes de résidus

Définition 4.5.1 (Systèmes de résidus)

Un système complet de résidus modulo n est un ensemble de n entiers deux à deux non congrus modulo n (par exemple $\{0,1,\dots,n-1\}$). Un système réduit est un ensemble de $\varphi(n)$ entiers premiers avec n, deux à deux non congrus.

Proposition 4.5.2 (Image affine d'un système complet)

Si $\{r_1,\dots,r_n\}$ est un système complet modulo n et $\gcd(a,n)=1$, alors $\{ar_1+b,\dots,ar_n+b\}$ en est un aussi, pour tout b.

Démonstration. Si $ar_i+b\equiv ar_j+b$, alors $a(r_i-r_j)\equiv 0$, et comme $\gcd(a,n)=1$ on simplifie : $r_i\equiv r_j$, donc $i=j$. On a n éléments deux à deux distincts modulo n. ∎

Exemple 4.5.3. *Soit p premier impair. Calculer $\sum_{k=1}^{p-1} k^m \bmod p$ selon les valeurs de $m\geq 1$.*

Si $(p-1)\mid m$, chaque $k^m\equiv 1$ par Fermat, donc la somme vaut $p-1\equiv -1 \pmod p$.

Sinon, soit g une racine primitive modulo p (chapitre 7) ; alors $\{1,g,\dots,g^{p-2}\}$ est un système réduit et

$$S=\sum_{k=1}^{p-1}k^m\equiv\sum_{j=0}^{p-2}g^{jm}\pmod p,\qquad \text{donc}\qquad (g^m-1)S\equiv\sum_{j=0}^{p-2}\left(g^{(j+1)m}-g^{jm}\right)=g^{m(p-1)}-1\equiv 0\pmod p.$$

Comme $g^m\not\equiv 1$ (car $(p-1)\nmid m$ et g est d'ordre $p-1$), l'entier g^m-1 est inversible modulo p, et l'on peut simplifier : $S\equiv 0\pmod p$.

4.6 Exercices

Exercice 4.1 ★. Quel est le dernier chiffre de 2026^{2026} ? Et les deux derniers ?

Exercice 4.2 ★. Montrer que $7\mid 3^{2n+1}+2^{n+2}$ pour tout $n\geq 0$.

Exercice 4.3 ★★. Montrer que $x^2+y^2+z^2\equiv 7\pmod 8$ est impossible ; en déduire que $7\cdot 4^k$ n'est jamais somme de trois carrés.

Exercice 4.4 ★★. Trouver tous les premiers p tels que $p\mid 2^p+1$.

Exercice 4.5 ★★. Montrer que si $p>3$ est premier, alors $24\mid p^2-1$.

Exercice 4.6 ★★★ (IMO 1990, problème 3). Trouver tous les entiers $n\geq 1$ tels que $n^2\mid 2^n+1$.

Exercice 4.7 ★★★. Soit p premier. Montrer que $\binom{2p}{p}\equiv 2\pmod p$ et, plus généralement, que $\binom{ap}{bp}\equiv\binom{a}{b}\pmod p$ (cas particulier du théorème de Lucas).

4.7 Corrigés

Solution de l'exercice 4.1. $2026\equiv 6\pmod{10}$, et $6^k\equiv 6\pmod{10}$ pour tout $k\geq 1$. Le dernier chiffre est 6.

Modulo 100 : $2026 \equiv 26$. On calcule $26^2 = 676 \equiv 76$, $26^3 \equiv 76 \cdot 26 = 1976 \equiv 76$. Donc $26^k \equiv 76 \pmod{100}$ pour $k \geq 2$. Les deux derniers chiffres sont 76.

Solution de l'exercice 4.2. $3^{2n+1} = 3 \cdot 9^n \equiv 3 \cdot 2^n \pmod 7$, et $2^{n+2} = 4 \cdot 2^n$. Donc la somme est congrue à $7 \cdot 2^n \equiv 0 \pmod 7$.

Solution de l'exercice 4.3. Modulo 8, un carré vaut 0, 1 ou 4. Les sommes de trois tels éléments sont $0,1,2,3,4,5,6,8,9,12$, soit, modulo 8, $\{0,1,2,3,4,5,6\}$: jamais 7.

Pour $7 \cdot 4^k$: par récurrence sur k. Si $x^2 + y^2 + z^2 = 7 \cdot 4^k$ avec $k \geq 1$, le membre de droite est $\equiv 0 \pmod 4$, ce qui force x, y, z tous pairs (les carrés valent 0 ou 1 modulo 4 : la seule façon d'avoir une somme $\equiv 0$ est $0+0+0$). En divisant par 4, on obtient une représentation de $7 \cdot 4^{k-1}$, et par descente on arrive à 7, impossible d'après ce qui précède.

Solution de l'exercice 4.4. $p = 3$ convient ($3 \mid 9$). Pour $p \neq 3$: par Fermat, $2^p \equiv 2 \pmod p$, donc $2^p + 1 \equiv 3 \pmod p$. Ainsi $p \mid 3$, donc $p = 3$: contradiction. (Le cas $p = 2$: $2 \nmid 5$.) Réponse : $p = 3$.

Solution de l'exercice 4.5. p est impair, donc $p = 2k+1$ et $p^2 - 1 = 4k(k+1)$, produit où $k(k+1)$ est pair : $8 \mid p^2 - 1$. De plus, p n'est pas divisible par 3, donc $p \equiv \pm 1 \pmod 3$ et $p^2 \equiv 1$, soit $3 \mid p^2 - 1$. Comme $\gcd(3,8) = 1$, $24 \mid p^2 - 1$.

Solution de l'exercice 4.6. Réponse : $n = 1$ et $n = 3$.

$n = 1$ convient. Supposons $n > 1$. Comme $n^2 \mid 2^n + 1$, n est impair. Soit p le plus petit facteur premier de n et $d = \mathrm{ord}_p(2)$. De $2^n \equiv -1 \pmod p$, on tire $2^{2n} \equiv 1$, donc $d \mid 2n$ et $d \nmid n$. Donc $v_2(d) = 1$, disons $d = 2e$ avec $e \mid n$. Par Fermat, $d \mid p-1$, donc $e \mid \gcd\left(n, \frac{p-1}{2}\right)$. Tout facteur premier de $\gcd(n, p-1)$ est $< p$ et divise n : impossible, sauf si ce PGCD vaut 1. Donc $\gcd(n, p-1) = 1$, d'où $e = 1$ et $d = 2$: $p \mid 2^2 - 1 = 3$, donc $p = 3$.

Écrivons $n = 3^k m$, $3 \nmid m$, $k \geq 1$. Le lemme LTE donne

$$v_3(2^n + 1) = v_3(2 + 1) + v_3(n) = 1 + k.$$

La condition $n^2 \mid 2^n + 1$ impose $2k = v_3(n^2) \leq 1 + k$, donc $k \leq 1$, soit $k = 1$.

Si $m > 1$, soit q son plus petit facteur premier ($q > 3$). Le même argument qu'au début, appliqué à q, donne $\mathrm{ord}_q(2) \mid \gcd(2n, q-1)$; les facteurs premiers de $\gcd(n, q-1)$ divisent n et sont $< q$, donc valent 3. Ainsi $\mathrm{ord}_q(2) \mid 6$, d'où $q \mid 2^6 - 1 = 63 = 3^2 \cdot 7$, soit $q = 7$. Mais $7 \mid n$ exigerait $2^n \equiv -1 \pmod 7$, or les puissances de 2 modulo 7 sont $\{1,2,4\}$ et $-1 \equiv 6$ n'y figure pas. Contradiction. Donc $m = 1$ et $n = 3$.

Vérification : $9 \mid 2^3 + 1 = 9$ ✓.

Solution de l'exercice 4.7. Dans $\mathbb{F}_p[X]$, $(1+X)^p = 1 + X^p$, car $p \mid \binom{p}{k}$ pour $1 \leq k \leq p-1$ (en effet $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$ et $p \nmid k$). Donc

$$(1+X)^{ap} = ((1+X)^p)^a \equiv (1+X^p)^a = \sum_b \binom{a}{b} X^{bp} \pmod p.$$

En comparant les coefficients de X^{bp} des deux côtés : $\binom{ap}{bp} \equiv \binom{a}{b} \pmod p$. Avec $a = 2$, $b = 1$: $\binom{2p}{p} \equiv 2 \pmod p$.

PARTIE II — Les classiques de l'arsenal olympique

CHAPITRE 5

5 Inverses modulaires, équations linéaires et théorème des restes chinois

Objectifs du chapitre.

- Définir et calculer l'inverse d'un entier modulo n.
- Résoudre $ax \equiv b \pmod{n}$ dans tous les cas.
- Énoncer, démontrer et surtout utiliser le théorème des restes chinois.
- Comprendre l'isomorphisme $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (pour $\gcd(m,n) = 1$) et son rôle dans les problèmes de construction.

5.1 Inverse modulaire

Définition 5.1.1 (Inverse modulaire)

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Un entier b est un inverse de a modulo n si $ab \equiv 1 \pmod{n}$. On le note alors a^{-1}.

Théorème 5.1.2 (Existence et unicité de l'inverse)

a possède un inverse modulo n si, et seulement si, $\gcd(a,n) = 1$. Cet inverse est alors unique modulo n.

Démonstration. Si $ab \equiv 1 \pmod{n}$, alors $ab - 1 = kn$, donc $ab - kn = 1$ et tout diviseur commun de a et n divise 1. Réciproquement, si $\gcd(a,n) = 1$, Bézout donne $au + nv = 1$, donc $au \equiv 1 \pmod{n}$ et $b = u$ convient.

Unicité : si $ab \equiv ab' \equiv 1$, alors $b \equiv b(ab') = (ba)b' \equiv b' \pmod{n}$. ∎

Définition 5.1.3 (Groupe des inversibles)

On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des classes inversibles modulo n. C'est un groupe pour la multiplication, de cardinal $\varphi(n)$ (indicatrice d'Euler, chapitre 6).

Méthode 5.1.4 — Calculer un inverse

Trois techniques, par ordre de rapidité en concours :

1. **À vue** : chercher k tel que $ak \equiv 1$ en testant lequel des nombres $1 + n, 1 + 2n, \ldots$ est divisible par a. Ex. : inverse de 7 modulo 31 : $1 + 31 = 32$, $1 + 62 = 63 = 7 \cdot 9$, donc $7^{-1} \equiv 9$.
2. **Euclide étendu** : dérouler l'algorithme d'Euclide puis remonter.
3. **Fermat** : si $n = p$ est premier et $p \nmid a$, $a^{-1} \equiv a^{p-2} \pmod{p}$.

Exemple 5.1.5. *Calculer l'inverse de* 17 *modulo* 101.

Euclide : $101 = 5 \cdot 17 + 16$, $17 = 1 \cdot 16 + 1$. On remonte :

$$1 = 17 - 16 = 17 - (101 - 5 \cdot 17) = 6 \cdot 17 - 101.$$

Donc $17^{-1} \equiv 6 \pmod{101}$. Vérification : $17 \cdot 6 = 102 \equiv 1$.

5.2 Équations linéaires modulaires

Théorème 5.2.1 (Équation linéaire modulaire)

Soit l'équation $ax \equiv b \pmod{n}$ et $d = \gcd(a, n)$.

- Si $d \nmid b$, il n'y a aucune solution.
- Si $d \mid b$, il y a exactement d solutions modulo n, formant une classe modulo n/d :

$$x \equiv \left(\frac{a}{d}\right)^{-1} \frac{b}{d} \pmod{\frac{n}{d}}.$$

Démonstration. $ax \equiv b \pmod{n}$ équivaut à l'existence de y avec $ax + ny = b$. Par Bézout, l'ensemble $\{ax + ny\}$ est l'ensemble des multiples de d : d'où la condition $d \mid b$. Si elle est vérifiée, en divisant par d on obtient $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ avec $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, donc une unique solution modulo n/d, qui se relève en d classes modulo n. ■

Exemple 5.2.2. *Résoudre* $12x \equiv 30 \pmod{42}$.

$d = \gcd(12,42) = 6$ et $6 \mid 30$: il y a 6 solutions. On simplifie : $2x \equiv 5 \pmod{7}$, donc $x \equiv 5 \cdot 2^{-1} \equiv 5 \cdot 4 = 20 \equiv 6 \pmod{7}$. Les solutions modulo 42 sont $x \in \{6,13,20,27,34,41\}$.

5.3 Le théorème des restes chinois

Théorème 5.3.1 (Théorème des restes chinois)

Soient $n_1, \ldots, n_k$ des entiers deux à deux premiers entre eux et $a_1, \ldots, a_k$ des entiers quelconques. Alors le système

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

admet une solution, unique modulo $N = n_1 n_2 \cdots n_k$.

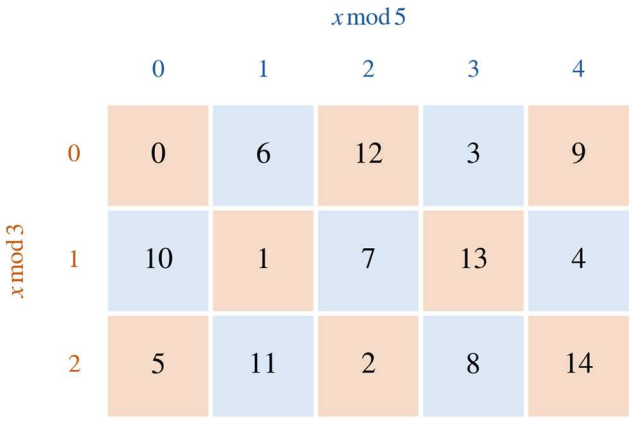
Démonstration. *Unicité.* Si x, x' sont deux solutions, $n_i \mid x - x'$ pour tout i. Les n_i étant deux à deux premiers entre eux, n_k est premier avec $n_1 \cdots n_{k-1}$ (corollaire 2.3.4 (ii), appliqué de proche en proche), et le corollaire 2.3.4 (i) donne, par récurrence sur k, $N \mid x - x'$.

Existence (constructive). Posons $N_i = N/n_i$. Comme $\gcd(N_i, n_i) = 1$, il existe M_i avec $N_i M_i \equiv 1 \pmod{n_i}$. Alors

$$x = \sum_{i=1}^{k} a_i N_i M_i$$

convient : modulo n_j, tous les termes $i \neq j$ s'annulent (car $n_j \mid N_i$) et il reste $a_j N_j M_j \equiv a_j$.

Existence (par comptage). L'application $\mathbb{Z}/N\mathbb{Z} \to \prod_i \mathbb{Z}/n_i\mathbb{Z}$, $x \mapsto (x \bmod n_i)_i$, est bien définie et injective d'après l'unicité ; les deux ensembles ayant N éléments, elle est bijective. C'est même un isomorphisme d'anneaux. ■



Le théorème des restes chinois pour 15 = 3 × 5 : chaque entier de 0 à 14 occupe une case différente du tableau (reste modulo 3, reste modulo 5), et toutes les cases sont remplies.

Exemple 5.3.2. *Résoudre* $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

$N = 105$. On peut procéder par substitutions successives, souvent plus rapides : $x \equiv 2 \pmod 3$ et $x \equiv 2 \pmod 7$ donnent $x \equiv 2 \pmod{21}$. Écrivons $x = 21t + 2$; la troisième condition devient $21t + 2 \equiv 3 \pmod 5$, soit $t \equiv 1 \pmod 5$. Donc $t = 5s + 1$ et $x = 105s + 23$:

$$x \equiv 23 \pmod{105}.$$

À retenir (Ce que le TRC signifie vraiment)

Le TRC dit qu'on peut prescrire indépendamment le comportement modulo chaque puissance de premier. En pratique, il sert surtout à construire des objets : « il existe n tel que… ». Chaque contrainte est traduite en une congruence modulo un premier (ou une puissance de premier) différent, puis le TRC les recolle.

Exemple 5.3.3. *Montrer qu'il existe* 2026 *entiers consécutifs dont aucun n'est sans facteur carré (c'est-à-dire : chacun est divisible par le carré d'un premier).*

Choisissons 2026 nombres premiers distincts $p_1, \dots, p_{2026}$. Les modules p_i^2 sont deux à deux premiers entre eux. Par le TRC, le système

$$n \equiv -i \pmod{p_i^2}, \qquad i = 1, \dots, 2026$$

possède une solution n. Alors $p_i^2 \mid n + i$ pour tout i, donc les entiers $n + 1, \dots, n + 2026$ conviennent (quitte à prendre n assez grand en ajoutant un multiple du produit).

Exemple 5.3.4 (Trois entiers consécutifs divisibles par des carrés). *Montrer qu'il existe une infinité d'entiers* n *tels que* n, $n + 1$, $n + 2$ *soient chacun divisibles par le carré d'un nombre premier.*

Le système $n \equiv 0 \pmod 4$, $n \equiv -1 \pmod 9$, $n \equiv -2 \pmod{25}$ admet des solutions formant une classe modulo 900 : par exemple $n = 548$ ($548 = 4 \cdot 137$, $549 = 9 \cdot 61$, $550 = 25 \cdot 22$). Tous les $n \equiv 548 \pmod{900}$ conviennent.

Méthode 5.3.5 — Reconnaître un problème de TRC

Signaux d'alerte :

- l'énoncé demande de prouver l'existence d'un entier vérifiant plusieurs conditions de divisibilité ;

- l'énoncé parle de k entiers consécutifs ayant chacun une propriété ;
- une fonction multiplicative doit prendre une valeur prescrite ;
- on veut fabriquer un contre-exemple « sur mesure ».

5.4 Application : structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

Théorème 5.4.1 (Structure du groupe des inversibles)

Si $\gcd(m,n)=1$, l'isomorphisme du TRC induit un isomorphisme de groupes

$$(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

En particulier, $\varphi(mn)=\varphi(m)\varphi(n)$.

Démonstration. x est inversible modulo mn si, et seulement si, $\gcd(x,mn)=1$, si, et seulement si, $\gcd(x,m)=1$ et $\gcd(x,n)=1$. L'isomorphisme d'anneaux du TRC respecte la multiplication et envoie 1 sur $(1,1)$; une classe x est donc inversible modulo mn (il existe y avec $xy\equiv 1$) si, et seulement si, son image $(x \bmod m, x \bmod n)$ est inversible composante par composante. La bijection se restreint donc en une bijection entre les inversibles, compatible avec la multiplication. En comptant les éléments, $\varphi(mn)=\varphi(m)\varphi(n)$. ■

5.5 Exercices

Exercice 5.1 ★. Résoudre $7x \equiv 3 \pmod{25}$ et $15x \equiv 9 \pmod{24}$.

Exercice 5.2 ★. Trouver le plus petit entier positif laissant les restes $1,2,3$ dans les divisions par $3,5,7$ respectivement.

Exercice 5.3 ★★. Montrer que pour tout $k \geq 1$, il existe k entiers consécutifs dont aucun n'est une puissance parfaite (c'est-à-dire de la forme m^t, $t \geq 2$).

Exercice 5.4 ★★. Soit $n \geq 1$. Montrer qu'il existe n entiers consécutifs dont chacun possède au moins 2026 diviseurs premiers distincts.

Exercice 5.5 ★★★ (IMO 1989, problème 5). Montrer que pour tout $n \geq 1$, il existe n entiers consécutifs dont aucun n'est une puissance d'un nombre premier.

Exercice 5.6 ★★★. Soit $P \in \mathbb{Z}[X]$ non constant. Montrer que l'ensemble des nombres premiers p divisant au moins un $P(n)$, $n \in \mathbb{Z}$, est infini.

5.6 Corrigés

Solution de l'exercice 5.1. $\gcd(7,25)=1$; $7\cdot 18 = 126 = 5\cdot 25+1$, donc $7^{-1}\equiv 18$ et $x \equiv 18\cdot 3 = 54 \equiv 4 \pmod{25}$.

$\gcd(15,24)=3$ et $3 \mid 9$: trois solutions. On simplifie : $5x \equiv 3 \pmod 8$, $5^{-1}\equiv 5$ (car $25\equiv 1$), donc $x \equiv 15 \equiv 7 \pmod 8$. Modulo 24 : $x \in \{7,15,23\}$.

Solution de l'exercice 5.2. Remarquons que $x\equiv 1 \pmod 3$, $x\equiv 2 \pmod 5$, $x\equiv 3 \pmod 7$ signifie $x+2\equiv 0 \pmod 3$, $x+3\equiv 0 \pmod 5$, $x+4\equiv 0 \pmod 7$: pas de motif commun. Procédons : $x\equiv 1 \pmod 3$ et $x\equiv 2 \pmod 5$ donnent $x\equiv 7 \pmod{15}$. Puis $x = 15t+7 \equiv 3 \pmod 7$: $15t \equiv 3-7 =$

$-4 \equiv 3 \pmod 7$, soit $t \equiv 3 \pmod 7$ (car $15 \equiv 1$). Donc $t = 7s + 3$ et $x = 105s + 52$. Le plus petit est $x = 52$.

Solution de l'exercice 5.3. Prenons k premiers distincts $p_1, \dots, p_k$ et imposons $n + i \equiv p_i \pmod{p_i^2}$, c'est-à-dire $v_{p_i}(n+i) = 1$ exactement. Un tel entier n'est pas une puissance parfaite : si $n + i = m^t$ avec $t \geq 2$, alors $v_{p_i}(n+i)$ serait multiple de $t \geq 2$, or il vaut 1. Le TRC (modules p_i^2 premiers entre eux) fournit n.

Solution de l'exercice 5.4. Choisissons $2026n$ premiers distincts $p_{i,j}$ $(1 \leq i \leq n,\ 1 \leq j \leq 2026)$ et imposons $N + i \equiv 0 \pmod{p_{i,1}p_{i,2}\cdots p_{i,2026}}$. Les n modules sont deux à deux premiers entre eux ; le TRC conclut : les entiers $N+1, \dots, N+n$ conviennent.

Solution de l'exercice 5.5. Prenons $2n$ premiers distincts $p_1, q_1, \dots, p_n, q_n$ et imposons

$$N + i \equiv 0 \pmod{p_i q_i}, \qquad i = 1, \dots, n.$$

Les modules $p_i q_i$ sont deux à deux premiers entre eux : le TRC donne N (que l'on choisit assez grand). Chaque $N + i$ est divisible par deux premiers distincts, donc n'est pas une puissance d'un nombre premier.

> **Remarque.**
> Ce problème d'IMO se résout donc en trois lignes, une fois identifié le « signal TRC » : n entiers consécutifs.

Solution de l'exercice 5.6. Écrivons $P(X) = a_0 + a_1 X + \cdots + a_d X^d$. Si $a_0 = 0$, tout premier p divise $P(p)$: c'est terminé. Supposons $a_0 \neq 0$ et supposons par l'absurde que seuls $p_1, \dots, p_k$ divisent des valeurs de P. Considérons

$$P(a_0 p_1 \cdots p_k t) = a_0 \Bigg(\underbrace{1 + a_1 p_1 \cdots p_k t + \cdots}_{\text{multiple de } p_1 \cdots p_k} \Bigg) = a_0 (1 + m p_1 \cdots p_k)$$

pour un entier m dépendant de t. Pour t assez grand, $|1 + m p_1 \cdots p_k| > 1$, donc ce facteur possède un diviseur premier q ; or $q \neq p_i$ pour tout i (car $1 + m p_1 \cdots p_k \equiv 1 \pmod{p_i}$). Ce q divise $P(a_0 p_1 \cdots p_k t)$ et n'est aucun des p_i : contradiction.

CHAPITRE 6

6 Les théorèmes de Fermat et d'Euler

Objectifs du chapitre.

- Calculer l'indicatrice d'Euler $\varphi(n)$ et connaître ses propriétés.
- Démontrer le petit théorème de Fermat de trois façons différentes.
- Démontrer le théorème d'Euler et savoir l'appliquer aux tours de puissances.
- Connaître les limites de ces théorèmes (nombres de Carmichael).

6.1 L'indicatrice d'Euler

Définition 6.1.1 (Indicatrice d'Euler)

Pour $n \geq 1$, $\varphi(n)$ est le nombre d'entiers $k \in \{1, \dots, n\}$ tels que $\gcd(k, n) = 1$. Autrement dit, $\varphi(n) = \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^\times)$.

Théorème 6.1.2 (Calcul de l'indicatrice)

φ est multiplicative : $\varphi(mn) = \varphi(m)\varphi(n)$ si $\gcd(m, n) = 1$. De plus, $\varphi(p^k) = p^k - p^{k-1}$, donc si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$,

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1).$$

Démonstration. La multiplicativité découle du TRC (théorème 5.4.1). Pour $\varphi(p^k)$: parmi $1, \dots, p^k$, les entiers non premiers avec p^k sont exactement les multiples de p, au nombre de p^{k-1}. ■

Proposition 6.1.3 (Identité de Gauss)

Pour tout $n \geq 1$:

$$\sum_{d \mid n} \varphi(d) = n.$$

Démonstration. Classons les entiers de $\{1, \dots, n\}$ selon $d = \gcd(k, n)$. Le nombre de k tels que $\gcd(k, n) = d$ est le nombre de $k' = k/d \in \{1, \dots, n/d\}$ avec $\gcd(k', n/d) = 1$, soit $\varphi(n/d)$. Donc $n = \sum_{d \mid n} \varphi(n/d) = \sum_{d \mid n} \varphi(d)$. ■

Exemple 6.1.4. *Calculer* $\varphi(2026)$.

$2026 = 2 \times 1013$, et 1013 est premier (il n'est divisible par aucun premier ≤ 31, et $32^2 > 1013$). Donc $\varphi(2026) = 1 \cdot 1012 = 1012$.

6.2 Petit théorème de Fermat

Théorème 6.2.1 (Petit théorème de Fermat)

Soit p premier. Pour tout $a \in \mathbb{Z}$:

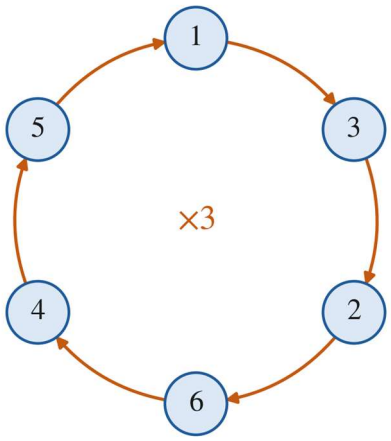
$$a^p \equiv a \pmod{p}.$$

Si de plus $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod{p}$.

Démonstration 1 (par les systèmes de résidus). Supposons $p \nmid a$. Les entiers $a, 2a, \dots, (p-1)a$ sont deux à deux non congrus modulo p (on peut simplifier par a) et aucun n'est $\equiv 0$. Ils forment donc une permutation de $1, 2, \dots, p-1$ modulo p. En multipliant :

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

Comme $\gcd\big((p-1)!, p\big) = 1$, on simplifie : $a^{p-1} \equiv 1$. ■



$$(3 \cdot 1)(3 \cdot 2)\cdots(3 \cdot 6) \equiv 1 \cdot 2 \cdots 6 \pmod{7}$$

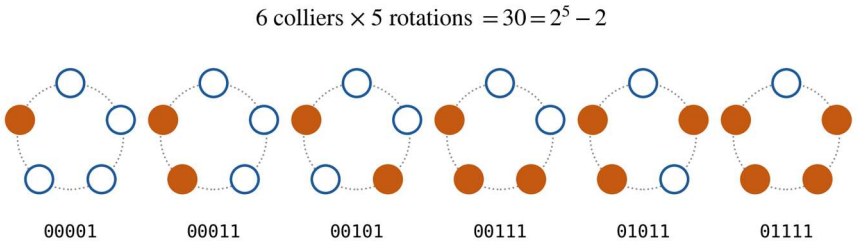
Multiplier par a = 3 permute les résidus non nuls modulo 7 : 1→3→2→6→4→5→1. Le produit des images est donc égal au produit des résidus.

Démonstration 2 (par récurrence et le binôme). Montrons $a^p \equiv a$ par récurrence sur $a \geq 0$. C'est vrai pour $a = 0$. Si c'est vrai pour a :

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1 \equiv a + 1 \pmod{p},$$

car $p \mid \binom{p}{k}$ pour $1 \leq k \leq p-1$: en effet $k\binom{p}{k} = p\binom{p-1}{k-1}$, donc $p \mid k\binom{p}{k}$, et comme $\gcd(p,k) = 1$, le lemme de Gauss donne $p \mid \binom{p}{k}$. Le cas $a < 0$ s'en déduit, puisque $a^p \bmod p$ ne dépend que de $a \bmod p$. ■

Démonstration 3 (combinatoire : colliers). Considérons les a^p mots de longueur p sur un alphabet de a couleurs, et la rotation ρ qui décale un mot d'un cran. Deux mots sont équivalents s'ils se déduisent l'un de l'autre par une puissance de ρ (même « collier »). Si un mot w vérifie $\rho^k(w) = w$ pour un k avec $0 < k < p$, alors, k étant inversible modulo p, il existe u avec $ku \equiv 1 \pmod{p}$, et $\rho(w) = \rho^{ku}(w) = w$: toutes les lettres sont égales. Les mots non monochromes ont donc p images distinctes $w, \rho(w), \dots, \rho^{p-1}(w)$ (si $\rho^i(w) = \rho^j(w)$ avec $i < j$, alors $\rho^{j-i}(w) = w$). Ils se répartissent en classes de p éléments exactement, et leur nombre $a^p - a$ est divisible par p. ■



Démonstration de Fermat par les colliers, pour p = 5 et a = 2 couleurs : les $2^5 - 2 = 30$ mots non monochromes se regroupent en 6 colliers de 5 rotations chacun.

Théorème 6.2.2 (Théorème d'Euler)

Si $\text{pgcd}(a, n) = 1$, alors

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

Démonstration. Soit $\{r_1, \ldots, r_{\varphi(n)}\}$ un système réduit de résidus modulo n. Comme $\text{pgcd}(a, n) = 1$, les ar_i forment encore un système réduit : ils sont premiers avec n et deux à deux non congrus. Donc

$$\prod_i (ar_i) \equiv \prod_i r_i \pmod{n} \Longrightarrow a^{\varphi(n)} \prod_i r_i \equiv \prod_i r_i \pmod{n}.$$

Le produit $\prod r_i$ est premier avec n : on peut simplifier. ■

À retenir (La règle des exposants)

Si $\text{pgcd}(a, n) = 1$, alors

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

Attention : cette réduction n'est valable que sous l'hypothèse de coprimalité. Sans elle, on décompose n en puissances de premiers et on utilise le TRC.

Exemple 6.2.3. *Calculer* $2^{2026^{2026}} \bmod 15$.

$\varphi(15) = 8$ et $\text{pgcd}(2,15) = 1$. Il faut donc $2026^{2026} \bmod 8$. Or $2026 \equiv 2 \pmod 8$ et $2026^{2026} = (2 \cdot 1013)^{2026} = 2^{2026} \cdot 1013^{2026} \equiv 0 \pmod 8$ (dès que l'exposant de 2 atteint 3). Donc

$$2^{2026^{2026}} \equiv 2^0 = 1 \pmod{15}.$$

Exemple 6.2.4. *Déterminer les trois derniers chiffres de* 7^{7^7}.

On veut $7^{7^7} \bmod 1000$. Comme $\text{pgcd}(7,1000) = 1$ et $\varphi(1000) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400$, il faut $7^7 \bmod 400$.

$\varphi(400) = 160$, et $7^7 \bmod 400$: $7^2 = 49$, $7^4 = 2401 \equiv 1 \pmod{400}$. Donc $7^7 = 7^4 \cdot 7^2 \cdot 7 \equiv 1 \cdot 49 \cdot 7 = 343 \pmod{400}$.

Reste à calculer $7^{343} \bmod 1000$. On a $7^4 \equiv 401 \pmod{1000}$, $7^{20} = (7^4)^5 \equiv 401^5$. Calculons $401^2 = 160801 \equiv 801$, $401^4 \equiv 801^2 = 641601 \equiv 601$, $401^5 \equiv 601 \cdot 401 = 241001 \equiv 1 \pmod{1000}$. Donc $7^{20} \equiv 1 \pmod{1000}$ et $343 = 17 \cdot 20 + 3$, d'où

$$7^{343} \equiv 7^3 = 343 \pmod{1000}.$$

Les trois derniers chiffres sont 343.

À retenir (Les nombres de Carmichael)

La réciproque de Fermat est fausse : il existe des entiers composés n tels que $a^{n-1} \equiv 1 \pmod{n}$ pour tout a premier avec n. Le plus petit est $561 = 3 \cdot 11 \cdot 17$. Ce sont les nombres de Carmichael ; le critère de Korselt (théorème 6.2.6 ci-dessous) les caractérise.

Exemple 6.2.5. *Vérifier le critère de Korselt pour* 561 *et montrer que* 561 *est de Carmichael.*

$561 = 3 \cdot 11 \cdot 17$, sans facteur carré. Et $560 = 2^4 \cdot 5 \cdot 7$ est divisible par $2 = 3-1$, $10 = 11-1$ et $16 = 17-1$. Si $\gcd(a, 561) = 1$, alors par Fermat $a^{560} = (a^2)^{280} \equiv 1 \pmod{3}$, $a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}$ et $a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}$. Par le TRC, $a^{560} \equiv 1 \pmod{561}$.

Théorème 6.2.6 (Critère de Korselt)

Un entier composé n vérifie $a^{n-1} \equiv 1 \pmod{n}$ pour tout a premier avec n si, et seulement si, n est sans facteur carré et $p-1 \mid n-1$ pour tout premier $p \mid n$.

Démonstration. *Condition suffisante.* C'est le raisonnement de l'exemple 6.2.5 : si $p \mid n$ et $\gcd(a, n) = 1$, alors $a^{p-1} \equiv 1 \pmod{p}$ et $p-1 \mid n-1$ donnent $a^{n-1} \equiv 1 \pmod{p}$; comme n est le produit de ses facteurs premiers distincts, deux à deux premiers entre eux, le TRC donne $a^{n-1} \equiv 1 \pmod{n}$.

Condition nécessaire. Supposons la propriété vraie. Si $p^2 \mid n$ pour un premier p, soit a un entier tel que $a \equiv 1 + p \pmod{p^2}$ et $a \equiv 1 \pmod{n'}$, où $n = p^{\alpha} n'$ avec $p \nmid n'$ (TRC) ; alors a est premier avec n. Par la formule du binôme, $(1+p)^{n-1} \equiv 1 + (n-1)p \pmod{p^2}$, donc $a^{n-1} \equiv 1 \pmod{p^2}$ impose $p \mid n-1$, ce qui contredit $p \mid n$. Donc n est sans facteur carré. Soit enfin $p \mid n$ et g une racine primitive modulo p (théorème 7.2.2) ; par le TRC, il existe $a \equiv g \pmod{p}$ et $a \equiv 1 \pmod{n/p}$, premier avec n. Alors $g^{n-1} \equiv a^{n-1} \equiv 1 \pmod{p}$, et comme g est d'ordre $p-1$, la proposition 7.1.2 donne $p-1 \mid n-1$. ■

6.3 Exercices

Exercice 6.1 ★. Calculer $\varphi(1000)$, $\varphi(210)$, $\varphi(p^2 q)$ pour p, q premiers distincts.

Exercice 6.2 ★. Quel est le reste de 3^{100} dans la division par 7 ? par 100 ?

Exercice 6.3 ★★. Montrer que $\varphi(n)$ est pair pour tout $n \geq 3$.

Exercice 6.4 ★★. Résoudre $\varphi(n) = 12$.

Exercice 6.5 ★★. Montrer que $n \mid \varphi(a^n - 1)$ pour tous $a, n \geq 2$.

Exercice 6.6 ★★★. Montrer que si $\varphi(n) \mid n-1$ et n est composé, alors n possède au moins trois facteurs premiers distincts. (Conjecture de Lehmer : un tel n n'existe pas ; elle est toujours ouverte.)

Exercice 6.7 ★★★ (IMO 2005, ISL). Soit $a > 1$ un entier. Montrer que l'ensemble des nombres premiers divisant au moins un terme de la suite $(a^n - 1)_{n \geq 1}$ est infini ; en déduire qu'une infinité de termes de cette suite possèdent un facteur premier ne divisant aucun terme précédent. (Version faible du théorème de Zsigmondy.)

6.4 Corrigés

Solution de l'exercice 6.1. $\varphi(1000) = \varphi(2^3)\varphi(5^3) = 4 \cdot 100 = 400$. $\varphi(210) = \varphi(2)\varphi(3)\varphi(5)\varphi(7) = 1 \cdot 2 \cdot 4 \cdot 6 = 48$. $\varphi(p^2q) = p(p-1)(q-1)$.

Solution de l'exercice 6.2. Modulo 7 : $\varphi(7) = 6$ et $100 = 16 \cdot 6 + 4$, donc $3^{100} \equiv 3^4 = 81 \equiv 4$.

Modulo 100 : $\varphi(100) = 40$ et $100 = 2 \cdot 40 + 20$, donc $3^{100} \equiv 3^{20}$. Or $3^4 = 81$, $3^5 = 243 \equiv 43$, $3^{10} \equiv 43^2 = 1849 \equiv 49$, $3^{20} \equiv 49^2 = 2401 \equiv 1$. Donc $3^{100} \equiv 1 \pmod{100}$.

Solution de l'exercice 6.3. Si n a un facteur premier impair p, alors $(p-1) \mid \varphi(n)$ et $p-1$ est pair. Sinon $n = 2^k$ avec $k \geq 2$ (car $n \geq 3$), et $\varphi(2^k) = 2^{k-1}$ est pair.

Autre preuve. Les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ se regroupent par paires $\{x, -x\}$, car $x \equiv -x$ imposerait $n \mid 2x$ avec $\gcd(x,n) = 1$, donc $n \mid 2$, ce qui est exclu pour $n \geq 3$.

Solution de l'exercice 6.4. Si $p^\alpha \parallel n$ avec p impair, alors $p^{\alpha-1}(p-1) \mid 12$, donc $p-1 \mid 12$ et $p \in \{3,5,7,13\}$. On énumère les n possibles :

$$n \in \{13,21,26,28,36,42\}.$$

Vérification : $\varphi(13) = 12$, $\varphi(21) = \varphi(3)\varphi(7) = 2 \cdot 6 = 12$, $\varphi(26) = 12$, $\varphi(28) = \varphi(4)\varphi(7) = 2 \cdot 6 = 12$, $\varphi(36) = \varphi(4)\varphi(9) = 2 \cdot 6 = 12$, $\varphi(42) = \varphi(2)\varphi(3)\varphi(7) = 12$.

Solution de l'exercice 6.5. Posons $m = a^n - 1$. Alors $\gcd(a,m) = 1$ et $a^n \equiv 1 \pmod{m}$. De plus, $\mathrm{ord}_m(a) = n$ exactement : si $a^k \equiv 1 \pmod{m}$ avec $0 < k < n$, alors $m \mid a^k - 1$, or $a^k - 1 < a^n - 1 = m$ et $a^k - 1 > 0$: impossible. Par Euler, $a^{\varphi(m)} \equiv 1 \pmod{m}$, donc $n = \mathrm{ord}_m(a) \mid \varphi(m)$ (proposition du chapitre 7).

Solution de l'exercice 6.6. n est impair : sinon $\varphi(n)$ est pair (car $n \geq 4$) et $n-1$ impair, donc $\varphi(n) \nmid n-1$.

n est sans facteur carré (en particulier, ce n'est pas une puissance de premier) : si $p^2 \mid n$, alors $p \mid \varphi(n)$ (car $\varphi(n)$ est divisible par $p^{v_p(n)-1}(p-1)$) et $p \mid n$, donc $p \nmid n-1$ et $\varphi(n) \nmid n-1$: contradiction.

n n'est pas produit de deux premiers distincts : si $n = pq$ avec $p < q$, alors $\varphi(n) = (p-1)(q-1) = n - p - q + 1$, donc $\varphi(n) \mid n-1$ donne $(p-1)(q-1) \mid p+q-2$. Or $(p-1)(q-1) > p+q-2$ dès que $p \geq 3$: en effet $(p-1)(q-1) - (p+q-2) = pq - 2p - 2q + 3 = (p-2)(q-2) - 1 > 0$ pour $p \geq 3$, $q \geq 5$. Contradiction.

Comme n est composé et sans facteur carré, il a au moins deux facteurs premiers distincts ; il en a donc au moins trois.

Solution de l'exercice 6.7. Supposons que l'ensemble S des premiers divisant un $a^n - 1$ soit fini, $S = \{p_1, \ldots, p_k\}$. Les p_i divisant a ne divisent jamais $a^n - 1$: on a donc $\gcd(a, p_i) = 1$ pour tout i. Soit N un entier tel que $a^N \equiv 1 \pmod{p_i^2}$ pour tout i (prendre $N = \varphi(p_1^2 \cdots p_k^2)$). Alors pour tout m, tous les facteurs premiers de $a^{mN} - 1$ sont dans S. Or, par le lemme LTE, $v_{p_i}(a^{mN} - 1) = v_{p_i}(a^N - 1) + v_{p_i}(m)$, donc

$$a^{mN} - 1 = \prod_i p_i^{v_{p_i}(a^N-1)+v_{p_i}(m)} \leq C \cdot m^k$$

pour une constante C, ce qui est incompatible avec la croissance exponentielle de a^{mN}. Contradiction : S est infini.

Enfin, chaque premier $p \in S$ divise un premier terme $a^{n_p} - 1$, et ne divise aucun terme précédent ; comme S est infini et qu'un terme n'a qu'un nombre fini de facteurs premiers, les indices n_p forment un ensemble infini, ce qui donne la seconde assertion.

CHAPITRE 7

7 Ordre multiplicatif et racines primitives

Objectifs du chapitre.

- Définir l'ordre multiplicatif et maîtriser sa propriété clé.
- Utiliser l'ordre pour contraindre les facteurs premiers de $a^n \pm 1$.
- Démontrer l'existence des racines primitives modulo p.
- Savoir compter les solutions de $x^k \equiv 1 \pmod{p}$.

7.1 L'ordre multiplicatif

Définition 7.1.1 (Ordre multiplicatif)

Soit $\gcd(a,n) = 1$. L'ordre de a modulo n, noté $\mathrm{ord}_n(a)$, est le plus petit entier $d \geq 1$ tel que $a^d \equiv 1 \pmod{n}$.

Il existe bien : par le théorème d'Euler, $a^{\varphi(n)} \equiv 1 \pmod{n}$, donc l'ensemble des exposants convenables est non vide.

Proposition 7.1.2 (Propriété fondamentale de l'ordre)

Soit $d = \mathrm{ord}_n(a)$. Alors pour tout $k \geq 0$:

$$a^k \equiv 1 \pmod{n} \Leftrightarrow d \mid k.$$

En particulier $d \mid \varphi(n)$, et $d \mid p-1$ si $n = p$ est premier.

Démonstration. ($\Leftarrow$) est clair. ($\Rightarrow$) Écrivons $k = dq + r$ avec $0 \leq r < d$. Alors $1 \equiv a^k = \left(a^d\right)^q a^r \equiv a^r \pmod{n}$. La minimalité de d force $r = 0$. ∎

Corollaire 7.1.3

Avec $d = \mathrm{ord}_n(a)$, pour tous entiers $i, j \geq 0$:

$$a^i \equiv a^j \pmod{n} \Leftrightarrow i \equiv j \pmod{d}.$$

Démonstration. Supposons $i \geq j$. Comme a est inversible modulo n, $a^i \equiv a^j$ équivaut (en multipliant par l'inverse de a^j) à $a^{i-j} \equiv 1$, c'est-à-dire, par la proposition 7.1.2, à $d \mid i-j$. ∎

Lemme (Ordre d'une puissance)

Si $\mathrm{ord}_n(a) = d$, alors pour tout $i \geq 1$, $\mathrm{ord}_n\left(a^i\right) = \dfrac{d}{\gcd(i,d)}$. En particulier a^i est d'ordre d si, et seulement si, $\gcd(i,d) = 1$.

Démonstration. Posons $e = \gcd(i,d)$, $i = ei'$, $d = ed'$ avec $\gcd(i',d') = 1$. Par la proposition 7.1.2, $\left(a^i\right)^k \equiv 1$ équivaut à $d \mid ik$, soit $ed' \mid ei'k$, soit $d' \mid i'k$, soit (Gauss) $d' \mid k$. Le plus petit $k \geq 1$ convenable est $d' = \dfrac{d}{e}$. ∎

À retenir

La technique « ordre ». C'est le réflexe numéro un de l'arithmétique olympique. Devant $p \mid a^n - 1$:

$$\mathrm{ord}_p(a) \mid n \text{ et } \mathrm{ord}_p(a) \mid p-1 \Longrightarrow \mathrm{ord}_p(a) \mid \mathrm{pgcd}(n, p-1).$$

Devant $p \mid a^n + 1$: alors $a^{2n} \equiv 1$, donc $\mathrm{ord}_p(a) \mid 2n$, mais $\mathrm{ord}_p(a) \nmid n$ (sinon $a^n \equiv 1$ et $a^n \equiv -1$, d'où $p \mid 2$, exclu pour p impair) ; donc $v_2\left(\mathrm{ord}_p(a)\right) = v_2(2n) = v_2(n) + 1$ (si l'on avait $v_2\left(\mathrm{ord}_p(a)\right) \leq v_2(n)$, le diviseur $\mathrm{ord}_p(a)$ de $2n$ diviserait n).

Proposition 7.1.4 (Facteurs premiers de $a^p - 1$)

Soient p un nombre premier et q un nombre premier tel que $q \mid a^p - 1$. Alors $q \mid a - 1$ ou $q \equiv 1 \pmod{p}$.

Démonstration. $d = \mathrm{ord}_q(a)$ divise p, donc $d = 1$ ou $d = p$. Si $d = 1$, alors $q \mid a - 1$. Si $d = p$, alors $p = d \mid q - 1$. ■

Exemple 7.1.5. *Trouver tous les facteurs premiers de $2^{11} - 1 = 2047$.*

Par la proposition 7.1.4, tout facteur premier q vérifie $q \equiv 1 \pmod{11}$ (car $q \nmid 2 - 1 = 1$). De plus q est impair, donc $q \equiv 1 \pmod{22}$: $q \in \{23, 67, 89, \ldots\}$. On teste : $2047 = 23 \cdot 89$.

Exemple 7.1.6. *Montrer qu'il existe une infinité de nombres premiers $\equiv 1 \pmod{n}$, pour tout $n \geq 1$ fixé.*

Version élémentaire pour $n = p$ premier : tout facteur premier q de $1 + a + \cdots + a^{p-1}$ vérifie $q = p$ ou $q \equiv 1 \pmod{p}$ (proposition 7.1.4, en factorisant $\frac{a^p - 1}{a - 1}$: si $q \mid a - 1$, alors $1 + a + \cdots + a^{p-1} \equiv p \pmod{q}$, d'où $q = p$). Supposons par l'absurde que $p_1, \ldots, p_k$ soient les seuls nombres premiers $\equiv 1 \pmod{p}$ et prenons $a = p \cdot p_1 \cdots p_k$. Le facteur $q = p$ est exclu (car $1 + a + \cdots + a^{p-1} \equiv 1 \pmod{p}$ quand $p \mid a$), de même que les p_i (pour la même raison) ; un facteur premier q de $1 + a + \cdots + a^{p-1} > 1$ fournit donc un nouveau nombre premier $\equiv 1 \pmod{p}$: contradiction, et il existe donc une infinité de tels nombres premiers. Le cas général se traite de la même façon via les polynômes cyclotomiques (chapitre 15).

7.2 Racines primitives

Définition 7.2.1 (Racine primitive)

On dit que g est une racine primitive modulo n si $\mathrm{ord}_n(g) = \varphi(n)$, c'est-à-dire si les puissances de g parcourent tout $(\mathbb{Z}/n\mathbb{Z})^\times$.

Théorème 7.2.2 (Existence des racines primitives modulo p)

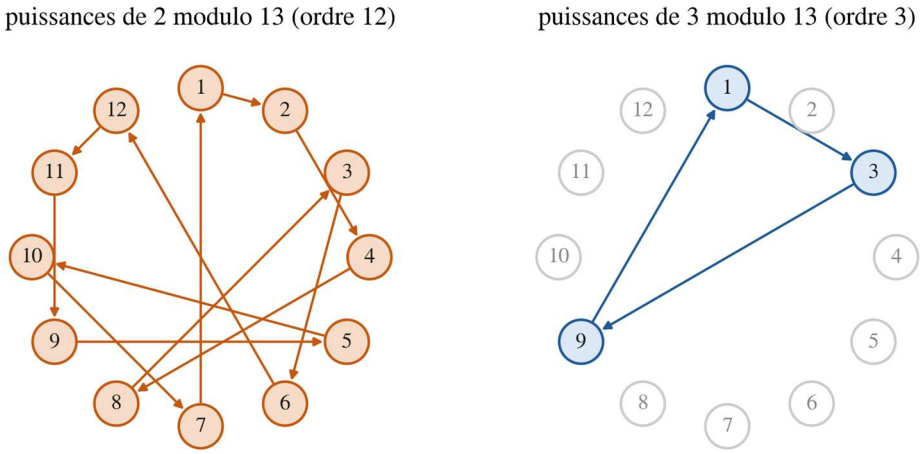
Si p est premier, il existe une racine primitive modulo p. Plus précisément, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique et possède exactement $\varphi(p-1)$ racines primitives.

Démonstration. Pour chaque $d \mid p - 1$, notons $\psi(d)$ le nombre d'éléments d'ordre exactement d dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Comme tout élément a un ordre divisant $p - 1$:

$$\sum_{d \mid p-1} \psi(d) = p - 1.$$

Montrons que $\psi(d) \leq \varphi(d)$. Si $\psi(d) > 0$, soit a d'ordre d. Les éléments $1, a, \ldots, a^{d-1}$ sont d solutions distinctes de $x^d \equiv 1 \pmod{p}$. Or ce polynôme de degré d a au plus d racines modulo p (théorème de Lagrange 7.2.3, ci-dessous), donc toutes les solutions sont les a^i. Les éléments d'ordre exactement d sont alors les a^i $(0 \leq i < d)$ avec $\gcd(i, d) = 1$ (lemme sur l'ordre d'une puissance, section 7.1), au nombre de $\varphi(d)$. Donc $\psi(d) \in \{0, \varphi(d)\}$.

Comme $\sum_{d \mid p-1} \varphi(d) = p - 1$ (identité de Gauss, proposition 6.1.3), l'égalité $\sum \psi(d) = p - 1$ force $\psi(d) = \varphi(d)$ pour tout d. En particulier $\psi(p-1) = \varphi(p-1) > 0$. ■



Puissances modulo 13 : 2 est une racine primitive (ses puissances parcourent les 12 résidus non nuls), tandis que 3 est d'ordre 3 (1 → 3 → 9 → 1).

Théorème 7.2.3 (Lagrange)

Soient p un nombre premier et $P \in \mathbb{Z}[X]$ de degré d dont le coefficient dominant n'est pas divisible par p. Alors P a au plus d racines modulo p (comptées sans multiplicité).

Démonstration. Récurrence sur d. Si $d = 0$, P est une constante non nulle modulo p : aucune racine. Si P n'a aucune racine, il n'y a rien à montrer. Sinon, soit a une racine : la division euclidienne des polynômes donne $P(X) = (X - a)Q(X) + P(a)$ avec $P(a) \equiv 0$, donc $P(X) \equiv (X - a)Q(X) \pmod{p}$, où Q est de degré $d - 1$ et de même coefficient dominant que P. Toute autre racine b vérifie $(b - a)Q(b) \equiv 0$; comme p est premier et $b \not\equiv a$, on a $Q(b) \equiv 0$. Par hypothèse de récurrence, Q a au plus $d - 1$ racines, donc P en a au plus d. ■

Attention.

Le théorème de Lagrange est faux modulo un nombre composé : $x^2 \equiv 1 \pmod{8}$ a quatre solutions $x \in \{1,3,5,7\}$. C'est pourquoi il n'existe pas toujours de racine primitive : modulo 8, tout élément inversible vérifie $x^2 \equiv 1$, donc aucun n'est d'ordre $\varphi(8) = 4$. (On peut démontrer qu'il existe une racine primitive modulo n exactement pour $n \in \{1,2,4,p^k,2p^k\}$ avec p premier impair ; nous n'utiliserons pas ce résultat.)

Proposition 7.2.4 (Nombre de solutions de $x^k \equiv 1$)

Soient p premier et $k \geq 1$. L'équation $x^k \equiv 1 \pmod{p}$ possède exactement $\gcd(k, p-1)$ solutions dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

Démonstration. Soit g une racine primitive et écrivons $x = g^t$. Alors

$$x^k \equiv 1 \Leftrightarrow (p-1) \mid kt \Leftrightarrow \frac{p-1}{d} \mid t, \quad \text{où } d = \gcd(k, p-1).$$

Il y a exactement d tels t modulo $p-1$. ■

Exemple 7.2.5. *Combien y a-t-il de résidus cubiques modulo* 31 *?*

L'application $f : x \mapsto x^3$ sur $(\mathbb{Z}/31\mathbb{Z})^\times$ vérifie $f(x) = f(y)$ si, et seulement si, $(xy^{-1})^3 \equiv 1$, c'est-à-dire si xy^{-1} est l'une des $\gcd(3,30) = 3$ solutions de $u^3 \equiv 1$ (proposition 7.2.4). Chaque valeur de f est donc atteinte exactement 3 fois, et l'image a $30/3 = 10$ éléments : il y a 10 résidus cubiques non nuls.

7.3 Exercices

Exercice 7.1 ★. Déterminer $\mathrm{ord}_{13}(2)$, $\mathrm{ord}_{13}(3)$, et trouver une racine primitive modulo 13.

Exercice 7.2 ★★. Montrer que tout facteur premier de $2^{2^n}+1$ est $\equiv 1 \pmod{2^{n+1}}$.

Exercice 7.3 ★★. Soit p un nombre premier impair. Montrer que tout facteur premier de $2^p - 1$ est de la forme $2kp+1$.

Exercice 7.4 ★★. Montrer que $n \mid \varphi(2^n - 1)$ pour tout $n \geq 1$.

Exercice 7.5 ★★★. Trouver tous les couples (a, n) d'entiers ≥ 2 tels que tout facteur premier de $a^n - 1$ divise $a - 1$.

Exercice 7.6 ★★★ (IMO 1999, problème 4). Déterminer tous les couples (n, p) d'entiers strictement positifs, avec p premier et $n \leq 2p$, tels que $(p-1)^n + 1$ soit divisible par n^{p-1}.

7.4 Corrigés

Solution de l'exercice 7.1. Modulo 13 : $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 \equiv 3$, $2^6 = 64 \equiv 12 \equiv -1$. L'ordre de 2 divise 12 ; il ne divise ni 6 (car $2^6 \equiv -1$) ni 4 (car $2^4 \equiv 3$), donc $\mathrm{ord}_{13}(2) = 12$: 2 est une racine primitive modulo 13. Enfin $3^3 = 27 \equiv 1$ et $3 \not\equiv 1$, donc $\mathrm{ord}_{13}(3) = 3$.

Solution de l'exercice 7.2. Soient $q \mid 2^{2^n}+1$ premier et $d = \mathrm{ord}_q(2)$. Alors $2^{2^{n+1}} \equiv 1$, donc $d \mid 2^{n+1}$, mais $2^{2^n} \equiv -1 \not\equiv 1$ (car $q > 2$), donc $d \nmid 2^n$. Ainsi $d = 2^{n+1}$, et $d \mid q-1$ donne $q \equiv 1 \pmod{2^{n+1}}$.

Application. Pour $F_5 = 2^{32}+1$, tout facteur premier est $\equiv 1 \pmod{64}$: $q \in \{193, 257, 449, 577, 641, \ldots\}$. C'est ainsi qu'Euler a trouvé le facteur 641 à la main.

Solution de l'exercice 7.3. Soit q un facteur premier de $2^p - 1$. Alors $\mathrm{ord}_q(2) \mid p$, et cet ordre n'est pas 1 (sinon $q \mid 1$). Donc $\mathrm{ord}_q(2) = p$ et $p \mid q-1$. Comme q est impair, $q-1$ est pair ; p étant impair, on obtient $2p \mid q-1$: $q = 2kp+1$.

Solution de l'exercice 7.4. Posons $m = 2^n - 1$. Alors $\mathrm{ord}_m(2) = n$, car $2^n \equiv 1 \pmod{m}$ et $0 < 2^k - 1 < m$ pour $1 \leq k < n$. Par la proposition 7.1.2, $n \mid \varphi(m)$.

Solution de l'exercice 7.5. Réponse : $n = 2$ et $a + 1$ une puissance de 2.

Soit p un facteur premier de n ; supposons p impair. Tout facteur premier q de $\frac{a^p-1}{a-1} = 1 + a + \cdots + a^{p-1}$ divise $a^p - 1$, qui divise $a^n - 1$; donc q divise $a - 1$ par hypothèse. Alors $a \equiv 1 \pmod q$ et $1 + a + \cdots + a^{p-1} \equiv p \pmod q$, donc $q = p$. Ainsi $1 + a + \cdots + a^{p-1} = p^j$ pour un $j \geq 1$, et $p \mid a - 1$. Le lemme LTE donne

$$v_p\left(\frac{a^p - 1}{a - 1}\right) = v_p(a^p - 1) - v_p(a - 1) = 1,$$

donc $j = 1$ et $1 + a + \cdots + a^{p-1} = p$, ce qui est impossible car $a \geq 2$ donne une somme $\geq 2^p - 1 > p$. Donc $n = 2^k$ avec $k \geq 1$.

Alors $a + 1 \mid a^n - 1$, donc tout facteur premier de $a + 1$ divise $a - 1$, donc divise $(a + 1) - (a - 1) = 2$: $a + 1 = 2^m$. Si $k \geq 2$, alors $a^2 + 1 \mid a^4 - 1 \mid a^n - 1$ et, de même, tout facteur premier de $a^2 + 1$ divise $a - 1$, donc divise $(a^2 + 1) - (a - 1)(a + 1) = 2$: $a^2 + 1$ est une puissance de 2 ; or a est impair, donc $a^2 + 1 \equiv 2 \pmod 4$, d'où $a^2 + 1 = 2$, $a = 1$: exclu. Donc $k = 1$, $n = 2$.

Réciproquement, si $n = 2$ et $a + 1 = 2^m$, alors a est impair et $a^2 - 1 = (a - 1)(a + 1)$ a pour facteurs premiers ceux de $a - 1$ et le nombre 2, qui divise $a - 1$: ces couples conviennent.

Solution de l'exercice 7.6. Réponse : $(n, p) = (1, p)$ pour tout premier p, $(2,2)$ et $(3,3)$.

Si $n = 1$, tout p convient. Supposons $n > 1$ et soit q le plus petit facteur premier de n. Comme $n^{p-1} \mid (p - 1)^n + 1$, on a $q \mid (p - 1)^n + 1$, donc $(p - 1)^{2n} \equiv 1 \pmod q$, et $d = \mathrm{ord}_q(p - 1)$ divise $2n$ mais pas n.

Si $p = 2$: $(p - 1)^n + 1 = 2$, donc $n^1 \mid 2$ et $n \leq 2p = 4$: $n \in \{1,2\}$. Le couple $(2,2)$ convient.

Supposons p impair. Alors $p - 1$ est pair, donc $(p - 1)^n + 1$ est impair ; ainsi n est impair et q est impair. Comme $d \mid 2n$, $d \nmid n$ et n est impair, on a $v_2(d) = 1$: $d = 2e$ avec $e \mid n$. Or $d \mid q - 1$, donc $e \mid \frac{q-1}{2}$ et $e \mid n$; les facteurs premiers de e divisent n et sont $< q$: donc $e = 1$ et $d = 2$, c'est-à-dire $q \mid (p - 1)^2 - 1 = p(p - 2)$ et $q \nmid p - 2$ (sinon $p - 1 \equiv 1$ et $d = 1$). Donc $q = p$.

Ainsi $p \mid n$ et, avec $n \leq 2p$ et n impair, $n = p$. La condition devient $p^{p-1} \mid (p - 1)^p + 1$. Par LTE ($p$ impair, $p \mid (p - 1) + 1$) :

$$v_p((p - 1)^p + 1) = v_p(p) + v_p(p) = 1 + 1 = 2.$$

Il faut donc $p - 1 \leq 2$, soit $p = 3$: $n = 3$, et en effet $3^2 = 9 \mid 2^3 + 1 = 9$.

CHAPITRE 8

8 Résidus quadratiques

Objectifs du chapitre.

- Définir le symbole de Legendre et le critère d'Euler.
- Déterminer les nombres premiers pour lesquels -1, 2, -2, 3 sont des carrés.
- Énoncer et utiliser la loi de réciprocité quadratique.
- Appliquer ces outils à des équations diophantiennes et aux sommes de deux carrés.

8.1 Le symbole de Legendre

Définition 8.1.1 (Résidu quadratique, symbole de Legendre)

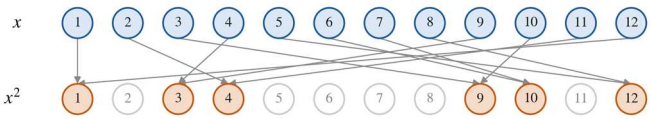
Soient p un nombre premier impair et $a \in \mathbb{Z}$. On dit que a est un résidu quadratique modulo p si $p \nmid a$ et s'il existe x tel que $x^2 \equiv a \pmod{p}$. Le symbole de Legendre est

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a, \\ +1 & \text{si } a \text{ est un résidu quadratique,} \\ -1 & \text{sinon.} \end{cases}$$

Proposition 8.1.2 (Nombre de résidus quadratiques)

Il y a exactement $\frac{p-1}{2}$ résidus quadratiques et $\frac{p-1}{2}$ non-résidus dans $\{1, \dots, p-1\}$.

Démonstration. L'application $x \mapsto x^2$ sur $(\mathbb{Z}/p\mathbb{Z})^\times$ est deux à un : $x^2 \equiv y^2$ équivaut à $p \mid (x-y)(x+y)$, c'est-à-dire (lemme d'Euclide) à $x \equiv \pm y$; et $x \not\equiv -x$, car sinon $p \mid 2x$, ce qui est exclu puisque p est impair et $p \nmid x$. Les $p-1$ éléments inversibles se groupent donc en $\frac{p-1}{2}$ paires $\{x, -x\}$ ayant le même carré, et l'image a $\frac{p-1}{2}$ éléments. ■



Les carrés modulo 13 : chaque résidu quadratique (en couleur) est atteint par exactement deux éléments x et −x ; il y a donc 6 résidus et 6 non-résidus.

Théorème 8.1.3 (Critère d'Euler)

Pour p premier impair et $p \nmid a$:

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

Démonstration. Soient g une racine primitive et $a = g^t$. Alors $a^{(p-1)/2} = g^{t(p-1)/2}$, qui vaut 1 si, et seulement si, $(p-1) \mid t\,\frac{p-1}{2}$, c'est-à-dire si, et seulement si, t est pair. Or a est un carré si, et seulement si, t est pair (si $t = 2s$, $a = (g^s)^2$; réciproquement, les carrés sont les g^{2s}). Enfin $a^{(p-1)/2}$ est une racine de $X^2 - 1$, donc vaut ± 1. ■

Proposition 8.1.4 (Multiplicativité)

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

En particulier, le produit de deux non-résidus est un résidu.

Démonstration. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$ (lemme d'Euclide) et les deux membres sont nuls. Sinon, par le critère d'Euler,

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

Les deux membres valent ± 1 et leur différence, qui appartient à $\{-2,0,2\}$, est divisible par $p \geq 3$: elle est donc nulle. Le cas particulier s'obtient avec $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$. ■

Théorème 8.1.5 (Lois complémentaires)

Pour p premier impair :

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{si } p \equiv 1 \pmod 4, \\ -1 & \text{si } p \equiv 3 \pmod 4; \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{si } p \equiv \pm 1 \pmod 8, \\ -1 & \text{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

Démonstration. *Première formule.* Par le critère d'Euler, $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$; les deux membres valent ± 1 et $p \geq 3$, donc ils sont égaux. Enfin $\frac{p-1}{2}$ est pair si, et seulement si, $p \equiv 1 \pmod 4$.

Seconde formule. Elle repose sur le lemme suivant, que nous démontrons complètement.

Lemme de Gauss. Soient p premier impair, $m = \frac{p-1}{2}$ et a un entier non divisible par p. Notons ν le nombre d'entiers $k \in \{1, \dots, m\}$ tels que le reste r_k de ka modulo p soit $> \frac{p}{2}$. Alors $\left(\frac{a}{p}\right) = (-1)^\nu$.

Preuve du lemme. Posons $s_k = r_k$ si $r_k < \frac{p}{2}$ et $s_k = p - r_k$ si $r_k > \frac{p}{2}$ (le cas $r_k = \frac{p}{2}$ est impossible, p étant impair ; et $r_k \neq 0$ car $p \nmid ka$). Dans les deux cas $1 \leq s_k \leq m$ et $s_k \equiv \pm ka \pmod p$. Les s_k sont deux à deux distincts : si $s_i = s_j$, alors $ia \equiv \pm ja$, et comme a est inversible, $i \equiv \pm j \pmod p$; or $0 < i + j < p$ exclut $i \equiv -j$, donc $i \equiv j$, puis $i = j$. Les m entiers $s_1, \dots, s_m$ sont donc exactement $1,2, \dots, m$. En multipliant les congruences $ka \equiv \pm s_k$, où le signe $-$ apparaît exactement ν fois,

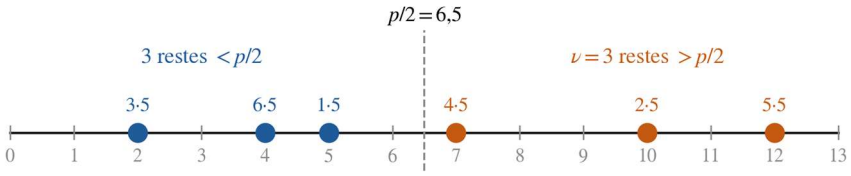
$$a^m\, m! = \prod_{k=1}^{m} (ka) \equiv (-1)^\nu \prod_{k=1}^{m} s_k = (-1)^\nu\, m! \pmod p.$$

Comme $p \nmid m!$, on simplifie : $a^m \equiv (-1)^\nu$, et le critère d'Euler donne $\left(\frac{a}{p}\right) \equiv (-1)^\nu$, d'où l'égalité (deux nombres ± 1 congrus modulo $p \geq 3$).

Application à $a = 2$. Les entiers $2,4, \dots, p-1$ sont déjà réduits modulo p. Ceux qui sont $< \frac{p}{2}$ sont les $2k$ avec $k < \frac{p}{4}$, au nombre de $\left\lfloor \frac{p}{4} \right\rfloor$; donc $\nu = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$. Écrivons $p = 8j + r$ avec $r \in \{1,3,5,7\}$:

p	$\frac{p-1}{2}$	$\left\lfloor\frac{p}{4}\right\rfloor$	ν	$\frac{p^2-1}{8}$
$8j+1$	$4j$	$2j$	$2j$ (pair)	$8j^2+2j$ (pair)
$8j+3$	$4j+1$	$2j$	$2j+1$ (impair)	$8j^2+6j+1$ (impair)
$8j+5$	$4j+2$	$2j+1$	$2j+1$ (impair)	$8j^2+10j+3$ (impair)
$8j+7$	$4j+3$	$2j+1$	$2j+2$ (pair)	$8j^2+14j+6$ (pair)

Dans tous les cas $\nu \equiv \frac{p^2-1}{8} \pmod 2$, donc $\left(\frac{2}{p}\right) = (-1)^{\nu} = (-1)^{\frac{p^2-1}{8}}$, qui vaut $+1$ exactement pour $p \equiv \pm 1 \pmod 8$. ■



Lemme de Gauss pour p = 13 et a = 5 : on réduit 5, 10, 15, 20, 25, 30 modulo 13 ; trois restes (10, 7, 12) dépassent 13/2, donc ν = 3 et (5/13) = −1.

Théorème 8.1.6 (Loi de réciprocité quadratique)

Soient $p \neq q$ deux nombres premiers impairs. Alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Autrement dit, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ sauf si $p \equiv q \equiv 3 \pmod 4$, auquel cas $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Démonstration (Eisenstein). *Étape 1 : lemme d'Eisenstein.* Soient p premier impair, $m = \frac{p-1}{2}$ et a un entier **impair** non divisible par p. Alors $\left(\frac{a}{p}\right) = (-1)^T$ où $T = \sum_{k=1}^{m} \left\lfloor\frac{ka}{p}\right\rfloor$.

Reprenons les notations de la démonstration du lemme de Gauss : $ka = p\left\lfloor\frac{ka}{p}\right\rfloor + r_k$. Notons B la somme des $r_k < \frac{p}{2}$ et C la somme des ν restes $r_k > \frac{p}{2}$. En sommant sur k :

$$a\sum_{k=1}^{m} k = pT + B + C.$$

D'autre part, les s_k parcourent $\{1, \dots, m\}$, donc

$$\sum_{k=1}^{m} k = \sum_{k=1}^{m} s_k = B + \sum_{r_k > p/2} (p - r_k) = B + \nu p - C.$$

En soustrayant, $(a-1)\sum_{k=1}^{m} k = p(T-\nu) + 2C$. Le membre de gauche est pair (a est impair), $2C$ aussi, donc $p(T-\nu)$ est pair, et comme p est impair, $T \equiv \nu \pmod 2$. Le lemme de Gauss donne alors $\left(\frac{a}{p}\right) = (-1)^{\nu} = (-1)^T$.

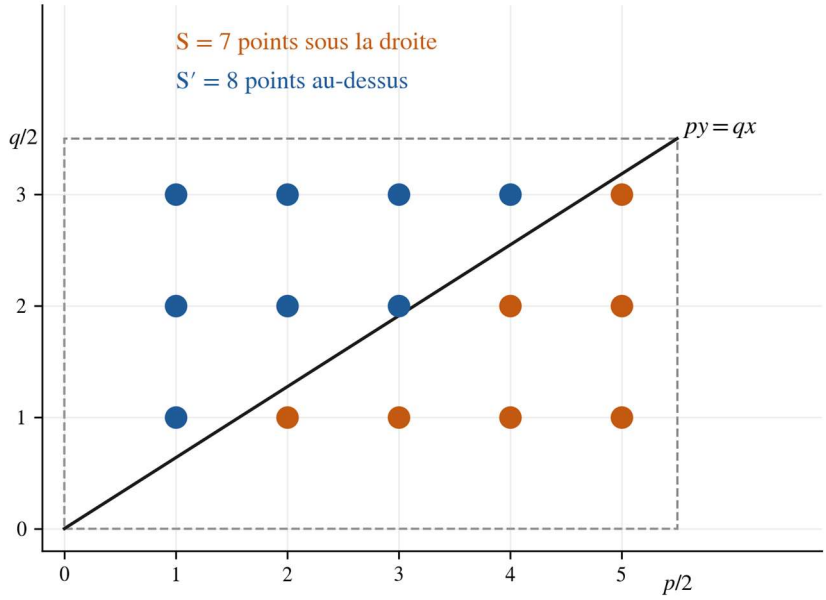
Étape 2 : comptage de points. Posons $m = \frac{p-1}{2}$, $n = \frac{q-1}{2}$ et considérons les mn points entiers (x, y) avec $1 \leq x \leq m$ et $1 \leq y \leq n$. Aucun n'est sur la droite $py = qx$: sinon $p \mid qx$, donc $p \mid x$ (Gauss, $\gcd(p, q) = 1$), impossible puisque $1 \leq x < p$.

- Pour x fixé, les points **sous** la droite sont ceux où $1 \le y < \frac{qx}{p}$. Comme $\frac{qx}{p} < \frac{q}{2}$, on a $\left\lfloor \frac{qx}{p} \right\rfloor \le n$, et il y a exactement $\left\lfloor \frac{qx}{p} \right\rfloor$ tels points. Au total, $S = \sum_{x=1}^{m} \left\lfloor \frac{qx}{p} \right\rfloor$.
- De même, les points **au-dessus** de la droite sont, pour y fixé, ceux où $1 \le x < \frac{py}{q}$; leur nombre total est $S' = \sum_{y=1}^{n} \left\lfloor \frac{py}{q} \right\rfloor$.

Chaque point est d'un côté et d'un seul, donc $S + S' = mn$.

Étape 3 : conclusion. Par le lemme d'Eisenstein appliqué à $a = q$ modulo p, puis à $a = p$ modulo q (les deux sont impairs), $\left(\frac{q}{p}\right) = (-1)^S$ et $\left(\frac{p}{q}\right) = (-1)^{S'}$. Donc

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S+S'} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \quad \blacksquare$$



Démonstration d'Eisenstein pour p = 11, q = 7 : les 5 × 3 = 15 points du rectangle se répartissent en S = 7 points sous la droite 11y = 7x et S′ = 8 au-dessus ; donc (7/11)(11/7) = (−1)¹⁵ = −1.

Méthode 8.1.7 — Calculer un symbole de Legendre

1. réduire a modulo p ;
2. factoriser a et utiliser la multiplicativité ;
3. traiter -1 et 2 par les lois complémentaires ;
4. pour les facteurs premiers impairs, retourner le symbole par réciprocité ;
5. itérer (c'est un « algorithme d'Euclide quadratique »).

Exemple 8.1.8. *Calculer* $\left(\frac{219}{383}\right)$ *(*383 *est premier).*

On a $219 = 3 \cdot 73$ et $383 \equiv 3 \pmod 4$. D'abord

$$\left(\frac{3}{383}\right) = -\left(\frac{383}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1,$$

car $383 \equiv 2 \pmod 3$ et $\left(\frac{2}{3}\right) = -1$ (puisque $3 \equiv 3 \pmod 8$). Ensuite $73 \equiv 1 \pmod 4$, donc

$$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right) = \left(\frac{18}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{9}{73}\right) = \left(\frac{2}{73}\right) = 1,$$

car $73 \equiv 1 \pmod 8$. Donc $\left(\frac{219}{383}\right) = 1 \cdot 1 = 1$.

8.2 Applications aux équations diophantiennes

Théorème 8.2.1 (Fermat, deux carrés)

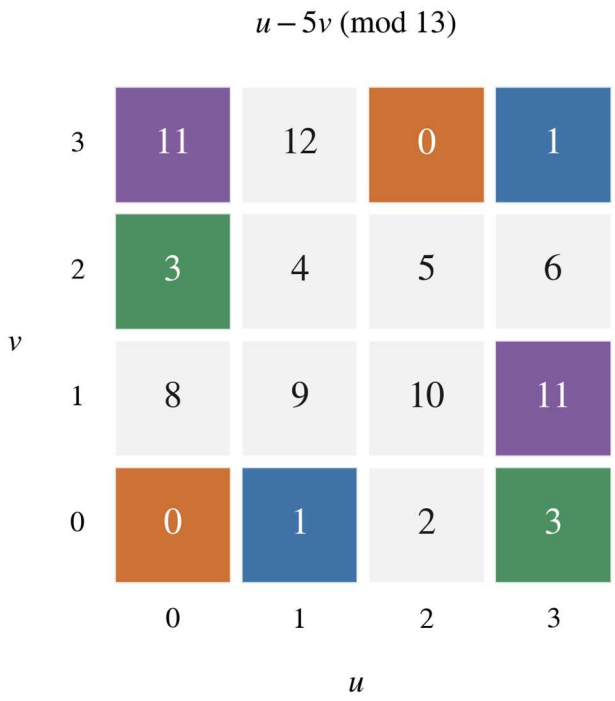
Un nombre premier impair p s'écrit $p = a^2 + b^2$ si, et seulement si, $p \equiv 1 \pmod 4$.

Démonstration. *Nécessité.* Modulo 4, $a^2 + b^2 \in \{0,1,2\}$, donc $p \equiv 1 \pmod 4$.

Suffisance (lemme de Thue). Si $p \equiv 1 \pmod 4$, il existe x tel que $x^2 \equiv -1 \pmod p$ (proposition 4.4.2). Posons $k = \lfloor \sqrt{p} \rfloor$ et considérons les $(k+1)^2 > p$ couples (u, v) avec $0 \leq u, v \leq k$. Par le principe des tiroirs, deux d'entre eux vérifient $u_1 - x v_1 \equiv u_2 - x v_2 \pmod p$. En posant $a = u_1 - u_2$ et $b = v_1 - v_2$, non tous deux nuls, on a $a \equiv x b \pmod p$ et $|a|, |b| \leq k < \sqrt{p}$. Alors

$$a^2 + b^2 \equiv x^2 b^2 + b^2 = b^2(x^2 + 1) \equiv 0 \pmod p,$$

et $0 < a^2 + b^2 < 2p$, donc $a^2 + b^2 = p$. ∎



Lemme de Thue pour p = 13 et x = 5 (5² ≡ −1) : les 16 couples (u, v) ∈{0,…,3}² prennent seulement 13 valeurs de u − 5v modulo 13 ; deux couples de même couleur donnent |a| = 3, |b| = 2 et 3² + 2² = 13.

Théorème 8.2.2 (Sommes de deux carrés)

Un entier $n \geq 1$ est somme de deux carrés si, et seulement si, tout nombre premier $p \equiv 3 \pmod 4$ apparaît dans la décomposition de n avec un exposant pair.

Démonstration. *Lemme.* Si $p \equiv 3 \pmod 4$ est premier et $p \mid a^2 + b^2$, alors $p \mid a$ et $p \mid b$. En effet, si $p \nmid b$, alors $(a b^{-1})^2 \equiv -1 \pmod p$, donc $\left(\frac{-1}{p}\right) = 1$, ce qui contredit le théorème 8.1.5 ; ainsi $p \mid b$, puis $p \mid a^2$ et $p \mid a$.

Nécessité. Montrons par récurrence forte sur $n \geq 1$ que, si $n = a^2 + b^2$, alors $v_p(n)$ est pair pour tout premier $p \equiv 3 \pmod 4$. Si $p \nmid n$, $v_p(n) = 0$. Si $p \mid n$, le lemme donne $a = pa'$, $b = pb'$, d'où $\frac{n}{p^2} = a'^2 + b'^2$, entier ≥ 1 et $< n$; par hypothèse de récurrence $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2$ est pair, donc $v_p(n)$ aussi.

Suffisance. L'identité de Brahmagupta–Fibonacci

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

(développer les deux membres) montre que l'ensemble des sommes de deux carrés est stable par produit. Or $2 = 1^2 + 1^2$, tout premier $p \equiv 1 \pmod 4$ est somme de deux carrés (théorème 8.2.1), et pour $p \equiv 3 \pmod 4$, $p^2 = p^2 + 0^2$. Si les premiers $p \equiv 3 \pmod 4$ figurent avec des exposants pairs, n est un produit de tels facteurs (et $1 = 1^2 + 0^2$), donc une somme de deux carrés. ■

Exemple 8.2.3. *Montrer que $x^2 - 5y^2 = 2$ n'a pas de solution entière.*

Modulo 5 : $x^2 \equiv 2 \pmod 5$. Or $\left(\frac{2}{5}\right) = -1$ (car $5 \equiv -3 \pmod 8$), donc 2 n'est pas un carré modulo 5. Impossible.

Exemple 8.2.4. *Soit p un nombre premier impair divisant $n^2 + 1$ pour un certain entier n. Montrer que $p \equiv 1 \pmod 4$.*

On a $n^2 \equiv -1 \pmod p$, donc $\left(\frac{-1}{p}\right) = 1$, ce qui impose $p \equiv 1 \pmod 4$.

Exemple 8.2.5. *Montrer que si p est premier et $p \mid a^2 + ab + b^2$ avec $\operatorname{pgcd}(a, b) = 1$, alors $p = 3$ ou $p \equiv 1 \pmod 3$.*

Comme a et b ne sont pas tous deux pairs, $a^2 + ab + b^2$ est impair : $p \neq 2$. De plus $p \nmid b$ (sinon $p \mid a^2$, donc $p \mid a$, ce qui contredit $\operatorname{pgcd}(a, b) = 1$). Posons $t = ab^{-1} \bmod p$: $t^2 + t + 1 \equiv 0$, donc $(2t + 1)^2 = 4(t^2 + t + 1) - 3 \equiv -3 \pmod p$. Si $p = 3$, c'est terminé. Sinon, $-3 \not\equiv 0$ et $\left(\frac{-3}{p}\right) = 1$. Or on calcule, par réciprocité,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right),$$

qui vaut 1 si, et seulement si, $p \equiv 1 \pmod 3$.

À retenir

Le tableau des « premiers admissibles ».

Forme	Premiers p divisant la forme avec $\operatorname{pgcd}(x, y) = 1$
$x^2 + y^2$	$p = 2$ ou $p \equiv 1 \pmod 4$
$x^2 + 2y^2$	$p = 2$ ou $p \equiv 1,3 \pmod 8$
$x^2 + 3y^2$	$p = 2$, $p = 3$ ou $p \equiv 1 \pmod 3$
$x^2 - 2y^2$	$p = 2$ ou $p \equiv \pm 1 \pmod 8$
$x^2 + xy + y^2$	$p = 3$ ou $p \equiv 1 \pmod 3$

Ce tableau est un outil de blocage : il permet de montrer qu'une équation n'a pas de solution, ou de contraindre fortement les facteurs premiers.

Justification du tableau.

Chaque ligne se démontre comme l'exemple 8.2.5. Soit p un premier impair divisant la forme, avec $\gcd(x,y)=1$; on vérifie d'abord que $p \nmid y$ (sinon p diviserait aussi x), puis on pose $t = xy^{-1} \bmod p$:

- x^2+y^2 : $t^2 \equiv -1$, donc $\left(\frac{-1}{p}\right)=1$, soit $p \equiv 1 \pmod 4$;
- x^2+2y^2 : $t^2 \equiv -2$, et $\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=1$ exactement pour $p \equiv 1,3 \pmod 8$ (lois complémentaires) ;
- x^2+3y^2 : $t^2 \equiv -3$; si $p \neq 3$, $\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)=1$ (calcul de l'exemple 8.2.5), soit $p \equiv 1 \pmod 3$;
- x^2-2y^2 : $t^2 \equiv 2$, et $\left(\frac{2}{p}\right)=1$ exactement pour $p \equiv \pm 1 \pmod 8$;
- x^2+xy+y^2 : c'est l'exemple 8.2.5.

Réciproquement, chaque premier indiqué divise effectivement une valeur de la forme avec $\gcd(x,y)=1$: pour p impair, il suffit de prendre $y=1$ et x une racine carrée de -1, -2, -3 ou 2 modulo p (ou de résoudre $t^2+t+1 \equiv 0$, ce qui revient à $(2t+1)^2 \equiv -3$) ; les cas $p=2$ et $p=3$ se vérifient directement ($1+1$, $0+2\cdot 1$, $1+3$, $0-2$, $0+3$, $1+1+1$).

8.3 Exercices

Exercice 8.1 ★. Calculer $\left(\frac{7}{31}\right)$, $\left(\frac{11}{101}\right)$ et $\left(\frac{-5}{97}\right)$.

Exercice 8.2 ★★. Soit $p>3$ un nombre premier. Montrer que $x^2 \equiv 3 \pmod p$ a une solution si, et seulement si, $p \equiv \pm 1 \pmod{12}$.

Exercice 8.3 ★★. Montrer que $x^4-y^4=z^2$ n'a pas de solution en entiers strictement positifs.

Exercice 8.4 ★★. Montrer qu'il existe une infinité de nombres premiers $\equiv 1 \pmod 8$.

Exercice 8.5 ★★★. Soit p un nombre premier tel que $p \equiv 3 \pmod 4$. Montrer que si $p \mid a^2+b^2$, alors $p \mid a$ et $p \mid b$. Montrer par ailleurs que $4^n(8m+7)$ n'est jamais somme de trois carrés.

Exercice 8.6 ★★★. Montrer que pour tout nombre premier p, l'équation $x^2+y^2+1 \equiv 0 \pmod p$ admet une solution.

8.4 Corrigés

Solution de l'exercice 8.1. $\left(\frac{7}{31}\right)$: $31 \equiv 3 \pmod 4$ et $7 \equiv 3 \pmod 4$, donc $\left(\frac{7}{31}\right)=-\left(\frac{31}{7}\right)=-\left(\frac{3}{7}\right)$. Or $3^3=27 \equiv 6 \equiv -1 \pmod 7$, donc $\left(\frac{3}{7}\right)=-1$ par le critère d'Euler. D'où $\left(\frac{7}{31}\right)=1$.

$\left(\frac{11}{101}\right)$: $101 \equiv 1 \pmod 4$, donc $\left(\frac{11}{101}\right)=\left(\frac{101}{11}\right)=\left(\frac{2}{11}\right)=-1$ (car $11 \equiv 3 \pmod 8$).

$\left(\frac{-5}{97}\right)=\left(\frac{-1}{97}\right)\left(\frac{5}{97}\right)=1\cdot\left(\frac{97}{5}\right)=\left(\frac{2}{5}\right)=-1$ (car $97 \equiv 1 \pmod 4$ et $97 \equiv 2 \pmod 5$).

Solution de l'exercice 8.2. Si $p \equiv 1 \pmod 4$: $\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)$, qui vaut 1 si, et seulement si, $p \equiv 1 \pmod 3$. Combiné : $p \equiv 1 \pmod{12}$.

Si $p \equiv 3 \pmod 4$: $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$, qui vaut 1 si, et seulement si, $p \equiv 2 \pmod 3$. Combiné : $p \equiv 11 \equiv -1 \pmod{12}$.

Solution de l'exercice 8.3. On utilise la descente infinie (chapitre 12). Supposons qu'il existe des solutions et choisissons-en une avec x minimal. Si un premier r divisait x et y, on aurait $r^4 \mid z^2$, donc $r^2 \mid z$, et $(x/r, y/r, z/r^2)$ serait une solution plus petite : ainsi $\operatorname{pgcd}(x,y) = 1$. De plus x est impair : sinon y et z seraient impairs et $y^4 + z^2 \equiv 2 \pmod 4$, alors que $x^4 \equiv 0 \pmod 4$. Le triplet (y^2, z, x^2), qui vérifie $(y^2)^2 + z^2 = (x^2)^2$, est donc pythagoricien primitif : il existe $m > n \geq 1$ premiers entre eux, de parités différentes, tels que l'on soit dans l'un des deux cas suivants.

- y impair : $y^2 = m^2 - n^2$, $z = 2mn$, $x^2 = m^2 + n^2$. Alors $m^4 - n^4 = (xy)^2$: le triplet (m, n, xy) est une solution avec $m < x$, ce qui contredit la minimalité.
- y pair : $y^2 = 2mn$, $z = m^2 - n^2$, $x^2 = m^2 + n^2$. Le triplet formé de m, n et x est pythagoricien primitif ; si e désigne celui des deux nombres m, n qui est pair et o l'autre, il existe $r > s \geq 1$ premiers entre eux tels que $e = 2rs$, $o = r^2 - s^2$ et $x = r^2 + s^2$. Alors $\left(\frac{y}{2}\right)^2 = rs(r^2 - s^2)$, produit de trois facteurs positifs deux à deux premiers entre eux : ce sont donc des carrés, $r = u^2$, $s = v^2$, $r^2 - s^2 = w^2$. On obtient $u^4 - v^4 = w^2$ avec $u \leq r < x$, ce qui contredit encore la minimalité.

Solution de l'exercice 8.4. Supposons que $p_1, \ldots, p_k$ soient les seuls nombres premiers $\equiv 1 \pmod 8$. Posons $N = (2p_1 \cdots p_k)^4 + 1$; soit q un facteur premier de N, impair et distinct des p_i. Alors $x^4 \equiv -1 \pmod q$ avec $x = 2p_1 \cdots p_k$, donc $x^8 \equiv 1$ et $x^4 \not\equiv 1$: $\operatorname{ord}_q(x) = 8$, d'où $8 \mid q - 1$, c'est-à-dire $q \equiv 1 \pmod 8$. Contradiction.

Solution de l'exercice 8.5. Si $p \nmid b$, alors $(ab^{-1})^2 \equiv -1 \pmod p$, donc $\left(\frac{-1}{p}\right) = 1$ et $p \equiv 1 \pmod 4$: contradiction. Donc $p \mid b$, puis $p \mid a^2$, donc $p \mid a$.

Trois carrés. Supposons $x^2 + y^2 + z^2 = 4^n(8m + 7)$. Si $n \geq 1$, la somme est divisible par 4 ; comme un carré vaut 0 ou 1 modulo 4, x, y, z sont pairs et $(x/2)^2 + (y/2)^2 + (z/2)^2 = 4^{n-1}(8m + 7)$. Une récurrence sur n (comme au corrigé de l'exercice 4.3) ramène ainsi à $n = 0$; or, modulo 8, une somme de trois carrés ne vaut jamais 7.

Solution de l'exercice 8.6. Pour $p = 2$: $x = 1$, $y = 0$ donne $x^2 + y^2 + 1 = 2 \equiv 0 \pmod 2$.

Pour p impair, considérons

$$A = \{x^2 \bmod p : x \in \mathbb{Z}\}, \qquad B = \{-1 - y^2 \bmod p : y \in \mathbb{Z}\}.$$

Chacun a $\frac{p+1}{2}$ éléments (les $\frac{p-1}{2}$ résidus non nuls, plus 0). Comme $|A| + |B| = p + 1 > p$, ils se rencontrent : il existe x, y avec $x^2 \equiv -1 - y^2$, c'est-à-dire $x^2 + y^2 + 1 \equiv 0 \pmod p$.

À retenir

Cet argument de comptage par tiroirs sur deux ensembles de taille $\frac{p+1}{2}$ est extrêmement fécond : il démontre aussi que tout élément de $\mathbb{F}_p$ est somme de deux carrés, et sert de brique au théorème des quatre carrés.

PARTIE III — Fonctions arithmétiques et parties entières

CHAPITRE 9

9 Fonctions arithmétiques

Objectifs du chapitre.

- Définir $\tau, \sigma, \varphi, \mu$ et savoir les calculer.
- Comprendre la notion de fonction multiplicative et son intérêt calculatoire.
- Maîtriser la convolution de Dirichlet et la formule d'inversion de Möbius.
- Résoudre des problèmes de comptage de diviseurs.

9.1 Les fonctions classiques

Définition 9.1.1 (Fonction arithmétique, fonction multiplicative)

Une fonction arithmétique est une application $f : \mathbb{N}^* \to \mathbb{C}$. Elle est multiplicative si $f(1) = 1$ et $f(mn) = f(m)f(n)$ dès que $\gcd(m, n) = 1$; complètement multiplicative si $f(mn) = f(m)f(n)$ pour tous m, n.

À retenir

Une fonction multiplicative est entièrement déterminée par ses valeurs sur les puissances de nombres premiers :

$$f\left(p_1^{\alpha_1} \cdots p_r^{\alpha_r}\right) = f\left(p_1^{\alpha_1}\right) \cdots f\left(p_r^{\alpha_r}\right).$$

(Par récurrence sur r : $p_r^{\alpha_r}$ est premier avec $p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}$, donc $f(n) = f\left(p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}\right) f\left(p_r^{\alpha_r}\right)$.) C'est la raison d'être du concept : réduire un calcul global à un calcul local en chaque premier.

Définition 9.1.2 (Fonctions diviseurs)

Pour $n \geq 1$:

$$\tau(n) = \sum_{d \mid n} 1, \qquad \sigma(n) = \sum_{d \mid n} d, \qquad \sigma_k(n) = \sum_{d \mid n} d^k.$$

Théorème 9.1.3 (Nombre et somme des diviseurs)

Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, alors

$$\tau(n) = \prod_{i=1}^{r} (\alpha_i + 1), \qquad \sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}.$$

Ces fonctions sont multiplicatives.

Démonstration. Par la proposition 3.2.2 (iii), les diviseurs positifs de n sont exactement les entiers $\prod_i p_i^{\beta_i}$ avec $0 \leq \beta_i \leq \alpha_i$, et deux choix distincts des β_i donnent deux diviseurs distincts (unicité de la décomposition, théorème 3.1.2). L'application $(\beta_1, \ldots, \beta_r) \mapsto \prod_i p_i^{\beta_i}$ est donc une bijection de $\prod_i \{0, \ldots, \alpha_i\}$ sur l'ensemble des diviseurs, d'où $\tau(n) = \prod_i (\alpha_i + 1)$.

Pour σ, développons le produit $\prod_{i=1}^{r}\left(1+p_i+\cdots+p_i^{\alpha_i}\right)$: on obtient la somme, sur tous les choix $(\beta_1,\dots,\beta_r)$, des produits $\prod_i p_i^{\beta_i}$, c'est-à-dire, par la bijection précédente, la somme de tous les diviseurs de n, chacun une fois. Il reste à sommer chaque facteur : $1+p+\cdots+p^{\alpha}=\frac{p^{\alpha+1}-1}{p-1}$ (somme géométrique).

Multiplicativité. Si $\operatorname{pgcd}(m,n)=1$, les premiers de m et de n sont distincts, et la décomposition de mn est la réunion de celles de m et de n ; les formules produits donnent $\tau(mn)=\tau(m)\tau(n)$ et $\sigma(mn)=\sigma(m)\sigma(n)$. Enfin $\tau(1)=\sigma(1)=1$. ■

Définition 9.1.4 (Fonction de Möbius)

$$\mu(n)=\begin{cases}1 & \text{si } n=1,\\ (-1)^r & \text{si } n \text{ est produit de } r \text{ premiers distincts},\\ 0 & \text{si } n \text{ est divisible par un carré} > 1.\end{cases}$$

Proposition 9.1.5 (Sommes de la fonction de Möbius)

μ est multiplicative et, pour tout $n\geq 1$,

$$\sum_{d\mid n}\mu(d)=\begin{cases}1 & \text{si } n=1,\\ 0 & \text{sinon.}\end{cases}$$

Démonstration. *Multiplicativité.* Si $\operatorname{pgcd}(m,n)=1$, mn est sans facteur carré si, et seulement si, m et n le sont, et le nombre de facteurs premiers de mn est alors la somme de ceux de m et de n ; d'où $\mu(mn)=\mu(m)\mu(n)$.

Somme. Pour $n=1$, la somme vaut $\mu(1)=1$. Si $n>1$ a pour facteurs premiers distincts $p_1,\dots,p_r$ (avec $r\geq 1$), seuls les diviseurs sans facteur carré contribuent, et il y en a $\binom{r}{k}$ ayant exactement k facteurs premiers :

$\sum_{d\mid n}\mu(d)=\sum_{k=0}^{r}\binom{r}{k}(-1)^k=(1-1)^r=0$. ■

9.2 Convolution de Dirichlet

Définition 9.2.1 (Convolution de Dirichlet)

Pour f,g arithmétiques, on pose

$$(f*g)(n)=\sum_{d\mid n}f(d)\,g\left(\frac{n}{d}\right)=\sum_{ab=n}f(a)g(b).$$

Proposition 9.2.2 (Propriétés de la convolution)

$*$ est commutative, associative, d'élément neutre ε défini par $\varepsilon(1)=1$ et $\varepsilon(n)=0$ pour $n>1$. De plus, la convolution de deux fonctions multiplicatives est multiplicative.

Démonstration. *Commutativité.* Elle se lit sur la forme symétrique $\sum_{ab=n}f(a)g(b)$, la somme portant sur les couples (a,b) d'entiers positifs de produit n.

Associativité. $\big((f*g)*h\big)(n) = \sum_{ehı=n}\big(\sum_{ab=e} f\,(a)g(b)\big)\,h(c)$ avec $c=h'$, soit $\sum_{abc=n} f\,(a)g(b)h(c)$, la somme portant sur les triplets d'entiers positifs de produit n. Le même calcul donne la même expression pour $f*(g*h)$.

Élément neutre. $(f*\varepsilon)(n) = \sum_{d\mid n} f\,(d)\varepsilon(n/d)$; seul le terme $d=n$ est non nul, et il vaut $f(n)$.

Multiplicativité. Soient f,g multiplicatives et $\gcd(m,n)=1$. L'application $(d_1,d_2)\mapsto d_1d_2$, des couples (diviseur de m, diviseur de n) vers les diviseurs de mn, est bijective : tout diviseur d de mn s'écrit $d=\gcd(d,m)\gcd(d,n)$, et cette écriture est unique car les facteurs premiers de d_1 sont ceux de m et ceux de d_2 ceux de n (proposition 3.2.2). De plus d_1 et d_2 sont premiers entre eux, ainsi que $\frac{m}{d_1}$ et $\frac{n}{d_2}$. Donc

$$\begin{aligned}(f*g)(mn) &= \sum_{d_1\mid m}\sum_{d_2\mid n} f\,(d_1d_2)\,g\left(\frac{m}{d_1}\cdot\frac{n}{d_2}\right) = \sum_{d_1\mid m}\sum_{d_2\mid n} f\,(d_1)g\left(\frac{m}{d_1}\right)f(d_2)g\left(\frac{n}{d_2}\right)\\ &= (f*g)(m)\,(f*g)(n),\end{aligned}$$

et $(f*g)(1)=f(1)g(1)=1$. ■

À retenir (Les relations à connaître)

Notons $\mathbf{1}(n)=1$, $\mathrm{Id}(n)=n$. Alors

$$\tau=\mathbf{1}*\mathbf{1},\qquad \sigma=\mathrm{Id}*\mathbf{1},\qquad \mathbf{1}*\mu=\varepsilon,\qquad \varphi*\mathbf{1}=\mathrm{Id}.$$

Les deux premières sont les définitions de τ et σ ; la troisième est la proposition 9.1.5 ; la dernière est la proposition 6.1.3 (identité de Gauss : $\sum_{d\mid n}\varphi\,(d)=n$).

Théorème 9.2.3 (Formule d'inversion de Möbius)

Soient f,g arithmétiques. Alors

$$g(n)=\sum_{d\mid n} f\,(d)\ \ \forall n \Leftrightarrow f(n)=\sum_{d\mid n}\mu\,(d)\,g\left(\frac{n}{d}\right)\ \ \forall n.$$

Démonstration. La première relation s'écrit $g=f*\mathbf{1}$, la seconde $f=g*\mu$. On utilise la commutativité, l'associativité et $\mathbf{1}*\mu=\varepsilon$ (propositions 9.2.2 et 9.1.5). En convolant par μ : $g*\mu=f*\mathbf{1}*\mu=f*\varepsilon=f$. La réciproque est analogue : si $f=g*\mu$, en convolant par $\mathbf{1}$ on obtient $f*\mathbf{1}=g*\mu*\mathbf{1}=g*\varepsilon=g$. ■

Exemple 9.2.4. *Retrouver la formule* $\varphi(n)=n\prod_{p\mid n}\left(1-\frac{1}{p}\right)$.

De $\varphi*\mathbf{1}=\mathrm{Id}$ on tire $\varphi=\mathrm{Id}*\mu$, soit

$$\varphi(n)=\sum_{d\mid n}\mu\,(d)\frac{n}{d}=n\sum_{d\mid n}\frac{\mu(d)}{d}=n\prod_{p\mid n}\left(1-\frac{1}{p}\right),$$

la dernière égalité étant l'exemple 9.2.5 ci-dessous appliqué à la fonction complètement multiplicative $f(d)=\frac{1}{d}$.

Exemple 9.2.5. *Soit f multiplicative. Montrer que* $\sum_{d\mid n}\mu\,(d)f(d)=\prod_{p\mid n}\big(1-f(p)\big)$.

$h\colon d\mapsto\mu(d)f(d)$ est multiplicative (produit de deux fonctions multiplicatives), donc sa fonction sommatoire $h*\mathbf{1}$ l'est aussi (proposition 9.2.2) ; il en est de même du membre de droite, produit de facteurs attachés aux premiers distincts. Il suffit d'évaluer en p^α : $\sum_{k=0}^{\alpha}\mu\left(p^k\right)f\left(p^k\right)=1-f(p)$.

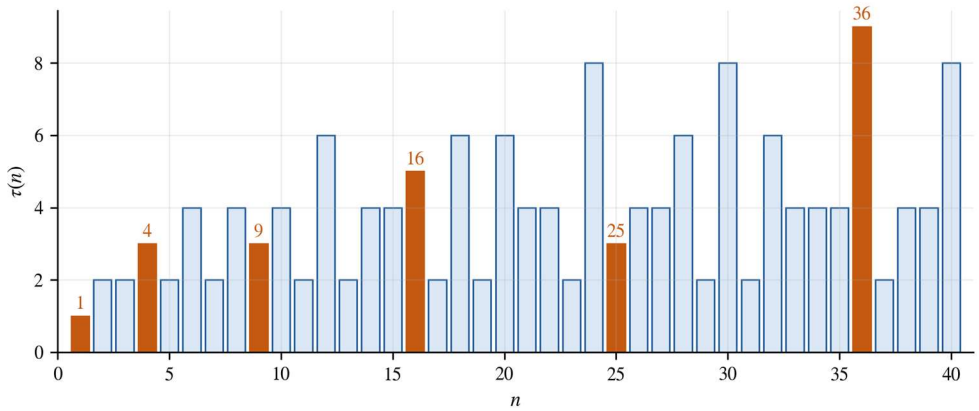
9.3 Problèmes de comptage de diviseurs

Exemple 9.3.1. *Déterminer le plus petit entier ayant exactement* 2026 *diviseurs.*

$2026 = 2 \times 1013$ avec 1013 premier. Les décompositions de 2026 en produit de facteurs > 1 sont 2026 et 2×1013. Donc $n = p^{2025}$ ou $n = p_1^{1012} p_2$. Dans chaque cas, le plus petit entier s'obtient avec les plus petits premiers, le plus grand exposant étant porté par le plus petit premier ($2^{1012} \cdot 3 < 3^{1012} \cdot 2$). Il reste à comparer 2^{2025} et $2^{1012} \cdot 3$: comme $3 < 2^{1013}$, le minimum est $n = 2^{1012} \cdot 3$.

Exemple 9.3.2. *Montrer que* $\tau(n)$ *est impair si, et seulement si,* n *est un carré parfait.*

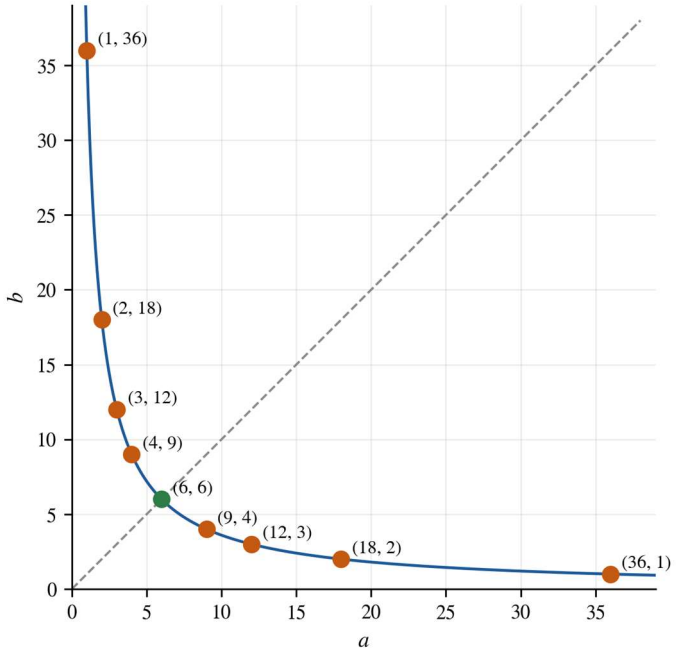
$\tau(n) = \prod(\alpha_i + 1)$ est impair si, et seulement si, tous les α_i sont pairs, si, et seulement si, n est un carré. (Interprétation directe : les diviseurs s'apparient par $d \leftrightarrow n/d$, et $d = n/d$ si, et seulement si, $d = \sqrt{n}$.)



Nombre de diviseurs τ(n) pour 1 ≤ n ≤ 40 : les valeurs impaires (en couleur) correspondent exactement aux carrés parfaits 1, 4, 9, 16, 25, 36.

Exemple 9.3.3. *Montrer que* $\prod_{d \mid n} d = n^{\tau(n)/2}$.

Notons P ce produit. En appariant d et n/d : $P^2 = \prod_{d \mid n} d \cdot \frac{n}{d} = n^{\tau(n)}$.



Les diviseurs de 36 sont les abscisses des points entiers de l'hyperbole ab = 36 ; la symétrie par rapport à la droite a = b réalise l'appariement d ↔ 36/d, et 6 = √36 est seul sur l'axe.

Définition 9.3.4 (Nombre parfait)

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

Théorème 9.3.5 (Euclide–Euler)

Un entier pair n est parfait si, et seulement si, $n = 2^{p-1}(2^p - 1)$ avec $2^p - 1$ premier.

Démonstration. Sens facile. Si $q = 2^p - 1$ est premier, $\sigma(2^{p-1}q) = (2^p - 1)(q + 1) = (2^p - 1)2^p = 2n$.

Réciproque. Écrivons $n = 2^k m$ avec m impair, $k \geq 1$. Par multiplicativité, $\sigma(n) = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m)$, et $\sigma(n) = 2n = 2^{k+1}m$. Comme $2^{k+1} - 1$ est impair, il est premier avec 2^{k+1}, donc (lemme de Gauss) $(2^{k+1} - 1) \mid m$; posons $m = (2^{k+1} - 1)M$. On obtient $\sigma(m) = 2^{k+1}M = m + M$. Or m et M sont deux diviseurs distincts de m (car $2^{k+1} - 1 \geq 3$), donc $\sigma(m) \geq m + M$, avec égalité si, et seulement si, ce sont les seuls diviseurs de m. Comme 1 divise m, cela impose $M = 1$, puis $\sigma(m) = m + 1$: $m = 2^{k+1} - 1$ n'a pour diviseurs que 1 et lui-même, il est premier. On conclut avec $p = k + 1$. ∎

Remarque.

On ignore toujours s'il existe un nombre parfait impair — c'est l'un des plus vieux problèmes ouverts des mathématiques.

9.4 Exercices

Exercice 9.1 ★. Calculer $\tau(720)$, $\sigma(720)$, $\varphi(720)$, $\mu(720)$.

Exercice 9.2 ★. Trouver tous les n tels que $\tau(n) = 6$ et $n < 100$.

Exercice 9.3 ★★. Montrer que $\sum_{d \mid n} \mu(d)\, \tau\left(\frac{n}{d}\right) = 1$ et $\sum_{d \mid n} \mu(d)\, \sigma\left(\frac{n}{d}\right) = n$.

Exercice 9.4 ★★. Montrer que $\sum_{d \mid n} \frac{\mu(d)^2}{\varphi(d)} = \frac{n}{\varphi(n)}$.

Exercice 9.5 ★★. Montrer que $\sigma(n)$ est impair si, et seulement si, n est un carré ou le double d'un carré.

Exercice 9.6 ★★★. Montrer que $\sum_{k=1}^{n} \operatorname{pgcd}(k, n) = \sum_{d \mid n} d\ \varphi\left(\frac{n}{d}\right)$.

Exercice 9.7 ★★★. Montrer que pour tout $n \geq 1$:

$$\sum_{d \mid n} \tau(d)^3 = \left(\sum_{d \mid n} \tau(d) \right)^2 .$$

9.5 Corrigés

Solution de l'exercice 9.1. $720 = 2^4 \cdot 3^2 \cdot 5$. $\tau = 5 \cdot 3 \cdot 2 = 30$. $\sigma = 31 \cdot 13 \cdot 6 = 2418$. $\varphi = 2^3(2-1) \cdot 3(3-1) \cdot (5-1) = 8 \cdot 6 \cdot 4 = 192$. $\mu(720) = 0$ (car $4 \mid 720$).

Solution de l'exercice 9.2. $\tau(n) = 6$ signifie $n = p^5$ ou $n = p^2 q$ (avec $p \neq q$ premiers). Pour $n < 100$: listons soigneusement les $p^2 q < 100$: $4 \cdot 3 = 12$, $4 \cdot 5 = 20$, $4 \cdot 7 = 28$, $4 \cdot 11 = 44$, $4 \cdot 13 = 52$, $4 \cdot 17 = 68$, $4 \cdot 19 = 76$, $4 \cdot 23 = 92$, $9 \cdot 2 = 18$, $9 \cdot 5 = 45$, $9 \cdot 7 = 63$, $9 \cdot 11 = 99$, $25 \cdot 2 = 50$, $25 \cdot 3 = 75$, $49 \cdot 2 = 98$. Plus $32 = 2^5$. Au total :

$$n \in \{12,18,20,28,32,44,45,50,52,63,68,75,76,92,98,99\}.$$

Solution de l'exercice 9.3. $\mu * \tau = \mu * \mathbf{1} * \mathbf{1} = \varepsilon * \mathbf{1} = \mathbf{1}$, donc la somme vaut 1. $\mu * \sigma = \mu * \mathbf{1} * \mathrm{Id} = \mathrm{Id}$, donc la somme vaut n.

Solution de l'exercice 9.4. La fonction $d \mapsto \mu(d)^2/\varphi(d)$ est multiplicative, donc sa fonction sommatoire F aussi. En p^α :

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

Donc $F(n) = n/\varphi(n)$.

Solution de l'exercice 9.5. σ est multiplicative, donc $\sigma(n)$ est impair si, et seulement si, $\sigma(p^\alpha)$ est impair pour tout $p^\alpha \parallel n$. Or $\sigma(p^\alpha) = 1 + p + \cdots + p^\alpha$ vaut $\alpha + 1$ modulo 2 si p est impair, et 1 si $p = 2$. Donc la condition est : α pair pour tout premier impair. Cela signifie $n = 2^k m^2$ avec m impair, soit n carré (si k pair) ou double d'un carré (si k impair).

Solution de l'exercice 9.6. Classons les $k \in \{1, \ldots, n\}$ selon $d = \mathrm{pgcd}(k, n)$: il y a $\varphi(n/d)$ valeurs de k pour chaque $d \mid n$. Donc

$$\sum_{k=1}^{n} \mathrm{pgcd}\,(k,n) = \sum_{d \mid n} d\ \varphi\left(\frac{n}{d}\right).$$

En particulier cette fonction $g = \mathrm{Id} * \varphi$ est multiplicative, avec $g(p^\alpha) = (\alpha+1)p^\alpha - \alpha p^{\alpha-1}$.

Solution de l'exercice 9.7. Les deux membres sont des fonctions multiplicatives de n : ce sont les fonctions sommatoires de τ^3 et de τ, la seconde étant élevée au carré, et la multiplicativité est stable par produit et par convolution avec $\mathbf{1}$. Il suffit donc de vérifier l'égalité sur $n = p^\alpha$.

Les diviseurs de p^α sont $1, p, \ldots, p^\alpha$, avec $\tau(p^k) = k + 1$. L'identité à démontrer devient

$$\sum_{k=0}^{\alpha} (k+1)^3 = \left(\sum_{k=0}^{\alpha} (k+1)\right)^2,$$

c'est-à-dire $1^3 + 2^3 + \cdots + N^3 = (1 + 2 + \cdots + N)^2$ avec $N = \alpha + 1$: c'est l'identité classique de Nicomaque, que l'on démontre en observant que

$$\left(\frac{m(m+1)}{2}\right)^2 - \left(\frac{(m-1)m}{2}\right)^2 = \frac{m^2}{4}[(m+1)^2 - (m-1)^2] = m^3,$$

et en sommant ces différences télescopiques pour $m = 1, \ldots, N$.

CHAPITRE 10

10 Partie entière et partie fractionnaire

Objectifs du chapitre.

- Manipuler $\lfloor x \rfloor$ et $\{x\}$ avec sûreté.
- Démontrer les identités classiques (Hermite, comptage de multiples).
- Utiliser la partie entière pour compter et pour encadrer.
- Traiter les problèmes de type « somme de parties entières ».

10.1 Propriétés de base

Définition 10.1.1 (Partie entière, partie fractionnaire)

Pour $x \in \mathbb{R}$, $\lfloor x \rfloor$ est l'unique entier n tel que $n \leq x < n+1$, et $\{x\} = x - \lfloor x \rfloor \in [0,1[$.

!\[Graphes de la partie entière (en escalier, fermée à gauche, ouverte à droite) et de la partie fractionnaire (en dents de scie, à valeurs dans [0, 1).

Proposition 10.1.2 (Règles de calcul)

Pour $x, y \in \mathbb{R}$ et $n \in \mathbb{Z}$:

(i) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$;

(ii) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$;

(iii) $\lfloor -x \rfloor = -\lfloor x \rfloor$ si $x \in \mathbb{Z}$, et $-\lfloor x \rfloor - 1$ sinon ;

(iv) $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor$ pour $n \geq 1$;

(v) pour $d \geq 1$ et $n \geq 1$, le nombre de multiples de d dans $\{1, \dots, n\}$ est $\lfloor n/d \rfloor$.

Démonstration. Tout repose sur la caractérisation : pour $m \in \mathbb{Z}$, $\lfloor x \rfloor = m \Leftrightarrow m \leq x < m+1$.

(i) De $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ on tire $\lfloor x \rfloor + n \leq x + n < \lfloor x \rfloor + n + 1$, et $\lfloor x \rfloor + n$ est entier.

(ii) $x + y = \lfloor x \rfloor + \lfloor y \rfloor + \{x\} + \{y\}$ avec $0 \leq \{x\} + \{y\} < 2$. Par (i), $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \{x\} + \{y\} \rfloor$, et le dernier terme vaut 0 ou 1.

(iii) Si $x \in \mathbb{Z}$, c'est clair. Sinon $\lfloor x \rfloor < x < \lfloor x \rfloor + 1$, donc $-\lfloor x \rfloor - 1 < -x < -\lfloor x \rfloor$, et $\lfloor -x \rfloor = -\lfloor x \rfloor - 1$.

(iv) Posons $m = \lfloor x/n \rfloor$: alors $mn \leq x < (m+1)n$. Comme mn est un entier $\leq x$, on a $mn \leq \lfloor x \rfloor$; et $\lfloor x \rfloor \leq x < (m+1)n$. Donc $m \leq \lfloor x \rfloor / n < m + 1$.

(v) Les multiples de d dans $\{1, \dots, n\}$ sont $d, 2d, \dots, kd$ où k est le plus grand entier tel que $kd \leq n$, c'est-à-dire $k \leq \frac{n}{d} < k + 1$: $k = \lfloor n/d \rfloor$. ∎

Attention.

$\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor$ en général ($x = y = 1/2$). En revanche, $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ pour n entier est toujours vrai. Ne confondez jamais les deux.

Théorème 10.1.3 (Identité d'Hermite)

Pour tout $x \in \mathbb{R}$ et $n \geq 1$:

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor.$$

Démonstration. Notons $f(x) = \sum_{k=0}^{n-1} \left\lfloor x + \frac{k}{n} \right\rfloor - \lfloor nx \rfloor$. Quand on remplace x par $x + \frac{1}{n}$, la somme devient $\sum_{k=1}^{n} \left\lfloor x + \frac{k}{n} \right\rfloor$: elle perd le terme $\lfloor x \rfloor$ et gagne le terme $\lfloor x + 1 \rfloor = \lfloor x \rfloor + 1$; elle augmente donc de 1. De même, $\left\lfloor n\left(x + \frac{1}{n}\right) \right\rfloor = \lfloor nx + 1 \rfloor = \lfloor nx \rfloor + 1$. Ainsi $f\left(x + \frac{1}{n}\right) = f(x)$: f est $\frac{1}{n}$-périodique.

Pour $x \in \left[0, \frac{1}{n}\right[$, on a $0 \leq x + \frac{k}{n} < \frac{k+1}{n} \leq 1$ pour $0 \leq k \leq n-1$, donc tous les termes de la somme sont nuls, et $0 \leq nx < 1$ donne $\lfloor nx \rfloor = 0$: $f(x) = 0$. Tout réel s'écrivant $x_0 + \frac{j}{n}$ avec $x_0 \in \left[0, \frac{1}{n}\right[$ et $j \in \mathbb{Z}$ (prendre $j = \lfloor nx \rfloor$), la périodicité donne $f \equiv 0$. ■

Exemple 10.1.4. *Calculer* $\sum_{k=1}^{100} \left\lfloor \frac{k}{3} \right\rfloor$.

Comptons : $\lfloor k/3 \rfloor$ vaut 0 pour $k = 1,2$; puis, pour $j \geq 1$, les k avec $\lfloor k/3 \rfloor = j$ sont $3j, 3j+1, 3j+2$, soit 3 valeurs, pour $j = 1, \ldots, 32$ (couvrant $k = 3$ à 98), puis $k = 99, 100$ donnent $j = 33$. Donc

$$S = 3\sum_{j=1}^{32} j + 2 \cdot 33 = 3 \cdot \frac{32 \cdot 33}{2} + 66 = 1584 + 66 = 1650.$$

10.2 La partie entière comme outil de comptage

Méthode 10.2.1 — Trois usages de la partie entière

Trois usages majeurs :

1. **Compter** : $\lfloor n/d \rfloor$ = nombre de multiples de d jusqu'à n. C'est la clé de la formule de Legendre et du crible.
2. **Encadrer** : $x - 1 < \lfloor x \rfloor \leq x$ transforme une identité exacte en inégalité exploitable.
3. **Discrétiser** : dans une équation faisant intervenir $\lfloor x \rfloor$, poser $x = n + \theta$ avec $n \in \mathbb{Z}$, $\theta \in [0,1[$.

Exemple 10.2.2. *Résoudre dans* $\mathbb{R}$ *:* $\lfloor x \rfloor \cdot \{x\} = 2026$.

Posons $n = \lfloor x \rfloor$, $\theta = \{x\} \in [0,1[$. Alors $n\theta = 2026$ avec $0 \leq n\theta < n$ (si $n > 0$). Donc $n > 2026$, soit $n \geq 2027$, et $\theta = 2026/n \in [0,1[$: toujours vrai pour $n \geq 2027$. Les solutions sont

$$x = n + \frac{2026}{n}, \qquad n \geq 2027 \text{ entier.}$$

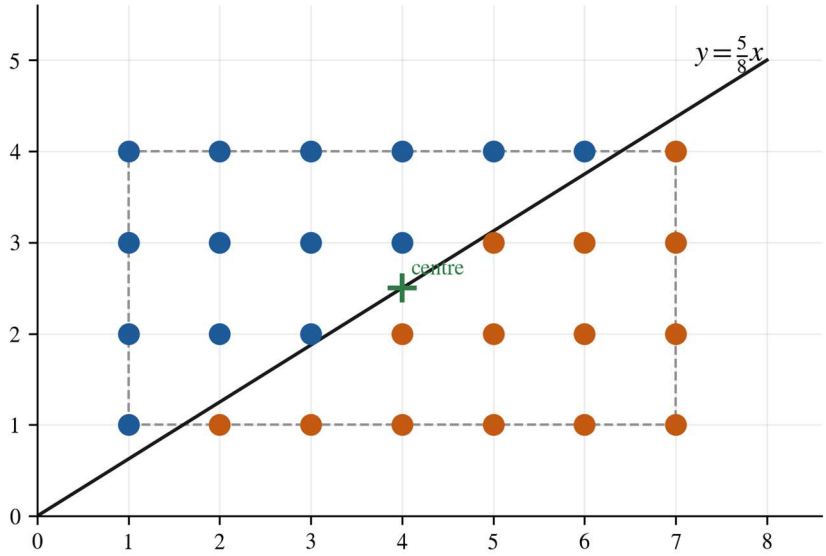
(Pour $n < 0$ le produit serait ≤ 0 ; pour $n = 0$ il vaut 0.)

Exemple 10.2.3 (Comptage des points sous une droite). *Soient* p, q *premiers entre eux. Montrer que*

$$\sum_{k=1}^{q-1} \left\lfloor \frac{kp}{q} \right\rfloor = \frac{(p-1)(q-1)}{2}.$$

La somme compte les points (k, ℓ) à coordonnées entières avec $1 \le k \le q-1$ et $1 \le \ell \le \frac{kp}{q}$ (il y en a $\left\lfloor \frac{kp}{q} \right\rfloor$ pour chaque k, et $\left\lfloor \frac{kp}{q} \right\rfloor \le p-1$ car $\frac{kp}{q} < p$), c'est-à-dire les points strictement sous la droite $y = \frac{p}{q}x$ dans le rectangle $[1, q-1] \times [1, p-1]$. Comme $\operatorname{pgcd}(p,q) = 1$, aucun point du rectangle n'est sur la droite : $q\ell = pk$ imposerait $q \mid k$ (lemme de Gauss), impossible pour $1 \le k \le q-1$. Par symétrie centrale (la transformation $(k, \ell) \mapsto (q-k, p-\ell)$ échange les points au-dessus et en dessous), il y en a exactement la moitié des $(p-1)(q-1)$ points du rectangle :

$$\frac{(p-1)(q-1)}{2}.$$

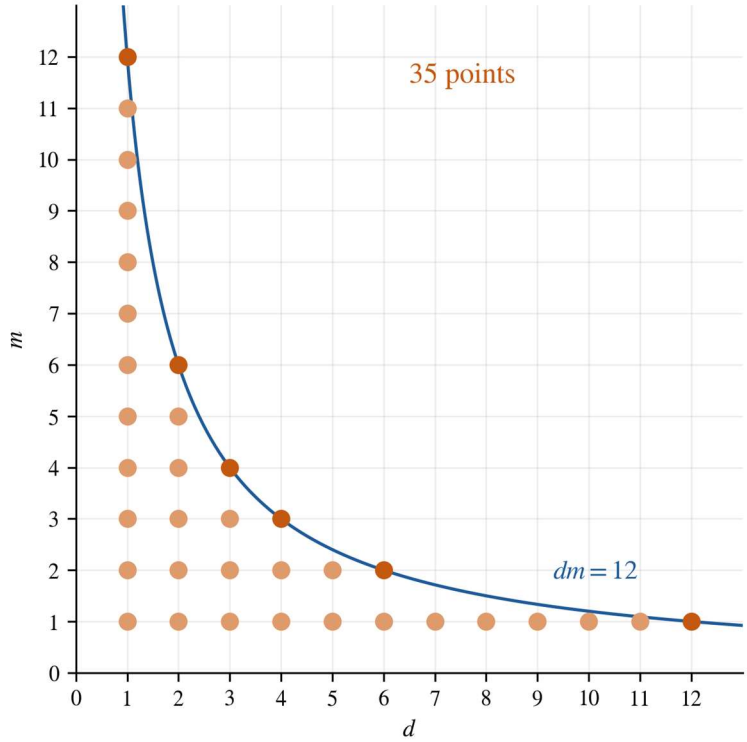


Points entiers sous la droite y = 5x/8 dans le rectangle [1, 7] × [1, 4] : la symétrie centrale de centre (4 ; 2,5) échange les 14 points situés sous la droite et les 14 points situés au-dessus.

Remarque.
C'est exactement le comptage qui apparaît dans la preuve d'Eisenstein de la loi de réciprocité quadratique (chapitre 8).

Exemple 10.2.4. *Montrer que* $\left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor = \sum_{k=1}^{n} \tau(k)$.

$\sum_{d=1}^{n} \lfloor n/d \rfloor$ compte les couples (d, m) d'entiers ≥ 1 avec $dm \le n$, c'est-à-dire $\sum_{k \le n} \#\{(d,m) : dm = k\} = \sum_{k \le n} \tau(k)$.



Pour n = 12, les points entiers (d, m) sous l'hyperbole dm = 12 : compter par colonnes donne Σ⌊12/d⌋, compter le long des hyperboles dm = k donne Σ τ(k) = 35.

10.3 Exercices

Exercice 10.1 ★. Calculer $\lfloor\sqrt{2026}\rfloor$ et $\sum_{k=1}^{2026}\left\lfloor\frac{2026}{k}\right\rfloor \bmod 2$.

Exercice 10.2 ★. Montrer que, pour tous réels x, y, $\lfloor 2x\rfloor+\lfloor 2y\rfloor \geq \lfloor x\rfloor+\lfloor y\rfloor+\lfloor x+y\rfloor$.

Exercice 10.3 ★★. Résoudre $\left\lfloor\frac{x-1}{2}\right\rfloor=\left\lfloor\frac{x}{3}\right\rfloor$ dans $\mathbb{Z}$.

Exercice 10.4 ★★. Montrer que pour tout $n \geq 1$, $\left\lfloor\sqrt{n}+\sqrt{n+1}\right\rfloor=\left\lfloor\sqrt{4n+2}\right\rfloor$.

Exercice 10.5 ★★. Déterminer la parité de $\sum_{k=1}^{n}\left\lfloor\frac{n}{k}\right\rfloor$.

Exercice 10.6 ★★★ (Théorème de Beatty). Soient $\alpha, \beta > 0$ irrationnels avec $\frac{1}{\alpha}+\frac{1}{\beta}=1$. Montrer que les suites $(\lfloor n\alpha\rfloor)_{n\geq 1}$ et $(\lfloor n\beta\rfloor)_{n\geq 1}$ partitionnent $\mathbb{N}^*$.

10.4 Corrigés

Solution de l'exercice 10.1. $45^2=2025\leq 2026<2116=46^2$, donc $\lfloor\sqrt{2026}\rfloor=45$.

Pour la somme : $\sum_{k\leq n}\lfloor n/k\rfloor=\sum_{k\leq n}\tau(k)$ (exemple 10.2.4). Or $\tau(k)$ est impair si, et seulement si, k est un carré. Le nombre de carrés ≤ 2026 est 45, donc la somme est $\equiv 45\equiv 1 \pmod 2$: elle est impaire.

Solution de l'exercice 10.2. Voir le corrigé de l'exemple 3.3.3 sur $\frac{(2m)!\,(2n)!}{m!\,n!\,(m+n)!}$ (chapitre 3) : on se ramène aux parties fractionnaires et on distingue selon que $\{x\}+\{y\}<1$ ou ≥ 1.

Précisément, posons $u = \{x\}$, $v = \{y\}$. Par la règle (i), les parties entières de x et y s'éliminent des deux membres et l'inégalité équivaut à $\lfloor 2u \rfloor + \lfloor 2v \rfloor \geq \lfloor u + v \rfloor$. Si $u + v < 1$, le membre de droite est nul. Si $u + v \geq 1$, il vaut 1, et l'un des deux nombres u, v est $\geq \frac{1}{2}$, donc le membre de gauche est ≥ 1.

Solution de l'exercice 10.3. Posons t la valeur commune. Alors

$$2t \leq x - 1 < 2t + 2 \qquad \text{et} \qquad 3t \leq x < 3t + 3.$$

Donc $x \in [2t + 1, 2t + 3[\cap [3t, 3t + 3[$. Cette intersection contient un entier si, et seulement si, $3t \leq 2t + 2$ et $2t + 1 \leq 3t + 2$, c'est-à-dire $-1 \leq t \leq 2$. On énumère (en ne gardant que les entiers) : $t = -1 : x \in [-1,1[\cap [-3,0[$, soit $x = -1$; $t = 0 : x \in [1,3[\cap [0,3[$, soit $x \in \{1,2\}$; $t = 1 : x \in [3,5[\cap [3,6[$, soit $x \in \{3,4\}$; $t = 2 : x \in [5,7[\cap [6,9[$, soit $x = 6$. D'où

$$x \in \{-1,1,2,3,4,6\}.$$

Solution de l'exercice 10.4. On a $\left(\sqrt{n} + \sqrt{n+1}\right)^2 = 2n + 1 + 2\sqrt{n(n+1)}$ et $4n + 2 = 2n + 1 + (2n + 1)$. Comme

$$2n = 2\sqrt{n \cdot n} < 2\sqrt{n(n+1)} < 2n + 1,$$

la dernière inégalité étant l'inégalité arithmético-géométrique stricte $\sqrt{n(n+1)} < \frac{n+(n+1)}{2}$, on obtient $4n + 1 < \left(\sqrt{n} + \sqrt{n+1}\right)^2 < 4n + 2$. Il suffit donc de montrer qu'aucun carré parfait n'est dans $]4n + 1, 4n + 2]$, ce qui revient à dire que $4n + 2$ n'est pas un carré : en effet un carré est $\equiv 0,1 \pmod 4$. Donc $\lfloor \sqrt{4n+1} \rfloor = \lfloor \sqrt{4n+2} \rfloor$, et comme $\sqrt{4n+1} < \sqrt{n} + \sqrt{n+1} < \sqrt{4n+2}$, les parties entières coïncident.

Solution de l'exercice 10.5. $\sum_{k=1}^{n} \lfloor n/k \rfloor = \sum_{k=1}^{n} \tau(k)$, et $\tau(k)$ est impair si, et seulement si, k est un carré. Donc la somme a la parité de $\lfloor \sqrt{n} \rfloor$, le nombre de carrés entre 1 et n.

Solution de l'exercice 10.6. Comme $\frac{1}{\alpha} + \frac{1}{\beta} = 1$ avec $\alpha, \beta > 0$, on a $\alpha, \beta > 1$; les deux suites sont donc strictement croissantes. Fixons $N \geq 1$. Le nombre de $n \geq 1$ tels que $\lfloor n\alpha \rfloor \leq N$ est le nombre de n avec $n\alpha < N + 1$ (l'égalité est exclue par irrationalité), soit $\left\lfloor \frac{N+1}{\alpha} \right\rfloor$. De même pour β. Or

$$\left\lfloor \frac{N+1}{\alpha} \right\rfloor + \left\lfloor \frac{N+1}{\beta} \right\rfloor = \frac{N+1}{\alpha} - \left\{ \frac{N+1}{\alpha} \right\} + \frac{N+1}{\beta} - \left\{ \frac{N+1}{\beta} \right\},$$

c'est-à-dire

$$\left\lfloor \frac{N+1}{\alpha} \right\rfloor + \left\lfloor \frac{N+1}{\beta} \right\rfloor = (N+1) - \left\{ \frac{N+1}{\alpha} \right\} - \left\{ \frac{N+1}{\beta} \right\}.$$

Les deux parties fractionnaires sont non nulles et de somme entière (car $\frac{N+1}{\alpha} + \frac{N+1}{\beta} = N + 1$), donc leur somme vaut 1. Ainsi le nombre total de termes $\leq N$ dans les deux suites réunies est exactement N (ce qui reste vrai pour $N = 0$, puisque tous les termes sont ≥ 1). En comparant les rangs N et $N - 1$, on voit que chaque entier $N \geq 1$ apparaît exactement une fois dans la réunion des deux suites.

PARTIE IV — Équations diophantiennes

CHAPITRE 11

11 Méthodes générales de résolution

Objectifs du chapitre.

- Résoudre complètement l'équation linéaire $ax + by = c$.
- Maîtriser les cinq grandes méthodes : factorisation, congruences, bornes, paramétrisation, monotonie.
- Savoir choisir la méthode adaptée à la forme de l'équation.

11.1 L'équation linéaire

Théorème 11.1.1 (Équation linéaire à deux inconnues)

L'équation $ax + by = c$ (avec a, b non tous deux nuls) admet des solutions entières si, et seulement si, $d = \gcd(a, b)$ divise c. Dans ce cas, si (x_0, y_0) est une solution particulière, l'ensemble des solutions est

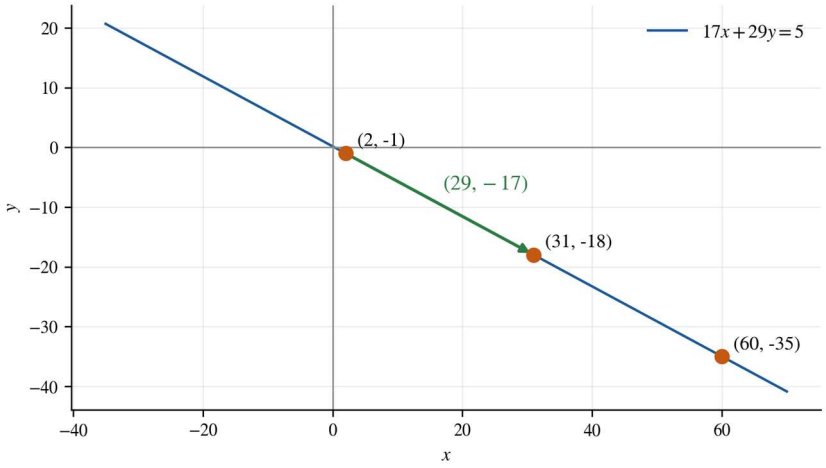
$$\left\{\left(x_0 + \frac{b}{d}t,\ y_0 - \frac{a}{d}t\right) : t \in \mathbb{Z}\right\}.$$

Démonstration. L'existence découle de Bézout : si $au + bv = d$ et $d \mid c$, alors $(x_0, y_0) = \left(\frac{c}{d}u, \frac{c}{d}v\right)$ est solution ; réciproquement, d divise $ax + by$ pour tous entiers x, y. Si (x, y) et (x_0, y_0) sont solutions, alors $a(x - x_0) = -b(y - y_0)$. En divisant par d : $\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0)$ avec $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, donc $\frac{b}{d} \mid x - x_0$ par Gauss. En écrivant $x - x_0 = \frac{b}{d}t$, on obtient $y - y_0 = -\frac{a}{d}t$. Inversement, ces couples sont bien solutions. ■

Exemple 11.1.2. *Résoudre* $17x + 29y = 5$ *en entiers.*

$\gcd(17,29) = 1$. Euclide : $29 = 17 + 12$, $17 = 12 + 5$, $12 = 2 \cdot 5 + 2$, $5 = 2 \cdot 2 + 1$. En remontant : $1 = 5 - 2 \cdot 2 = 5 - 2(12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12 = 5(17 - 12) - 2 \cdot 12 = 5 \cdot 17 - 7 \cdot 12 = 5 \cdot 17 - 7(29 - 17) = 12 \cdot 17 - 7 \cdot 29$. Donc $17 \cdot 12 + 29 \cdot (-7) = 1$, et en multipliant par 5 : $(x_0, y_0) = (60, -35)$. Les solutions sont

$$(x, y) = (60 + 29t,\ -35 - 17t), \qquad t \in \mathbb{Z}.$$



Les solutions entières de 17x + 29y = 5 sont les points entiers de la droite, régulièrement espacés du vecteur (29, −17) ; entre deux solutions consécutives, la droite ne rencontre aucun autre point entier.

11.2 Méthode 1 : la factorisation

Méthode 11.2.1 — Factorisation

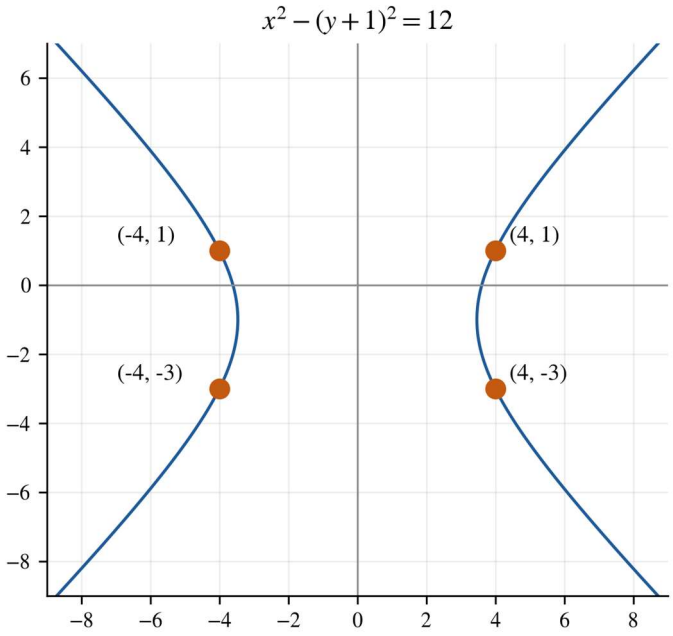
Ramener l'équation à $\prod A_i = N$ avec A_i entiers et N constant, puis énumérer les factorisations de N. Techniques utiles :

- multiplier par une constante pour compléter un produit (truc de Simon) ;
- reconnaître $x^2 - y^2$, $x^3 \pm y^3$, Sophie Germain ;
- isoler une variable puis chasser les dénominateurs.

Exemple 11.2.2. *Résoudre $x^2 = y^2 + 2y + 13$ en entiers.*

$x^2 = (y+1)^2 + 12$, donc $x^2 - (y+1)^2 = 12$, soit $(x - y - 1)(x + y + 1) = 12$. Les deux facteurs ont même parité (leur somme $2x$ est paire), donc sont tous deux pairs : $(2,6)$, $(6,2)$, $(-2,-6)$, $(-6,-2)$. On obtient

$$(x, y) \in \{(4,1), (4,-3), (-4,1), (-4,-3)\}.$$



L'hyperbole x² − (y + 1)² = 12 et ses quatre points entiers (±4, 1) et (±4, −3), obtenus par factorisation de 12 en deux facteurs pairs.

Exemple 11.2.3. *Trouver tous les entiers n tels que $n^2+19n+92$ soit un carré parfait.*

Posons $n^2+19n+92=k^2$ avec $k\geq 0$. En multipliant par 4 : $(2n+19)^2+7=4k^2$, soit $(2k-2n-19)(2k+2n+19)=7$. Les factorisations de 7 : $(1,7)$ et $(-7,-1)$ (et leurs symétriques). De $2k-2n-19=1,\ 2k+2n+19=7$ on tire $4k=8,\ k=2,\ 4n+38=6,\ n=-8$. Le cas $(7,1)$ donne $n=-11$; les cas négatifs donneraient $k<0$. On vérifie : $n=-8$: $64-152+92=4=2^2$ ✓ ; $n=-11$: $121-209+92=4$ ✓.

11.3 Méthode 2 : les congruences

Méthode 11.3.1 — Congruences

Réduire modulo un entier bien choisi pour obtenir une contradiction ou une contrainte. Rappel du dictionnaire des modules (chapitre 4) : carrés → modules $4,8,3,5,16$; cubes → $9,7$; puissances k-ièmes → premier p avec $k \mid p-1$.

Exemple 11.3.2. *Montrer que $x^2+y^2=3z^2$ n'a que la solution nulle.*

Supposons qu'il existe une solution entière non nulle, et choisissons-en une avec $x^2+y^2+z^2\geq 1$ minimal (principe du bon ordre). Modulo 3 : $x^2+y^2\equiv 0$, et les carrés valent $0,1$ modulo 3. Donc $x\equiv y\equiv 0\pmod 3$. Écrivons $x=3x'$, $y=3y'$: $9x'^2+9y'^2=3z^2$, donc $3(x'^2+y'^2)=z^2$ et $3\mid z$, $z=3z'$. On obtient $x'^2+y'^2=3z'^2$, solution non nulle avec une somme $x'^2+y'^2+z'^2$ strictement plus petite : contradiction.

Exemple 11.3.3. *Résoudre $x^3+y^3+z^3=2026$ modulo 9 : que peut-on dire ?*

Les cubes valent $0,\pm 1$ modulo 9, donc $x^3+y^3+z^3\in\{-3,\dots,3\}$ modulo 9. Or $2026=9\cdot 225+1$, donc $2026\equiv 1$: compatible. La congruence ne suffit donc pas à conclure — c'est un exemple où la méthode échoue, et il faut chercher autre chose. (En revanche, $x^3+y^3+z^3=4$ ou 5 est impossible car $4,5\equiv\pm 4\pmod 9$.)

À retenir

Une congruence qui « passe » ne prouve rien. Ne concluez jamais à l'existence de solutions à partir d'un test modulaire : il ne fournit que des obstructions.

11.4 Méthode 3 : bornes et inégalités

Méthode 11.4.1 — Bornes et inégalités

Encadrer une inconnue entre deux puissances consécutives, ou montrer qu'une expression est strictement comprise entre deux carrés consécutifs — auquel cas elle ne peut être un carré.

Exemple 11.4.2. *Montrer que $n^4+n^3+n^2+n+1$ n'est un carré parfait que pour $n=3$ (et $n=0,-1$).*

Notons $N=n^4+n^3+n^2+n+1$. Pour $n=0$, $N=1$ est un carré. Pour $n\neq 0$, comparons $4N$ avec $(2n^2+n)^2$ (remarquons que $2n^2+n=n(2n+1)\geq 0$). On a

$$4(n^4+n^3+n^2+n+1)=(2n^2+n)^2+3n^2+4n+4>(2n^2+n)^2,$$

car $3n^2+4n+4=2n^2+(n+2)^2>0$, et

$$(2n^2+n+2)^2=4n^4+4n^3+9n^2+4n+4>4n^4+4n^3+4n^2+4n+4\Leftrightarrow 5n^2>0.$$

Donc $(2n^2+n)^2<4N<(2n^2+n+2)^2$. Si $N=k^2$ avec $k\geq 0$, alors $4N=(2k)^2$ et, les trois nombres $2n^2+n$, $2k$, $2n^2+n+2$ étant positifs, $2n^2+n<2k<2n^2+n+2$; donc $2k=2n^2+n+1$ et $4N=(2n^2+n+1)^2$, ce qui donne, en développant, $4n^4+4n^3+4n^2+4n+4=4n^4+4n^3+5n^2+2n+1$, c'est-à-dire

$$n^2-2n-3=0\Leftrightarrow n=3 \text{ ou } n=-1.$$

Réciproquement, $n=3$ donne $N=121=11^2$ ✓ et $n=-1$ donne $N=1$ ✓.

Exemple 11.4.3. *Résoudre en entiers strictement positifs : $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1$.*

Supposons $x\leq y\leq z$. Alors $1\leq\frac{3}{x}$, donc $x\leq 3$; et $\frac{1}{x}<1$ donc $x\geq 2$.

- $x=2$: $\frac{1}{y}+\frac{1}{z}=\frac{1}{2}$ avec $y\leq z$, donc $y\leq 4$ et $y\geq 3$. $y=3\Rightarrow z=6$; $y=4\Rightarrow z=4$.
- $x=3$: $\frac{1}{y}+\frac{1}{z}=\frac{2}{3}$, donc $y\leq 3$ et $y\geq 2$, mais $y\geq x=3$: $y=3$, $z=3$.

Solutions (à permutation près) : $(2,3,6)$, $(2,4,4)$, $(3,3,3)$.

À retenir (Le réflexe « ordonner les variables »)

Dans une équation symétrique, supposer $x\leq y\leq z$ ne coûte rien et borne immédiatement la plus petite variable. C'est le premier geste à faire.

11.5 Méthode 4 : paramétrisation

Exemple 11.5.1. *Trouver tous les points rationnels du cercle $x^2+y^2=1$.*

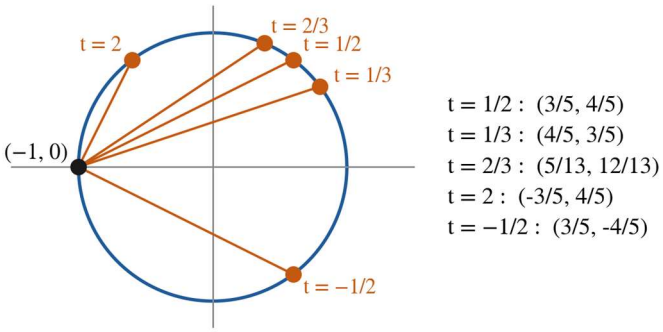
Soit (x, y) un point rationnel du cercle, distinct de $(-1,0)$. La droite passant par $(-1,0)$ et (x, y) a une pente rationnelle $t = \frac{y}{x+1}$. Réciproquement, en intersectant la droite $y = t(x + 1)$ avec le cercle :

$$x^2 + t^2(x + 1)^2 = 1 \Longrightarrow (x + 1)[(x - 1) + t^2(x + 1)] = 0,$$

d'où

$$x = \frac{1 - t^2}{1 + t^2}, \qquad y = \frac{2t}{1 + t^2}.$$

Le facteur $x + 1$ est non nul puisque $(x, y) \neq (-1,0)$ (si $x = -1$, alors $y = 0$). Réciproquement, pour tout $t \in \mathbb{Q}$, ces formules définissent un point rationnel, et il est sur le cercle car $(1 - t^2)^2 + (2t)^2 = (1 + t^2)^2$. Tous les points rationnels du cercle autres que $(-1,0)$ s'obtiennent donc ainsi, t décrivant $\mathbb{Q}$, et la correspondance $t \leftrightarrow (x, y)$ est bijective.



Paramétrisation rationnelle du cercle unité : la droite de pente t issue de (−1, 0) recoupe le cercle en un point rationnel si, et seulement si, t est rationnel (ici t = 1/2, 1/3, 2/3, 2 et −1/2).

> **Remarque.**
> Cette « projection stéréographique » est le mécanisme profond derrière la paramétrisation des triplets pythagoriciens (chapitre suivant).

11.6 Méthode 5 : monotonie et descente

Traitée au chapitre 12 (descente infinie) et au chapitre 16 (saut de Viète).

11.7 Exercices

Exercice 11.1 ★. Résoudre $6x + 15y = 27$ en entiers.

Exercice 11.2 ★. Résoudre $\frac{1}{x} + \frac{1}{y} = \frac{1}{12}$ en entiers strictement positifs.

Exercice 11.3 ★★. Résoudre $x^2 + y^2 = 2026$ en entiers.

Exercice 11.4 ★★. Résoudre $2^x - 3^y = 1$ et $3^x - 2^y = 1$ en entiers positifs.

Exercice 11.5 ★★. Montrer que $x! + y! = z!$ n'a, en entiers strictement positifs, que la solution $(1,1,2)$.

Exercice 11.6 ★★★. Résoudre $x^2 + y^2 + z^2 = 2xyz$ en entiers.

Exercice 11.7 ★★★ (IMO 2006, problème 4). Déterminer tous les couples (x, y) d'entiers tels que $1 + 2^x + 2^{2x+1} = y^2$.

11.8 Corrigés

Solution de l'exercice 11.1. $\gcd(6,15) = 3$ divise 27. On simplifie : $2x + 5y = 9$. Solution particulière : $(x, y) = (2,1)$. Solutions générales : $(2 + 5t, 1 - 2t)$, $t \in \mathbb{Z}$.

Solution de l'exercice 11.2. En multipliant par $12xy$: $12(x + y) = xy$, soit $xy - 12x - 12y = 0$, soit $(x - 12)(y - 12) = 144$.

Nécessairement $x > 12$: si $x \leq 12$ alors $\frac{1}{x} \geq \frac{1}{12}$ et $\frac{1}{x} + \frac{1}{y} > \frac{1}{12}$. De même $y > 12$. Les deux facteurs sont donc des diviseurs positifs de 144, qui en compte 15 ; on obtient les 15 solutions

$$(x, y) \in \{(13,156), (14,84), (15,60), (16,48), (18,36), (20,30), (21,28), (24,24)\}$$

et leurs symétriques.

Solution de l'exercice 11.3. $2026 = 2 \cdot 1013$. Or 1013 est premier et $1013 \equiv 1 \pmod 4$, donc 1013 est somme de deux carrés : $1013 = 22^2 + 23^2 = 484 + 529$ ✓. Par l'identité de Brahmagupta–Fibonacci, $2 \cdot 1013 = (1^2 + 1^2)(22^2 + 23^2) = (22 + 23)^2 + (22 - 23)^2 = 45^2 + 1^2$. Donc $2026 = 45^2 + 1^2$. Comme 1013 est premier, cette écriture est unique à l'ordre et aux signes près : $(x, y) = (\pm 45, \pm 1)$ et $(\pm 1, \pm 45)$, soit 8 solutions.

Solution de l'exercice 11.4. $2^x - 3^y = 1$. Si $y = 0$: $2^x = 2$, $x = 1$. Si $y \geq 1$, modulo 3 : $2^x \equiv 1$, donc x est pair, $x = 2u$. Alors $(2^u - 1)(2^u + 1) = 3^y$. Les deux facteurs sont premiers entre eux (différence 2, tous deux impairs), donc $2^u - 1 = 1$ et $2^u + 1 = 3^y$: $u = 1$, $3^y = 3$, $y = 1$. Solutions : $(x, y) = (2,1)$ et $(1,0)$.

$3^x - 2^y = 1$. Modulo 8 pour $y \geq 3$: $3^x \equiv 1 \pmod 8$ donc x pair, $x = 2u$, et $(3^u - 1)(3^u + 1) = 2^y$. Les deux facteurs sont des puissances de 2 paires, de PGCD 2, donc $3^u - 1 = 2$ et $3^u + 1 = 2^{y-1}$: $u = 1$, $4 = 2^{y-1}$, $y = 3$, $x = 2$. Pour $y \leq 2$: $y = 0$ donne $3^x = 2$, impossible ; $y = 1$ donne $3^x = 3$, $x = 1$; $y = 2$ donne $3^x = 5$, impossible. Solutions : $(1,1)$ et $(2,3)$.

> **Remarque.**
> Ce sont les cas élémentaires du théorème de Mihăilescu (ex-conjecture de Catalan, 2002) : la seule solution de $a^p - b^q = 1$ avec $a, b, p, q \geq 2$ est $3^2 - 2^3 = 1$.

Solution de l'exercice 11.5. Par symétrie, supposons $x \leq y$. Alors $z > y$ (car $z! > y!$), donc $z \geq y + 1$ et $z! \geq (y + 1)\, y!$. Or $x! + y! \leq 2\, y!$, donc $y + 1 \leq 2$, soit $y \leq 1$: $y = 1$, $x = 1$, $z! = 2$, $z = 2$.

Solution de l'exercice 11.6. Seule solution : $(0,0,0)$. Montrons plus généralement, pour tout entier $k \geq 1$, que si $x^2 + y^2 + z^2 = 2^k xyz$, alors x, y, z sont pairs.

Le membre de droite est pair, donc $x^2 + y^2 + z^2$ est pair : le nombre d'impairs parmi x, y, z est 0 ou 2. Si deux sont impairs, disons x, y, alors z est pair et $x^2 + y^2 + z^2 \equiv 1 + 1 + 0 = 2 \pmod 4$, alors que $2^k xyz$ est divisible par 4 (car z est pair) : contradiction. Donc x, y, z sont tous pairs.

Écrivons alors $x = 2x'$, $y = 2y'$, $z = 2z'$: $4(x'^2 + y'^2 + z'^2) = 2^k \cdot 8x'y'z'$, soit $x'^2 + y'^2 + z'^2 = 2^{k+1} x'y'z'$, équation du même type. En partant de $k = 1$ et en itérant, on voit que x, y, z sont divisibles par 2^j pour tout j : c'est la descente infinie, et donc $x = y = z = 0$.

Solution de l'exercice 11.7. Réponse : $(x, y) = (0, \pm 2)$ et $(4, \pm 23)$.

Si $x \leq -2$, alors $0 < 2^x + 2^{2x+1} < 1$ et le membre de gauche n'est pas entier ; si $x = -1$, il vaut 2, qui n'est pas un carré. Quitte à changer y en $-y$, supposons $y > 0$. Pour $x = 0$: $1 + 1 + 2 = 4 = 2^2$ ✓. Supposons $x \geq 1$. L'équation s'écrit

$$2^x(1 + 2^{x+1}) = y^2 - 1 = (y - 1)(y + 1).$$

y est impair, $y = 2k + 1$, donc $(y-1)(y+1) = 4k(k+1)$ avec $k(k+1)$ pair : $v_2(y^2-1) \geq 3$, donc $x \geq 3$. Écrivons $y - 1 = 2a$, $y + 1 = 2b$ avec $b = a + 1$, $a \geq 1$, ab pair, donc

$$2^{x-2}(1 + 2^{x+1}) = a(a+1).$$

Comme $1 + 2^{x+1}$ est impair et que a, $a + 1$ sont premiers entre eux, 2^{x-2} divise a ou $a + 1$.

Cas 1 : $a = 2^{x-2}m$. Alors $m(a+1) = 1 + 2^{x+1}$ avec $a + 1 = 2^{x-2}m + 1$, donc $m(2^{x-2}m + 1) = 1 + 2^{x+1}$, soit $2^{x-2}m^2 + m - 1 = 2^{x+1}$, c'est-à-dire $m - 1 = 2^{x-2}(8 - m^2)$. Comme $m \geq 1$, il faut $m^2 \leq 8$, donc $m \in \{1,2\}$; m est impair (car m divise $1 + 2^{x+1}$), et $m = 1$ donne $0 = 7 \cdot 2^{x-2}$: impossible. (Avec $m = 2$ on aurait d'ailleurs $1 = 4 \cdot 2^{x-2}$, impossible.)

Cas 2 : $a + 1 = 2^{x-2}m$. Alors $am = 1 + 2^{x+1}$ avec $a = 2^{x-2}m - 1$: $m(2^{x-2}m - 1) = 1 + 2^{x+1}$, soit $2^{x-2}m^2 - m - 1 = 2^{x+1}$, donc $m + 1 = 2^{x-2}(m^2 - 8)$. Comme $m + 1 > 0$, $m \geq 3$. Comme $x \geq 3$, on a $m + 1 \geq 2(m^2 - 8)$, soit $2m^2 - m - 17 \leq 0$, ce qui impose $m \leq 3$. Donc $m = 3$: $4 = 2^{x-2} \cdot 1$, donc $x = 4$, $a + 1 = 4 \cdot 3 = 12$, $a = 11$, $y = 2a + 1 = 23$ ✓ (en effet $1 + 16 + 512 = 529 = 23^2$).

Conclusion : $(x, y) \in \{(0, \pm 2), (4, \pm 23)\}$.

CHAPITRE 12

12 Triplets pythagoriciens et descente infinie

Objectifs du chapitre.

- Paramétrer complètement les triplets pythagoriciens.
- Comprendre et appliquer la méthode de descente infinie de Fermat.
- Démontrer le cas $n = 4$ du grand théorème de Fermat.

12.1 L'équation de Pythagore

Définition 12.1.1 (Triplet pythagoricien)

Un triplet pythagoricien est un triplet (a, b, c) d'entiers strictement positifs avec $a^2 + b^2 = c^2$. Il est primitif si $\gcd(a, b, c) = 1$.

Théorème 12.1.2 (Paramétrisation des triplets pythagoriciens)

Les triplets pythagoriciens primitifs avec b pair sont exactement

$$a = m^2 - n^2, \qquad b = 2mn, \qquad c = m^2 + n^2,$$

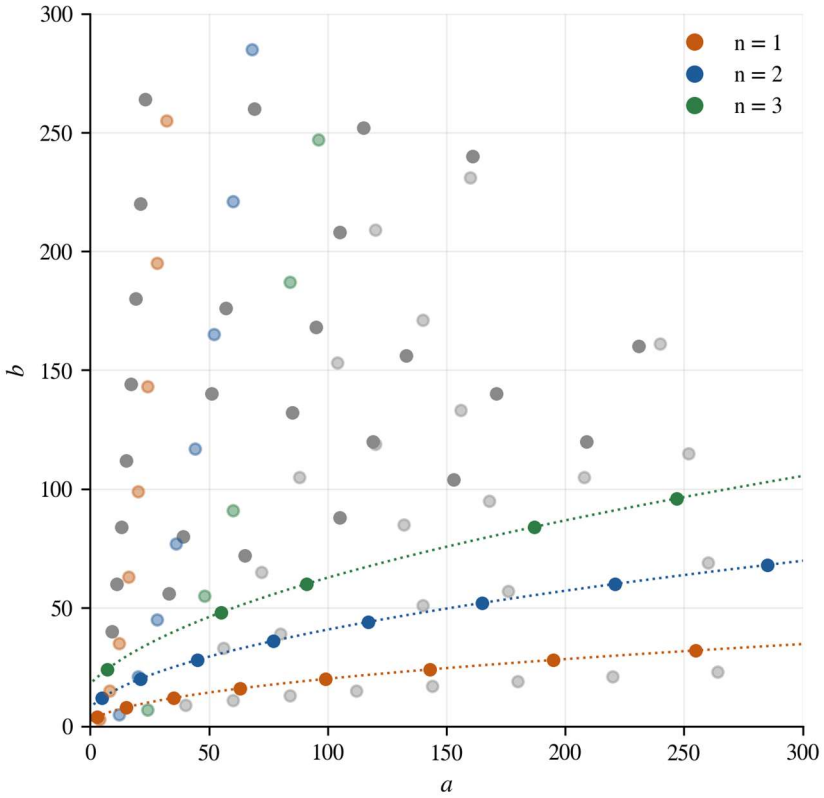
où $m > n \geq 1$, $\gcd(m, n) = 1$ et $m \not\equiv n \pmod 2$.

Démonstration. Ces triplets conviennent : $(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$. Ce sont des entiers strictement positifs puisque $m > n \geq 1$. Ils sont primitifs : un premier p divisant a et c diviserait $c + a = 2m^2$ et $c - a = 2n^2$; comme c est impair (car m, n de parités différentes), p est impair et diviserait m et n : exclu.

Réciproque. Soit (a, b, c) primitif. a et b ne peuvent être tous deux pairs (primitivité) ni tous deux impairs (sinon $c^2 \equiv 2 \pmod 4$). Supposons a impair, b pair ; alors c est impair. Écrivons

$$\left(\frac{b}{2}\right)^2 = \frac{c - a}{2} \cdot \frac{c + a}{2}.$$

Les deux facteurs sont des entiers premiers entre eux : un diviseur commun d diviserait leur somme c et leur différence a, donc $d \mid \gcd(a, c) = 1$ (un premier divisant a et c diviserait b^2, donc b, contredisant la primitivité). Leur produit étant un carré, chacun est un carré (lemme du produit, ci-dessous) : $\frac{c+a}{2} = m^2$, $\frac{c-a}{2} = n^2$ avec $m > n \geq 1$. D'où $c = m^2 + n^2$, $a = m^2 - n^2$, $b = 2mn$, avec $m, n \geq 1$ (car $c > a$) et $m > n$ (car $a > 0$) ; $\gcd(m, n) = 1$, puisqu'un diviseur commun diviserait $m^2 = \frac{c+a}{2}$ et $n^2 = \frac{c-a}{2}$, premiers entre eux ; et $m \not\equiv n \pmod 2$ (sinon $c = m^2 + n^2$ serait pair). ∎



Les triplets pythagoriciens primitifs (a, b) avec c ≤ 300 : chaque point correspond à un couple (m, n) premiers entre eux de parités différentes ; pour n fixé, les points décrivent une parabole (en pointillés pour n = 1, 2, 3).

À retenir (Le lemme du produit)

Si $uv = w^k$ avec $\gcd(u, v) = 1$ et $u, v > 0$, alors u et v sont des puissances k-ièmes. Ce lemme (démontré par les valuations p-adiques) est le moteur de toutes les paramétrisations. Il apparaît dans presque tous les problèmes d'équations diophantiennes de niveau IMO.

Lemme (Lemme du produit)

Soient $k \geq 2$ et $u_1, \ldots, u_r$ des entiers strictement positifs deux à deux premiers entre eux. Si $u_1 u_2 \cdots u_r$ est une puissance k-ième, alors chaque u_i est une puissance k-ième.

Démonstration. Soit p un nombre premier. Comme les u_i sont deux à deux premiers entre eux, p divise au plus l'un d'eux, disons u_j (s'il n'en divise aucun, toutes les valuations en p sont nulles). Alors, par la proposition 3.2.2 (i), $v_p(u_j) = v_p(u_1 \cdots u_r) = k\, v_p(w)$ est un multiple de k, et $v_p(u_i) = 0$ pour $i \neq j$. Toutes les valuations de chaque u_i sont donc multiples de k, et $u_i = \left(\prod_p p^{v_p(u_i)/k}\right)^k$. ■

Attention.

L'hypothèse de positivité est indispensable pour k pair ($(-1)(-4) = 2^2$), et l'hypothèse de co-primalité aussi ($2 \cdot 8 = 4^2$).

12.2 La descente infinie

Méthode 12.2.1 — Descente infinie de Fermat

Pour montrer qu'une équation n'a pas de solution en entiers positifs :

1. supposer qu'il en existe une, et choisir celle qui minimise une quantité positive (par exemple c, ou $x+y+z$) ;
2. construire à partir d'elle une solution strictement plus petite ;
3. conclure à une contradiction (une suite strictement décroissante d'entiers positifs n'existe pas).

Théorème 12.2.2 (Fermat, cas n = 4)

L'équation $x^4+y^4=z^2$ n'a pas de solution en entiers strictement positifs. En particulier, $x^4+y^4=z^4$ n'en a pas non plus.

Démonstration. Supposons qu'il existe des solutions et choisissons-en une, (x,y,z), avec z minimal.

Réduction au cas primitif. Soit $g=\gcd(x,y)$. Alors $g^4 \mid z^2$, donc $4v_p(g)\le 2v_p(z)$ pour tout p, c'est-à-dire $g^2 \mid z$ (proposition 3.2.2). Le triplet $\left(\frac{x}{g},\frac{y}{g},\frac{z}{g^2}\right)$ est encore solution ; par minimalité de z, $g=1$.

Première paramétrisation. Le triplet (x^2,y^2,z) est pythagoricien, et primitif car $\gcd(x^2,y^2)=1$. Quitte à échanger x et y, y^2 est pair et x impair ; par le théorème 12.1.2,

$$x^2=m^2-n^2,\qquad y^2=2mn,\qquad z=m^2+n^2,$$

avec $m>n\ge 1$, $\gcd(m,n)=1$, $m\not\equiv n \pmod 2$.

Seconde paramétrisation. On a $x^2+n^2=m^2$ avec $\gcd(n,m)=1$: le triplet (x,n,m) est pythagoricien primitif. Si n était impair, m serait pair et $x^2=m^2-n^2\equiv -1\equiv 3 \pmod 4$, ce qui est impossible ; donc n est pair, et le théorème 12.1.2 donne

$$x=r^2-s^2,\qquad n=2rs,\qquad m=r^2+s^2,\qquad r>s\ge 1,\quad \gcd(r,s)=1.$$

Descente. Alors $y^2=2mn=4rs(r^2+s^2)$; y est pair et $\left(\frac{y}{2}\right)^2=rs(r^2+s^2)$. Les trois facteurs r, s, r^2+s^2 sont deux à deux premiers entre eux : $\gcd(r,s)=1$, et un premier divisant r et r^2+s^2 diviserait s^2, donc s (de même en échangeant r et s). Par le lemme du produit, chacun est un carré :

$$r=u^2,\qquad s=v^2,\qquad r^2+s^2=w^2,$$

avec $u,v,w\ge 1$. D'où $u^4+v^4=w^2$: c'est une nouvelle solution en entiers strictement positifs, avec

$$w\le w^2=m\le m^2<m^2+n^2=z.$$

Ainsi $w<z$, ce qui contredit la minimalité de z. Il n'y a donc pas de solution.

Conséquence. Si $x^4+y^4=z^4$, alors (x,y,z^2) serait solution de $x^4+y^4=Z^2$: impossible. ∎

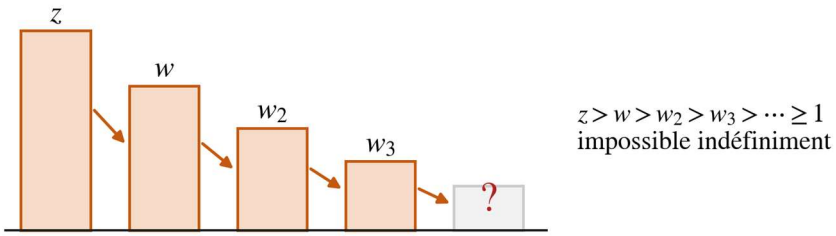


Schéma de la descente infinie : chaque solution (x, y, z) en fournit une autre (u, v, w) avec w < z ; une suite strictement décroissante d'entiers positifs ne peut être infinie.

Exemple 12.2.3. *Montrer qu'il n'existe pas de triangle rectangle à côtés entiers dont l'aire soit un carré parfait.*

Un tel triangle donnerait $a^2 + b^2 = c^2$ et $\frac{ab}{2} = d^2$. Quitte à diviser les côtés par $g = \gcd(a, b, c)$ (l'aire est alors divisée par g^2 et reste un carré, car un rationnel dont le carré est entier est entier), on peut supposer le triplet primitif. Avec la paramétrisation, $ab = 2mn(m^2 - n^2) = 2mn(m - n)(m + n)$ et l'aire vaut $mn(m - n)(m + n) = d^2$. Les quatre facteurs sont positifs et deux à deux premiers entre eux : $\gcd(m, n) = 1$; $\gcd(m, m \pm n) = \gcd(m, n) = 1$ et de même pour n ; enfin un diviseur commun de $m - n$ et $m + n$ divise $2m$ et $2n$, et il est impair car $m - n$ l'est, donc il divise $\gcd(m, n) = 1$. Par le lemme du produit, chacun est un carré : $m = p^2$, $n = q^2$, $m - n = r^2$, $m + n = s^2$. Alors $r^2 s^2 = m^2 - n^2$ et $s^2 + r^2 = 2m = 2p^2$, $s^2 - r^2 = 2n$. On aboutit à $p^4 - q^4 = (rs)^2$, dont on montre par descente (exercice 12.4) qu'elle n'a pas de solution en entiers strictement positifs.

12.3 Exercices

Exercice 12.1 ★. Trouver tous les triplets pythagoriciens primitifs avec $c \leq 30$.

Exercice 12.2 ★★. Montrer que dans tout triplet pythagoricien, $60 \mid abc$.

Exercice 12.3 ★★. Montrer que $x^2 + y^2 = 3(u^2 + v^2)$ n'a que la solution nulle.

Exercice 12.4 ★★. Montrer que $x^4 - y^4 = z^2$ n'a pas de solution en entiers strictement positifs.

Exercice 12.5 ★★★. Montrer que $x^3 + 2y^3 + 4z^3 = 0$ n'a que la solution nulle.

Exercice 12.6 ★★★. Montrer que $x^2 + y^2 + z^2 = 3xyz$ possède une infinité de solutions en entiers strictement positifs (équation de Markov).

12.4 Corrigés

Solution de l'exercice 12.1. (m, n) avec $m > n$, $\gcd(m, n) = 1$, parités différentes : $(2,1) \to (3,4,5)$; $(3,2) \to (5,12,13)$; $(4,1) \to (15,8,17)$; $(4,3) \to (7,24,25)$; $(5,2) \to (21,20,29)$.

Solution de l'exercice 12.2. Il suffit de traiter le cas primitif. $60 = 4 \cdot 3 \cdot 5$.

4 : $b = 2mn$ avec m, n de parités différentes, donc mn est pair et $4 \mid b$.

3 : si $3 \mid mn$, alors $3 \mid b$; si $3 \nmid m$ et $3 \nmid n$, alors $m^2 \equiv n^2 \equiv 1 \pmod 3$ et $3 \mid m^2 - n^2 = a$.

5 : si $5 \mid mn$, alors $5 \mid b$. Sinon, les carrés modulo 5 valant $0, \pm 1$, on a $m^2, n^2 \in \{1,4\}$; si $m^2 \equiv n^2$ alors $5 \mid a$, sinon $m^2 + n^2 \equiv 5 \equiv 0$ et $5 \mid c$.

Solution de l'exercice 12.3. Supposons une solution non nulle avec $|x| + |y| + |u| + |v|$ minimal. Modulo 3 : $x^2 + y^2 \equiv 0$ force $3 \mid x$ et $3 \mid y$ (les carrés valent $0,1$). Alors $9 \mid 3(u^2 + v^2)$, donc $3 \mid u^2 +$

v^2, donc $3 \mid u$ et $3 \mid v$. Ainsi $\left(\frac{x}{3}, \frac{y}{3}, \frac{u}{3}, \frac{v}{3}\right)$ est une solution non nulle plus petite : contradiction par descente.

Solution de l'exercice 12.4. Supposons une solution avec x minimal ; alors $\gcd(x, y) = 1$ (sinon on divise x, y par leur PGCD g et z par g^2). Alors $(y^2)^2 + z^2 = (x^2)^2$, triplet pythagoricien primitif.

Cas 1 : z pair. $y^2 = m^2 - n^2$, $z = 2mn$, $x^2 = m^2 + n^2$. Alors $x^2 y^2 = m^4 - n^4$ est un carré, donc (m, n, xy) est solution de $m^4 - n^4 = t^2$ avec $m^2 < m^2 + n^2 = x^2$, donc $m < x$: descente.

Cas 2 : y^2 pair. $z = m^2 - n^2$, $y^2 = 2mn$, $x^2 = m^2 + n^2$. Comme $\gcd(m, n) = 1$ et $mn = 2\left(\frac{y}{2}\right)^2$, on écrit $\{m, n\} = \{2a^2, b^2\}$. Comme $m^2 + n^2 = x^2$, le triplet formé de b^2, $2a^2$ et x est pythagoricien primitif, de terme pair $2a^2$. Par le théorème 12.1.2, $b^2 = r^2 - s^2$, $2a^2 = 2rs$, $x = r^2 + s^2$ avec $\gcd(r, s) = 1$. De $rs = a^2$ on tire $r = p^2$, $s = q^2$, puis $p^4 - q^4 = b^2$: (p, q, b) est une nouvelle solution, avec $p \leq p^2 = r < r^2 + s^2 = x$, donc $p < x$: descente.

Dans les deux cas, on contredit la minimalité de x.

Solution de l'exercice 12.5. Supposons $(x, y, z) \neq (0,0,0)$ avec $|x| + |y| + |z|$ minimal. Modulo 2 : $x^3 \equiv 0$, donc x est pair, $x = 2x'$. Alors $8x'^3 + 2y^3 + 4z^3 = 0$, soit $4x'^3 + y^3 + 2z^3 = 0$: y est pair, $y = 2y'$, d'où $4x'^3 + 8y'^3 + 2z^3 = 0$, soit $2x'^3 + 4y'^3 + z^3 = 0$: z pair, $z = 2z'$, et $x'^3 + 2y'^3 + 4z'^3 = 0$: (x', y', z') est une solution non nulle avec $|x'| + |y'| + |z'| < |x| + |y| + |z|$, contradiction avec la minimalité.

Solution de l'exercice 12.6. $(1,1,1)$ est solution. Si (x, y, z) est solution, fixons y, z : l'équation $X^2 - 3yzX + (y^2 + z^2) = 0$ a pour racines x et $x' = 3yz - x = \frac{y^2 + z^2}{x}$, qui est un entier strictement positif. Donc (x', y, z) est encore solution. Partant de $(1,1,1)$ on obtient $(2,1,1)$, puis $(5,2,1)$, $(13,5,1)$, $(29,5,2)$, …

Ces solutions sont bien en nombre infini : si $x \geq y \geq z \geq 1$ est une solution, remplacer z par $z' = 3xy - z \geq 3x - x = 2x > x$ fournit une solution dont le plus grand terme est strictement plus grand. En itérant, on obtient une infinité de solutions distinctes.

> **Remarque.**
> C'est exactement le mécanisme du saut de Viète (chapitre 16), utilisé ici dans le sens « ascendant ».

CHAPITRE 13

13 L'équation de Pell

Objectifs du chapitre.

- Montrer que $x^2 - dy^2 = 1$ possède toujours une solution non triviale.
- Engendrer toutes les solutions à partir de la solution fondamentale.
- Utiliser l'équation de Pell pour construire des familles infinies en olympiades.

13.1 Existence d'une solution non triviale

Théorème 13.1.1 (Existence d'une solution non triviale)

Soit $d > 0$ un entier qui n'est pas un carré parfait. Alors l'équation

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

possède une solution en entiers avec $y \neq 0$.

Démonstration (Dirichlet). *Étape 0 : $\sqrt{d}$ est irrationnel.* Si $\sqrt{d} = \frac{a}{b}$ avec $a, b \geq 1$, alors $db^2 = a^2$ et, pour tout premier p, $v_p(d) = 2v_p(a) - 2v_p(b)$ est pair ; par la proposition 3.2.2 (v), d serait un carré. En conséquence, si $a + b\sqrt{d} = a' + b'\sqrt{d}$ avec a, b, a', b' entiers, alors $a = a'$ et $b = b'$.

Étape 1 : approximation de Dirichlet. Soit $Q \geq 1$ un entier. Les $Q + 1$ réels $\{j\sqrt{d}\}$, $0 \leq j \leq Q$, sont dans $[0,1[$, que l'on découpe en Q intervalles $\left[\frac{i}{Q}, \frac{i+1}{Q}\right[$. Par le principe des tiroirs, deux d'entre eux, $\{i\sqrt{d}\}$ et $\{j\sqrt{d}\}$ avec $i > j$, tombent dans le même intervalle ; en posant $q = i - j \in \{1, \ldots, Q\}$ et $p = \lfloor i\sqrt{d} \rfloor - \lfloor j\sqrt{d} \rfloor$, on obtient

$$\left|q\sqrt{d} - p\right| = \left|\{i\sqrt{d}\} - \{j\sqrt{d}\}\right| < \frac{1}{Q} \leq \frac{1}{q}.$$

Il existe ainsi une infinité de couples (p, q) avec $q \geq 1$ et $\left|p - q\sqrt{d}\right| < \frac{1}{q}$: si l'on n'en avait qu'un nombre fini, les quantités $\left|p - q\sqrt{d}\right|$ correspondantes seraient toutes > 0 (étape 0) ; en choisissant Q avec $\frac{1}{Q}$ plus petit que chacune d'elles, on obtiendrait un nouveau couple. On a de plus $p > q\sqrt{d} - 1 \geq \sqrt{d} - 1 > 0$. Pour ces couples,

$$|p^2 - dq^2| = \left|p - q\sqrt{d}\right| \cdot \left(p + q\sqrt{d}\right) < \frac{1}{q}\left(2q\sqrt{d} + \frac{1}{q}\right) \leq 2\sqrt{d} + 1.$$

Étape 2 : deux couples de même norme et congrus. L'entier $p^2 - dq^2$ ne prend qu'un nombre fini de valeurs (celles de $]-2\sqrt{d} - 1, 2\sqrt{d} + 1[$) ; par le principe des tiroirs infini, il existe un entier k tel que $p^2 - dq^2 = k$ pour une infinité de couples, et $k \neq 0$ car $\sqrt{d}$ est irrationnel. Les couples $(p \bmod |k|,\ q \bmod |k|)$ ne prennent que k^2 valeurs ; il existe donc deux couples **distincts** (p_1, q_1), (p_2, q_2) de norme k avec $p_1 \equiv p_2$ et $q_1 \equiv q_2 \pmod{|k|}$.

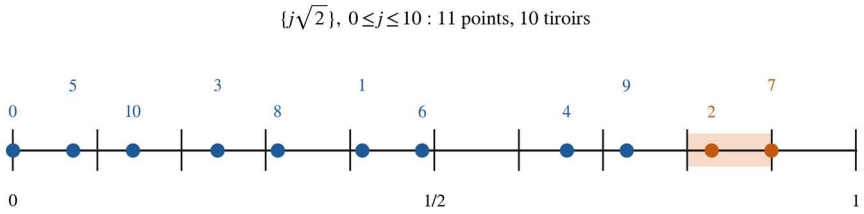
Étape 3 : division. Comme $\left(p_2 + q_2\sqrt{d}\right)\left(p_2 - q_2\sqrt{d}\right) = k$, posons

$$x + y\sqrt{d} = \frac{p_1 + q_1\sqrt{d}}{p_2 + q_2\sqrt{d}} = \frac{\left(p_1 + q_1\sqrt{d}\right)\left(p_2 - q_2\sqrt{d}\right)}{k}, \qquad \text{soit} \qquad x = \frac{p_1p_2 - dq_1q_2}{k}, \quad y = \frac{p_2q_1 - p_1q_2}{k}.$$

Modulo $|k|$: $p_1p_2 - dq_1q_2 \equiv p_1^2 - dq_1^2 = k \equiv 0$ et $p_2q_1 - p_1q_2 \equiv p_1q_1 - p_1q_1 = 0$; donc $x, y \in \mathbb{Z}$. Par ailleurs, $(x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$ et le même calcul avec $-\sqrt{d}$ donnent

$$x^2 - dy^2 = \frac{(p_1^2 - dq_1^2)(p_2^2 - dq_2^2)}{k^2} = \frac{k \cdot k}{k^2} = 1.$$

Enfin $y \neq 0$: sinon $x^2 = 1$, et $p_1 + q_1\sqrt{d} = \pm(p_2 + q_2\sqrt{d})$; les deux membres étant positifs, le signe est $+$, et l'étape 0 donne $(p_1, q_1) = (p_2, q_2)$, ce qui est exclu. Le couple $(|x|, |y|)$ est la solution cherchée. ■



Principe des tiroirs de Dirichlet pour √2 et Q = 10 : parmi les 11 parties fractionnaires {j√2}, 0 ≤ j ≤ 10, deux tombent dans le même intervalle de longueur 1/10 (ici j = 2 et j = 7), d'où |5√2 − 7| < 1/10.

Définition 13.1.2 (Solution fondamentale)

La solution fondamentale (x_1, y_1) est la solution de $x^2 - dy^2 = 1$ en entiers $x_1, y_1 > 0$ pour laquelle x_1 (ou, ce qui revient au même, y_1) est minimal.

Théorème 13.1.3 (Toutes les solutions)

Toutes les solutions en entiers strictement positifs de $x^2 - dy^2 = 1$ sont données par

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n, \qquad n \geq 1.$$

Autrement dit, avec $\alpha = x_1 + y_1\sqrt{d}$:

$$x_n = \frac{\alpha^n + \overline{\alpha}^n}{2}, \qquad y_n = \frac{\alpha^n - \overline{\alpha}^n}{2\sqrt{d}}, \qquad \overline{\alpha} = x_1 - y_1\sqrt{d}.$$

Elles vérifient la récurrence

$$x_{n+1} = x_1x_n + d\,y_1y_n, \qquad y_{n+1} = x_1y_n + y_1x_n.$$

Démonstration. Pour $\beta = u + v\sqrt{d}$ $(u, v \in \mathbb{Z})$, notons $\overline{\beta} = u - v\sqrt{d}$ son conjugué et $N(\beta) = \beta\overline{\beta} = u^2 - dv^2$ sa norme ; l'écriture $u + v\sqrt{d}$ est unique (étape 0 ci-dessus).

(a) La conjugaison et la norme sont multiplicatives. En développant, $(u + v\sqrt{d})(u' + v'\sqrt{d}) = (uu' + dvv') + (uv' + u'v)\sqrt{d}$, et le même calcul avec $-\sqrt{d}$ montre que $\overline{\beta\beta'} = \overline{\beta}\,\overline{\beta'}$. D'où $N(\beta\beta') = \beta\beta'\overline{\beta}\,\overline{\beta'} = N(\beta)N(\beta')$.

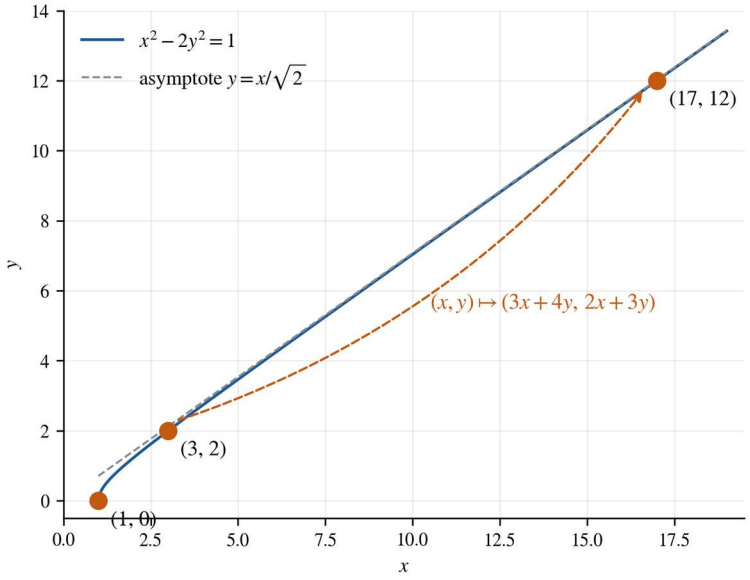
(b) Une solution $\beta = u + v\sqrt{d}$ de norme 1 vérifie $u, v > 0$ si, et seulement si, $\beta > 1$. Si $u, v \geq 1$, $\beta \geq 1 + \sqrt{d} > 1$. Réciproquement, si $\beta > 1$, alors $\overline{\beta} = \beta^{-1} \in]0,1[$, donc $u = \frac{\beta + \overline{\beta}}{2} > 0$ et $v\sqrt{d} = \frac{\beta - \overline{\beta}}{2} > 0$.

(c) $\alpha = x_1 + y_1\sqrt{d}$ est la plus petite solution > 1. Pour les solutions positives, $v = \sqrt{(u^2 - 1)/d}$ est une fonction croissante de u, donc $u + v\sqrt{d}$ aussi ; minimiser x_1 revient à minimiser y_1 et α. Avec (b), toute solution $\beta > 1$ vérifie $\beta \geq \alpha$.

Les puissances de α sont des solutions. Par (a), $N(\alpha^n) = N(\alpha)^n = 1$; α^n s'écrit $x_n + y_n\sqrt{d}$ avec x_n, y_n entiers (développement), et $\alpha^n > 1$, donc $x_n, y_n > 0$ par (b).

Ce sont les seules. Soit $\beta = x + y\sqrt{d}$ une solution avec $x, y > 0$; alors $\beta > 1$ et, α étant > 1, il existe un unique $n \geq 1$ tel que $\alpha^n \leq \beta < \alpha^{n+1}$ ($n \geq 1$ car $\beta \geq \alpha$ par (c)). Posons $\gamma = \beta\alpha^{-n} = \beta\,\overline{\alpha}^{\,n}$ (car $\alpha\overline{\alpha} = 1$). C'est un élément de la forme $u + v\sqrt{d}$ à coefficients entiers, de norme $N(\beta)N(\overline{\alpha})^n = 1$, et $1 \leq \gamma < \alpha$. Si $\gamma > 1$, γ serait une solution positive (b) strictement inférieure à α, ce qui contredit (c). Donc $\gamma = 1$ et $\beta = \alpha^n$.

Formules. En conjuguant, $x_n - y_n\sqrt{d} = \overline{\alpha^n} = \overline{\alpha}^{\,n}$; en ajoutant et en retranchant $x_n + y_n\sqrt{d} = \alpha^n$, on obtient les expressions de x_n et y_n. Enfin $\alpha^{n+1} = \alpha \cdot \alpha^n = \big(x_1 + y_1\sqrt{d}\big)\big(x_n + y_n\sqrt{d}\big)$, et le développement de (a) donne la récurrence. ■



L'hyperbole $x^2 - 2y^2 = 1$ et ses points entiers (1, 0), (3, 2), (17, 12), … ; ils s'approchent de l'asymptote $y = x/\sqrt{2}$, et chacun se déduit du précédent par $(x, y) \mapsto (3x + 4y, 2x + 3y)$.

Exemple 13.1.4. *Résoudre $x^2 - 2y^2 = 1$.*

Solution fondamentale : $(3,2)$ car $9 - 8 = 1$. Les solutions sont données par $\big(3 + 2\sqrt{2}\big)^n$:

$$(3,2),\ (17,12),\ (99,70),\ (577,408),\ \ldots$$

avec $x_{n+1} = 3x_n + 4y_n$, $y_{n+1} = 2x_n + 3y_n$.

Attention.

L'équation négative $x^2 - dy^2 = -1$ n'a pas toujours de solution : $x^2 - 3y^2 = -1$ est impossible modulo 3 ($x^2 \equiv -1 \pmod 3$ n'a pas de solution). On démontre en théorie des fractions continues qu'elle est résoluble si, et seulement si, le développement en fraction continue de $\sqrt{d}$ a une période impaire ; nous admettons ce résultat, qui n'est pas utilisé dans la suite.

13.2 Applications olympiques

Méthode 13.2.1 — Reconnaître Pell

Signaux :

- l'énoncé demande de montrer qu'il existe une infinité d'entiers vérifiant une propriété quadratique ;
- une équation de la forme $x^2 - dy^2 = k$ apparaît après manipulation ;
- on cherche des entiers n tels que $an^2 + bn + c$ soit un carré ;
- des « nombres triangulaires carrés », des « carrés consécutifs », etc.

Exemple 13.2.2. *Montrer qu'il existe une infinité d'entiers n tels que n, $n+1$, $n+2$ soient chacun somme de deux carrés.*

Construction. Posons $n = 8t^2$. Alors : $n = (2t)^2 + (2t)^2$; $n + 2 = 2(4t^2 + 1)$ est somme de deux carrés si, et seulement si, $4t^2 + 1$ l'est — ce qui est vrai : $4t^2 + 1 = (2t)^2 + 1^2$, et le double d'une somme de deux carrés est somme de deux carrés, par $2(a^2 + b^2) = (a + b)^2 + (a - b)^2$.

Reste $n + 1 = 8t^2 + 1$: cherchons t tel que $8t^2 + 1$ soit un carré, $8t^2 + 1 = s^2$, c'est-à-dire $s^2 - 8t^2 = 1$: équation de Pell, de solution fondamentale $(3,1)$, donc (théorème 13.1.3) il y a une infinité de tels t, deux à deux distincts puisque $y_{n+1} > y_n$. Pour ces t, $n + 1 = s^2 = s^2 + 0^2$.

Exemple 13.2.3. *Trouver tous les entiers $n \geq 1$ tels que $\frac{n(n+1)}{2}$ soit un carré parfait (nombres triangulaires carrés).*

$$\frac{n(n+1)}{2} = m^2 \Leftrightarrow n^2 + n = 2m^2 \Leftrightarrow (2n+1)^2 - 8m^2 = 1.$$

C'est l'équation de Pell avec $d = 8$ et $x = 2n + 1$; réciproquement, toute solution (x, m) en entiers positifs a x impair ($x^2 = 1 + 8m^2$), donc fournit $n = \frac{x-1}{2} \geq 1$: solution fondamentale $(3,1)$, d'où $(x, m) = (3,1), (17,6), (99,35), (577,204)$, … et

$$n = 1,8,49,288,1681, \ldots$$

13.3 Exercices

Exercice 13.1 ★. Trouver la solution fondamentale de $x^2 - 3y^2 = 1$, $x^2 - 5y^2 = 1$, $x^2 - 13y^2 = 1$.

Exercice 13.2 ★★. Montrer que si $d > 0$ est un carré parfait, $x^2 - dy^2 = 1$ n'a que les solutions triviales $(\pm 1, 0)$.

Exercice 13.3 ★★. Montrer qu'il existe une infinité de couples (n, m) tels que $1 + 2 + \cdots + n = (n+1) + (n+2) + \cdots + m$.

Exercice 13.4 ★★★. Montrer qu'il n'existe aucun entier $n \geq 1$ tel que $2n^2 + 1$, $3n^2 + 1$ et $6n^2 + 1$ soient simultanément des carrés parfaits.

Exercice 13.5 ★★★. Montrer que si $x^2 - dy^2 = 1$ a la solution fondamentale (x_1, y_1), alors $y_1 \mid y_n$ pour toute solution (x_n, y_n) ; puis montrer que la suite (y_n) est une suite récurrente linéaire d'ordre 2.

13.4 Corrigés

Solution de l'exercice 13.1. $d = 3$: $(2,1)$ car $4 - 3 = 1$. $d = 5$: $(9,4)$ car $81 - 80 = 1$. $d = 13$: $(649,180)$ — la solution fondamentale peut être très grande, ce qui illustre l'intérêt des fractions continues.

Solution de l'exercice 13.2. Si $d = k^2$ avec $k \geq 1$, alors $x^2 - k^2y^2 = (x - ky)(x + ky) = 1$, donc $x - ky = x + ky = \pm 1$, d'où $y = 0$ et $x = \pm 1$.

Solution de l'exercice 13.3. La condition s'écrit $2 \cdot \frac{n(n+1)}{2} = \frac{m(m+1)}{2}$, soit $m^2 + m - 2n^2 - 2n = 0$. En multipliant par 4 et en complétant les carrés :

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

C'est l'équation de Pell négative $X^2 - 2Y^2 = -1$, dont $(1,1)$ est la solution fondamentale ; elle a une infinité de solutions $(1,1), (7,5), (41,29), (239,169), \ldots$ (toutes à composantes impaires, car $X^2 \equiv 1 \pmod 8$ impose $Y^2 \equiv 1 \pmod 4$), d'où une infinité de couples (n, m) :

$$(n, m) = (2,3), (14,20), (84,119), \ldots$$

Solution de l'exercice 13.4. Supposons $2n^2 + 1 = a^2$, $3n^2 + 1 = b^2$ et $6n^2 + 1 = c^2$ avec $n \geq 1$ et $a, b, c > 0$. Alors

$$(abc)^2 = (2n^2 + 1)(3n^2 + 1)(6n^2 + 1) = 36n^6 + 36n^4 + 11n^2 + 1.$$

Comparons avec le carré de $6n^3 + 3n$:

$$(6n^3 + 3n)^2 = 36n^6 + 36n^4 + 9n^2.$$

Ainsi $(abc)^2 - (6n^3 + 3n)^2 = 2n^2 + 1 > 0$.

D'autre part,

$$(6n^3 + 3n + 1)^2 = (6n^3 + 3n)^2 + 2(6n^3 + 3n) + 1 = (6n^3 + 3n)^2 + 12n^3 + 6n + 1,$$

et $12n^3 + 6n + 1 > 2n^2 + 1$ dès que $n \geq 1$. On obtient donc l'encadrement strict

$$(6n^3 + 3n)^2 < (abc)^2 < (6n^3 + 3n + 1)^2,$$

ce qui est impossible : $(abc)^2$ serait un carré parfait strictement compris entre deux carrés consécutifs.

À retenir

Cette technique — multiplier les contraintes entre elles, puis coincer le produit entre deux carrés consécutifs — est l'une des plus efficaces devant un système de conditions « tel nombre est un carré ».

Solution de l'exercice 13.5. De $x_{n+1} + y_{n+1}\sqrt{d} = \left(x_n + y_n\sqrt{d}\right)\left(x_1 + y_1\sqrt{d}\right)$ on tire

$$x_{n+1} = x_1x_n + dy_1y_n, \qquad y_{n+1} = x_1y_n + y_1x_n.$$

La seconde relation montre, par récurrence immédiate, que $y_1 \mid y_n$ pour tout $n \geq 1$. En éliminant x_n (via $y_1x_n = y_{n+1} - x_1y_n$ et $x_1^2 - dy_1^2 = 1$), on obtient

$$y_{n+2} = x_1y_{n+1} + y_1(x_1x_n + dy_1y_n) = 2x_1y_{n+1} - (x_1^2 - dy_1^2)y_n,$$

c'est-à-dire la récurrence linéaire

$$y_{n+2} = 2x_1\, y_{n+1} - y_n,$$

et de même $x_{n+2} = 2x_1x_{n+1} - x_n$.

PARTIE V — Techniques de haut niveau et problèmes d'IMO

CHAPITRE 14

14 Le lemme LTE (Lifting the Exponent)

Objectifs du chapitre.

- Énoncer et démontrer le lemme LTE dans les cas p impair et $p = 2$.
- Calculer exactement $v_p(a^n \pm b^n)$.
- Reconnaître les problèmes où LTE est l'outil décisif.

14.1 Le cas p impair

Lemme 14.1.1 (Minoration de la valuation)

Soient a, b des entiers et p un premier tel que $p \mid a - b$ et $p \nmid ab$. Alors, pour tout $c \geq 1$,

$$v_p(a^c - b^c) \geq v_p(a - b) + v_p(c).$$

Démonstration. Montrons d'abord que, pour $\ell \geq 1$, $p^\ell \mid a - b$ implique $p^{\ell+1} \mid a^p - b^p$. En écrivant $a = b + p^\ell t$:

$$a^p = (b + p^\ell t)^p = b^p + p\, b^{p-1} p^\ell t + \binom{p}{2} b^{p-2} p^{2\ell} t^2 + \cdots,$$

tous les termes après b^p étant divisibles par $p^{\ell+1}$: pour $1 \leq j \leq p-1$, le terme $\binom{p}{j} b^{p-j} p^{j\ell} t^j$ est divisible par $p \cdot p^\ell$ car $p \mid \binom{p}{j}$ (voir la démonstration 2 du petit théorème de Fermat, chapitre 6) ; et le dernier terme $p^{p\ell} t^p$ est divisible par $p^{\ell+1}$ car $p\ell \geq 2\ell \geq \ell + 1$. Donc $p^{\ell+1} \mid a^p - b^p$.

Par récurrence sur k (en appliquant ce qui précède au couple $\left(a^{p^k}, b^{p^k}\right)$), $p^{v_p(a-b)+k}$ divise $a^{p^k} - b^{p^k}$. Soit $k = v_p(c)$ et $c = p^k c'$. Comme $x - y$ divise $x^{c'} - y^{c'}$ (factorisation $x^{c'} - y^{c'} = (x-y)(x^{c'-1} + \cdots + y^{c'-1})$), on a, avec $x = a^{p^k}$ et $y = b^{p^k}$, $a^{p^k} - b^{p^k} \mid a^c - b^c$, et on conclut. ∎

Théorème 14.1.2 (Lemme LTE, cas p impair)

Soient p un premier impair et a, b des entiers tels que $p \mid a - b$, $p \nmid a$ et $p \nmid b$. Alors, pour tout $n \geq 1$,

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

Démonstration. Disons qu'un entier $n \geq 1$ est *bon* s'il vérifie la conclusion pour tous a, b admissibles. Si m et n sont bons, mn l'est aussi : appliquer la formule à (a^m, b^m) puis à (a, b),

$$v_p(a^{mn} - b^{mn}) = v_p(a^m - b^m) + v_p(n) = v_p(a - b) + v_p(m) + v_p(n) = v_p(a - b) + v_p(mn).$$

Comme 1 est bon, il suffit de traiter $n = q$ premier.

Cas $q \neq p$. On a $\frac{a^q - b^q}{a - b} = a^{q-1} + a^{q-2}b + \cdots + b^{q-1} \equiv q a^{q-1} \pmod p$ (car $a \equiv b$), quantité non divisible par p. Donc $v_p(a^q - b^q) = v_p(a - b) = v_p(a - b) + v_p(q)$.

Cas $q = p$. Écrivons $a = b + p^k c$ avec $k = v_p(a - b) \geq 1$ et $p \nmid c$. Le binôme donne

$$a^p - b^p = p^{k+1}b^{p-1}c + \binom{p}{2}b^{p-2}p^{2k}c^2 + \cdots + p^{kp}c^p.$$

Le premier terme a pour valuation exactement $k+1$ (car $p \nmid bc$). Les termes d'indice $2 \le j \le p-1$ ont une valuation $\ge 1+jk \ge 1+2k \ge k+2$ (car $p \mid \binom{p}{j}$), et le dernier, $p^{kp}c^p$, une valuation $kp \ge 3k \ge k+2$: c'est ici qu'intervient $p \ge 3$. Par la proposition 3.2.2 (ii), la somme a pour valuation exactement $k+1$. Donc $v_p(a^p - b^p) = k+1 = v_p(a-b) + v_p(p)$. ■

Corollaire 14.1.3 (Cas d'une somme)

Sous les mêmes hypothèses avec $p \mid a+b$ (au lieu de $p \mid a-b$), et pour n impair :

$$v_p(a^n + b^n) = v_p(a+b) + v_p(n).$$

Démonstration. Appliquer le théorème à a et $-b$: $a^n - (-b)^n = a^n + b^n$ car n est impair. ■

14.2 Le cas $p = 2$

Théorème 14.2.1 (Lemme LTE, cas p = 2)

Soient a, b des entiers impairs et $n \ge 1$.

- Si n est pair : $v_2(a^n - b^n) = v_2(a-b) + v_2(a+b) + v_2(n) - 1$.
- Si n est impair : $v_2(a^n - b^n) = v_2(a-b)$.

Démonstration. Pour n impair, $\frac{a^n - b^n}{a-b}$ est une somme de n termes impairs, donc impaire.

Pour n pair, écrivons $n = 2^s m$ avec m impair, $s \ge 1$. Alors

$$a^n - b^n = (a^m - b^m)(a^m + b^m)(a^{2m} + b^{2m}) \cdots \left(a^{2^{s-1}m} + b^{2^{s-1}m}\right).$$

Le premier facteur a pour valuation $v_2(a-b)$, le deuxième $v_2(a+b)$ (de même, $\frac{a^m + b^m}{a+b}$ est une somme de m termes impairs), et chacun des $s-1$ suivants est de la forme $u^2 + v^2$ avec u, v impairs, donc $\equiv 2 \pmod 4$: valuation exactement 1. Au total $v_2(a-b) + v_2(a+b) + (s-1)$, et $s = v_2(n)$. ■

Attention.

Vérifiez systématiquement les hypothèses : $p \mid a-b$, $p \nmid a$, $p \nmid b$, et, pour le corollaire, n impair. Appliquer LTE hors de son domaine est l'erreur la plus fréquente. Et n'oubliez jamais que le cas $p = 2$ obéit à une formule différente.

14.3 Applications

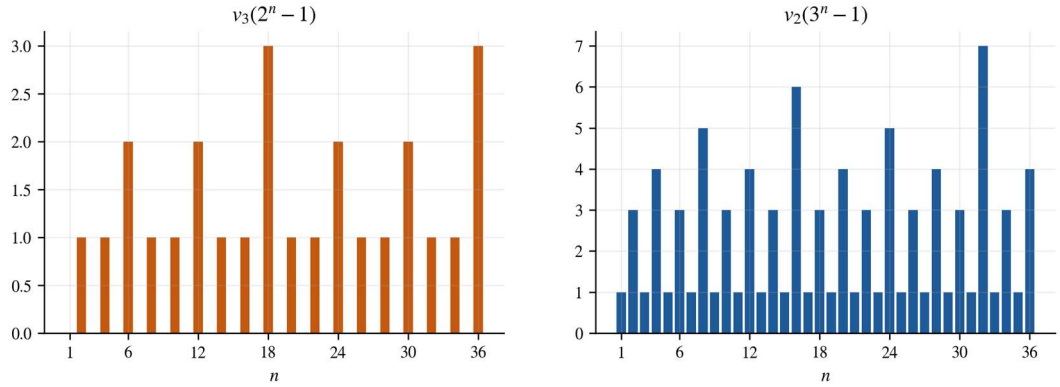
Exemple 14.3.1. *Déterminer tous les $n \ge 1$ tels que $3^k \mid 2^n - 1$, pour $k \ge 1$ fixé.*

$3 \mid 2^n - 1$ impose n pair, $n = 2m$. Alors $2^n - 1 = 4^m - 1$ et LTE ($p = 3$, $3 \mid 4 - 1$) donne

$$v_3(4^m - 1) = v_3(3) + v_3(m) = 1 + v_3(m).$$

Donc $3^k \mid 2^n - 1 \Leftrightarrow n = 2m$ avec $v_3(m) \ge k-1$, c'est-à-dire

$$2 \cdot 3^{k-1} \mid n.$$



Le lemme LTE en images. À gauche : $v_3(2^n-1)$, nulle pour n impair et égale à 1 + $v_3(n)$ pour n pair. À droite : $v_2(3^n-1)$, égale à 1 pour n impair et à 2 + $v_2(n)$ pour n pair.

Exemple 14.3.2. *Soit p un premier impair et a un entier tel que $a^p \equiv 1 \pmod{p^n}$ avec $n \geq 1$. Montrer que $a \equiv 1 \pmod{p^{n-1}}$.*

$a^p \equiv 1 \pmod{p}$ et, par Fermat, $a^p \equiv a \pmod{p}$: donc $a \equiv 1 \pmod{p}$. LTE s'applique :

$$n \leq v_p(a^p - 1) = v_p(a-1) + v_p(p) = v_p(a-1) + 1,$$

donc $v_p(a-1) \geq n-1$.

Exemple 14.3.3 (Bulgarie). *Montrer que si $3^n - 2^n$ est une puissance d'un nombre premier, alors n est premier.*

Posons $3^n - 2^n = p^e$ avec $e \geq 1$ (p est impair car $3^n - 2^n$ est impair, et $p \neq 3$; on a $n \geq 2$ car $3 - 2 = 1$).

n n'a pas deux facteurs premiers distincts. Si $q_1 \neq q_2$ divisent n, alors $3^{q_i} - 2^{q_i} \mid 3^n - 2^n = p^e$, donc chacun est une puissance de p. Or ces deux nombres sont premiers entre eux : si un premier r les divise tous deux, alors $r \neq 2$ (ils sont impairs) et $r \neq 3$ ($3^q - 2^q \equiv -2^q \not\equiv 0 \pmod{3}$) ; en posant $u \equiv 3 \cdot 2^{-1} \pmod{r}$, on a $u^{q_1} \equiv u^{q_2} \equiv 1$, donc l'ordre de u divise $\gcd(q_1, q_2) = 1$ (proposition 7.1.2), soit $u \equiv 1$ et $r \mid 3 - 2 = 1$: absurde. Deux puissances de p premières entre elles ne peuvent être toutes deux > 1 ; or $3^q - 2^q \geq 9 - 4 = 5$ pour $q \geq 2$: contradiction.

n n'est pas de la forme q^k avec $k \geq 2$. Sinon, $3^q - 2^q \mid 3^n - 2^n$ et $p \mid 3^q - 2^q$. Par LTE appliqué à $A = 3^q$, $B = 2^q$ (qui ne sont pas divisibles par p) :

$$v_p(3^n - 2^n) = v_p\left(A^{q^{k-1}} - B^{q^{k-1}}\right) = v_p(A-B) + v_p\left(q^{k-1}\right).$$

Si $p \neq q$, cela vaut $v_p(3^q - 2^q)$, donc $3^n - 2^n$ et $3^q - 2^q$, qui sont deux puissances de p (le second divise le premier), ont même valuation en p : ils sont donc égaux, ce qui est absurde puisque $n > q$ et que $m \mapsto 3^m - 2^m$ est strictement croissante ($3^{m+1} - 2^{m+1} - (3^m - 2^m) = 2 \cdot 3^m - 2^m > 0$). Si $p = q$, alors $q \mid 3^q - 2^q$, mais par Fermat $3^q - 2^q \equiv 3 - 2 = 1 \pmod{q}$: absurde.

Ainsi n, qui n'a qu'un facteur premier q et n'est pas de la forme q^k avec $k \geq 2$, vaut q : n est premier.

Exemple 14.3.4 (IMO 1990). *Trouver tous les entiers $n \geq 1$ tels que $n^2 \mid 2^n + 1$.*

Réponse : $n \in \{1, 3\}$. Les deux conviennent ($1 \mid 3$ et $9 \mid 9$). Soit $n > 1$ une solution ; n est impair, car $2^n + 1$ l'est.

Le plus petit facteur premier de n est 3. Soit p le plus petit facteur premier de n et $d = \mathrm{ord}_p(2)$. De $2^n \equiv -1 \pmod{p}$ on tire $2^{2n} \equiv 1$, donc $d \mid 2n$; et $d \mid p - 1$ (Fermat et proposition 7.1.2). Un facteur

premier impair de d diviserait n et serait $< p$: impossible ; et $v_2(d) \leq v_2(2n) = 1$. Donc $d \mid 2$, $p \mid 2^2 - 1 = 3$, et $p = 3$.

$v_3(n) = 1$. Par LTE (corollaire 14.1.3, avec $3 \mid 2 + 1$ et n impair), $v_3(2^n + 1) = v_3(3) + v_3(n) = 1 + v_3(n)$. La condition $n^2 \mid 2^n + 1$ impose $2v_3(n) \leq 1 + v_3(n)$, soit $v_3(n) \leq 1$; donc $v_3(n) = 1$.

$n = 3$. Écrivons $n = 3m$ avec $3 \nmid m$, et supposons $m > 1$; soit q le plus petit facteur premier de m ($q \geq 5$) et $e = \mathrm{ord}_q(2)$. Comme ci-dessus, $e \mid 2n$ et $e \mid q - 1$. Un facteur premier impair de e divise n et est $< q$, donc c'est 3, avec $v_3(e) \leq v_3(n) = 1$; et $v_2(e) \leq 1$. Donc $e \mid 6$, $q \mid 2^6 - 1 = 63 = 3^2 \cdot 7$, et $q = 7$. Mais les puissances de 2 modulo 7 sont 1,2,4, donc $2^n + 1 \not\equiv 0 \pmod 7$: contradiction. Ainsi $m = 1$ et $n = 3$.

14.4 Exercices

Exercice 14.1 ★. Calculer $v_5(2016^{100} - 1)$ et $v_2(3^{2026} - 1)$.

Exercice 14.2 ★★. Déterminer $v_7\left(2^{7^{2026}} - 2\right)$.

Exercice 14.3 ★★. Soit $k \geq 1$ fixé. Déterminer tous les entiers $n \geq 1$ tels que $2^k \mid 3^n - 1$.

Exercice 14.4 ★★★. Soient $a > b > 0$ des entiers premiers entre eux et q un nombre premier. Montrer que si p est un premier impair divisant $\frac{a^q - b^q}{a - b}$, alors $p \equiv 1 \pmod q$ ou $p = q$.

Exercice 14.5 ★★★. Déterminer tous les triplets (x, y, z) d'entiers ≥ 1 tels que $2^x + 3^y = z^2$.

14.5 Corrigés

Solution de l'exercice 14.1. $2016 \equiv 1 \pmod 5$, donc LTE : $v_5(2016^{100} - 1) = v_5(2015) + v_5(100) = 1 + 2 = 3$.

$3^{2026} - 1$: $a = 3$, $b = 1$ impairs, $n = 2026$ pair. Donc $v_2(3^{2026} - 1) = v_2(2) + v_2(4) + v_2(2026) - 1 = 1 + 2 + 1 - 1 = 3$.

Solution de l'exercice 14.2. $2^{7^{2026}} - 2 = 2\left(2^{7^{2026} - 1} - 1\right)$. Comme $\mathrm{ord}_7(2) = 3$ et $7^{2026} - 1 \equiv 1 - 1 = 0 \pmod 3$, posons $N = 7^{2026} - 1 = 3M$. Alors $2^N - 1 = 8^M - 1$ et $7 \mid 8 - 1$, donc LTE :

$$v_7(8^M - 1) = v_7(7) + v_7(M) = 1 + v_7(M).$$

Or $M = \frac{7^{2026} - 1}{3}$ n'est pas divisible par 7 (car $7^{2026} - 1 \equiv -1 \pmod 7$). Donc la valuation cherchée vaut 1.

Solution de l'exercice 14.3. Si n est impair, $3^n - 1 \equiv 3 - 1 = 2 \pmod 4$ (car $3^n \equiv 3 \pmod 4$), donc $v_2(3^n - 1) = 1$. Si n est pair, le lemme LTE version $p = 2$ donne

$$v_2(3^n - 1) = v_2(3 - 1) + v_2(3 + 1) + v_2(n) - 1 = 1 + 2 + v_2(n) - 1 = 2 + v_2(n).$$

Par conséquent :

- $k = 1$: tout $n \geq 1$ convient ;
- $k = 2$: les n pairs ;
- $k \geq 3$: il faut $2 + v_2(n) \geq k$, c'est-à-dire $2^{k-2} \mid n$.

En résumé, pour $k \geq 2$: $2^k \mid 3^n - 1 \Leftrightarrow 2^{\max(1, k-2)} \mid n$.

Solution de l'exercice 14.4. On a $\frac{a^q-b^q}{a-b} = a^{q-1} + a^{q-2}b + \cdots + b^{q-1}$. Si p divisait b, il diviserait a^{q-1}, donc a, ce qui est exclu puisque $\gcd(a,b) = 1$; de même $p \nmid a$. Soit alors $d = \mathrm{ord}_p(ab^{-1})$, ordre de ab^{-1} modulo p (bien défini car $p \nmid b$). De $p \mid a^q - b^q$ on tire $d \mid q$, donc $d = 1$ ou $d = q$.

Si $d = 1$, alors $p \mid a - b$, et LTE donne $v_p(a^q - b^q) = v_p(a-b) + v_p(q)$, soit $v_p\left(\frac{a^q-b^q}{a-b}\right) = v_p(q)$; comme cette valuation est ≥ 1, on obtient $p \mid q$, donc $p = q$.

Sinon $d = q$, et $q = d \mid p - 1$ (petit théorème de Fermat), soit $p \equiv 1 \pmod q$.

Solution de l'exercice 14.5. Modulo 3 : $z^2 \equiv 2^x$, et les carrés valent 0 ou 1 modulo 3 ; comme $3 \nmid z$ (sinon $3 \mid 2^x$), on a $2^x \equiv 1 \pmod 3$, donc x est pair, $x = 2u$ avec $u \geq 1$. Alors $3^y = z^2 - 2^{2u} = (z - 2^u)(z + 2^u)$. Les deux facteurs sont des puissances de 3 dont le PGCD divise 2^{u+1} et est une puissance de 3 : donc leur PGCD vaut 1, d'où $z - 2^u = 1$ et $z + 2^u = 3^y$. Ainsi $3^y = 2^{u+1} + 1$.

Modulo 8 : si $u \geq 2$, $3^y \equiv 1 \pmod 8$, donc y est pair, $y = 2v$, et $2^{u+1} = 3^{2v} - 1 = (3^v - 1)(3^v + 1)$. Ces deux facteurs sont des puissances de 2 de PGCD 2, donc $3^v - 1 = 2$ et $3^v + 1 = 2^u$: $v = 1$, $2^u = 4$, $u = 2$, $x = 4$, $y = 2$, $z = 1 + 2^2 = 5$. Vérification : $16 + 9 = 25$.

Si $u = 1$: $3^y = 5$, impossible (le cas $u = 0$, qui donnerait $3^y = 3$, $y = 1$, est exclu car $x \geq 1$).

Réponse : $(x, y, z) = (4,2,5)$.

CHAPITRE 15

15 Zsigmondy et polynômes cyclotomiques

Objectifs du chapitre.

- Énoncer le théorème de Zsigmondy et connaître ses exceptions.
- Comprendre les polynômes cyclotomiques et leurs facteurs premiers.
- Utiliser ces outils pour tuer un problème en trois lignes — avec prudence.

15.1 Diviseurs primitifs

Définition 15.1.1 (Diviseur primitif)

Soient $a > b \geq 1$ des entiers premiers entre eux. Un nombre premier p est un **diviseur primitif** de $a^n - b^n$ s'il divise $a^n - b^n$ mais ne divise aucun $a^k - b^k$ pour $1 \leq k < n$.

Proposition 15.1.2 (Caractérisation par l'ordre)

p est un diviseur primitif de $a^n - b^n$ si, et seulement si, $\mathrm{ord}_p(ab^{-1}) = n$. Dans ce cas, $p \equiv 1 \pmod{n}$.

Démonstration. Si p divise $a^k - b^k$ pour un $k \geq 1$, alors $p \nmid b$ (sinon $p \mid a^k$, donc $p \mid a$, ce qui contredit $\mathrm{pgcd}(a, b) = 1$) ; b est donc inversible modulo p, et $p \mid a^k - b^k$ équivaut à $(ab^{-1})^k \equiv 1$, c'est-à-dire (proposition 7.1.2) à $\mathrm{ord}_p(ab^{-1}) \mid k$. Ainsi p divise $a^n - b^n$ sans diviser les $a^k - b^k$, $k < n$, si, et seulement si, l'ordre divise n et ne divise aucun $k < n$, c'est-à-dire vaut n. Enfin, par le petit théorème de Fermat et la proposition 7.1.2, $n = \mathrm{ord}_p(ab^{-1}) \mid p - 1$. ■

Théorème 15.1.3 (Théorème de Zsigmondy)

Soient $a > b \geq 1$ des entiers premiers entre eux et $n \geq 1$. Alors $a^n - b^n$ possède un diviseur primitif, sauf dans les cas suivants :

- $n = 1$ et $a - b = 1$;
- $n = 2$ et $a + b$ est une puissance de 2 ;
- $n = 6$, $a = 2$, $b = 1$ (en effet $2^6 - 1 = 63 = 7 \cdot 9$, et $7 \mid 2^3 - 1$, $3 \mid 2^2 - 1$).

Version additive : $a^n + b^n$ possède un diviseur primitif sauf pour $n = 3$, $a = 2$, $b = 1$ ($2^3 + 1 = 9$).

Remarque.

La démonstration, qui repose sur les polynômes cyclotomiques, est donnée intégralement à la section 15.3.

À retenir

Usage en compétition. Zsigmondy est un théorème difficile, dont la démonstration (section 15.3) est trop longue pour être reproduite en temps limité. Beaucoup de jurys l'acceptent, mais

> un problème dont Zsigmondy vient à bout en une ligne est presque toujours conçu pour être résolu autrement. Règle pratique : utilisez Zsigmondy pour trouver la réponse rapidement, puis rédigez une solution élémentaire (LTE, ordre, taille).

Exemple 15.1.4. *Trouver tous les entiers $a, n \geq 2$ tels que tout facteur premier de $a^n - 1$ divise $a - 1$.*

Avec Zsigmondy. Un diviseur primitif de $a^n - 1$ ne divise pas $a - 1$ (sauf si $n = 1$). Il faut donc être dans un cas d'exception : $n = 2$ avec $a + 1$ puissance de 2, ou $(a, n) = (2,6)$ — ce dernier ne convient pas car $7 \mid 2^6 - 1$ et $7 \nmid 1$. Réponse : $n = 2$ et $a + 1 = 2^k$.

Sans Zsigmondy. Voir le corrigé de l'exercice 7.5, entièrement élémentaire.

15.2 Polynômes cyclotomiques

Définition 15.2.1 (Polynôme cyclotomique)

Le n-ième polynôme cyclotomique est

$$\Phi_n(X) = \prod_{1 \leq k \leq n,\ \mathrm{pgcd}(k,n)=1} \left(X - e^{2i\pi k/n}\right).$$

Théorème 15.2.2 (Propriétés fondamentales)

$\Phi_n \in \mathbb{Z}[X]$, il est unitaire de degré $\varphi(n)$, et

$$X^n - 1 = \prod_{d \mid n} \Phi_d\,(X).$$

Par inversion de Möbius (multiplicative) : $\Phi_n(X) = \prod_{d \mid n} \left(X^d - 1\right)^{\mu(n/d)}$.

Démonstration. Posons $\omega = e^{2i\ /n}$. Le degré de Φ_n est le nombre d'entiers $k \in \{1, \ldots, n\}$ premiers avec n, soit $\varphi(n)$, et Φ_n est unitaire par définition.

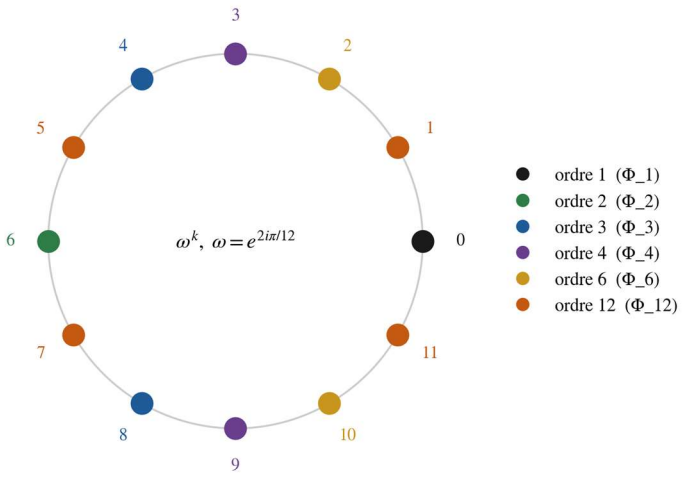
Factorisation. Les racines de $X^n - 1$ sont les n nombres distincts ω^k, $1 \leq k \leq n$, donc $X^n - 1 = \prod_{k=1}^{n} (X - \omega^k)$. Classons-les selon leur ordre (dans le groupe multiplicatif $\mathbb{C}^*$) : l'ordre de ω^k est $d = \frac{n}{\mathrm{pgcd}(k,n)}$ (lemme sur l'ordre d'une puissance, chapitre 7, dont la démonstration vaut dans tout groupe), qui divise n. Pour $d \mid n$, les racines n-ièmes de l'unité d'ordre exactement d sont les racines primitives d-ièmes, c'est-à-dire les $e^{2i\ \ /d}$ avec $\mathrm{pgcd}(j, d) = 1$: ce sont exactement les racines de Φ_d. En regroupant, $X^n - 1 = \prod_{d \mid n} \Phi_d\,(X)$.

Coefficients entiers. Par récurrence forte sur n : $\Phi_1 = X - 1$. Si $\Phi_d \in \mathbb{Z}[X]$ pour tout $d < n$, le polynôme $F = \prod_{d \mid n,\ d<n} \Phi_d$ est unitaire à coefficients entiers, et $X^n - 1 = \Phi_n F$. La division euclidienne de $X^n - 1$ par le polynôme unitaire F s'effectue dans $\mathbb{Z}[X]$ (on ne divise jamais par un coefficient autre que 1) : $X^n - 1 = QF + R$ avec $Q, R \in \mathbb{Z}[X]$ et $\deg R < \deg F$. Par unicité de la division euclidienne dans $\mathbb{C}[X]$, $Q = \Phi_n$ et $R = 0$; donc $\Phi_n \in \mathbb{Z}[X]$.

Inversion. Dans le corps des fractions rationnelles,

$$\prod_{d \mid n} \left(X^d - 1\right)^{\mu(n/d)} = \prod_{d \mid n} \prod_{e \mid d} \Phi_e^{\mu(n/d)} = \prod_{e \mid n} \Phi_e^{\sum_{e \mid d \mid n} \mu(n/d)}.$$

En posant $d = ef$, l'exposant vaut $\sum_{f \mid n/e} \mu\left(\frac{n/e}{f}\right) = \sum_{g \mid n/e} \mu(g)$, qui vaut 1 si $e = n$ et 0 sinon (proposition 9.1.5). Il reste Φ_n. ■



Les racines 12-ièmes de l'unité, classées selon leur ordre d ∈{1, 2, 3, 4, 6, 12} : chaque classe est l'ensemble des racines de Φ_d, ce qui illustre X¹² − 1 = Φ₁Φ₂Φ₃Φ₄Φ₆Φ₁₂.

Exemple 15.2.3. $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$, $\Phi_6 = X^2 - X + 1$ et, pour p premier, $\Phi_p = X^{p-1} + \cdots + X + 1$.

Théorème 15.2.4 (Facteurs premiers des valeurs cyclotomiques)

Soient $a \in \mathbb{Z}$ et p un nombre premier divisant $\Phi_n(a)$. Alors

$$p \equiv 1 \pmod{n} \quad \text{ou} \quad p \mid n.$$

Plus précisément, dans le second cas, p est le plus grand facteur premier de n et $p^2 \nmid \Phi_n(a)$ (sauf si $n = p = 2$).

Démonstration. Nous démontrons un énoncé un peu plus général, dont nous aurons besoin pour Zsigmondy. Pour des entiers a, b, posons $\Phi_n(a,b) = b^{\varphi(n)}\Phi_n\left(\frac{a}{b}\right)$ (si $b \neq 0$), c'est-à-dire, en écrivant $\Phi_n = \sum_j c_j X^j$, $\Phi_n(a,b) = \sum_j c_j\, a^j b^{\varphi(n)-j} \in \mathbb{Z}$: c'est la version homogène, et $\Phi_n(a,1) = \Phi_n(a)$. En homogénéisant l'identité du théorème 15.2.2 (les degrés $\varphi(d)$, $d \mid n$, ont pour somme n), on obtient $a^n - b^n = \prod_{d \mid n} \Phi_d\,(a,b)$.

Lemme. Soient a, b premiers entre eux, $n \geq 1$, et p un premier divisant $\Phi_n(a,b)$. Alors $p \nmid ab$; notons e l'ordre de ab^{-1} modulo p. Ou bien $e = n$ (et alors $n \mid p-1$) ; ou bien $n = p^k e$ avec $k \geq 1$, p est le plus grand facteur premier de n, et $v_p\big(\Phi_n(a,b)\big) = 1$ sauf si $n = 2$.

Preuve. Comme $p \mid a^n - b^n$ et $\gcd(a,b) = 1$, $p \nmid ab$; soit $c \equiv ab^{-1} \pmod{p}$. De $c^n \equiv 1$ on tire $e \mid n$. Écrivons $n = p^k m$ avec $p \nmid m$. Comme $x^p \equiv x \pmod{p}$ pour tout x (Fermat), $c^m \equiv c^{mp^k} = c^n \equiv 1$, donc $e \mid m$.

Soit q un premier divisant n. On a l'identité $X^n - 1 = \big(X^{n/q} - 1\big)Q_q(X)$ avec $Q_q = 1 + X^{n/q} + \cdots + X^{(q-1)n/q}$; par le théorème 15.2.2, $Q_q = \prod_{d \mid n,\, d \nmid n/q} \Phi_d$, produit qui contient Φ_n. En homogénéisant, avec $A = a^{n/q}$ et $B = b^{n/q}$,

$$\Phi_n(a,b) \text{ divise } Q_q(a,b) = A^{q-1} + A^{q-2}B + \cdots + B^{q-1} = \frac{A^q - B^q}{A - B} \quad (\text{si } A \neq B).$$

Supposons $e < n$ et soit q un premier divisant $\frac{n}{e}$. Alors $e \mid \frac{n}{q}$, donc $c^{n/q} \equiv 1$, c'est-à-dire $A \equiv B \pmod p$, et $Q_q(a,b) \equiv qB^{q-1} \pmod p$. Comme $p \mid Q_q(a,b)$ et $p \nmid B$, on obtient $p \mid q$, soit $q = p$. Ainsi $\frac{n}{e}$ est une puissance p^j de p avec $j \geq 1$; comme $p \nmid e$ (car $e \mid m$), on a $e = m$ et $j = k \geq 1$. De plus $e \mid p - 1$, donc tous les facteurs premiers de m sont $< p$: p est le plus grand facteur premier de n.

Enfin, prenons $q = p$: $A \equiv B \pmod p$ car $e = m \mid \frac{n}{p}$. Si p est impair, le lemme LTE (théorème 14.1.2) donne $v_p(A^p - B^p) = v_p(A - B) + 1$, donc $v_p\left(Q_p(a,b)\right) = 1$ et $v_p\big(\Phi_n(a,b)\big) \leq 1$. Si $p = 2$, alors $m \mid p - 1 = 1$, donc $n = 2^k$; si $k \geq 2$, $\frac{n}{2}$ est pair, a, b sont impairs (car $2 \mid a^n - b^n$), donc A et B sont des carrés impairs, $A \equiv B \equiv 1 \pmod 8$, et $Q_2(a,b) = A + B \equiv 2 \pmod 8$: $v_2\big(\Phi_n(a,b)\big) \leq 1$. ▫

Démonstration du théorème. On applique le lemme avec $b = 1$: si $p \mid \Phi_n(a)$, ou bien $\mathrm{ord}_p(a) = n$ et $p \equiv 1 \pmod n$, ou bien $p \mid n$, p est le plus grand facteur premier de n et $p^2 \nmid \Phi_n(a)$ (sauf si $n = p = 2$). ■

	$2^n - 1$	facteurs premiers			
$n = 1$	1	1 (aucun facteur premier)			
$n = 2$	3	3			
$n = 3$	7	7			
$n = 4$	15	3	5		
$n = 5$	31	31			
$n = 6$	63	3^2	7	← aucun diviseur primitif	
$n = 7$	127	127			
$n = 8$	255	3	5	17	
$n = 9$	511	7	73		
$n = 10$	1023	3	11	31	
$n = 11$	2047	23	89		
$n = 12$	4095	3^2	5	7	13

Facteurs premiers de $2^n - 1$ pour $1 \leq n \leq 12$: en couleur, les diviseurs primitifs (d'ordre exactement n). Seuls n = 1 et n = 6 n'en ont pas, conformément au théorème de Zsigmondy.

Exemple 15.2.5. *Montrer qu'il existe une infinité de nombres premiers $p \equiv 1 \pmod n$, pour tout $n \geq 1$.*

Supposons que $p_1, \ldots, p_k$ soient les seuls. Posons $N = np_1 \cdots p_k$ et considérons $\Phi_n(mN)$ pour m assez grand : c'est un entier > 1 en valeur absolue (car Φ_n est unitaire non constant). Soit p un de ses facteurs premiers. Par le théorème 15.2.4, $p \equiv 1 \pmod n$ ou $p \mid n$. Or $\Phi_n(mN) \equiv \Phi_n(0) \pmod N$, et $\Phi_n(0) = \pm 1$: en effet, en évaluant $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ en 0, on obtient $-1 = \prod_{d \mid n} \Phi_d(0)$, produit d'entiers ; donc $p \nmid N$: en particulier $p \nmid n$, donc $p \equiv 1 \pmod n$, et $p \neq p_i$ pour tout i. Contradiction.

À retenir

Ce raisonnement est la version élémentaire du théorème de Dirichlet dans le cas de la progression arithmétique des entiers $\equiv 1 \pmod n$. Il est parfaitement rédigeable en compétition et évite d'invoquer un théorème hors programme.

15.3 Démonstration du théorème de Zsigmondy

Lemme 15.3.1 (Deux identités cyclotomiques)

Soient P un nombre premier et $m \geq 1$ un entier non divisible par P. Alors

$$\text{(i)}\quad \Phi_m(X^P) = \Phi_m(X)\,\Phi_{Pm}(X)\,; \qquad \text{(ii)}\quad \Phi_{P^k m}(X) = \Phi_{Pm}\left(X^{P^{k-1}}\right) \quad (k \geq 1).$$

Démonstration. On utilise $X^N - y = \prod_{x^N = y}(X - x)$ pour $y \neq 0$ (les N racines N-ièmes de y sont distinctes) et le lemme sur l'ordre d'une puissance : si x est d'ordre t, x^N est d'ordre $\frac{t}{\operatorname{pgcd}(t,N)}$.

(i) $\Phi_m(X^P) = \prod_y (X^P - y)$, où y parcourt les racines primitives m-ièmes ; c'est le produit des $X - x$ pour les x tels que x^P soit d'ordre m. Un tel x vérifie $x^{Pm} = 1$, donc son ordre t divise Pm, et $\frac{t}{\operatorname{pgcd}(t,P)} = m$ impose $t = m$ ou $t = Pm$. Réciproquement, les x d'ordre m ou Pm conviennent (car $P \nmid m$). Les racines sont donc celles de Φ_m et de Φ_{Pm}, toutes simples ; les degrés concordent ($P\varphi(m) = \varphi(m) + \varphi(Pm)$), d'où (i).

(ii) De même, $\Phi_{Pm}\left(X^{P^{k-1}}\right)$ est le produit des $X - x$ pour les x tels que $x^{P^{k-1}}$ soit d'ordre Pm. Si x est d'ordre t, alors $t \mid P^k m$; en écrivant $t = P^j m'$ avec $m' \mid m$, l'ordre de $x^{P^{k-1}}$ est $P^{\max(j-k+1,0)}m'$, qui vaut Pm si, et seulement si, $j = k$ et $m' = m$, c'est-à-dire $t = P^k m$. On obtient exactement les racines de $\Phi_{P^k m}$, et les degrés concordent ($P^{k-1}\varphi(Pm) = \varphi\left(P^k m\right)$). ■

Démonstration du théorème 15.1.3 (Zsigmondy). Soient $a > b \geq 1$ premiers entre eux. Pour $n \geq 1$, $\Phi_n(a,b) = \prod_\zeta (a - \zeta b)$, où ζ parcourt les racines primitives n-ièmes de l'unité ; c'est un entier strictement positif (pour $n \geq 3$, les facteurs se groupent en paires conjuguées de produit $|a - \zeta b|^2 > 0$). Si p est un premier divisant $\Phi_n(a,b)$ et si, avec les notations du lemme de la démonstration du théorème 15.2.4, l'ordre de ab^{-1} modulo p vaut n, alors p est un diviseur primitif (proposition 15.1.2).

Cas $n = 1$. La condition « ne divise aucun $a^k - b^k$, $k < 1$ » est vide : $a - b$ a un diviseur primitif si, et seulement si, $a - b > 1$.

Cas $n = 2$. Un premier impair $p \mid a + b$ ne divise pas $a - b$ (sinon $p \mid 2a$ et $p \mid 2b$, donc $p \mid a$ et $p \mid b$) : c'est un diviseur primitif de $a^2 - b^2$. Le premier 2, lui, n'est jamais primitif (s'il divise $a + b$, a et b sont impairs et $2 \mid a - b$). Il y a donc un diviseur primitif si, et seulement si, $a + b$ n'est pas une puissance de 2.

Cas $n \geq 3$. Supposons que $a^n - b^n$ n'ait pas de diviseur primitif. Pour ζ non réel, $|a - \zeta b|^2 = (a-b)^2 + 2ab(1 - \cos\theta) > (a-b)^2 \geq 1$ (où $\zeta = e^{i\theta}$), donc $\Phi_n(a,b) > 1$ admet un facteur premier p. Par le lemme, $n = P^k m$ où $P = p$ est le plus grand facteur premier de n, $k \geq 1$, $m = \operatorname{ord}_P(ab^{-1}) \mid P - 1$, et tout facteur premier de $\Phi_n(a,b)$ est égal à P, avec exposant 1 : ainsi $\Phi_n(a,b) = P$. Montrons que c'est impossible, sauf si $(n,a,b) = (6,2,1)$.

Posons $A = a^{P^{k-1}}$, $B = b^{P^{k-1}}$, de sorte que $A > B \geq 1$. Par le lemme 15.3.1 (ii) puis (i), homogénéisés,

$$P = \Phi_n(a,b) = \Phi_{Pm}(A,B) = \frac{\Phi_m(A^P, B^P)}{\Phi_m(A,B)} = \prod_\zeta \frac{A^P - \zeta B^P}{A - \zeta B},$$

le produit portant sur les $\varphi(m)$ racines primitives m-ièmes ζ.

- Si $m = 1$: $P = \frac{A^P - B^P}{A-B} = A^{P-1} + A^{P-2}B + \cdots + B^{P-1}$, somme de P entiers ≥ 1 dont le premier est ≥ 2 ; elle est $> P$: contradiction.
- Si $m \geq 2$: alors $P \geq 3$ (car $m \mid P-1$). Comme $|A^P - \zeta B^P| \geq A^P - B^P$ et $0 < |A - \zeta B| \leq A + B$, on obtient $P \geq \left(\frac{A^P - B^P}{A+B}\right)^{\varphi(m)}$. Montrons que $A^P - B^P > P(A+B)$ sauf si $(A,B,P) = (2,1,3)$; on aura alors $\frac{A^P - B^P}{A+B} > P > 1$, et le membre de droite dépassera P : contradiction. Le membre de gauche décroît et celui de droite croît avec B ; il suffit donc de traiter $B = A-1$, soit $A^P - (A-1)^P > P(2A-1)$. Or $A^P - (A-1)^P = \sum_{j=0}^{P-1} A^j (A-1)^{P-1-j} \geq P(A-1)^{P-1}$.
  - Si $A \geq 4$: $(A-1)^{P-1} \geq (A-1)^2 > 2A-1$ (car $A^2 - 4A + 2 > 0$).
  - Si $A = 3$: pour $P \geq 5$, $2^{P-1} \geq 16 > 5$; pour $P = 3$, on vérifie directement $27 - 8 = 19 > 15$ et $27 - 1 = 26 > 12$.
  - Si $A = 2$ (donc $B = 1$) : il faut $2^P - 1 > 3P$, vrai pour $P = 5$ ($31 > 15$) et, par récurrence, pour tout $P \geq 5$; pour $P = 3$, on a $7 \leq 9$: c'est le seul cas d'échec.

  Reste $(A,B,P) = (2,1,3)$: $a^{3^{k-1}} = 2$ impose $k = 1$, $a = 2$, $b = 1$, et $m \mid 2$, $m \geq 2$ donne $m = 2$, $n = 6$. Effectivement $\Phi_6(2,1) = 4 - 2 + 1 = 3 = P$: c'est l'exception.

Version additive. Un diviseur primitif p de $a^{2n} - b^{2n}$ divise $a^n + b^n$ (il divise $(a^n - b^n)(a^n + b^n)$ sans diviser $a^n - b^n$), et ne divise aucun $a^k + b^k$ avec $k < n$ (sinon il diviserait $a^{2k} - b^{2k}$ avec $2k < 2n$). Les exceptions pour $2n$ sont $2n = 2$ (mais pour $n = 1$, tout facteur premier de $a + b \geq 3$ convient) et $2n = 6$ avec $(a,b) = (2,1)$: d'où l'unique exception $2^3 + 1 = 9$. ■

15.4 Exercices

Exercice 15.1 ★★. Calculer $\Phi_{12}(X)$ et $\Phi_{15}(X)$.

Exercice 15.2 ★★. Montrer que si $p \mid \Phi_n(a)$ et $p \nmid n$, alors $\mathrm{ord}_p(a) = n$.

Exercice 15.3 ★★★. Déterminer tous les couples (a,n) d'entiers strictement positifs tels que $a^n + 1$ soit une puissance de 2.

Exercice 15.4 ★★★. Montrer que pour tout $n \geq 2$, $n \neq 6$, $2^n - 1$ possède un facteur premier ne divisant aucun $2^k - 1$ pour $1 \leq k < n$, et que ce facteur est $\equiv 1 \pmod{n}$. Peut-on toujours en trouver deux distincts ? (Discuter à l'aide de Zsigmondy et du théorème 15.2.4.)

15.5 Corrigés

Solution de l'exercice 15.1. $\Phi_{12}(X) = X^4 - X^2 + 1$ (degré $\varphi(12) = 4$). $\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$ (degré $\varphi(15) = 8$).

Solution de l'exercice 15.2. Reprendre la preuve du théorème 15.2.4 : si $\mathrm{ord}_p(a) = d < n$, alors a est racine multiple de $X^n - 1$ modulo p, donc $p \mid n$ — exclu.

Solution de l'exercice 15.3. Cherchons $a, n \geq 1$ avec $a^n + 1 = 2^m$.

Si $a = 1$: $2 = 2^1$, tout n convient. Supposons donc $a \geq 2$; alors a est impair (sinon $a^n + 1$ est impair et > 1).

n n'a pas de facteur premier impair. Si q est un nombre premier impair divisant n, posons $A = a^{n/q}$ (impair, ≥ 3). Alors

$$a^n + 1 = A^q + 1 = (A+1)(A^{q-1} - A^{q-2} + \cdots - A + 1),$$

et le second facteur est une somme de q termes impairs, donc impair ; il vaut au moins $A^{q-1} - A^{q-2} \geq 2$, donc il est impair et > 1 : il ne peut diviser une puissance de 2. Contradiction.

Donc $n = 2^s$. Si $s \geq 1$, alors $a^n = \left(a^{n/2}\right)^2$ est un carré impair, donc $a^n \equiv 1 \pmod 8$, d'où $a^n + 1 \equiv 2 \pmod 8$: la seule puissance de 2 possible est 2 elle-même, soit $a^n = 1$, impossible pour $a \geq 2$.

Conclusion : $s = 0$, c'est-à-dire $n = 1$, et $a + 1$ est une puissance de 2.

Réponse : $a = 1$ (avec n quelconque), ou $n = 1$ avec $a = 2^m - 1$.

Solution de l'exercice 15.4. Appliquons Zsigmondy avec $a = 2$, $b = 1$: l'exception $n = 1$, $a - b = 1$ est écartée par $n \geq 2$; l'exception $n = 2$ ne se produit pas car $a + b = 3$ n'est pas une puissance de 2 ; reste l'exception $n = 6$. Pour $n \geq 2$, $n \neq 6$, $2^n - 1$ possède donc un diviseur primitif p, et $p \equiv 1 \pmod n$ par la proposition 15.1.2.

On ne peut pas en garantir deux. Comme $2^n - 1 = \prod_{d|n} \Phi_d(2)$, les diviseurs primitifs de $2^n - 1$ sont exactement les facteurs premiers de $\Phi_n(2)$ ne divisant pas n (exercice 15.2) ; d'après le théorème 15.2.4, $\Phi_n(2)$ admet au plus un facteur premier non primitif, de multiplicité 1. Il y a donc deux diviseurs primitifs distincts dès que $\Phi_n(2)$, privé de ce facteur éventuel, n'est pas une puissance d'un nombre premier — ce qui arrive souvent, mais pas toujours : pour $n = 7$, $2^7 - 1 = 127$ est premier ; pour $n = 8$, $2^8 - 1 = 255 = 3 \cdot 5 \cdot 17$ avec $3 \mid 2^2 - 1$ et $5 \mid 2^4 - 1$, de sorte que $17 = \Phi_8(2)$ est le seul diviseur primitif. Plus généralement, chaque nombre premier de Mersenne $2^p - 1$ ($p = 2,3,5,7,13,17,19,31,\ldots$) fournit un contre-exemple, et l'on ne sait même pas s'il en existe une infinité.

CHAPITRE 16

16 Le saut de Viète (Vieta jumping)

Objectifs du chapitre.

- Comprendre le mécanisme : une équation symétrique, de degré 2 en chacune des variables, engendre une involution sur les solutions.
- Maîtriser le schéma standard de la descente par saut de Viète.
- Traiter le problème 6 de l'IMO 1988, archétype de la méthode.

16.1 Le mécanisme

Supposons qu'une équation diophantienne $F(x,y)=0$ soit de degré 2 en x : $x^2 - S(y)x + P(y) = 0$. Si (x_0, y_0) est une solution, alors x_0 est racine de ce trinôme, et l'autre racine

$$x_1 = S(y_0) - x_0 = \frac{P(y_0)}{x_0}$$

est encore un entier (première expression) et donne une nouvelle solution (x_1, y_0). La première expression prouve l'intégralité, la seconde contrôle le signe et la taille.

Méthode 16.1.1 — Schéma standard

1. Supposer l'existence d'une solution « mauvaise » et choisir celle qui minimise $x+y$ (avec $x \geq y$).
2. Fixer y et voir l'équation comme un trinôme en x ; calculer l'autre racine x'.
3. Montrer que x' est un entier (somme des racines) et que $x' > 0$ (produit des racines, ou évaluation du trinôme en un point).
4. Montrer que $x' < x$ (souvent même $x' < y \leq x$) : la solution formée de x' et y a une somme strictement plus petite. Contradiction.

16.2 Le problème archétype

Théorème 16.2.1 (IMO 1988, problème 6)

Soient a, b des entiers strictement positifs tels que $ab+1$ divise a^2+b^2. Alors $\frac{a^2+b^2}{ab+1}$ est un carré parfait.

Démonstration. Posons $k = \frac{a^2+b^2}{ab+1}$, entier ≥ 1, et supposons, par l'absurde, que k n'est pas un carré parfait. L'ensemble des couples (a,b) d'entiers ≥ 0 solutions de

$$a^2 + b^2 = k(ab+1) \qquad (*)$$

est non vide (il contient le couple de l'énoncé) ; choisissons-en un qui minimise $a+b$, et, quitte à échanger, $a \geq b$. On a $b \geq 1$: si $b=0$, alors $a^2 = k$ serait un carré.

Fixons b et considérons $(*)$ comme une équation du second degré en x :

$$x^2 - (kb)x + (b^2 - k) = 0.$$

Elle admet a pour racine ; l'autre racine est

$$a' = kb - a = \frac{b^2 - k}{a}.$$

La première égalité montre que a' est un entier.

$a' \neq 0$: sinon $b^2 = k$, et k serait un carré.

$a' > 0$: si $a' < 0$, alors $a' \leq -1$ et

$$a'^2 - kba' + b^2 - k \geq 1 + kb + b^2 - k = 1 + b^2 + k(b-1) > 0$$

(car $a'^2 \geq 1$ et $-kba' \geq kb$), ce qui contredit le fait que a' est racine.

$a' < a$: comme $a \geq b$, on a

$$a' = \frac{b^2 - k}{a} < \frac{b^2}{a} \leq \frac{a^2}{a} = a,$$

l'inégalité stricte venant de $k > 0$.

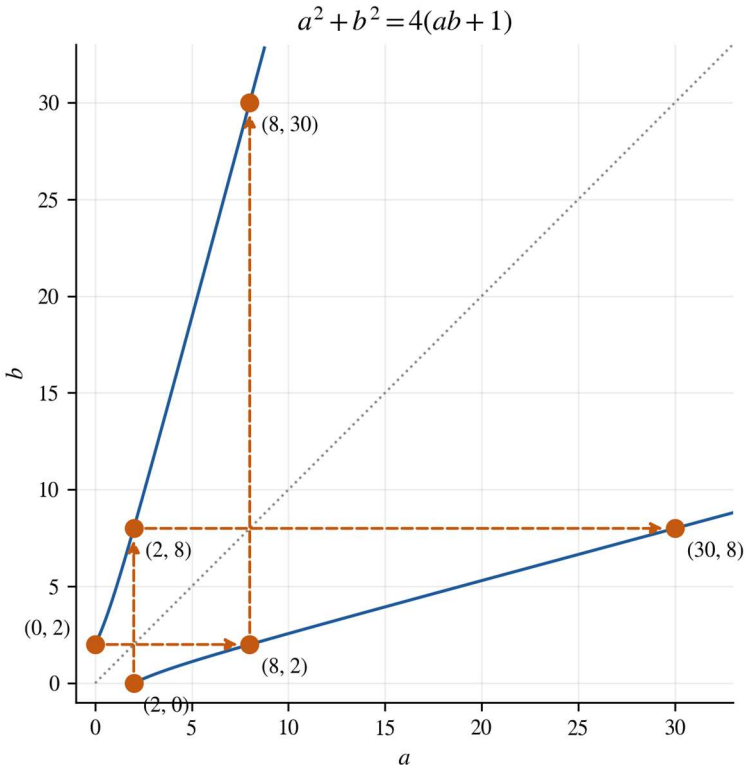
Le couple (a', b) est donc une solution de $(*)$ en entiers positifs (l'équation est symétrique, l'ordre importe peu) avec $a' + b < a + b$: contradiction avec la minimalité.

Donc k est un carré parfait. ■

Remarque.

La structure des solutions est d'ailleurs explicite : si $k = t^2$ avec $t \geq 2$, les solutions en entiers strictement positifs avec $a \geq b$ sont les couples (a_{n+1}, a_n), $n \geq 1$, obtenus par itération du saut $a_{n+1} = t^2 a_n - a_{n-1}$ à partir de $a_0 = 0$, $a_1 = t$; la plus petite est $(a_2, a_1) = (t^3, t)$.

Justification. Si (a, b) est une solution avec $a \geq b \geq 1$, le calcul précédent (qui n'utilisait pas l'hypothèse « k non carré » pour établir $a' \geq 0$ et $a' < a$) montre que $a' = kb - a = \frac{b^2 - k}{a}$ vérifie $0 \leq a' < \frac{b^2}{a} \leq b$; le saut $(a, b) \mapsto (b, a')$ fait donc strictement décroître la somme et aboutit, après un nombre fini d'étapes, à un couple $(b, 0)$, c'est-à-dire $b^2 = k$, $b = t$. En remontant (le saut inverse est $(b, c) \mapsto (kb - c, b)$), toute solution s'obtient à partir de $(t, 0)$ par la récurrence $a_{n+1} = t^2 a_n - a_{n-1}$; réciproquement, chaque saut transforme une solution en solution, et pour $t \geq 2$ la suite est strictement croissante ($a_{n+1} - a_n = (t^2 - 2)a_n + (a_n - a_{n-1}) > 0$ par récurrence).



Saut de Viète pour k = 4 (t = 2) : les points entiers de la conique a² + b² = 4(ab + 1) dans le premier quadrant sont (0, 2), (2, 8), (8, 30), … ; chaque saut, alternativement horizontal et vertical, relie deux solutions consécutives.

Exemple 16.2.2 (IMO 2007, problème 5). *Soient a, b des entiers strictement positifs tels que $4ab - 1$ divise $(4a^2 - 1)^2$. Montrer que $a = b$.*

Étape 1 : reformulation. Modulo $4ab - 1$, on a $4ab \equiv 1$, donc

$$b(4a^2 - 1) = a(4ab) - b \equiv a - b \pmod{4ab - 1}.$$

Comme $\gcd(b, 4ab - 1) = 1$, la condition $4ab - 1 \mid (4a^2 - 1)^2$ équivaut à $4ab - 1 \mid b^2(4a^2 - 1)^2$, c'est-à-dire

$$4ab - 1 \mid (a - b)^2.$$

Étape 2 : saut de Viète. Supposons qu'il existe une solution avec $a \neq b$ et posons $k = \frac{(a-b)^2}{4ab-1} \geq 1$. Parmi les couples (a, b) d'entiers > 0 vérifiant $(a - b)^2 = k(4ab - 1)$, choisissons celui qui minimise $a + b$, avec $a > b$.

Développons : $a^2 - (2b + 4kb)a + (b^2 + k) = 0$. L'autre racine est

$$a' = 2b + 4kb - a = \frac{b^2 + k}{a},$$

donc a' est un entier (première expression) strictement positif (seconde expression), et (a', b) est encore solution, puisque a' est racine du même trinôme.

Montrons que $a' < b$. Si $a' \geq b$, alors $aa' = b^2 + k \geq ab$, donc $k \geq b(a - b)$. En reportant :

$$(a - b)^2 = k(4ab - 1) \geq b(a - b)(4ab - 1),$$

d'où $a - b \geq b(4ab - 1) = 4ab^2 - b$, soit $a \geq 4ab^2$ et $1 \geq 4b^2$: impossible.

Donc $a' < b$, et (b, a') est une solution avec $b \neq a'$ et $b + a' < a + b$: contradiction avec la minimalité. Ainsi $a = b$.

16.3 Exercices

Exercice 16.1 ★★. Montrer que si des entiers $x, y > 0$ vérifient $\frac{x^2+y^2+1}{xy} \in \mathbb{Z}$, alors cette valeur est 3.

Exercice 16.2 ★★★. Soient $a, b > 0$ des entiers tels que $ab \mid a^2 + b^2 + 1$. Montrer que $\frac{a^2+b^2+1}{ab} = 3$.

Exercice 16.3 ★★★. Trouver tous les entiers k tels que $\frac{a^2+b^2}{ab-1} = k$ ait une solution en entiers $a, b > 0$.

Exercice 16.4 ★★★★. Sachant que si $\frac{a^2+b^2}{ab+1} = k$ alors k est un carré (théorème 16.2.1), décrire toutes les solutions pour $k = 4$.

16.4 Corrigés

Solution des exercices 16.1 et 16.2. Posons $k = \frac{a^2+b^2+1}{ab}$ et prenons une solution minimisant $a + b$ avec $a \geq b$. L'équation $a^2 - kba + (b^2 + 1) = 0$ a pour seconde racine $a' = kb - a = \frac{b^2+1}{a}$, entier > 0. Si $a > b$, alors $a' = \frac{b^2+1}{a} \leq \frac{b^2+1}{b+1} \leq b$, donc (b, a') est plus petite : la minimalité impose $a = b$. Alors $a^2 \mid 2a^2 + 1$, donc $a^2 \mid 1$, $a = b = 1$ et $k = 3$.

Solution de l'exercice 16.3. Réponse : $k = 5$.

Soit (a, b) une solution en entiers > 0 de $a^2 + b^2 = k(ab - 1)$, avec $a \geq b$, choisie de sorte que $a + b$ soit minimal.

Étape 1 : le saut. Vu comme trinôme en a,

$$a^2 - kb\,a + (b^2 + k) = 0,$$

la seconde racine vaut $a' = kb - a = \frac{b^2+k}{a}$: c'est un entier strictement positif, et (a', b) est encore une solution. La minimalité de $a + b$ impose $a' \geq a$, c'est-à-dire $a^2 \leq b^2 + k$.

Étape 2 : majoration de k. En reportant dans l'équation,

$$k(ab - 1) = a^2 + b^2 \leq 2b^2 + k \Longrightarrow k(ab - 2) \leq 2b^2.$$

Si $b \geq 3$, alors $a \geq b \geq 3$ donne $ab - 2 \geq b^2 - 2 \geq 7$, donc

$$k \leq \frac{2b^2}{b^2 - 2} \leq \frac{18}{7} < 3.$$

Mais $k \leq 2$ est impossible : l'inégalité $2ab \leq a^2 + b^2$ donnerait $a^2 + b^2 = k(ab - 1) \leq 2ab - 2 \leq a^2 + b^2 - 2$. Donc $b \leq 2$.

Étape 3 : les deux cas.

- $b = 1$: $k = \frac{a^2+1}{a-1}$. Comme $a^2 + 1 = (a - 1)(a + 1) + 2$, il faut $a - 1 \mid 2$, donc $a \in \{2,3\}$, et $k = 5$ dans les deux cas.
- $b = 2$: $k = \frac{a^2+4}{2a-1}$. Comme $4(a^2 + 4) = (2a - 1)(2a + 1) + 17$, il faut $2a - 1 \mid 17$, donc $a \in \{1,9\}$; avec $a \geq b = 2$: $a = 9$ et $k = \frac{85}{17} = 5$.

Ainsi $k = 5$ est la seule valeur possible, et elle est atteinte : en repartant de $(2,1)$ et en itérant le saut $a_{n+1} = 5a_n - a_{n-1}$, on obtient la famille infinie $(2,1), (9,2), (43,9), (206,43), \ldots$

Solution de l'exercice 16.4. Pour $k = 4$: on cherche les couples (a, b) solutions de $a^2 + b^2 = 4(ab + 1)$. La solution minimale en entiers strictement positifs est $(a, b) = (8,2)$ (car $64 + 4 = 68 = 4 \cdot 17$). Le saut donne $a_{n+1} = 4a_n - a_{n-1}$ avec $(a_0, a_1) = (0,2)$: 0,2,8,30,112, ..., et les solutions sont les couples consécutifs (a_{n+1}, a_n), $n \geq 1$, et leurs symétriques (a_n, a_{n+1}).

CHAPITRE 17

17 Coefficients binomiaux et arithmétique

Objectifs du chapitre.

- Calculer $v_p\left(\binom{n}{k}\right)$ (théorèmes de Legendre et Kummer).
- Utiliser le théorème de Lucas.
- Exploiter le coefficient binomial central et le postulat de Bertrand.

17.1 Valuation d'un coefficient binomial

Théorème 17.1.1 (Kummer)

Soient p premier et $0 \leq k \leq n$. Alors $v_p\left(\binom{n}{k}\right)$ est égal au nombre de retenues lorsqu'on additionne k et $n-k$ en base p.

Démonstration. Notons $\ell = n-k$. Par la seconde formule de Legendre (théorème 3.3.1), $v_p(m!) = \frac{m - S_p(m)}{p-1}$, où $S_p(m)$ est la somme des chiffres de m en base p. Donc

$$v_p\left(\binom{n}{k}\right) = v_p(n!) - v_p(k!) - v_p(\ell!) = \frac{S_p(k) + S_p(\ell) - S_p(n)}{p-1}.$$

Écrivons $k = \sum k_i p^i$, $\ell = \sum \ell_i p^i$, $n = \sum n_i p^i$, et effectuons l'addition posée $k + \ell = n$: en notant $c_i \in \{0,1\}$ la retenue reçue par la position i (avec $c_0 = 0$), on a, pour chaque position,

$$k_i + \ell_i + c_i = n_i + p\, c_{i+1}.$$

En sommant sur toutes les positions (la dernière retenue émise est nulle, puisque n a assez de chiffres), on obtient $S_p(k) + S_p(\ell) + C = S_p(n) + pC$, où $C = \sum_i c_i = \sum_i c_{i+1}$ est le nombre de retenues. Donc $S_p(k) + S_p(\ell) - S_p(n) = (p-1)C$, et $v_p\left(\binom{n}{k}\right) = C$. ∎

Corollaire 17.1.2

Soit p premier et $n \geq 2$. On a $p \mid \binom{n}{k}$ pour tout $1 \leq k \leq n-1$ si, et seulement si, n est une puissance de p.

Démonstration. *Si* $n = p^m$ $(m \geq 1)$ et $1 \leq k \leq n-1$: de $k\binom{n}{k} = n\binom{n-1}{k-1}$ on tire $v_p(k) + v_p\left(\binom{n}{k}\right) \geq m$; comme $k < p^m$, $v_p(k) < m$, donc $v_p\left(\binom{n}{k}\right) \geq 1$.

Si n n'est pas une puissance de p, soit p^m la plus grande puissance de p inférieure ou égale à n ; alors $p^m < n$, et l'écriture de n en base p a pour premier chiffre $n_m \geq 1$ en position m. Prenons $k = p^m \in \{1, \ldots, n-1\}$: l'entier $n - p^m$ a les mêmes chiffres que n, sauf le chiffre de position m qui vaut $n_m - 1$. L'addition de p^m et de $n - p^m$ ne produit aucune retenue (aux positions $< m$ on ajoute 0 ; en position m, $(n_m - 1) + 1 = n_m \leq p-1$). Par le théorème de Kummer, $p \nmid \binom{n}{p^m}$. ∎

Théorème 17.1.3 (Lucas)

Soient p premier et $n = \sum n_i p^i$, $k = \sum k_i p^i$ les écritures en base p. Alors

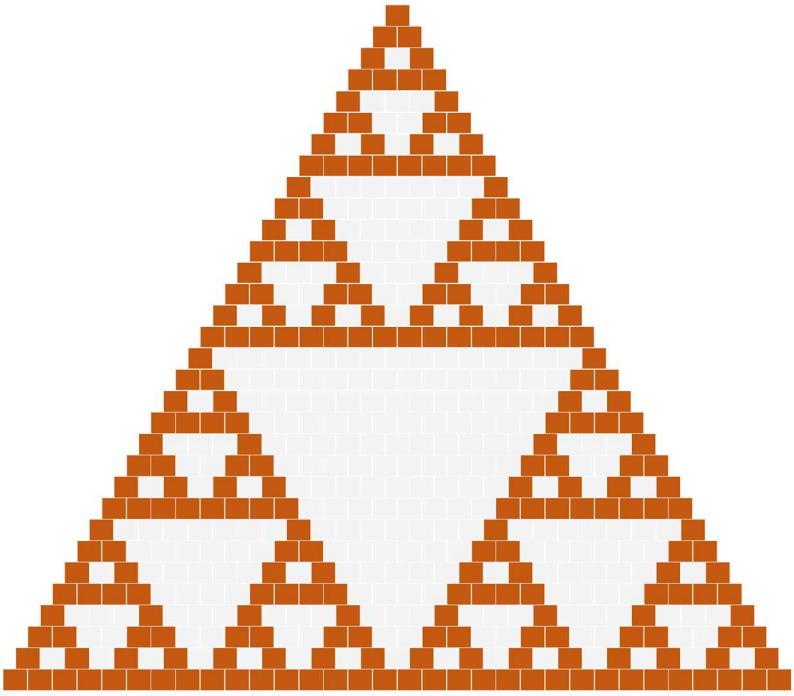
$$\binom{n}{k} \equiv \prod_i \binom{n_i}{k_i} \pmod{p},$$

avec la convention $\binom{a}{b} = 0$ si $b > a$.

Démonstration. Travaillons dans $\mathbb{F}_p[X]$, c'est-à-dire avec des polynômes à coefficients considérés modulo p. Comme $p \mid \binom{p}{j}$ pour $1 \le j \le p-1$, on a $(A+B)^p = A^p + B^p$ pour tous polynômes A, B, et par récurrence sur i, $(1+X)^{p^i} = \left((1+X)^{p^{i-1}}\right)^p = \left(1+X^{p^{i-1}}\right)^p = 1 + X^{p^i}$. Donc

$$(1+X)^n = \prod_i \left((1+X)^{p^i}\right)^{n_i} = \prod_i \left(1+X^{p^i}\right)^{n_i} = \prod_i \sum_{j=0}^{n_i} \binom{n_i}{j} X^{jp^i}.$$

En développant le produit, on obtient une somme de termes $\prod_i \binom{n_i}{j_i} X^{\sum_i j_i p^i}$ avec $0 \le j_i \le n_i \le p-1$. Par unicité de l'écriture en base p, l'exposant $\sum_i j_i\, p^i$ vaut k si, et seulement si, $j_i = k_i$ pour tout i ; ce choix n'est possible que si $k_i \le n_i$ pour tout i. Le coefficient de X^k est donc $\prod_i \binom{n_i}{k_i}$ (nul si un k_i dépasse n_i, conformément à la convention). En comparant avec le coefficient $\binom{n}{k}$ de X^k dans $(1+X)^n$, on conclut. ■



Le triangle de Pascal modulo 2 (32 premières lignes) : les cases colorées sont les coefficients impairs. Par Lucas, C(n, k) est impair si, et seulement si, chaque chiffre binaire de k est inférieur au chiffre correspondant de n ; on voit apparaître le triangle de Sierpiński.

Exemple 17.1.4. *Calculer* $\binom{1000}{500} \bmod 7$.

On a $1000 = 2\cdot 343 + 6\cdot 49 + 2\cdot 7 + 6 = (2,6,2,6)_7$ et $500 = 1\cdot 343 + 3\cdot 49 + 1\cdot 7 + 3 = (1,3,1,3)_7$. Donc, par le théorème de Lucas,

$$\binom{1000}{500} \equiv \binom{2}{1}\binom{6}{3}\binom{2}{1}\binom{6}{3} = 2\cdot 20\cdot 2\cdot 20 = 1600 \equiv 4 \pmod 7,$$

puisque $1600 = 7\cdot 228 + 4$.

17.2 Le coefficient central et Bertrand

Proposition 17.2.1 (Encadrement du coefficient central)

Pour tout $n \geq 1$,

$$\frac{4^n}{2n+1} \leq \binom{2n}{n} \leq 4^n.$$

Démonstration. Par la formule du binôme, $\sum_{k=0}^{2n}\binom{2n}{k} = (1+1)^{2n} = 4^n$; tous les termes étant positifs, $\binom{2n}{n} \leq 4^n$. Par ailleurs $\frac{\binom{2n}{k}}{\binom{2n}{k-1}} = \frac{2n-k+1}{k} \geq 1$ si, et seulement si, $k \leq n$: la suite des coefficients croît jusqu'à $k = n$ puis décroît, et $\binom{2n}{n}$ est le plus grand des $2n+1$ termes. Donc $4^n \leq (2n+1)\binom{2n}{n}$. ∎

Théorème 17.2.2 (Postulat de Bertrand)

Pour tout $n \geq 1$, il existe un premier p avec $n < p \leq 2n$.

Démonstration (Erdős). *Étape 1 : $\prod_{p\leq x} p < 4^x$ pour tout réel $x \geq 1$* (produit sur les nombres premiers). Il suffit de montrer $\prod_{p\leq m} p \leq 4^{m-1}$ pour tout entier $m \geq 1$, par récurrence forte. C'est vrai pour $m = 1$ et $m = 2$. Si $m > 2$ est pair, m n'est pas premier et le produit est celui de $m-1$. Si $m = 2s+1$, les premiers p avec $s+2 \leq p \leq 2s+1$ divisent $\binom{2s+1}{s} = \frac{(2s+1)!}{s!\,(s+1)!}$ (ils divisent le numérateur mais pas le dénominateur), et $\binom{2s+1}{s} = \binom{2s+1}{s+1}$ sont deux termes de la somme $\sum_k \binom{2s+1}{k} = 2^{2s+1}$, d'où $\binom{2s+1}{s} \leq 4^s$. Donc

$$\prod_{p\leq 2s+1} p = \prod_{p\leq s+1} p \cdot \prod_{s+2\leq p\leq 2s+1} p \leq 4^s \cdot 4^s = 4^{m-1}.$$

Étape 2 : $p^{v_p\left(\binom{2n}{n}\right)} \leq 2n$ pour tout premier p. Par la formule de Legendre, $v_p\left(\binom{2n}{n}\right) = \sum_{i\geq 1}\left(\left\lfloor\frac{2n}{p^i}\right\rfloor - 2\left\lfloor\frac{n}{p^i}\right\rfloor\right)$. Chaque terme vaut 0 ou 1 (car $\lfloor 2y\rfloor - 2\lfloor y\rfloor \in \{0,1\}$ par la proposition 10.1.2 (ii)) et il est nul dès que $p^i > 2n$. Donc $v_p \leq r$, où $p^r \leq 2n < p^{r+1}$. En particulier, si $p > \sqrt{2n}$, $v_p\left(\binom{2n}{n}\right) \leq 1$.

Étape 3 : si $n \geq 3$ et $\frac{2n}{3} < p \leq n$, alors $p \nmid \binom{2n}{n}$. On a $p \geq 3$, donc $p^2 \geq 3p > 2n$: seul le terme $i = 1$ subsiste, et $2 \leq \frac{2n}{p} < 3$, $1 \leq \frac{n}{p} < \frac{3}{2}$, d'où $v_p = 2 - 2\cdot 1 = 0$.

Étape 4 : conclusion pour $n \geq 4000$. Supposons qu'aucun premier ne soit dans $]n, 2n]$. Les facteurs premiers de $\binom{2n}{n}$ divisent $(2n)!$, donc sont $\leq 2n$, et, par l'étape 3, ils sont $\leq \frac{2n}{3}$. Par l'étape 2, les premiers $p \leq \sqrt{2n}$ (il y en a au plus $\sqrt{2n}$) contribuent chacun au plus $2n$, et les autres au plus p ; avec l'étape 1 et la proposition 17.2.1,

$$\frac{4^n}{2n+1} \leq \binom{2n}{n} \leq (2n)^{\sqrt{2n}} \prod_{p\leq 2n/3} p < (2n)^{\sqrt{2n}}\, 4^{2n/3}.$$

Comme $2n+1<(2n)^2$, on obtient $4^{n/3}<(2n)^{\sqrt{2n}+2}$, soit, avec $x=2n$, $h(x)=\frac{x\ln 2}{3}-(\sqrt{x}+2)\ln x<0$. Or, pour $x\geq 8000$,

$$h'(x)=\frac{\ln 2}{3}-\frac{\ln x}{2\sqrt{x}}-\frac{1}{\sqrt{x}}-\frac{2}{x}\geq 0{,}231-0{,}051-0{,}012-0{,}001>0,$$

car $\frac{\ln x}{\sqrt{x}}$ décroît pour $x>e^2$; et $h(8000)\approx 1848{,}4-821{,}8>0$. Donc $h(x)>0$ pour $x\geq 8000$: contradiction dès que $n\geq 4000$.

Étape 5 : les petites valeurs. Les nombres

$$2,\ 3,\ 5,\ 7,\ 13,\ 23,\ 43,\ 83,\ 163,\ 317,\ 631,\ 1259,\ 2503,\ 4001$$

sont premiers, et chacun est strictement inférieur au double du précédent. Pour $1\leq n<4000$, soit q le plus petit terme de cette liste strictement supérieur à n : si $q=2$, alors $n=1$ et $q\in]1,2]$; sinon, le terme précédent q' vérifie $q'\leq n$, donc $n<q<2q'\leq 2n$. ■

[L'inégalité d'Erdős en échelle logarithmique : ln(4^{n/3}) croît linéairement, tandis que ln((2n)^{√(2n)+2}) croît comme √n · ln n ; les deux courbes se croisent bien avant n = 4000, ce qui rend l'hypothèse « pas de premier dans]n, 2n] » intenable.](/home/claude/tomes/t3v2/fig/t3_bertrand.png){width=12cm}

Exemple 17.2.3. *Montrer que $\binom{2n}{n}$ n'est jamais une puissance parfaite pour $n\geq 2$.*

Par Bertrand, il existe un premier p avec $n<p\leq 2n$. Alors p divise $(2n)!$ exactement une fois (par Legendre : $\left\lfloor\frac{2n}{p}\right\rfloor=1$ car $p\leq 2n<2p$, et $p^2>n^2\geq 2n$ pour $n\geq 2$) et ne divise pas $(n!)^2$ (car $p>n$). Donc $v_p\left(\binom{2n}{n}\right)=1$: ce n'est pas une puissance k-ième avec $k\geq 2$.

17.3 Exercices

Exercice 17.1 ★★. Montrer que $\binom{2n}{n}$ est divisible par $n+1$ (nombres de Catalan).

Exercice 17.2 ★★. Déterminer $v_2\left(\binom{2n}{n}\right)$ en fonction de n.

Exercice 17.3 ★★★. Montrer que $\prod_{n<p\leq 2n}p\mid\binom{2n}{n}$, puis en déduire que $\prod_{n<p\leq 2n}p\leq 4^n$.

Exercice 17.4 ★★★. Montrer que $\binom{n}{k}$ est impair pour tout $0\leq k\leq n$ si, et seulement si, $n=2^m-1$.

17.4 Corrigés

Solution de l'exercice 17.1.

$$\frac{1}{n+1}\binom{2n}{n}=\binom{2n}{n}-\binom{2n}{n+1},$$

différence de deux entiers, donc entier.

Solution de l'exercice 17.2. Par la formule de Legendre,

$$v_2\left(\binom{2n}{n}\right)=\frac{2S_2(n)-S_2(2n)}{1}=S_2(n),$$

car $S_2(2n)=S_2(n)$. Donc $v_2\left(\binom{2n}{n}\right)$ est le nombre de 1 dans l'écriture binaire de n. En particulier, $\binom{2n}{n}$ est toujours pair pour $n\geq 1$.

Solution de l'exercice 17.3. Soit p un premier avec $n < p \leq 2n$. Alors p divise $(2n)!$ exactement une fois, car le seul multiple de p inférieur ou égal à $2n$ est p lui-même ($2p > 2n$) et $p^2 > n^2 \geq 2n$ pour $n \geq 2$ (pour $n = 1$, on a directement $\binom{2}{1} = 2$). En revanche, $p > n$ ne divise pas $n!$, donc pas $(n!)^2$. Par conséquent

$$v_p\left(\binom{2n}{n}\right) = v_p\big((2n)!\big) - 2v_p(n!) = 1 - 0 = 1.$$

Ces premiers étant deux à deux distincts, leur produit divise $\binom{2n}{n}$.

Enfin $\binom{2n}{n} \leq \sum_k \binom{2n}{k} = 4^n$, d'où

$$\prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq 4^n.$$

Remarque.
Cette majoration est la brique centrale de la preuve d'Erdős du postulat de Bertrand. Jointe à sa variante $\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m} \leq 4^m$ (qui s'obtient de la même façon), elle donne aussi la borne $\prod_{p\leq x} p \leq 4^x$ par récurrence.

Solution de l'exercice 17.4. Par le théorème de Lucas modulo 2 : $\binom{n}{k}$ est impair si, et seulement si, chaque chiffre binaire de k est inférieur ou égal au chiffre correspondant de n. C'est vrai pour tout $k \leq n$ si, et seulement si, tous les chiffres binaires de n valent 1, c'est-à-dire $n = 2^m - 1$.

CHAPITRE 18

18 Stratégie de résolution et problèmes d'IMO

Objectifs du chapitre.

- Disposer d'une méthode d'attaque systématique face à un problème inconnu.
- Éviter les erreurs de rédaction qui coûtent des points.
- S'entraîner sur des problèmes réellement posés à l'IMO.

18.1 La méthode d'attaque en sept temps

Méthode 18.1.1 — Que faire devant un problème d'arithmétique ?

1. **Expérimenter.** Calculer les petits cas : $n = 1,2,3,4,5$. Presque tous les problèmes de type « trouver tous les n » révèlent leur réponse en cinq minutes de calcul. Ne sautez jamais cette étape.
2. **Conjecturer la réponse.** Elle oriente toute la preuve : on sait alors ce qu'il faut exclure.
3. **Chercher une factorisation.** Toute expression algébrique doit être factorisée avant toute chose.
4. **Tester des congruences.** Modules $4,8,3,9,5,7,16$ selon le dictionnaire du chapitre 4.
5. **Choisir un premier et regarder les valuations.** Notamment si l'énoncé contient $a^n \pm b^n$ (LTE) ou des factorielles (Legendre).
6. **Contrôler la taille.** Encadrer entre deux puissances consécutives ; ordonner les variables ; majorer le nombre de cas.
7. **Chercher une descente.** Minimalité, saut de Viète, plus petit facteur premier.

À retenir (Les trois techniques les plus rentables)

1. Le plus petit facteur premier p de n : il force $\text{pgcd}(n, p-1) = 1$, donc un ordre minuscule.
2. L'ordre multiplicatif : si $a^n \equiv 1 \pmod p$, alors $\text{ord}_p(a) \mid \text{pgcd}(n, p-1)$.
3. La minimalité : « prenons la solution la plus petite » transforme un problème d'existence en contradiction.

Attention — Erreurs de rédaction qui coûtent cher.

- Oublier de vérifier la réciproque lorsqu'on a raisonné par conditions nécessaires.
- Oublier les cas dégénérés : $n = 0$, $n = 1$, variables nulles ou négatives, $p = 2$.
- Écrire « il est clair que » devant une étape non triviale.
- Utiliser LTE sans vérifier $p \nmid a$, $p \nmid b$, $p \mid a - b$.
- Invoquer Dirichlet ou Zsigmondy sans nécessité.
- Diviser une congruence par un nombre non premier avec le module.

18.2 Problèmes d'IMO entièrement corrigés

Exemple 18.2.1 (IMO 1988, problème 6). *Soient a, b des entiers strictement positifs tels que $ab + 1 \mid a^2 + b^2$. Montrer que $\frac{a^2+b^2}{ab+1}$ est un carré.*

Solution : voir le théorème 16.2.1 et sa démonstration (chapitre 16, saut de Viète).

Exemple 18.2.2 (IMO 1992, problème 1). *Trouver tous les entiers $1 < a < b < c$ tels que $(a-1)(b-1)(c-1)$ divise $abc - 1$.*

Posons $k = \frac{abc-1}{(a-1)(b-1)(c-1)}$, entier ≥ 1.

Parité. Si a est pair, alors abc est pair, donc $abc - 1$ est impair, ce qui force $(a-1)(b-1)(c-1)$ impair, donc b et c pairs. Si a est impair et que l'un de b, c est pair, alors $abc - 1$ est impair mais $a - 1$ est pair : contradiction. Donc a, b, c ont tous la même parité.

Majoration de k.

$$k < \frac{abc}{(a-1)(b-1)(c-1)} = \frac{a}{a-1} \cdot \frac{b}{b-1} \cdot \frac{c}{c-1}.$$

Si a, b, c sont impairs, $a \geq 3$, $b \geq 5$, $c \geq 7$, donc $k < \frac{3}{2} \cdot \frac{5}{4} \cdot \frac{7}{6} = \frac{35}{16} < 3$, soit $k \leq 2$. Si a, b, c sont pairs, $a \geq 2$, $b \geq 4$, $c \geq 6$, donc $k < 2 \cdot \frac{4}{3} \cdot \frac{6}{5} = \frac{16}{5} < 4$, soit $k \leq 3$. Enfin $k \geq 2$ car $abc - 1 > (a-1)(b-1)(c-1)$.

Cas impair, $k = 2$. $abc - 1 = 2(a-1)(b-1)(c-1)$. Si $a \geq 7$: $k < \frac{7}{6} \cdot \frac{9}{8} \cdot \frac{11}{10} < 1{,}45 < 2$: exclu. Donc $a \in \{3,5\}$.

- $a = 3$: $3bc - 1 = 4(b-1)(c-1)$, soit $bc - 4b - 4c + 5 = 0$, soit $(b-4)(c-4) = 11$. Donc $b = 5$, $c = 15$. Vérification : $2 \cdot 4 \cdot 14 = 112$ et $3 \cdot 5 \cdot 15 - 1 = 224 = 2 \cdot 112$ ✓.
- $a = 5$: $5bc - 1 = 8(b-1)(c-1)$, soit $3bc - 8b - 8c + 9 = 0$, soit $(3b-8)(3c-8) = 37$: $3b - 8 = 1$ donne $b = 3 < a$: exclu.

Cas pair. $a = 2$: $2bc - 1$ est impair, donc k est impair : $k = 3$. Alors $2bc - 1 = 3(b-1)(c-1)$, soit $bc - 3b - 3c + 4 = 0$, soit $(b-3)(c-3) = 5$: $b = 4$, $c = 8$. Vérification : $1 \cdot 3 \cdot 7 = 21$ et $2 \cdot 4 \cdot 8 - 1 = 63 = 3 \cdot 21$ ✓. Si $a \geq 4$: $k < \frac{4}{3} \cdot \frac{6}{5} \cdot \frac{8}{7} < 2$: exclu.

Réponse : $(a, b, c) = (3,5,15)$ et $(2,4,8)$.

Exemple 18.2.3 (IMO 1994, problème 4). *Déterminer tous les couples (m, n) d'entiers strictement positifs tels que $\frac{n^3+1}{mn-1}$ soit un entier.*

Étape 1 : symétrisation. Comme $mn \equiv 1 \pmod{mn-1}$,

$$m^3(n^3+1) = (mn)^3 + m^3 \equiv 1 + m^3 \pmod{mn-1},$$

et $\gcd(m, mn-1) = 1$, donc $mn - 1 \mid n^3 + 1 \Leftrightarrow mn - 1 \mid m^3 + 1$: le problème est symétrique en m, n. Supposons donc $m \geq n$.

Étape 2 : réduction de degré. De $mn - 1 \mid n^3 + 1$ on tire

$$m(n^3+1) = n^2(mn-1) + n^2 + m \Rightarrow mn - 1 \mid n^2 + m.$$

Étape 3 : majoration. Comme $n^2 + m > 0$, on a $n^2 + m \geq mn - 1$, donc

$$m(n-1) \leq n^2 + 1 \Rightarrow m \leq \frac{n^2+1}{n-1} = n + 1 + \frac{2}{n-1} \qquad (n \geq 2).$$

Pour $n \geq 4$: $m \leq n+1$. Combiné à $m \geq n$:

- $m = n$: $n^2 - 1 \mid n^2 + n$, donc $n^2 - 1 \mid n + 1$, donc $n - 1 \mid 1$: $n = 2$, exclu ici ($n \geq 4$).
- $m = n + 1$: $n^2 + n - 1 \mid n^2 + n + 1$, donc $n^2 + n - 1 \mid 2$: impossible pour $n \geq 4$.

Donc $n \leq 3$.

Étape 4 : petits cas (avec $m \geq n$).

- $n = 1$: $m - 1 \mid 2$, donc $m \in \{2,3\}$.
- $n = 2$: $2m - 1 \mid 9$, donc $2m - 1 \in \{1,3,9\}$, $m \in \{1,2,5\}$; avec $m \geq 2$: $m \in \{2,5\}$.
- $n = 3$: $3m - 1 \mid 28$ et $3m - 1 \equiv 2 \pmod 3$, donc $3m - 1 \in \{2,14\}$, $m \in \{1,5\}$; avec $m \geq 3$: $m = 5$.

Réponse (en rétablissant la symétrie) :

$$(m,n) \in \{(2,1),(3,1),(1,2),(2,2),(5,2),(1,3),(5,3),(2,5),(3,5)\}.$$

Exemple 18.2.4 (IMO 1998, problème 4). *Déterminer tous les couples (a,b) d'entiers strictement positifs tels que $ab^2 + b + 7$ divise $a^2b + a + b$.*

Étape 1. Formons la combinaison qui élimine a^2 :

$$b(a^2b + a + b) - a(ab^2 + b + 7) = b^2 - 7a.$$

Donc $ab^2 + b + 7 \mid b^2 - 7a$.

Étape 2 : discussion du signe.

- Si $b^2 - 7a = 0$: alors $7 \mid b^2$, donc $7 \mid b$; posons $b = 7k$, d'où $a = 7k^2$. Vérifions : $ab^2 + b + 7 = 7^3k^4 + 7k + 7$ et $a^2b + a + b = 7^3k^5 + 7k^2 + 7k = k(7^3k^4 + 7k + 7)$ ✓.
- Si $b^2 - 7a > 0$: alors $b^2 - 7a \geq ab^2 + b + 7 > b^2$ (car $a \geq 1$), absurde.
- Si $b^2 - 7a < 0$: alors $7a - b^2 \geq ab^2 + b + 7$, donc $7a > ab^2$, soit $b^2 < 7$: $b \in \{1,2\}$.

Étape 3 : les deux cas restants.

- $b = 1$: $a + 8 \mid 7a - 1$. Or $7(a+8) = 7a + 56$, donc $a + 8 \mid 57 = 3 \cdot 19$. Comme $a + 8 \geq 9$: $a + 8 \in \{19,57\}$, soit $a \in \{11,49\}$. Vérification : $(11,1)$ donne $11 + 1 + 7 = 19$ et $121 + 11 + 1 = 133 = 7 \cdot 19$ ✓ ; $(49,1)$ donne $49 + 1 + 7 = 57$ et $2401 + 49 + 1 = 2451 = 43 \cdot 57$ ✓.
- $b = 2$: $4a + 9 \mid 7a - 4$. Or $4(7a - 4) = 7(4a + 9) - 79$, donc $4a + 9 \mid 79$ (premier), et $4a + 9 \geq 13$: $4a + 9 = 79$, $a = 17{,}5$: pas de solution.

Réponse : $(a,b) \in \{(11,1),(49,1)\} \cup \{(7k^2, 7k) : k \geq 1\}$.

Exemple 18.2.5 (IMO 2005, problème 4). *Soit $a_n = 2^n + 3^n + 6^n - 1$. Déterminer tous les entiers $k \geq 1$ premiers avec tous les a_n.*

Réponse : $k = 1$.

Il suffit de montrer que tout nombre premier p divise au moins un a_n.

Cas $p = 2$: $a_2 = 4 + 9 + 36 - 1 = 48$, divisible par 2. Cas $p = 3$: 48 est aussi divisible par 3.

Cas $p \geq 5$: prenons $n = p - 2 \geq 3$. Par le petit théorème de Fermat, $2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod p$, donc

$$2^{p-2} \equiv 2^{-1}, \qquad 3^{p-2} \equiv 3^{-1}, \qquad 6^{p-2} \equiv 6^{-1} \pmod p.$$

Or, dans $\mathbb{Z}/p\mathbb{Z}$,

$$2^{-1} + 3^{-1} + 6^{-1} = \frac{3 + 2 + 1}{6} = \frac{6}{6} = 1.$$

Donc $a_{p-2} \equiv 1 - 1 = 0 \pmod{p}$.

Ainsi tout premier divise un terme de la suite : le seul k premier avec tous les a_n est $k = 1$.

Exemple 18.2.6 (IMO 2007, problème 5). *Soient a, b des entiers strictement positifs tels que $4ab - 1 \mid (4a^2 - 1)^2$. Montrer que $a = b$.*

Solution : voir l'exemple 16.2.2 (chapitre 16).

Exemple 18.2.7 (IMO 1990, problème 3). *Trouver tous les entiers $n > 1$ tels que $n^2 \mid 2^n + 1$.*

Solution : voir le corrigé de l'exercice 4.6 (chapitre 4). Réponse : $n = 3$.

Exemple 18.2.8 (IMO 2006, problème 4). *Résoudre $1 + 2^x + 2^{2x+1} = y^2$ en entiers.*

Solution : voir le corrigé de l'exercice 11.7 (chapitre 11). Réponse : $(x, y) = (0, \pm 2)$ et $(4, \pm 23)$.

18.3 Banque d'entraînement

Voici, pour finir, une sélection de problèmes à chercher sans corrigé : c'est là que se fait l'essentiel du progrès. L'indication entre crochets donne l'outil principal.

1. (IMO 1984, problème 6) Soient $0 < a < b < c < d$ des entiers impairs tels que $ad = bc$, $a + d = 2^k$ et $b + c = 2^m$. Montrer que $a = 1$. [taille + valuations]
2. (IMO 1997, problème 6) Pour $n \geq 1$, soit $f(n)$ le nombre d'écritures de n comme somme de puissances de 2. Montrer que, pour $n \geq 3$, $2^{n^2/4} < f(2^n) < 2^{n^2/2}$. [récurrence]
3. (IMO 2003, problème 2) Trouver tous les couples (a, b) d'entiers strictement positifs tels que $\frac{a^2}{2ab^2 - b^3 + 1}$ soit un entier strictement positif. [bornes + factorisation]
4. (IMO 2011, problème 1) Pour un ensemble $A = \{a_1, a_2, a_3, a_4\}$ de quatre entiers strictement positifs distincts, de somme s_A, on note n_A le nombre de paires $\{i, j\}$ $(i < j)$ telles que $a_i + a_j$ divise s_A. Déterminer les ensembles A pour lesquels n_A est maximal. [ordre + taille]
5. (IMO 2014, shortlist N) Divers. [LTE]
6. (USAMO 1991) Montrer que pour tout n il existe n entiers consécutifs dont aucun n'est sans facteur carré. [TRC]
7. (Iran TST) Montrer que $\varphi(n) \mid n$ si, et seulement si, $n = 1$ ou $n = 2^a 3^b$ $(a \geq 1, b \geq 0)$. [calcul de φ]
8. (Balkanique) Soit $p > 3$ premier. Montrer que $p^2 \mid \binom{2p}{p} - 2$. [Wolstenholme]
9. (Baltic Way) Montrer que $2^{2^n} - 1$ a au moins n facteurs premiers distincts pour tout $n \geq 1$. [Zsigmondy]
10. (Tournoi des villes) Trouver tous les entiers $n \geq 1$ tels que $n \mid 2^n - 1$. [ordre]
11. (China TST) Montrer que pour tout k, il existe une infinité de n tels que $n \mid 2^n + k$. [LTE + récurrence]
12. (Putnam) Montrer que $\sum_{k=1}^{n} \frac{1}{k}$ n'est jamais entier pour $n \geq 2$ (déjà traité) et que $\sum_{k=1}^{n} \frac{1}{2k-1}$ non plus. [valuations 2-adique et 3-adique]

À retenir (Le mot de la fin)

Un problème d'arithmétique d'IMO n'exige presque jamais un théorème que vous ne connaissez pas. Il exige de combiner deux ou trois outils élémentaires dans le bon ordre — et surtout, d'avoir la patience de calculer les petits cas avant de théoriser. Bon travail, et bonne chance.

PARTIE VI — Annexes

ANNEXE A

A Formulaire complet

Ce formulaire est à connaître par cœur. Il ne remplace pas le cours : il sert de contrôle final avant une compétition.

A.1 Divisibilité et PGCD

À retenir (résultats à connaître par cœur)

- Division euclidienne : $a = bq + r$, $0 \leq r < b$, unique.
- $\text{pgcd}(a, b) = \text{pgcd}(b, a - kb)$ pour tout k.
- Bézout : $\exists\, u, v \in \mathbb{Z},\ au + bv = \text{pgcd}(a, b)$.
- Gauss : $a \mid bc$ et $\text{pgcd}(a, b) = 1 \Rightarrow a \mid c$.
- $\text{pgcd}(a, b)\,\text{ppcm}(a, b) = |ab|$.
- $\text{pgcd}(a^m - 1, a^n - 1) = a^{\text{pgcd}(m,n)} - 1$ (pour $a \geq 2$).
- $\text{pgcd}(F_m, F_n) = F_{\text{pgcd}(m,n)}$ (Fibonacci).
- $a - b \mid a^n - b^n$; $a + b \mid a^n + b^n$ pour n impair.
- Sophie Germain : $a^4 + 4b^4 = (a^2 + 2b^2 - 2ab)(a^2 + 2b^2 + 2ab)$.
- Simon : $xy + ax + by = (x + b)(y + a) - ab$.

A.2 Valuations et factorisation

À retenir

- $v_p(ab) = v_p(a) + v_p(b)$; $v_p(a + b) \geq \min\big(v_p(a), v_p(b)\big)$, avec égalité si $v_p(a) \neq v_p(b)$.
- $a \mid b \Leftrightarrow \forall p,\ v_p(a) \leq v_p(b)$.
- Legendre : $v_p(n!) = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - S_p(n)}{p-1}$, où $S_p(n)$ est la somme des chiffres de n en base p.
- Kummer : $v_p\left(\binom{n}{k}\right)$ = nombre de retenues dans l'addition $k + (n - k)$ en base p.
- Lemme du produit : $uv = w^k$ avec $u, v \geq 1$ et $\text{pgcd}(u, v) = 1 \Rightarrow u, v$ sont des puissances k-ièmes.

A.3 Congruences

À retenir

- $ac \equiv bc \pmod{n} \Leftrightarrow a \equiv b \pmod{n/\text{pgcd}(n, c)}$.
- Fermat : p premier $\Rightarrow a^p \equiv a \pmod{p}$, et $a^{p-1} \equiv 1 \pmod{p}$ si $p \nmid a$.
- Euler : $\text{pgcd}(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$.
- Wilson : pour $p \geq 2$, $(p - 1)! \equiv -1 \pmod{p} \Leftrightarrow p$ premier.

- TRC : modules premiers entre eux deux à deux ⇒ système résoluble, solution unique modulo le produit.
- Ordre (pour $\text{pgcd}(a,n)=1$) : $a^k \equiv 1 \pmod{n} \Leftrightarrow \text{ord}_n(a) \mid k$; et $\text{ord}_n(a) \mid \varphi(n)$.
- $p \mid a^n - 1 \Rightarrow \text{ord}_p(a) \mid \text{pgcd}(n, p-1)$.
- p premier impair, $p \mid a^n + 1 \Rightarrow v_2\left(\text{ord}_p(a)\right) = v_2(n) + 1$.
- Lagrange : un polynôme de degré d, de coefficient dominant non divisible par p, a au plus d racines modulo p.
- Racine primitive : il en existe une modulo n si, et seulement si, $n \in \{1,2,4,p^k,2p^k\}$, p premier impair.

A.4 Résidus quadratiques

À retenir

Dans ce qui suit, p et q désignent des nombres premiers impairs distincts, et $p \neq 3$ dans les critères relatifs à ± 3.

- Euler : $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.
- $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{4}$.
- $\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{8}$.
- $\left(\frac{-2}{p}\right) = 1 \Leftrightarrow p \equiv 1,3 \pmod{8}$.
- $\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{12}$.
- $\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{3}$.
- Réciprocité : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.
- Pour p premier : $p = a^2 + b^2 \Leftrightarrow p = 2$ ou $p \equiv 1 \pmod{4}$.
- $n \geq 1$ est somme de deux carrés si, et seulement si, tout premier $p \equiv 3 \pmod{4}$ apparaît dans sa décomposition avec un exposant pair.
- Trois carrés : n n'est pas somme de trois carrés si, et seulement si, $n = 4^a(8b+7)$ avec $a, b \geq 0$.
- Quatre carrés (Lagrange) : tout entier naturel est somme de quatre carrés.

A.5 Fonctions arithmétiques

À retenir

Pour $n = \prod p_i^{\alpha_i}$:

- $\tau(n) = \prod(\alpha_i + 1)$; $\sigma(n) = \prod \frac{p_i^{\alpha_i+1}-1}{p_i-1}$.
- $\varphi(n) = n\prod_{p \mid n}\left(1 - \frac{1}{p}\right)$; $\sum_{d \mid n} \varphi(d) = n$.

- $\sum_{d|n} \mu(d) = [n = 1]$; inversion de Möbius.
- $\tau(n)$ impair $\Leftrightarrow n$ carré ; $\prod_{d|n} d = n^{\tau(n)/2}$.
- $\sum_{k \le n} \left\lfloor \frac{n}{k} \right\rfloor = \sum_{k \le n} \tau(k)$.
- Nombres parfaits pairs : $2^{p-1}(2^p - 1)$ avec $2^p - 1$ premier.

A.6 Outils avancés

À retenir

- LTE (p impair, $p \mid a - b$, $p \nmid ab$) : $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$.
- LTE (p impair, $p \mid a + b$, $p \nmid ab$, n impair) : $v_p(a^n + b^n) = v_p(a + b) + v_p(n)$.
- LTE ($p = 2$, a, b impairs, n pair) : $v_2(a^n - b^n) = v_2(a - b) + v_2(a + b) + v_2(n) - 1$.
- Zsigmondy ($a > b \ge 1$ premiers entre eux) : $a^n - b^n$ a un diviseur premier primitif sauf pour ($n = 1$, $a - b = 1$), ($n = 2$, $a + b$ puissance de 2), ($n = 6$, $a = 2$, $b = 1$).
- Cyclotomiques : $p \mid \Phi_n(a) \Rightarrow p \equiv 1 \pmod n$ ou $p \mid n$.
- Lucas : $\binom{n}{k} \equiv \prod_i \binom{n_i}{k_i} \pmod p$, où n_i et k_i sont les chiffres de n et k en base p.
- Pell : pour $d \ge 2$ non carré, $x^2 - dy^2 = 1$ a toujours une solution non triviale ; si (x_1, y_1) est la plus petite solution positive, toutes les solutions positives s'obtiennent par $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$.
- Bertrand : pour tout $n \ge 1$, il existe un nombre premier dans $]n, 2n]$.

ANNEXE B

B Plan d'entraînement sur six mois

Ce plan suppose environ 6 à 8 heures par semaine consacrées à l'arithmétique. Il alterne systématiquement théorie et résolution, selon le principe : on n'apprend pas un outil, on apprend à le déclencher.

Mois	Contenu théorique	Travail de résolution
1	Chapitres 1–3 : divisibilité, Euclide, Bézout, nombres premiers, valuations, formule de Legendre.	Tous les exercices ★ et ★★ des chapitres 1–3. Objectif : automatiser la factorisation et l'argument de taille.
2	Chapitres 4–5 : congruences, choix du module, critères, Wilson, TRC.	Exercices des chapitres 4–5, puis 10 problèmes de niveau olympiade nationale sur les congruences.
3	Chapitres 6–7 : Fermat, Euler, φ, ordre multiplicatif, racines primitives.	Le « pack ordre » : tous les problèmes du type $n \mid a^n \pm 1$. C'est le mois le plus rentable de tout le plan.
4	Chapitres 8–10 : résidus quadratiques, réciprocité, fonctions arithmétiques, parties entières.	Exercices ★★★ des chapitres 8–10 ; deux tests chronométrés de 90 minutes sur un problème.
5	Chapitres 11–13 : équations diophantiennes, Pythagore, descente, Pell.	15 équations diophantiennes variées. Rédiger intégralement au moins 5 solutions, comme en compétition.
6	Chapitres 14–18 : LTE, Zsigmondy, saut de Viète, binomiaux, stratégie.	Les problèmes d'IMO du chapitre 18, puis la banque d'entraînement. Deux simulations complètes de 4 h 30 avec un problème d'arithmétique.

À retenir (trois règles d'or de l'entraînement)

1. 45 minutes minimum sur un problème avant de regarder la solution.
2. Rédiger au moins une solution sur trois entièrement, comme si elle était notée. On perd plus de points en rédaction qu'en idées.
3. Tenir un carnet d'erreurs : pour chaque problème raté, noter en une phrase l'idée manquante. Relire ce carnet chaque semaine.

ANNEXE C

C Table des difficultés et index des méthodes

C.1 Index des méthodes par symptôme

Symptôme dans l'énoncé	Outil à déclencher
$d \mid A$ et $d \mid B$	combinaison linéaire $xA + yB$ (ch. 1)
$\frac{f(n)}{g(n)} \in \mathbb{Z}$	Euclide symbolique (ch. 2)
carrés, cubes, puissances	congruences modulo $4,8,9,3,5,7,16$ (ch. 4)
factorielles, $\binom{n}{k}$	formule de Legendre, Kummer (ch. 3, 17)
« il existe n tel que… »	théorème des restes chinois (ch. 5)
k entiers consécutifs	TRC (ch. 5)
$a^k \bmod n$ avec k énorme	Euler + réduction de l'exposant (ch. 6)
$p \mid a^n \pm 1$	ordre multiplicatif (ch. 7)
$n \mid a^n \pm 1$	plus petit facteur premier + ordre (ch. 7)
$x^2 \equiv a \pmod p$	symbole de Legendre (ch. 8)
$x^2 + y^2$, $x^2 + ky^2$	premiers admissibles, réciprocité (ch. 8)
$\tau, \sigma, \varphi, \mu$	multiplicativité, convolution (ch. 9)
$\lfloor \cdot \rfloor$, comptage	partie entière (ch. 10)
produit = constante	factorisation, truc de Simon (ch. 11)
équation symétrique	ordonner les variables (ch. 11)
$a^2 + b^2 = c^2$	paramétrisation pythagoricienne (ch. 12)
« pas de solution »	descente infinie (ch. 12)
« une infinité de solutions »	équation de Pell (ch. 13)
$v_p(a^n \pm b^n)$ exact	lemme LTE (ch. 14)
facteur premier nouveau	Zsigmondy, cyclotomiques (ch. 15)
équation de degré 2 symétrique en x et y	saut de Viète (ch. 16)
$\binom{n}{k} \bmod p$	Lucas (ch. 17)

C.2 Bibliographie

- T. Andreescu, D. Andrica, *Number Theory: Structures, Examples, and Problems*, Birkhäuser.
- A. Engel, *Problem-Solving Strategies*, Springer (traduction française : *Solutions d'expert*, Cassini).
- T. Belhaj Soulami, *Les olympiades de mathématiques : réflexes et stratégies*, Ellipses.
- M. Aassila, *Objectif Olympiades de Mathématiques*, tome 5 : arithmétique.
- H.-B. Yu, *Problems of Number Theory in Mathematical Competitions*, World Scientific.
- **Mathraining** (mathraining.be) : cours et exercices en ligne, avec correction automatique — la progression de la section Théorie des nombres suit exactement celle de ce livre.

- **AoPS** (artofproblemsolving.com) : archives complètes des IMO et des shortlists.
- **POFM** (maths-olympiques.fr) : la préparation olympique française, avec ses polycopiés et ses tests.

  NB : Ce livre est à but éducatif uniquement. Il a été réalisé avec recours à l'IA.

À propos de l'auteur

Ali AKIR

Ali AKIR est formateur bénévole depuis 2017 au sein de l'Association Tunisienne de Compétitions et de Culture Mathématique (ATCCM), où il prépare des élèves tunisiens aux olympiades internationales de mathématiques (IMO, PAMO, AMO, OFM…). Il a occupé le rôle de coordinateur régional du Pan-African Mathematical Olympiad (PAMO) pour l'Afrique, ainsi que celui de coordinateur de l'Olympiade Francophone de Mathématiques (OFM). Il forme également des formateurs dans le cadre de programmes régionaux de préparation olympique.

La collection ATOMATH rassemble l'ensemble de son enseignement olympique, organisé en quatre tomes : Algèbre, Géométrie, Arithmétique et Combinatoire.

ATOMATH

TOME III : ARITHMÉTIQUE

La collection ATOMATH propose un parcours complet de préparation aux Olympiades internationales de mathématiques. Ce troisième tome est entièrement consacré à l'arithmétique olympique, c'est-à-dire à la théorie des nombres telle qu'elle apparaît en compétition.

L'arithmétique occupe une place singulière dans les compétitions internationales : à l'IMO, un problème sur six en moyenne relève directement de cette discipline. Sa particularité réside dans le fait que le bagage théorique nécessaire est étonnamment restreint, mais la distance entre la connaissance d'un théorème et son application créative au bon moment est immense. C'est précisément cette distance que ce tome entend combler.

Conçu pour accompagner l'élève depuis le niveau junior jusqu'au niveau senior exigé par l'IMO, cet ouvrage ne suppose aucun prérequis au-delà du programme du lycée. Chaque notion est rigoureusement introduite, démontrée, puis mise à l'épreuve sur des exemples résolus et une large banque d'exercices gradués.

Au programme :

- **Fondements :** divisibilité, algorithme d'Euclide, Bézout, valuation p-adique et congruences.
- **Les classiques :** restes chinois, théorèmes de Fermat et d'Euler, ordre multiplicatif et résidus quadratiques.
- **Fonctions arithmétiques :** convolution de Dirichlet et parties entières.
- **Équations diophantiennes :** méthodes de résolution, descente infinie et équation de Pell.
- **Techniques de haut niveau :** lemme LTE, Zsigmondy, saut de Viète et problèmes d'IMO.

Ali AKIR
Formateur olympique