que sais-je ?

# ARITHMÉTIQUE
## ET
## THÉORIE DES NOMBRES

PAR JEAN ITARD


PRESSES UNIVERSITAIRES
DE FRANCE

# ARITHMÉTIQUE
# ET THÉORIE DES NOMBRES

« QUE SAIS-JE ? »
LE POINT DES CONNAISSANCES ACTUELLES
N° 1093

# ARITHMÉTIQUE ET THÉORIE DES NOMBRES

par

Jean ITARD
*Agrégé de l'Université*

TROISIÈME ÉDITION MISE A JOUR

PRESSES UNIVERSITAIRES DE FRANCE
108, BOULEVARD SAINT-GERMAIN, PARIS
1973

*VINGT-SIXIÈME MILLE*


Dépôt légal. — 1re édition : 4e trimestre 1963
3e édition : 1er trimestre 1973

# INTRODUCTION

L'existence dans la collection « Que sais-je ? » d'un ouvrage sur *Les nombres premiers* nous a amené, pour éviter les doubles emplois, à ne traiter ici ni de la plupart des propriétés des nombres premiers, ni de la théorie des congruences, des indices, ni de la très remarquable loi de réciprocité des résidus quadratiques, trouvée par Legendre et démontrée par Gauss. Nous ne nous occupons pas non plus, et pour les mêmes raisons, des théorèmes de Fermat et de Wilson ni du théorème de Bachet : tout nombre est carré ou somme de deux, de trois ou de quatre carrés au plus. En revanche, si nous ne considérons aucun corps algébrique autre que Q, corps des rationnels, nous avons réservé un chapitre aux fractions continues et aux approximations des irrationnels.

Toutes les études qui suivent sont classiques, bien que peu enseignées en France. Elles peuvent servir d'introduction aux mathématiques modernes.

Nous supposons admise la notion de nombre entier, et ses extensions : fractions, nombres rationnels, nombres réels.

Sans prétendre écrire une histoire continue de la théorie des nombres, histoire qui, pour être bien comprise, exigerait des lecteurs une connaissance préalable de cette théorie, nous nous sommes systématiquement placé à un point de vue historique. C'est que l'arithmétique théorique est un domaine

des mathématiques où l'on saisit le mieux le caractère humain et collectif de ces sciences. Chaque chercheur, quelque génial qu'il soit, travaille sur l'acquis et souvent avec les techniques mêmes de ses prédécesseurs, heureux s'il accroît la richesse commune ou s'il perfectionne et simplifie les méthodes.

Même les découvertes les plus spectaculaires et les plus imprévues : méthode de la descente de Fermat ; fractions continues de Lagrange ; congruences de Gauss ; loi de réciprocité des résidus quadratiques de Legendre ; nombres idéaux de Kummer, etc., s'insèrent dans une tradition continue dont nous avons le bonheur de pouvoir suivre encore les enchaînements.

CHAPITRE PREMIER

# PRÉLIMINAIRES

Nous appelons *Arithmétique* l'étude élémentaire des propriétés des nombres entiers et des nombres rationnels, établies avant le XVIII^e siècle, et *Théorie des nombres* les développements nés des recherches précédentes à partir de ce XVIII^e siècle. Mais il n'y a pas de frontière bien précise entre ces deux domaines, et si Legendre publie en 1797-1798 un *Essai sur la théorie des nombres*, l'ouvrage fondamental de Gauss s'appelle en 1801 *Disquisitiones arithmeticae*.

## Les nombres figurés

Parmi les plus anciens travaux relatifs à l'arithmétique telle qu'elle est ainsi conçue, on doit citer, au VI^e siècle avant notre ère, la théorie du pair et de l'impair, premier exemple d'une étude de congruence (ici de module 2), et celle des nombres figurés (nombres triangulaires, carrés, pentagonaux, pyramidaux, cubes, etc.), qui se rapproche davantage de l'étude des séries et de l'analyse combinatoire que de l'arithmétique théorique telle qu'elle est conçue de nos jours.

Un *nombre triangulaire* est la somme de $n$ entiers consécutifs commençant à l'unité.

En désignant par $T_n$ un triangulaire (dont $n$ est appelé la « racine triangulaire ») on a donc :

$$T_n = 1 + 2 + 3 + \ldots + (n-2) + (n-1) + n$$

ou $$T_n = n + (n-1) + (n-2) + \ldots + 3 + 2 + 1$$

et, par addition :

$$2\,T_n = (n+1) + (n+1) + (n+1) + \ldots + (n+1) + (n+1) + (n+1)$$
$$= n(n+1)$$

soit enfin $$T_n = \frac{1}{2}\,n(n+1)$$

Un *nombre carré* $C_n$ est la somme des $n$ premiers impairs. Sa « racine carrée » est $n$ :

$$C_n = 1 + 3 + 5 + \ldots + (2n-5) + (2n-3) + (2n-1)$$
$$= (2n-1) + (2n-3) + (2n-5) + \ldots + 5 + 3 + 1$$

et, par addition
$$2\,C_n = 2n \times n$$

soit $$C_n = n^2$$

De même un *nombre pentagonal* est la somme des $n$ premiers termes d'une progression arithmétique de premier terme 1, de raison 3 :

$$P_n = 1 + 4 + \ldots + (3n-2) = \frac{1}{2}\,n(3n-1)$$

Un *nombre hexagonal* est la somme des $n$ premiers termes d'une progression arithmétique de premier terme 1, de raison 4 :

$$H_n = n(2n-1), \text{ etc.}$$

Le *Pyramidal* de racine $n$ est la somme des $n$ premiers triangulaires :

$$\Pi_n = 1 + 3 + 6 + 10 + \ldots + \frac{1}{2}\,n(n+1)$$

Montrons qu'il est égal à $\frac{1}{6}\,n(n+1)(n+2)$, pour tout $n$. Pour cela vérifions d'abord cette loi pour

$n = 1$ : $\Pi_1 = 1$ et $\frac{1}{6}.1.2.3 = 1$. De même pour $n = 2$

$\Pi_2 = 1 + 3 = 4$ et $\frac{1}{6} n(n+1)(n+2) = \frac{1}{6}.2.3.4 = 4$

Admettons l'exactitude de la relation pour la racine $n$, c'est-à-dire admettons que, pour un $n$ déterminé, on ait

$$\Pi_n = \frac{1}{6} n(n+1)(n+2)$$

Le pyramidal de racine $(n+1)$ s'obtient par définition, en ajoutant à $\Pi_n$ le triangulaire de racine $n+1$ ou $\frac{1}{2}(n+1)(n+2)$ :

$$\Pi_{n+1} = \frac{1}{6} n(n+1)(n+2) + \frac{1}{2}(n+1)(n+2)$$

$$= \frac{1}{6}(n+1)(n+2)[n+3]$$

ce qui est conforme à la formule à démontrer.

La loi est donc *héréditaire*, c'est-à-dire que si elle est vraie pour $n$, elle est vraie pour $(n+1)$. Mais elle est vraie pour $n = 1$, elle est donc vraie pour tout $n$.

Nous venons ici d'utiliser un raisonnement par *récurrence* ou *induction complète*, un des types de raisonnements les plus utilisés en théorie des nombres.

### Le triangle arithmétique

Les nombres naturels, triangulaires, pyramidaux, apparaissent dans le *triangle arithmétique*, que l'on trouve au Moyen Age, par exemple en Chine et dans des manuscrits byzantins, très connu des algébristes

de la Renaissance, mais étudié d'une façon systématique au XVII^e siècle par Blaise Pascal :

```
1
1  1
1  2   1
1  3   3   1
1  4   6   4   1
1  5  10  10   5  1
1  6  15  20  15  6  1
. . . . . . . . . . . .
. . . . . . . . . . . . . .
```

Chaque nombre du triangle est obtenu en ajoutant le nombre qui le précède dans sa colonne au nombre qui précède celui-ci dans sa propre ligne horizontale. En numérotant les colonnes à partir de 0, indice de la colonne des unités, et en numérotant les lignes à partir de l'indice 0, réservé à la première ligne qui ne contient qu'un seul 1, notons $C^j_i$ le nombre qui figure dans la *ligne horizontale i*, et dans la colonne verticale *j*. Alors, la loi de formation du triangle s'écrit :

$$C^j_i = C^j_{i-1} + C^{j-1}_{i-1}$$

Les nombres naturels sont les $C^1_n$, les triangulaires sont les $C^2_n$, les pyramidaux les $C^3_n$. En Analyse Combinatoire $C^p_n$ est le nombre de combinaisons de $n$ objets $p$ à $p$.

En notant $n\,!$ (factorielle de $n$) le produit des $n$ premiers entiers, on peut écrire

$$C^j_i = \frac{i\,!}{j\,!\,(i-j)\,!} \quad \text{d'où} \quad C^j_i = C^{j-1}_i \times \frac{i-j+1}{j}$$

La colonne $j = 1$ correspond aux nombres naturels 1, 2, 3, ... Vérifions pour elle l'exactitude de la formule que nous venons de donner sans justification :

$$\frac{i\,!}{1\,!\,(i-1)\,!} = \frac{1.2.3 \ldots (i-1)\,i}{1 \times 1.2.3 \ldots (i-1)} = i$$

Le naturel de rang $i$ est bien $i$, et la formule est vérifiée pour cette colonne.

On peut la vérifier généralement en utilisant encore ici le raisonnement par récurrence. C'est ce que fait d'ailleurs Pascal et son Traité est un des premiers ouvrages où ce type de raisonnement a été systématiquement et consciemment utilisé : « Quoique cette proposition ait une infinité de cas, j'en donnerai une démonstration bien courte, en supposant deux lemmes.

« Le 1, qui est évident de soi-même, que cette proposition se rencontre dans la seconde base (notre ligne d'indice 1).

« Le 2, que si cette proposition se trouve dans une base quelconque, elle se trouvera nécessairement dans la base suivante.

« D'où il se voit qu'elle est nécessairement dans toutes les bases : car elle est dans la seconde base par le premier lemme ; donc par le second elle est dans la troisième base, donc dans la quatrième, et à l'infini. »

### Les nombres de Bernoulli

Nous avons, pour définir les nombres triangulaires, totalisé les entiers naturels, et trouvé, en posant

$$\Sigma n = 1 + 2 + 3 + \ldots + n$$

$$\Sigma n = \frac{n(n+1)}{2} = \frac{n^2}{2} + \frac{n}{2}$$

On peut se proposer plus généralement de totaliser les carrés, les cubes, etc., des $n$ premiers entiers. C'est ce que firent plusieurs algébristes des XVI^e^ et XVII^e^ siècles, par exemple Faulhaber (1580-1635) qui poussa jusqu'à la 17^e^ puissance, puis Pascal

qui donna une méthode générale, mais surtout Jacques Bernoulli, au début du XVIII^e siècle.

Il forme le tableau suivant :

**Somme des puissances**

$$\Sigma n = \frac{1}{2} n^2 + \frac{1}{2} n$$

$$\Sigma n^2 = \frac{1}{3} n^3 + \frac{1}{2} n^2 + \frac{1}{6} n$$

$$\Sigma n^3 = \frac{1}{4} n^4 + \frac{1}{2} n^3 + \frac{1}{4} n^2$$

$$\Sigma n^4 = \frac{1}{5} n^5 + \frac{1}{2} n^4 + \frac{1}{3} n^3 * - \frac{1}{30} n$$

$$\Sigma n^5 = \frac{1}{6} n^6 + \frac{1}{2} n^5 + \frac{5}{12} n^4 * - \frac{1}{12} n^2$$

$$\Sigma n^6 = \frac{1}{7} n^7 + \frac{1}{2} n^6 + \frac{1}{2} n^5 * - \frac{1}{6} n^3 * + \frac{1}{42} n$$

. . . . . .

Puis il ajoute qu'en général

$$\Sigma n^c = \frac{1}{c+1} n^{c+1} + \frac{1}{2} n^c + \frac{c}{2} A n^{c-1} + \frac{c(c-1)(c-2)}{4!} B n^{c-3} + \frac{c(c-1)(c-2)(c-3)(c-4)}{6!} C n^{c-5} + \frac{c(c-1)(c-2)(c-3)(c-4)(c-5)(c-6)}{8!} D n^{c-7} \text{ etc...}$$

Les lettres A, B, C, D, représentent, dans l'ordre, les coefficients du dernier terme des expressions de $\Sigma n^2$, $\Sigma n^4$, $\Sigma n^6$, $\Sigma n^8$, à savoir

$$A = \frac{1}{6}, \quad B = -\frac{1}{30}, \quad C = \frac{1}{42}, \quad D = -\frac{1}{30}$$

Chacun d'eux se calcule en complétant la valeur de $\Sigma n^c$ pour $n = 1$.

Ainsi pour $\Sigma n^7$, première des lignes du tableau de

Bernoulli que nous n'avons pas reproduites, nous trouvons, par sa formule,

$$\Sigma n^7 = \frac{1}{8} n^8 + \frac{1}{2} n^7 + \frac{7}{2} An^6 + \frac{7.6.5}{4!} Bn^4 + \frac{7.6.5.4.3}{6!} Cn^2$$

ou, en employant les valeurs de A, B, C, qu'il nous donne,

$$\Sigma n^7 = \frac{1}{8} n^8 + \frac{1}{2} n^7 + \frac{7}{12} n^6 - \frac{7}{24} n^4 + \frac{1}{12} n^2$$

En faisant $n = 1$, on trouve

$$1 = \frac{1}{8} + \frac{1}{2} + \frac{7}{12} - \frac{7}{24} + \frac{1}{12}$$

ce qui est exact.

Mais le calcul de $\Sigma n^8$, par sa vérification pour $n = 1$, nous ferait découvrir la valeur de D si nous l'ignorions :

$$\Sigma n^8 = \frac{1}{9} n^9 + \frac{1}{2} n^8 + \frac{8}{2} An^7 + \frac{8.7.6}{4!} Bn^5 + \frac{8.7.6.5.4}{6!} Cn^3 + \frac{8.7.6.5.4.3.2}{8!} Dn$$

ou, en remplaçant A, B et C par leurs valeurs

$$\Sigma n^8 = \frac{1}{9} n^9 + \frac{1}{2} n^8 + \frac{2}{3} n^7 - \frac{7}{15} n^5 + \frac{2}{9} n^3 + Dn$$

Faisons $n = 1$, il vient :

$$1 = \frac{1}{9} + \frac{1}{2} + \frac{2}{3} - \frac{7}{15} + \frac{2}{9} + D$$

ce qui nous permet de calculer $D = -\frac{1}{30}$.

Les nombres A, B, C, D suffiraient pour exprimer $\Sigma n^9$, et l'expression de $\Sigma n^{10}$ donnerait le nombre suivant E, à savoir $\frac{5}{66}$. Ces nombres rationnels A, B, C, ..., etc., très importants, en particulier en

# Que sais-je ?

*Collection dirigée par Paul Angoulvent*

## *Derniers titres parus*

1461. **Le Niger** (P. Donaint et Fr. Lancrenon).
1462. **Le mariage et le divorce** (M. Delmas-Marty).
1463. **Les Alpes** (P. Veyret).
1464. **La gauche en France de 1789 à nos jours** (J. Defrasne).
1465. **Le droit international des affaires** (J. Schapira).
1466. **La philosophie allemande** (M. Dupuy).
1467. **La photométrie** (J. Terrien et F. Desvignes).
1468. **L'avenir de l'agriculture française** (P. Le Roy).
1469. **Le mimétisme** (G. Pasteur).
1470. **L'Himalaya** (J. Dupuis).
1471. **La gestion informatique** (Ch. Berthet et W. Mercouroff).
1472. **Les politiques agraires** (R. Gadille).
1473. **L'astrophysique nucléaire** (J. Audouze et S. Vauclair).
1474. **Le droit de la famille** (M. Delmas-Marty).
1475. **L'épistémologie** (R. Blanché).
1476. **L'athlétisme** (A. Gardien, M. Houvion, R. Prost et R. Thomas).
1477. **L'ionosphère** (A. Haubert).
1478. **Les maladies du squelette** (Fl. Coste).
1479. **Les termes de marine** (P. Sizaire).
1480. **La fiabilité** (P. Chapouille).
1481. **Le siècle de saint Louis** (P. Labal).
1482. **L'administration économique** (P. Fourneret).
1483. **Histoire de la langue grecque** (J. Humbert).
1484. **Le budget de l'Etat** (J.-M. Cotteret et Cl. Emeri).
1485. **La littérature hispano-américaine** (J. Joset).
1486. **La police** (M. Le Clère).
1487. **Histoire de l'Ecosse** (J.-Cl. Crapoulet).
1488. **L'informatique médicale** (M. Adin).
1489. **Le Zaïre** (R. Cornevin).
1490. **L'escrime** (R. Cléry).
1491. **L'économie forestière** (R. Viney).
1492. **Les styles du meuble français** (G. Janneau).
1493. **Les partis politiques sn Allemagne fédéaale** (Estievenart).
1494. **Les intersexualités** (Gilbert-Dreyfus).
1495. **Les règlements internationaux** (A. Neurrisse).
1496. **Les organes des sens** (A. Goudot).
1497. **Histoire de Monaco** (J.-B. Robert).
1498. **L'anthropologie criminelle** (P. Grapin).
1499. **Les transports maritimes** (A. Boyer).
1500. **La prospective** (A.-Cl. Decouflé).
1501. **Attila et les Huns** (L. Hambis).
1502. **Servomécanismes et régulateurs** (A. Fossard).
1503. **La dérive des continents** (M. Roubault).
1504. **Les Incas** (H. Favre).
1505. **La chimie quantique** (R. Daudel).
1506. **Les enfants inadaptés** (R. Perron).
1507. **Le Rhône** (J.-P. Ritter).
1508. **L'amour** (P. Burney).
1509. **Les ondes hertziennes** (Th. Kahan).
1510. **La pensée chrétienne** (H. Rousseau).
1511. **L'espéranto** (P. Janton).
1512. **L'aide sociale en France** (A. Thévenet).
1513. **Grammaire de l'italien** (G. Genot).
1514. **La drogue** (Y. Pélicier et G. Thuillier).
1515. **Les transports routiers** (A. Boyer).
1516. **Le crédit à la consommation** (B. Moschetto et A. Plagnol).
1517. **L'objection de conscience** (J.-P. Cattelain).
1518. **Le droit de la pharmacie** (B. Cristau).
1519. **Grammaire du chinois** (V. Alleton).
1520. **La rage** (A. Gamet).

Participant d'une démarche de transmission de fictions ou de savoirs rendus difficiles d'accès par le temps, cette édition numérique redonne vie à une œuvre existant jusqu'alors uniquement sur un support imprimé, conformément à la loi n° 2012-287 du 1er mars 2012 relative à l'exploitation des Livres Indisponibles du XXe siècle.

Cette édition numérique a été réalisée à partir d'un support physique parfois ancien conservé au sein des collections de la Bibliothèque nationale de France, notamment au titre du dépôt légal. Elle peut donc reproduire, au-delà du texte lui-même, des éléments propres à l'exemplaire qui a servi à la numérisation.

Cette édition numérique a été fabriquée par la société FeniXX au format PDF.

La couverture reproduit celle du livre original conservé au sein des collections de la Bibliothèque nationale de France, notamment au titre du dépôt légal.

*

La société FeniXX diffuse cette édition numérique en accord avec l'éditeur du livre original, qui dispose d'une licence exclusive confiée par la Sofia – Société Française des Intérêts des Auteurs de l'Écrit – dans le cadre de la loi n° 2012-287 du 1er mars 2012.

Avec le soutien du

CNL Centre national du livre