Chapitre 1 : Préliminaires et outils fondamentaux

Introduction

La théorie des nombres est l'une des plus anciennes et des plus belles branches des mathématiques. Ses problèmes sont simples et claires en ce qui concerne leurs formulation, mais ils pourraient avoir besoin de grands efforts pour les résoudre. Dans ce sens, nous trouvons de nombreux problèmes qui ont été soulevés depuis longtemps, et qui n'ont pas trouvé de solution jusqu'à ce jour, nous en mentionnerons, ci-dessous, quelques-uns

1. (Conjecture de Goldbach) Est-ce que chaque entier pair supérieur à 2 est la somme des nombres premiers distincts?

2. (Problème de nombres premiers jumeaux) Y a-t-il une infinité de nombres premiers p tels que $p+2$ est également un nombre premier?

3. Conjecture de Dickson (1904).

Nous donnons ci-après quelques outils principaux et que l'on trouve d'habitude au début de chaque cours de théorie des nombres

Théorème du bon order 1 (Théorème de Zermelo). Chaque sous-ensemble non vide S de l'ensemble des entiers naturels $\mathbb{N}$, a un plus petit élément.

Exemple 1. Il n'y a pas d'entier dans l'intervalle$]0,1[$.

Preuve. Supposons le contraire i.e.

$$S = \{n \in \mathbb{N} \,|0 < n < 1\} \neq \emptyset.$$

Alors, d'après le théorème du bon order, S a un plus petit élément $0 < m$. D'où

$$0 < m^2 < m < 1.$$

Ce qui signifie que $m^2 \in S$ et $m^2 < m$, mais ceci contredit le fait que m est le plus petit élément de S.

Exemple 2. $\sqrt{3}$ est irrationnel.

Preuve. Supposons que $\sqrt{3} = \frac{a}{b}$ où a et b sont deux entiers positifs. posons

$$A = \left\{ n\sqrt{3} \mid n > 0 \text{ entier et } n\sqrt{3} > 0 \text{ entier} \right\}.$$

Alors $A \neq \emptyset$ ($b \in A$). D'où, d'après le théorème du bon order, A possède un plus petitt élément j. Alors $j = k\sqrt{3} > 0$ entier, $k > 0$ entier. D'où $(j-k)\sqrt{3} \in A$ car $j-k$ est un entier positif et $(j-k)\sqrt{3} = 3k - k\sqrt{3}$ est aussi entier positif. D'autre part $(j-k)\sqrt{3} = 3k - k\sqrt{3} < k\sqrt{3} = j$. Ceci contredit le fait que j est le plus petit élément de A.

Théorème 2 (Principe des tiroirs de Dirichlet). Si $m+1$ objets sont rangés dans m tiroirs, alors il y aura au moins un tiroir qui contient deux objets ou plus.

Exemple 1. Dans un groupe avec au moins 8 personnes, il doit y avoir au moins deux personnes qui sont nées le même jour.

,

Exemple 2. Soit $m > 1$ et $(x_i)_{1 \leq i \leq p}$ une suite de nombres entiers contenant au moins $m+1$ entiers i.e. ($p \geq m+1$). Alors il existe deux nombres de cette suite dont la différence est divisible par m.

Preuve. Par la division Euclidienne il existe, pour chaque $1 \leq i \leq p$, des entiers uniques q_i et r_i tels que $x_i = mq_i + r_i$ où $0 \leq r_i < m$. D'où on a $m+1$ entiers r_i qui appartiennent à l'ensemble fini $\{0, 1, ..., m-1\}$ contenant m éléments. Par conséquent, d'après le principe des tiroirs, il existent deux entiers x_{i_1} et x_{i_2} pour lesquelles $r_{i_1} = r_{i_2}$. Alors dans ce cas

$$\begin{aligned} x_{i_1} - x_{i_2} &= (mq_{i_1} + r_{i_1}) - (mq_{i_2} + r_{i_2}) \\ &= m(q_{i_1} - q_{i_2}). \end{aligned}$$

ce qui signifie que m divise $x_{i_1} - x_{i_2}$.

Théorème 3 (Théorème d'approximation de Dirichlet). Si α est un nombre réel et n est un entier positif, alors il existe des entiers p et q avec $1 \leq p \leq n$ tels que $|p\alpha - q| < \dfrac{1}{n}$.

Preuve. Considérons les $n+1$ nombers $\{0\alpha\}, \{\alpha\}, \{2\alpha\}, ..., \{n\alpha\}$ qui sont respectivement les parties fractionnaires des nombres $j\alpha$ où $j = 0, 1, ..., n$. Alors, pour $j = 0, 1, ..., n$, on a $\{j\alpha\} \in [0, 1[$ car $\{j\alpha\} = j\alpha - \lfloor j\alpha \rfloor$. L'intervalle $[0, 1[$ peut être écrit selon la réunion disjointe suivante formée par n intervalles

$$[0, 1[= \underset{0 \leq i \leq n-1}{\cup} \left[\frac{i}{n}, \frac{i+1}{n}\right[.$$

D'autre part on a $n+1$ réels $\{j\alpha\}$ ($j = 0, 1, ..., n$) dans ces n intervalles. D'où, par le principe des tiroirs, deux de ces réels sont dans le même intervalle; notons les par $\{j_1\alpha\}$ et $\{j_2\alpha\}$ où on suppose que $j_2 < j_1$. Donc $|\{j_1\alpha\} - \{j_2\alpha\}| < \frac{1}{n}$ i.e. $|(j_1\alpha - \lfloor j_1\alpha \rfloor) - (j_2\alpha - \lfloor j_2\alpha \rfloor)| < \frac{1}{n}$. D'où

$$|(j_1 - j_2)\,\alpha - (\lfloor j_1\alpha \rfloor - \lfloor j_2\alpha \rfloor)| < \frac{1}{n}.$$

La preuve est achevée en prenant $p = j_1 - j_2$ et $q = \lfloor j_1\alpha \rfloor - \lfloor j_2\alpha \rfloor$.

Théorème 4 (Premier principe de l'iduction mathématiques). Un ensemble S d'entiers positifs qui contient l'entier 1 et qui a la propriété que chaque fois qu'il contient un entier k il contient également $k+1$, doit contenir tous les entiers positifs.

Théorème 5 (Deuxième principe de l'induction mathématique). Un ensemble S d'entiers positifs qui contient l'entier 1 et qui a la propriété, que pour tout entier positif n s'il contient tous les entiers positifs $1, 2, ..., n$ il contient également l'entier $n+1$, doit contenir tous les entiers positifs.

Exemple 1. Montrer que pour tout entier positif n, on a

$$\sum_{j=1}^{n} (2j-1) = 1 + 3 + ... + (2n-1) = n^2.$$

Preuve. Pour $n = 1$, on a $\sum\limits_{j=1}^{1} (2j-1) = 1 = 1^2$. Supposons que pour $n \geq 1$, on a

$$\sum_{j=1}^{n} (2j-1) = n^2.$$

Maintenant, en utilisant l'hypothèse de récurrence, on a

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

Exemple 2. Soit la suite $(a_n)_{n\geq 1}$ définie par la relation $a_n = 3a_{n-1} - 2a_{n-2}$, où $a_1 = 3$ et $a_2 = 5$. Montrer par le deuxième principe d'induction mathématiques que $a_n = 1 + 2^n$, $n \geq 1$.

Preuve. On vérifie facilement que $a_1 = 3$ et $a_2 = 5$. Supposons que la relation est vérifiée pour les entiers $1, 2, ..., n$ avec $n \geq 2$. Prouvons pour $n + 1$. Ona

$$\begin{aligned}a_{n+1} = 3a_n - 2a_{n-1} &= 3(1+2^n) - 2(1+2^{n-1})\\ &= 1 + 3.2^n - 2^n\\ &= 1 + 2^{n+1}.\end{aligned}$$

Théorème 6 (Inégalité des moyennes). Soit $a_1, a_2, ..., a_n$ des nombres réels, alors

$$(a_1 a_2 ... a_n)^{\frac{1}{n}} \leq \frac{a_1 + a_2 + ... + a_n}{n}.$$

avec égalité ssi $a_1 = a_2 = ... = a_n$.

Théorème 7 (Cauchy-Schwarz). Soit $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n$ des nombres réels, alors

$$\left(\sum_{j=1}^{n} a_i b_i\right)^2 \leq \sum_{j=1}^{n} a_i^2 . \sum_{j=1}^{n} b_i^2.$$

Théorème binomial

Nous commençons d'abord par définir le coefficient binomial.

Définition. Soit $n \geq 0$ un entier et k un entier satisfaisant $0 \leq k \leq n$. Nous définissons $\begin{pmatrix} n \\ k \end{pmatrix}$ comme étant la quantité $\frac{n!}{k!\,(n-k)!}$, lorsque $0 \leq n < k$,

$\begin{pmatrix} n \\ k \end{pmatrix} = 0$. Par convention $0! = 1$.

Il est démontré que $\begin{pmatrix} n \\ k \end{pmatrix}$ est un entier.

Théorème 8 (Pascal's Identity). Soient n and k des entiers positifs els que $n \geq k$. Alors

$$\begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k-1 \end{pmatrix} = \begin{pmatrix} n+1 \\ k \end{pmatrix}.$$

Théorème 9 (Binôme de Newton). Soit a, $b \in \mathbb{R}$ et $n \in \mathbb{N}$. Alors

$$(a+b)^n = \sum_{j=0}^{n} \begin{pmatrix} n \\ j \end{pmatrix} a^{n-j} b^j.$$

Preuve. Nous utilisons le principe de l'iduction mathématiques. Pour $n = 1$, on a

$$(a+b)^1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} a^1 b^0 + \begin{pmatrix} 1 \\ 1 \end{pmatrix} a^0 b^1.$$

Comme $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1$, $(a+b)^1 = a+b$. Ceci signifie que le théorème est vrai pour $n = 1$.

Supposons que le théorème est vrai pour un entier positif n. Démontrons le théorème pour $n+1$.

$$\begin{aligned} (a+b)^{n+1} &= (a+b)^n (a+b) \\ &= \left[\sum_{j=0}^{n} \begin{pmatrix} n \\ j \end{pmatrix} a^{n-j} b^j \right] (a+b) \\ &= \sum_{j=0}^{n} \begin{pmatrix} n \\ j \end{pmatrix} a^{n-j+1} b^j + \sum_{j=0}^{n} \begin{pmatrix} n \\ j \end{pmatrix} a^{n-j} b^{j+1}. \end{aligned}$$

Nous modifions les deux dernières sommes comme suit

$$\sum_{j=0}^{n} \begin{pmatrix} n \\ j \end{pmatrix} a^{n-j+1} b^j = a^{n+1} + \sum_{j=1}^{n} \begin{pmatrix} n \\ j \end{pmatrix} a^{n-j+1} b^j$$

et

$$\begin{aligned}\sum_{j=0}^{n}\binom{n}{j}a^{n-j}b^{j+1} &= \sum_{j=0}^{n-1}\binom{n}{j}a^{n-j}b^{j+1}+b^{n+1}\\ &= \sum_{j=1}^{n}\binom{n}{j-1}a^{n-j+1}b^{j}+b^{n+1}.\end{aligned}$$

D'où, nous trouvons

$$(a+b)^{n+1}=a^{n+1}+\sum_{j=1}^{n}\left[\binom{n}{j}+\binom{n}{j-1}\right]a^{n-j+1}b^{j}+b^{n+1}.$$

Par l'identité de pascal on a $\binom{n}{j}+\binom{n}{j-1}=\binom{n+1}{j}$. D'où

$$\begin{aligned}(a+b)^{n+1} &= a^{n+1}+\sum_{j=1}^{n}\binom{n+1}{j}a^{n-j+1}b^{j}+b^{n+1}\\ &= \sum_{j=0}^{n+1}\binom{n+1}{j}a^{n-j+1}b^{j}.\end{aligned}$$

Ainsi la preuve est terminée.

Théorème 10 (Principe d'inclusion-exclusion). Soit A un ensemble contenant N éléments e soit p_1, p_2, ..., p_r les propriétés différentes qu'un élément de A peut posséder. Si $n\left(p_{i_1},p_{i_2},...,p_{i_k}\right)$ désigne le nombre d'éléments de A possédant toutes les propriétés p_{i_1}, p_{i_2}, ..., p_{i_k}, alors le nombre d'éléments de A ne possédant aucune des r propriétés est :

$$\begin{gathered}N-\left(n\left(p_1\right)+n\left(p_2\right)+...+n\left(p_r\right)\right)+\\ \left[n\left(p_1,p_2\right)+n\left(p_1,p_3\right)+..+n\left(p_1,p_r\right)+n\left(p_2,p_3\right)+n\left(p_2,p_4\right)+..+n\left(p_2,p_r\right)+..+n\left(p_{r-1},p_r\right)\right]\\ -\left[n\left(p_1,p_2,p_3\right)+n\left(p_1,p_2,p_4\right)+......+n\left(p_{r-2},p_{r-1},p_r\right)\right]\\ +....+\left(-1\right)^{r}n\left(p_1,p_2,...,p_r\right).\end{gathered}$$

Exemple. Parmi 20 étudiants, 10 étudient les mathématiques, 11 étudient la physique et 4 étudient les deux. Combien y-a-t-il d'étudiants qui n'étudient ni les mathématiques ni la physique?

Réponse. La formule à appliquer dans ce cas est $N-\left(n\left(p_1\right)+n\left(p_2\right)\right)+n\left(p_1,p_2\right)$. D'où le nombre demandé est $20-(11+10)+4=3$.

Références.

[1] A Adler, J E Coury, *The theory of numbers: A text and source book of problems*,
Jones and Bartlett Publ., Boston (1995); ISBN-10:0867204729.
[2] Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, 1991 by John Wiley & Sons, Inc. .
[3] Kenneth H. Rosen, *Elementary Number Theory & Its Applications*, 2011, Library of Congress Cataloging-in-Publication Data.
[4] Melvyn B. Nathanson, *Elementary Methods in Number Theory, Springer 2000.*

Exercices

Exo 1. Démontrer que la formule $\sum_{j=1}^{n}(-1)^j j^2 = (-1)^n \sum_{j=1}^{n} j$ est valable pour chaque entier positif n.
Exo 2. Montrer que $a+b$ est un facteur de $a^{2n-1}+b^{2n-1}$ pour chaque entier $1 \leq n$.
Exo 3. Supposons que parmi n points, $2 \leq n$, dans un plan donné, aucune combinaison de trois points n'est en ligne droite. Montrer que le nombre de droites possibles passant par deux de ces points est $\frac{n(n-1)}{2}$.
Exo 4. Montrer que tout entier $7 < n$ peut s'écrire comme une somme ne contenant que les nombres 3 ou 5. Par exemple, $8 = 3+5$, $9 = 3+3+3$, $10 = 5+5$.
Exo 5. Montrer que parmi 51 entiers positifs arbitraires, on peut en trouver deux dont la différence est divisible par 50.
Exo 6. Soient a, b et c trois entiers vérifiant $a^6 + 2b^6 = 4c^6$. Montrer que $a = b = c = 0$.
Exo 7. Montrer que si n est un entier positif, alors

$$\binom{n}{k} = \binom{n}{k+1} \Longleftrightarrow n = 2k+1.$$

Exo 8. Montrer que

$$\binom{r}{r} + \binom{r+1}{r} + ... + \binom{n}{r} = \binom{n+1}{r+1}$$

où n et r sont des entiers avec $1 \leq r \leq n$.

Exo 9. Montrer que si n est un entier positif, alors

a) $\binom{2n}{0} + \binom{2n}{2} + \binom{2n}{4} + ... + \binom{2n}{2n} = 2^{2n-1}$.

b) $\binom{2n}{1} + \binom{2n}{3} + \binom{2n}{5} + ... + \binom{2n}{2n-1} = 2^{2n-1}$.

Exo 10. Soit S un ensemble de 10 entiers distincts choisis parmi les nombres 1, 2, 3,..., 99. Montrer que S contient toujours deux sous-ensembles disjoints dont la somme de leurs éléments respectifs est la même.

Exo 11. Trouver le nombre d'entier dans l'ensemble $S = \{1, 2, 3, ..., 6300\}$ qui ne sont divisible ni par 3 ni par 4.