International Journal of Innovation and Scientific Research
ISSN 2336-0046 Vol. 77 No. 1 Feb. 2025, pp. 139-154

http://www.ijisr.issr-journals.org/

Formalisation algébrique du crible d'Eratosthène

[Algebraic formalization of the sieve of Eratosthenes]

Mushiwalyahyage Zaluka[1], Safari Mukeru[2], and Déborah Amani Faraja[3]

[1]Département de Mathématique-Physique, Institut Supérieur Pédagogique de Bukavu (ISP, BUKAVU), Bukavu, RD Congo

[2]Department of Decision Sciences, School of Economics and Financial Sciences, College of Economics and Management Sciences, Université Sud-Africaine (UNISA), Pretoria, South Africa

[3]Ecole des Mines, Université Officielle de Bukavu (U.O.B), Bukavu, RD Congo

ABSTRACT: This paper presents, in algebraic form, the set of prime numbers as obtained by the sieve of Eratosthenes and as contained in an arithmetic progression. In this way, it unifies old and recent studies on prime numbers: Euclid's theorem, Dirichlet's theorem, Green-Tao's theorem, the conjecture of twin primes (generalized by Polignac) and Chebyshev's Bias Phenomenon. It re-demonstrates the three theorems, solves Chebyshev's Bias Phenomenon, demonstrates the twin primes conjecture and elucidates Polignac's conjecture.

KEYWORDS: number, composite, prime, twins, sieve, Eratosthenes, theorem, conjecture.

RESUME: Cet article écrit, sous forme algébrique, l'ensemble des nombres premiers tels qu'ils s'obtiennent par le crible d'Eratosthène et tels qu'ils sont contenus dans une progression arithmétique. De cette manière, il unifie les études, anciennes et récentes, sur les nombres premiers: le théorème d'Euclide, le théorème de Dirichlet, le théorème de Green-Tao, la conjecture des nombres premiers jumeaux (généralisée par Polignac) et le Phénomène de Biais de Tchebychev. Il redémontre les trois théorèmes, résout le Phénomène de Biais de Tchebychev, démontre la conjecture des nombres premiers jumeaux et élucide la conjecture de Polignac.

MOTS-CLEFS: nombre, composé, premier, jumeaux, crible, Eratosthène, théorème, conjecture.

1 INTRODUCTION

Un nombre entier naturel a est dit premier lorsque l'ensemble $\mathfrak{D}_a$ de ses diviseurs est une paire; i.e. $a > 1$ et a n'est divisible que par 1 et par lui-même. Deux nombres a et b sont dits étrangers ou premiers entre eux si leur dernier diviseur commun est égal à 1; i.e. $ddc(a, b) = 1$. L'étude des nombres entiers naturels premiers consiste à en rechercher des propriétés en vue d'établir un certain ordre dans leur répartition parmi leurs homologues entiers naturels.

Il est connu, d'une part, que l'ensemble des nombres entiers naturels premiers est infini (théorème d'Euclide). La démonstration en est purement élémentaire (raisonnement par l'absurde) et l'on peut déterminer, par le crible d'Eratosthène, tous les nombres entiers naturels premiers inférieurs ou égaux à une limite fixée; ce qui conduit à la théorie des cribles. Il est connu, d'autre part, que si a et b sont deux nombres étrangers, alors il existe une infinité des nombres entiers naturels premiers de la forme $ax + b$; $x \in \mathbb{N}$ (théorème de L. Dirichlet). La démonstration en est analytique (en 1838), et inaugure le début de la théorie analytique des nombres. Même élémentaire par A. Selberg (en 1949), la démonstration du théorème de L. Dirichlet

n'a pas de rapport avec celle du théorème d'Euclide. Pourtant, sur le plan algébrique, le premier théorème est un cas particulier du second pour $a = 1\ et\ b = 2$; $ddc(1,2) = 1$; i.e. « Il existe une infinité de nombres premiers de la forme $x + 2$; $x \in \mathbb{N}$. »

Par ailleurs, l'étude de la distribution des nombres premiers dans $\mathbb{N}$ ou, mieux, dans $\mathbb{N} \setminus \{0,1\}$, se fait de plus en plus au moyen de l'étude de la différence entre deux nombres premiers consécutifs p_k et p_{k+1} ou non consécutifs p et q. Deux cas particuliers sont en vogue: la conjecture des nombres premiers jumeaux et sa forme faible. La conjecture stipule que: « Est infini, l'ensemble des nombres premiers p_k et p_{k+1} tels que $p_{k+1} - p_k = 2$. » Et, la forme faible de cette conjecture est le théorème de Y. Zhang selon lequel: « Est infini, l'ensemble des nombres premiers p et q tels que $p < q\ et\ q - p < 70.10^6$ »[1]. A l'annonce de ce dernier résultat, la Communauté Mathématique Internationale voyait, dans un bref délai, la réduction de l'écart 70.10^6 entre p et q à 3. Certes, l'écart fut abaissé respectivement à 600 par Maynard et à 246 dans un projet Polymath [2]. Néanmoins, il n'est pas encore passé à 3. Entre-temps, la conjecture des nombres premiers jumeaux peut être associée au théorème d'Euclide: « La situation est choquante, car 33 mots suffisent pour démontrer qu'il existe une infinité de nombres premiers. Les deux problèmes sont très proches, mais l'un est facile et, l'autre, bloqué » ([3], p. 232).

Eu égard à ce qui précède, l'étude des liens entre les questions susmentionnées sur les nombres premiers est un problème ouvert et actuel dont nous voudrions contribuer à la résolution par cet article intitulé « Formalisation algébrique du crible d'Eratosthène ».

2 MATERIEL ET METHODES

Comme le titre l'indique, nous retournons à l'origine des nombres premiers: nous supprimons la limite dans le crible d'Eratosthène, en exécutons le processus indéfiniment et écrivons le résultat sous une forme algébrique. Concrètement, nous caractérisons l'ensemble des nombres entiers naturels premiers: nous définissons l'ensemble des nombres entiers naturels composés et en déduisons, par complémentarité dans $\mathbb{N} \setminus \{0,1\}$, l'ensemble des nombres entiers naturels premiers. Cette façon de faire isolerait les nombres premiers pour mieux les étudier. Grâce à la condition pour qu'une partie non vide de l'ensemble $\mathbb{N}$ soit finie ou infinie, nous énonçons la condition pour que sa partie complémentaire dans $\mathbb{N}$ soit finie ou infinie et, cette dernière condition, permet d'appliquer la formalisation algébrique du crible d'Eratosthène à la théorie des nombres.

Par conséquent, le fond de cet article est subdivisé en trois parties. La première est intitulée « Partie finie de l'ensemble $\mathbb{N}$ ». Elle comprend les conditions pour qu'une partie non vide de $\mathbb{N}$ et sa partie complémentaire dans $\mathbb{N}$ soient finies ou infinies. La deuxième partie est intitulée « L'ensemble des nombres entiers naturels composés multiples de p_k $(k \geq 2)$ et non multiples de p_i $(1 \leq i \leq k- 1)$ ». C'est l'ensemble des nombres que l'on barre dans le processus du crible d'Eratosthène. La troisième partie est intitulée « Nombres premiers dans une progression arithmétique ». Elle améliore la deuxième et ouvre aux applications de la formalisation algébrique du crible d'Eratosthène que sont: la ré-démonstration des théorèmes d'Euclide, de Dirichlet et de Green-Tao; la résolution du Phénomène de Biais de Tchebychev; la démonstration de la conjecture des nombres premiers jumeaux et l'élucidation de la conjecture de Polignac.

3 RÉSULTATS

3.1 PARTIE FINIE DE L'ENSEMBLE $\mathbb{N}$

Nous voudrions rappeler la condition pour qu'une partie de $\mathbb{N}$ soit finie, l'adapter à notre sujet et l'appliquer pour démontrer des résultats dans la suite de ce travail.

Théorème 1

Une partie non vide de $\mathbb{N}$ est finie si et seulement si elle est majorée ([4], p. 68).

Théorème 2

Soient A une partie infinie de $\mathbb{N}$ et $B = \mathbb{N}\setminus A$.

(1) B est fini si et seulement s'il existe $q \in \mathbb{N}$ tel que pour tout $q' \in \mathbb{N}$ avec $q' \geq q$, on ait

$$q' \in A$$

(2) B est infini si et seulement si pour tout $q \in \mathbb{N}$, il existe $q' \in \mathbb{N}$ avec $q' \geq q$ tel que $q' \notin A$

Démonstration

D'après le théorème 1, B est fini (resp. infini) si et seulement si B est majoré (resp. n'est pas majoré). En se servant de la définition de la différence des ensembles, on a le théorème 2.

3.2 Ensemble Des Naturels Composes Multiples De p_k Et Non Multiples De p_i

Pour tout entier $k \geq 1$, p_k désignera le nombre premier de rang k. Par exemple $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. De plus, on notera $\pi_k = p_1 \times p_2 \times \ldots \times p_k$ et, par M_k, l'ensemble des nombres entiers naturels qui sont multiples composés de p_k et non multiples de p_i pour tous les $i = 1,2, \ldots, k-1$, i.e.

$M_k = \{x \in \mathbb{N} / x \text{ est multiple de } p_k, \text{ mais pas multiple de } p_i, \text{pour tout } i = 1,2, \ldots, k-1\}$.

Théorème 3

Pour tout entier $k \geq 2$,

$$M_k = \bigcup_{p_k \leq p < p_k + \pi_{k-1}} \{(\pi_k)n + p_k p, n \in \mathbb{N}\}$$

Démonstration

Soit un entier $k \geq 2$. Alors $\{n\pi_k \ ; \ n \in \mathbb{N}\}$ est l'ensemble des multiples des p_i $(1 \leq i \leq k)$.

Considérons $X_m = n\pi_k + m$; $n \in \mathbb{N}$. Alors X_m est multiple d'un p_i si et seulement si m l'est. Supposons que m est un multiple composé de p_k , mais n'est multiple d'aucun p_i

$(1 \leq i \leq k-1)$. Alors il existe $u \in \mathbb{N} \setminus \{0,1\}$ et u non multiple de p_i tel que

$m = up_k \text{ et } u \geq p_k$ (1). Dans ce cas, $X_m = p_k(n\pi_{k-1} + u)$. Posons $V_u = n\pi_{k-1} + u$. Alors u est le reste de la division euclidienne de V_u par π_{k-1}; i.e. $0 \leq u < \pi_{k-1}$.

Or, d'après (1), $u \geq p_k$. Donc une translation du reste donne $p_k \leq u < p_k + \pi_{k-1}$ (2). Mais, u n'est multiple d'aucun p_i. Donc u est premier: $u = p$ et $p_k \leq p < p_k + \pi_{k-1}$. Il s'ensuit que $X_m = n\pi_k + p_k p$ $(n \in \mathbb{N})$ et $M_k = \cup\{n\pi_k + p_k p, p_k \leq p < p_k + \pi_{k-1}\}$. CQFD

Remarque

On peut aussi écrire $M_k = (\pi_k)\mathbb{N} + \{p_k p : p \text{ premier et } p_k \leq p < p_k + \pi_{k-1}\}$.

Exemples

1. $k = 2 \Rightarrow p_1 = 2$ et $p_2 = 3$: $\pi_1 = 2, \pi_2 = 6, p_2 \leq p < p_2 + \pi_1$ donne $3 \leq p < 5$; i.e. $p = 3$ et $M_2 = \{6n + 9, n \in \mathbb{N}\}$ est l'ensemble des nombres entiers naturels multiples impairs composés de 3.
2. $k = 3 \Rightarrow p_1 = 2, \ p_2 = 3$ et $p_3 = 5$: $\pi_2 = 6, \ \pi_3 = 30, p_3 \leq p < p_3 + \pi_2$ donne $5 \leq p < 11$; i.e. $p \in \{5,7\}$ et $M_3 = \{30n + 25, n \in \mathbb{N}\} \cup \{30n + 35, n \in \mathbb{N}\}$

$= \{30n + 25, 30n + 35; \ n \in \mathbb{N}\} = 30\mathbb{N} + \{25,35\}$ est l'ensemble des multiples composés de 5, non multiples de 2 et de 3.

3. $k = 4 \Rightarrow p_1 = 2, p_2 = 3, p_3 = 5$ et $p_4 = 7$: $\pi_3 = 30, \pi_4 = 210$,

$p_4 \leq p < p_4 + \pi_3$ donne $7 \leq p < 37$; i.e. $p \in \{7,11,13,17,19,23,29,31\}$ et

$M_4 = 210\mathbb{N} + \{49, 77, 91, 119, 133, 161, 203, 217\}$ est l'ensemble des multiples composés de 7, non multiples de 2, 3 et 5.

Cas particulier

En particulier $k = 1 \Longrightarrow p_1 = 2$ et $M_1 = \{2n + 4, n \in \mathbb{N}\}$ est l'ensemble des entiers naturels pairs composés.

Corollaire 1

Soit $\mathbb{N}_c$ l'ensemble des entiers naturels composés. Alors $\mathbb{N}_c = \cup_{k=1}^{\infty} M_k$

Démonstration

Évident par définition des ensembles M_k.

Corollaire 2

Soit $\mathbb{N}_p$ l'ensemble des nombres entiers naturels premiers. Alors $\mathbb{N}_p = (\mathbb{N} + 2) \setminus \mathbb{N}_c$.

Démonstration

Évident par complémentarité des ensembles $\mathbb{N}_c$ et $\mathbb{N}_p$ dans $\mathbb{N} \setminus \{0,1\} = \mathbb{N} + 2$.

Remarques

- Le théorème 3 et ses deux corollaires constituent la formalisation algébrique du crible d'Eratosthène.
- La détermination de l'ensemble M_k présente deux inconvénients. Primo, elle exige la connaissance préalable du nombre premier p_k ($k \geq 2$), de tous les nombres premiers p_i ($1 \leq i \leq k - 1$) et p ($p_k \leq p < p_k + \pi_{k-1}$). Ainsi, l'ensemble des nombres composés et celui des nombres premiers s'obtiennent en fonction de nombres premiers. Secundo, le cardinal de l'ensemble $\{p \in \mathbb{N}_p / p_k \leq p < p_k + \pi_{k-1}\}$ augmente rapidement avec la valeur de $p_k + \pi_{k-1}$. Pour les contourner, nous recourons à la détermination des nombres premiers contenus dans une progression arithmétique.

3.3 NOMBRES PREMIERS DANS UNE PROGRESSION ARITHMETIQUE

3.3.1 PROGRESSION ARITHMETIQUE ET CONGRUENCE MODULO UN ENTIER

$\forall a \in \mathbb{N}^*$, l'ensemble des classes résiduelles modulo a est noté et défini par:

$\mathbb{Z}/_{a\mathbb{Z}} = \mathbb{Z}_a = \{\dot{0}, \dot{1}, \dots, a \dot{-} 1\}$; avec $\dot{0} = a\mathbb{Z}$, $\dot{1} = a\mathbb{Z} + 1$,..., $a \dot{-} 1 = a\mathbb{Z} + a - 1$.

Il est connu que $(\mathbb{Z}_a, \otimes)$ n'est pas un groupe. Mais si a est premier, alors $(\mathbb{Z}_a^*, \otimes)$ est un groupe abélien; avec $\mathbb{Z}_a^* = \mathbb{Z}_a \setminus \{\dot{0}\}$. Dans ce cas, a est premier avec 1, 2,..., a – 1.

Il s'ensuit que $(\mathbb{Z}_a^*, \otimes)$ est un cas particulier du cas général suivant:

Théorème 4

Soit $\mathcal{H}_a = \{\dot{z} \in \mathbb{Z}_a \ / \ ddc(a, z) = 1\}$. Alors on a

- $Card\ \mathcal{H}_a = \varphi(a)$; avec φ l'indicateur d'EULER.
- $(\mathcal{H}_a, \otimes)$ est un groupe commutatif

Démonstration:

Par définition de $\mathcal{H}_a$ et de $\varphi(a)$, (1) est trivial. Aussi, (2) est connu ([5], pp. 81-82)

Conséquence

L'étude des cas particuliers montre que, dans $\mathcal{H}_2$, H_3, $\mathcal{H}_4$, H_6, $\mathcal{H}_8$, $\mathcal{H}_{12}$ et $\mathcal{H}_{24}$ tout élément est involutif (symétrique de lui-même). Sont – ils les seuls groupes, de ce genre, qui possèdent cette caractéristique ? Pour répondre à cette question, nous avons besoin des lemmes suivants:

Lemme 1

Soit p_k le nombre premier de rang k. Alors $\forall k \in \mathbb{N} \setminus \{0, 1\},\ p_k < 2^k$ [6].

Lemme 2

$\forall n \in \mathbb{N}\ et\ n \geq 6, 4^{n+1} < \prod_{j=1}^{n} p_j$.

Démonstration

- $n = 6 \Longrightarrow 4^{6+1} = 4^7 = 16384$ et $\prod_{j=1}^{6} p_j = 2.3.5.7.11.13 = 30030$:

  $16384 < 30030$; ce qui traduit que la propriété est vraie pour $n = 6$.

- Supposons que $4^{n+1} < \prod_{j=1}^{n} p_j$ et montrons que $4^{n+2} < \prod_{j=1}^{n+1} p_j$.

  $4^{n+2} = 4.4^{n+1} < 4.\prod_{j=1}^{n} p_j$ (1)

  Or, $\forall n \geq 6, 4 < p_{n+1}$. Donc $4.\prod_{j=1}^{n} p_j < p_{n+1} \prod_{j=1}^{n} p_j = \prod_{j=1}^{n+1} p_j$ (2)

Par suite, (1) et (2) donnent $4^{n+2} < \prod_{j=1}^{n+1} p_j$.

Théorème 5

Tout élément de $\mathcal{H}_a$ est involutif si et seulement si $a \in \{2, 3, 4, 6, 8, 12, 24\}$.

Démonstration

- $\forall n \in \mathbb{N}, ddc\ (2,2n+5) = 1$: $\dot{2} \in \mathbb{N}_{2n+5}\ et\ \dot{2}\otimes\dot{2} = \dot{4} \neq \dot{1}$.
- $\forall n \in \mathbb{N}, 6n+10\ et\ 6n+14$ sont étrangers avec 3: $\dot{3} \in \mathbb{N}_{6n+10}, \dot{3} \in \mathbb{N}_{6n+14}$

  $et\ \dot{3}\otimes\dot{3} = \dot{9} \neq \dot{1}$.
- $\forall n \in \mathbb{N}, 30n+18, 30n+36, 30n+42\ et\ 30n+54$ sont étrangers avec 5:

  $\dot{5} \in \mathbb{N}_{30n+18}, \dot{5} \in \mathbb{N}_{30n+36}, \dot{5} \in \mathbb{N}_{30n+42}, \dot{5} \in \mathbb{N}_{30n+54}\ et\ \dot{5}\otimes\dot{5} = \dot{25} \neq \dot{1}$.
- $\forall n \in \mathbb{N}, 210n+30, 210n+60, 210n+90, 210n+120, 210n+150\ et\ 210n+180$ sont étrangers avec 7: $\dot{7} \in \mathbb{N}_{210n+30}, \dot{7} \in \mathbb{N}_{210n+60}, \dot{7} \in \mathbb{N}_{210n+90}$,

  $\dot{7} \in \mathbb{N}_{210n+120}, \dot{7} \in \mathbb{N}_{210n+150}, \dot{7} \in \mathbb{N}_{210n+180}\ et\ \dot{7}\otimes\dot{7} = \dot{49} \neq \dot{1}$.
- Raisonnement analogue pour les progressions arithmétiques de raison 2310, avec

  $\dot{11}\otimes\dot{11} = \dot{121} \neq \dot{1}$ et pour les progressions arithmétiques de raison 30030, avec

  $\dot{13}\otimes\dot{13} = \dot{169} \neq \dot{1}$.
- Soient m ∈ ℕ $(m \geq 6)$ et $n \in \mathbb{N}$. Considérons l'entier naturel

$q_m = (1 + r + np_{m+1})\pi_m$; avec $\pi_m = \prod_{k=1}^{m} p_k$ et $r \in \mathbb{N}\ (0 \leq r \leq p_{m+1} - 2)$ et p_k le nombre entier naturel premier de rang k.

Démontrons que $p_{m+1}^{\cdot} \in \mathbb{N}_{q_m}$ et $p_{m+1}^{\cdot}\otimes p_{m+1}^{\cdot} \neq \dot{1}$.

1. Par construction, $p_{m+1} < q_m\ et\ ddc\ (p_{m+1}, q_m) = 1$; i.e. $p_{m+1}^{\cdot} \in \mathbb{N}_{q_m}$.
2. D'après le lemme 1, $p_{m+1} < 2^{m+1}$ et, en élevant les deux membres au carré, on a

$p_{m+1}^2 < 4^{m+1}$.

Or, d'après le lemme 2, $\forall m \in \mathbb{N}\ et\ m \geq 6, 4^{m+1} < \pi_m$. Donc $p_{m+1}^2 < \pi_m$.

Mais, $\pi_m < (1 + r + np_{m+1})\pi_m = q_m$. Donc $p_{m+1}^2 < q_m$.

Par suite $p_{m+1}^{\cdot}\otimes p_{m+1}^{\cdot} = \widehat{p_{m+1}^2} \neq \dot{1}$. CQFD

3.3.2 RESTRICTION À L'ENSEMBLE ℕ

Exploitons la multiplication des classes dans $\mathcal{H}_a$ en la particularisant à l'ensemble $\mathbb{N}_a = \{\dot{z} \cap \mathbb{N} / \dot{z} \in \mathcal{H}_a\}$. Pour des raisons pratiques, remplaçons la classe de 1 par la classe de a + 1 (ces deux classes sont égales). Posons $E_i = \{ax + b_i; x \in \mathbb{N}\}$,

$E = \{E_i; 1 \leq i \leq \varphi(a)\}$ et $G = \{E_iE_j; 1 \leq i \leq j \leq \varphi(a)\}$; avec $ddc(a, b_i) = 1$.

Il est évident que $E_i = \dot{b_i}\ (1 < b_i \leq a + 1)$. Ainsi, $E = \mathbb{N}_a$ et $card\ G = \frac{\varphi(a)[1+\varphi(a)]}{2}$

Exemples

❖ $a = 5 \Longrightarrow E_1 = \{5x+2\} = \dot{2}, E_2 = \{5x+3\} = \dot{3}, E_3 = \{5x+4\} = \dot{4}$ et

$E_4 = \{5x+6\} = \dot{6} : \mathbb{N}_5 = \{\dot{2}, \dot{3}, \dot{4}, \dot{6}\} = \{E_1, E_2, E_3, E_4\} = E$ et

$G = \{E_1E_1, E_1E_2, E_1E_3, E_1E_4, E_2E_2, E_2E_3, E_2E_4, E_3E_3, E_3E_4, E_4E_4\}$.

❖ $a = 6 \Longrightarrow E_1 = \{6x+5\} = \dot{5}$ et $E_2 = \{6x+7\} = \dot{7} : \mathbb{N}_6 = \{\dot{5}, \dot{7}\} = \{E_1, E_2\} = E$ et

$G = \{E_1E_1, E_1E_2, E_2E_2\}$.

❖ $a = 2 \Longrightarrow E_1 = \{2x+3\} = \dot{3} : \mathbb{N}_2 = \{\dot{3}\} = E$ et $G = \{E_1E_1\}$.

3.3.3 ENSEMBLE DES NOMBRES PREMIERS CONTENUS DANS UNE PROGRESSION ARITHMETIQUE

3.3.3.1 PRÉLIMINAIRES

Théorème 6

Soient $a \in \mathbb{N}^*$; b, c $\in \mathbb{N} \setminus \{0,1\}$ tels que $ddc(a,bc) = 1$. Définissons l'ensemble

$A = \{axy + bx + cy;\ (x,y) \in \mathbb{N} \times \mathbb{N}\}$. Alors $\mathbb{N} \setminus A \neq \emptyset$.

Démonstration

Il est évident que $A \sqsubset \mathbb{N}$. Pour démontrer que $\mathbb{N} \setminus A \neq \emptyset$, il suffit d'exhiber au moins un élément de l'ensemble $\mathbb{N}$ qui n'est pas élément de l'ensemble A. L'ensemble $\mathbb{N}$ étant totalement ordonné par la relation $\leq$, déterminons les premiers éléments de l'ensemble A en faisant varier x et y dans l'ensemble $\mathbb{N}$. Alors on a

$A = \{0, c, 2c, 3c, 4c, b, a+b+c, 2a+b+2c, 3a+b+3c, 4a+b+4c, \dots\}$.

Or, $a \in \mathbb{N}^*$; b, c$\in \mathbb{N} \setminus \{0,1\}$. Donc, par exemple, $1 \in \mathbb{N}\ et\ 1 \notin A$. CQFD

Remarque

Si la résolution de l'équation diophantienne $axy + bx + cy = d$ dans $\mathbb{N} \times \mathbb{N}$ est préalablement connue, le lemme suivant démontre automatiquement le théorème 6.

Lemme : Soient $a \in \mathbb{N}^*$; b, c $\in\ \mathbb{N} \setminus \{0,1\}$ tels que $ddc(a,bc) = 1$. Alors l'équation

$axy + bx + cy = 1$ est impossible dans $\mathbb{N} \times \mathbb{N}$.

Démonstration

$axy + bx + cy = 1$ (1)

$\Leftrightarrow bc\,(axy + bx + cy) = bc.$

$\Leftrightarrow a(bx)(cy) + bc\,(bx + cy) = bc$ (2)

Posons $S = bx + cy$ et $P = (bx)(cy)$. Alors (2) devient:

$aP + bcS = bc$ (3)

$\Leftrightarrow P = bck$ et $S = 1 - ak$; k $\in \mathbb{Z}$

S $\in \mathbb{N} \Leftrightarrow 1 - ak \geq 0 \Leftrightarrow ak \leq 1 \Leftrightarrow k = 0\ ou\ a = 1\ et\ k = 1.$

- k = 0 ⇒P = 0 et S = 1 ⇒ $bx = 1\ et\ cy = 0\ ou\ bx = 0\ et\ cy = 1$; ce qui est impossible dans $\mathbb{N}$, car $b, c \in \mathbb{N} \setminus \{0,1\}$.
- a = 1 et k = 1 ⇒ $P = bc\ et\ S = 0$: $bx\ et\ cy$ n'existent pas dans $\mathbb{N}$; x et y aussi car , $c \in \mathbb{N} \setminus \{0,1\}$.

Proposition 1

$\forall \dot{x}, \dot{y} \in \mathbb{N}_a, \dot{x} \otimes \dot{y} \subset \dot{xy}$ strictement; i.e. $\dot{x} \otimes \dot{y} \neq \dot{xy}$

Démonstration

Soient $\dot{x}, \dot{y} \in \mathbb{N}_a$. Alors $\dot{x} = a\mathbb{N} + x$, $\dot{y} = a\mathbb{N} + y$ et $\dot{x} \otimes \dot{y} = (a\mathbb{N} + x)(a\mathbb{N} + y)$; avec $ddc(a,x) = 1$ et $ddc(a,y) = 1$.

Soit $r \in \dot{x} \otimes \dot{y}$. Alors $\exists u, v \in \mathbb{N} / r = (au + x)(av + y)$;

i.e. $r = a^2uv + auy + avx + xy = a(auv + uy + vx) + xy \in \dot{xy}$ (mod a).

D'où $\dot{x} \otimes \dot{y} \subset \dot{xy}$

Inversement, soit $m \in \dot{xy}$. Alors $\exists n \in \mathbb{N} / m = an + xy$.

Supposons, par l'absurde, que $m \in \dot{x} \otimes \dot{y}$. Alors $\exists s, t \in \mathbb{N} / m = a(ast + sy + tx) + xy$ et en identifiant, on a $ast + sy + tx = n\ \forall m = an + xy$; avec $ddc(a,x) = 1$ et

$ddc(a,y) = 1$; i.e. $ddc(a,xy) = 1$.

Ainsi, $\{ast + ys + xt\} = \mathbb{N}$; avec $ddc(a,xy) = 1$; ce qui contredit le théorème 6.

Exemple

Si $a = 3$, alors $\mathbb{N}_3 = \{\dot{2}, \dot{4}\} = \{3\mathbb{N} + 2, 3\mathbb{N} + 4\} : \dot{2} \otimes \dot{4} \subset \dot{2}$ et $\dot{2} \otimes \dot{4} \neq \dot{2}$.

En effet, $(3s + 2)(3t + 4) = 9st + 12s + 6t + 8 = (9st + 12s + 6t + 6) + 2$

$=3(3st + 4s + 2t + 2) + 2 \in \dot{2}$.

Par contre, $\{3st + 4s + 2t + 2\} = \{(3t + 4)s + 2t + 2\} = \{2t + 2, 5t + 6, 8t + 10, 11t + 14, \dots\}$

$= \{2, 4, 6, 8, 10, 12, \dots, 6, 11, 16, 21, 26, 31, 36, \dots, 10, 18, 26, 34, 42, \dots, 14, 25, 36, 47, \dots\}$

$= \{2, 4, 6, 8, 10, 11, 12, 14, \dots\} : \mathbb{N} \setminus \{3st + 4s + 2t + 2\} = \{0, 1, 3, 5, 7, 9, 13, \dots\} \neq \emptyset$; i.e.

$2, 5, 11, 17, 23, 41, \dots$ appartiennent à $\dot{2}$, mais n'appartiennent pas à $\dot{2} \otimes \dot{4}$.

3.3.3.2 PRINCIPE

$E_i = \{ax + b_i; x \in \mathbb{N}\}$, $E = \{E_i; 1 \leq i \leq \varphi(a)\}$ et $G = \{E_i E_j; 1 \leq i \leq j \leq \varphi(a)\}$; avec $ddc(a, b_i) = 1$.

Définissons, dans G, la relation $\Re$ par $E_i E_j \Re E_k E_l \Leftrightarrow \exists E_m \in E \ / \ E_i E_j \sqsubset E_m \ et \ E_k E_l \sqsubset E_m$.

Par définition, $\Re$ est une relation d'équivalence dans G. Si on simplifie la notation par

$\widehat{E_i E_j} = \dot{E_m} = \{E_i E_j \in G / E_i E_j \sqsubset E_m\}$, alors on obtient ${}^{G}/_{\Re} = \{\dot{E}_i; 1 \leq i \leq \varphi(a)\}$ et $card \ {}^{G}/_{\Re} = card \ E$. Soit $\mathbb{N}_{pc}(E_i)$ l'ensemble des nombres premiers contenus dans E_i. Alors $\mathbb{N}_{pc}(E_i) = \{n \in \mathbb{N} \ / \ n \in N_p \ et \ n \in E_i\} = \mathbb{N}_p \cap E_i$ et on a le résultat suivant.

Théorème fondamental

$\mathbb{N}_{pc}(E_i) = E_i \setminus \dot{E}_\iota$.

Démonstration

Soit $z \in \mathbb{N}_{pc}(E_i)$. Alors, par définition, $z \in E_i \ et \ z \in \mathbb{N}_p$; i.e. $z \in E_i \ et \ z \notin \dot{E}_\iota$;

i.e. $z \in E_i \setminus \dot{E}_\iota$. D'où $\mathbb{N}_{pc}(E_i) \subset E_i \setminus \dot{E}_\iota$.

Réciproquement, soit $z \in E_i \setminus \dot{E}_\iota$. Alors $z \in E_i$ et $z \notin \dot{E}_\iota$. Supposons, par l'absurde, que z est un nombre entier naturel composé. Alors $\exists j \in [1, \varphi(a)] \cap \mathbb{N} \ / \ i \neq j \ et \ z \in \dot{E}_j$;

i.e. $\exists E_k E_l \sqsubset E_j \ / \ z \in E_k E_l$; i.e. $\exists u, v \in \mathbb{N} \ / \ z = (au + b_k)(av + b_l)$; i.e

$z = a^2uv + ab_l u + ab_k v + b_l b_k$. En effectuant la division euclidienne de $b_l b_k$ par a,

$b_l b_k = ac_j + b_j$ et $z = a(auv + b_l u + b_k v + c_j) + b_j$; ce qui traduit que $z \in E_j$.

Or, $z \in E_i$. Donc $z \in E_i \cap E_j$; ce qui contredit le fait que $E_i \cap E_j = \emptyset$. Par suite, la supposition est fausse; z est plutôt un nombre entier naturel premier de E_i ; i.e. $z \in \mathbb{N}_{pc}(E_i)$.

D'où $E_i \setminus \dot{E}_\iota \subset \mathbb{N}_{pc}(E_i)$. CQFD

Corollaire

$\mathbb{N}_{pc}(E_i) = E_i \setminus \dot{E}_\iota \Leftrightarrow \cup[\mathbb{N}_{pc}(E_i)] = \cup(E_i \setminus \dot{E}_\iota) = (\cup E_i) \setminus (\cup \dot{E}_\iota); \ 1 \leq i \leq \varphi(a)$.

Démonstration

- $\mathbb{N}_{pc}(E_i) = E_i \setminus \dot{E}_\iota \Longrightarrow \cup[\mathbb{N}_{pc}(E_i)] = \cup(E_i \setminus \dot{E}_\iota)$ (Compatibilité de l'égalité avec la réunion).
- $\cup[\mathbb{N}_{pc}(E_i)] = \cup(E_i \setminus \dot{E}_\iota) \Longrightarrow \mathbb{N}_{pc}(E_i) = E_i \setminus \dot{E}_\iota$, car $[\mathbb{N}_{pc}(E_i)] \cap [\mathbb{N}_{pc}(E_j)] = \emptyset$ et $(E_i \setminus \dot{E}_\iota) \cap (E_j \setminus \dot{E}_j) = \emptyset$.
- $\cup(E_i \setminus \dot{E}_\iota) = (\cup E_i) \setminus (\cup \dot{E}_\iota)$, car $\forall i \in [1, \varphi(a)] \cap \mathbb{N}, \dot{E}_\iota \subset E_i$ et,

  $\forall i \neq j, E_i \cap E_j = \emptyset$ (Un cas particulier où la réunion est distributive par rapport à la différence).

Remarque

Le théorème fondamental améliore la forme algébrique du crible d'Eratosthène.

En effet, soient $ETR(a)$ l'ensemble des nombres entiers naturels premiers avec a et $n_a = \min\limits_{1\leq i\leq \varphi(a)}\{b_i\}$. Alors

- $E = \{E_i; 1 \leq i \leq \varphi(a)\}$ est une partition de $ETR(a)$.

  Ainsi, $ETR(a) = \cup\{E_i; 1 \leq i \leq \varphi(a)\}$

  $ETR(a) \subset \mathbb{N} \setminus \{0,1, \dots, n_a - 1\}$

- La primalité subdivise $ETR(a)$ en deux classes:

  – La classe des nombres entiers naturels premiers; l'ensemble $\cup\left[\mathbb{N}_{pc}(E_i)\right]$.

  – La classe des nombres entiers naturels composés; l'ensemble $\cup\ \dot{E}_\iota$.

3.3.3.3 CONSÉQUENCE: THÉORÈME DE GREEN-TAO

a) Enoncé

« La suite des nombres premiers contient des suites arithmétiques arbitrairement longues. » [7]

b) Interprétation

Pour un nombre entier naturel quelconque k, il existe une suite arithmétique de k termes formée uniquement de nombres premiers. Sous cette forme, le théorème de Green-Tao devient, pratiquement, un cas particulier de notre théorème fondamental.

c) Nouvel énoncé

Soient $E_i = \{ax + b_i\}$; avec $b_i \in \mathbb{N}_p$ et $1 \leq i \leq \varphi(a)$; m_i le plus petit élément de $\dot{E}_\iota$ pour i fixé et $p\mathbb{N}_{pc}(E_i)$ l'ensemble des « Premiers nombres premiers contenus dans E_i ». Alors on a

$p\mathbb{N}_{pc}(E_i) = \left\{n \in \mathbb{N}_{pc}(E_i)/b_i \leq n < m_i\right\}$.

Démonstration

Évident. D'après le théorème fondamental, $\mathbb{N}_{pc}(E_i) = E_i \setminus \dot{E}_\iota$. Comme $b_i \in \mathbb{N}_p$, m_i est le premier nombre entier naturel composé de E_i. Ainsi, tous les éléments de E_i, qui précèdent m_i, sont des nombres entiers naturels premiers.

d) Remarques

1) Si $m = card\left[p\mathbb{N}_{pc}(E_i)\right]$, alors m dépend de b_i et de m_i ; i.e. m est arbitraire: la longueur d'une suite des premiers nombres premiers successifs d'une progression arithmétique est arbitraire.
2) Si b_i est composé, alors $m_i = b_i$, $p\mathbb{N}_{pc}(E_i) = \emptyset$ et $m = 0$.
3) La suite arithmétique de k termes formée uniquement de nombres premiers peut ne pas commencer par le premier terme de $E_i = \{ax + b_i\}$. Mais, une translation la ramènerait au cas susmentionné (nouvel énoncé).

e) Exemples

- $a = 6 \Rightarrow \mathbb{N}_6 = \left\{\dot{5}, \dot{7}\right\} : E = \{E_1, E_2\}\ et\ G = \{E_1E_1, E_1E_2, E_2E_2\}$; avec $E_1 = \{6x + 5\}$ et $E_2 = \{6x + 7\}$. $E_1E_1 \sqsubset E_2$, $E_1E_2 \sqsubset E_1$ et $E_2E_2 \sqsubset E_2 : \dot{E}_1 = \{E_1E_2\}$ et $\dot{E}_2 = \{E_1E_1, E_2E_2\}$.

  ❖ $\mathbb{N}_{pc}(E_1) = E_1 \setminus \dot{E}_1 = E_1 \setminus \{E_1E_2\}$ et $\mathbb{N}_{pc}(E_2) = E_2 \setminus \dot{E}_2 = E_2 \setminus \{E_1E_1, E_2E_2\}$

  $= E_2 \setminus (E_1E_1 \cup E_2E_2)$.

  ❖ $n_6 = \min\limits_{1\leq i\leq \varphi(6)}\{b_i\} = \min\limits_{1\leq i\leq 2}\{b_i\} = \min\{5,7\} = 5$ et $ETR(6) \sqsubset \mathbb{N} \setminus \{0,1, \dots ,4\}$.

  ❖ $5 \in \mathbb{N}_p$ et $7 \in \mathbb{N}_p \Longrightarrow m_1 = \min\{35\} = 35 : p\mathbb{N}_{pc}(E_1) = \{5,11,17,23,29\}$ et $m = 5$.

  Aussi, $m_2 = \min\{25,49\} = 25 : p\mathbb{N}_{pc}(E_2) = \{7,13,19\}$ et $m = 3$.

- Pour $a = 5$, $E_3 = \{5x + 4\}$ possède le même nombre des nombres entiers naturels premiers que $E_3' = \{5x + 19\}$. Même chose pour $E_4 = \{5x + 6\}$ et $E_4' = \{5x + 11\}$.

3.3.3.4 EXPLICITATION

Soit $E_i = \{az + b_i\}$; avec $z \in \mathbb{N}$ et $ddc(a, b_i) = 1$.

Posons $E_l = \{ax + b_l\}$ et $E_k = \{ay + b_k\}$ pour avoir $E_l E_k = a^2xy + ab_k x + ab_l y + b_l b_k$

$= a(axy + b_k x + b_l y + c_{lk}) + b_i$; avec c_{lk} et b_i respectivement le quotient et le reste de la division euclidienne de $b_l b_k$ par a.

Le nombre de ces produits est fini: il existe $m \in \mathbb{N}$ $(1 \leq m \leq \varphi(a))$ tel que

$\dot{E}_\iota = \bigcup_{l,k}(E_l E_k)$; $1 \leq l \leq k \leq m$.

Posons $H_{lk} = \{axy + b_k x + b_l y + c_{lk}\}$ et $H(a, i) = \bigcup \{H_{lk};\ 1 \leq l \leq k \leq m\}$.

Proposition 2

$\mathbb{N}_{pc}(E_i) = \{az + b_i\}, z \in \mathbb{N} \setminus H(a, i)$.

$= (a\mathbb{N} + b_i) \setminus [aH(a, i) + b_i]$.

Corollaire

$\mathbb{N}_{pc}(E_i)$ est infini (respectivement fini) si et seulement si $\mathbb{N} \setminus H(a, i)$ est infini (respectivement fini).

Remarque

Concrètement, les ensembles H_{lk} $(1 \leq l \leq k \leq m)$ sont:

$H_{11} = \{axy + b_1 x + b_1 y + c_{11}\}$, $H_{12} = \{axy + b_2 x + b_1 y + c_{12}\}$,...,

$H_{1m} = \{axy + b_m x + b_1 y + c_{1m}\}$, $H_{22} = \{axy + b_2 x + b_2 y + c_{22}\}$,...,

$H_{2m} = \{axy + b_m x + b_2 y + c_{2m}\}$,..., $H_{mm} = \{axy + b_m x + b_m y + c_{mm}\}$.

Exemple

$a = 6 \Rightarrow E_1 = \{6x + 5\}$ et $E_2 = \{6x + 7\} : H_{11} = \{6xy + 6x + 6y + 3\}$,

$H_{12} = \{6xy + 7x + 5y + 5\}$ et $H_{22} = \{6xy + 7x + 7y + 7\}$; $H(6,1) = H_{12}$ et

$H(6,2) = H_{11} \cup H_{22}$.

$\mathbb{N}_{pc}(E_1) = \{6z + 5, z \in \mathbb{N} \setminus H(6,1)\} = (6\mathbb{N} + 5) \setminus [6H(6,1) + 5]$.

$\mathbb{N}_{pc}(E_2) = \{6z + 7, z \in \mathbb{N} \setminus H(6,2)\} = (6\mathbb{N} + 7) \setminus [6H(6,2) + 7]$.

Théorème 7 (de DIRICHLET)

L'ensemble $\mathbb{N}_{pc}(E_i)$ est infini.

Démonstration:

Supposons, par l'absurde, que $\mathbb{N}_{pc}(E_i)$ est fini. Alors, d'après le corollaire de la proposition 2, $\mathbb{N} \setminus H(a, i)$ est fini et, d'après le théorème 2,

$\exists q \in \mathbb{N} \,/\, \forall q' \in \mathbb{N}\ et\ q' \geq q, on\ ait\ q' \in H(a, i)$.

Or, $q' \geq q \Leftrightarrow \exists u \in \mathbb{N} \,/\, q' = q + u \Leftrightarrow u = q' - q \in \mathbb{N}$.

Et $q \in H(a, i) \Leftrightarrow \exists x, y \in \mathbb{N} \,/\, q' = axy + b_1 x + b_1 y + c_{11}$ ou... ou

$q' = axy + b_m x + b_m y + c_{mm}$.

Donc $u = axy + b_1 x + b_1 y + c_{11} - q$ ou... ou $u = axy + b_m x + b_m y + c_{mm} - q$.

Par suite, les ensembles $\mathbb{N}_q = \{q \in \mathbb{N} / q' \geq q\}$ et $H(a, i)_q = \{q'' \in H(a, i) / q'' \geq q\}$ vérifient $\mathbb{N}_q = H(a, i)_q$

$= \{q + u, u \in \mathbb{N}\}$.

Soient x_q et y_q des nombres entiers naturels tels que $q = ax_q y_q + b_1 x_q + b_1 y_q + c_{11}$ ou... ou $q = ax_q y_q + b_m x_q + b_m y_q + c_{mm}$. Posons $x = z + x_q$ et $y = v + y_q$. Alors, $\forall u \in \mathbb{N}, u = avz + (ax_q + b_1)v + (ay_q + b_1)z$ ou... ou

$u = avz + (ax_q + b_m)v + (ay_q + b_m)z$; avec $ddc[a, (ax_q + b_l)(ay_q + b_k)] = 1$; ce qui contredit le théorème 6.

D'où la supposition est fausse; l'ensemble $\mathbb{N} \setminus H(a,i)$ est plutôt infini et il en est de même de l'ensemble $\mathbb{N}_{pc}(E_i)$. CQFD

Remarques

- Non seulement la démarche algébrique montre que $\mathbb{N}_{pc}(E_i)$ est infini, mais aussi et surtout elle en donne la détermination.
- Dans la suite et pour a fixé dans $\mathbb{N}^*$, nous définissons les ensembles

$S(a,i,q) = H(a,i) - q.$

3.3.3.5 PHÉNOMÈNE DE BIAIS DE TCHEBYCHEV

a) Problème

Tchebychev ou Tchebyscheff a constaté qu'il semblait exister une prédominance assez sensible des nombres premiers de la forme $4x + 3$ par rapport à ceux de la forme $4x + 5$ (théorème d'oscillation). Ce constat est actuellement étudié sous l'appellation de « Phénomène de Biais de Tchebychev » et formulé de la manière suivante: les nombres premiers de l'une des formes $4x + 3$ et $4x + 5$ sont-ils plus rares que ceux de l'autre forme ? [8]

b) Résolution: Corollaire du théorème fondamental

Le « Phénomène de Biais de Tchebychev » est un corollaire de notre théorème fondamental. Par ailleurs, le constat de Tchebychev n'est plus unique; il se justifie par la définition des ensembles $\mathbb{N}_{pc}(E_i)$:

- Si $Card\ \dot{E}_\iota < Card\ \dot{E}_\jmath$, alors la densité des nombres entiers naturels premiers est plus grande dans $\mathbb{N}_{pc}(E_i)$ que dans $\mathbb{N}_{pc}(E_j)$; $i \neq j$.
- Si $Card\ \dot{E}_\iota = Card\ \dot{E}_\jmath$, alors les ensembles $\mathbb{N}_{pc}(E_i)$ et $\mathbb{N}_{pc}(E_j)$ ont la même densité; $i \neq j$.

En effet, d'après le théorème fondamental, $\mathbb{N}_{pc}(E_i) = E_i \setminus \dot{E}_\iota$ et $\mathbb{N}_{pc}(E_j) = E_j \setminus \dot{E}_\jmath$. Supposons que $Card\ \dot{E}_\iota < Card\ \dot{E}_\jmath$. Alors le nombre de(s) produit(s) E_kE_l contenu(s) dans E_i est inférieur à celui de(s) produit(s) E_kE_l contenu(s) dans E_j. Les ensembles E_i et E_j étant de même nature et, les produits E_kE_l, de même nature dans $\mathbb{N}$, les éléments de $\mathbb{N}_{pc}(E_j)$ sont plus rares que ceux de $\mathbb{N}_{pc}(E_i)$: E_j renferme plus de nombres entiers naturels composés que E_i. Par ailleurs, si $Card\ \dot{E}_\iota = Card\ \dot{E}_\jmath$, alors les ensembles E_i et E_j renferment le même nombre des nombres entiers naturels composés.

c) Exemples

- $a = 4 \Rightarrow E_1 = \{4x + 3\}$ et $E_2 = \{4x + 5\}$. $\mathbb{N}_{pc}(E_1) = E_1 \setminus \dot{E}_1 = E_1 \setminus \{E_1E_2\}$

  $= E_1 \setminus (E_1E_2)$ et $\mathbb{N}_{pc}(E_2) = E_2 \setminus \dot{E}_2 = E_2 \setminus \{E_1E_1, E_2E_2\} = E_2 \setminus [(E_1E_1) \cup (E_2E_2)]$:

  $\dot{E}_1$ comprend un seul produit tandis que $\dot{E}_2$ comprend deux produits et la répartition des éléments de E_1 est plus dense que celle des éléments de E_2.

- On observe la même chose pour $a = 6$: $E_1 = \{6x + 5\}$ et $E_2 = \{6x + 7\}$.

  $\mathbb{N}_{pc}(E_1) = E_1 \setminus \dot{E}_1 = E_1 \setminus \{E_1E_2\} = E_1 \setminus (E_1E_2)$ et $\mathbb{N}_{pc}(E_2) = E_2 \setminus \dot{E}_2$

  $= E_2 \setminus \{E_1E_1, E_2E_2\} = E_2 \setminus [(E_1E_1) \cup (E_2E_2)]$: $\dot{E}_1$ comprend un seul produit tandis que $\dot{E}_2$ comprend deux produits, de sorte que la répartition des éléments de E_1 soit plus dense que celle des éléments de E_2.

- $a = 5 \Rightarrow E_1 = \{5x + 2\}$, $E_2 = \{5x + 3\}$, $E_3 = \{5x + 4\}$ et $E_4 = \{5x + 6\}$.

  $\mathbb{N}_{pc}(E_1) = E_1 \setminus \{E_1E_4, E_2E_3\} = E_2 \setminus [(E_1E_4) \cup (E_2E_3)]$, $\mathbb{N}_{pc}(E_2) = E_2 \setminus \{E_1E_3, E_2E_4\}$

  $= E_2 \setminus [(E_1E_3) \cup (E_2E_4)]$, $\mathbb{N}_{pc}(E_3) = E_3 \setminus \{E_1E_1, E_2E_2, E_3E_4\}$

  $= E_3 \setminus [(E_1E_1) \cup (E_2E_2) \cup (E_3E_4)]$ et $\mathbb{N}_{pc}(E_4) = E_4 \setminus \{E_1E_2, E_3E_3, E_4E_4\}$

  $= E_4 \setminus [(E_1E_2) \cup (E_3E_3) \cup (E_4E_4)]$.

Ainsi, les nombres premiers de la forme $5x + 2$ et de la forme $5x + 3$ se répartissent de la même manière. Aussi, les nombres premiers de la forme $5x + 4$ et de la forme $5x + 6$ se répartissent de la même manière. Par contre, il existe une prédominance assez sensible des nombres premiers de la forme $5x + 2$ et de la forme $5x + 3$ par rapport à ceux de la forme $5x + 4$ et de la forme $5x + 6$.

d) Remarque

Lorsque le nombre a est fixé dans $\mathbb{N}^*$, la répartition des nombres entiers naturels premiers est plus dense dans certaines des $\varphi(a)$ progressions arithmétiques que dans d'autres. Deux progressions arithmétiques ont la même densité si leurs mêmes nombres de termes possèdent presque les mêmes nombres des nombres entiers naturels premiers; i.e. pour une infinité des mêmes nombres de termes, elles ont les mêmes nombres des nombres entiers naturels premiers. Nous n'abordons pas l'étude globale de la raréfaction des nombres premiers. Une synthèse assez suffisante existe ([3], pp. 197-230), ainsi qu'une récente estimation du rapport $\varphi(a)/a$ ([9], pp. 6-8).

3.3.3.6 CAS PARTICULIERS: THÉORÈME D'EUCLIDE

a) Ensemble des nombres entiers naturels premiers

En particulier si $a = 1$, alors $E_1 = \{x + 2\}$ et $G = E_1E_1$. Dans ce cas, $\mathbb{N}_{pc}(E_1) = E_1 \setminus G = \mathbb{N}_p$ est l'ensemble des nombres entiers naturels premiers (1 n'est pas pris en considération).

Or, $G = \{(x + 2)(y + 2), x, y \in \mathbb{N}\} = \{(xy + 2x + 2y + 2) + 2\} = S(1, 1, 0) + 2.$

Donc $\mathbb{N}_p = \{z + 2;\ z \in \mathbb{N}\setminus S(1, 1, 0)\} = (\mathbb{N} + 2) \setminus [S(1, 1, 0) + 2]$

Euclide a établi arithmétiquement que l'ensemble $\mathbb{N}_p$ est infini. La démonstration algébrique en est automatiquement un cas particulier du théorème de Dirichlet.

b) Ensemble des nombres entiers naturels impairs premiers

En particulier si $a = 2$, alors $E_1 = \{2x + 3\}$ et $G = E_1E_1$. Dans ce cas

$\mathbb{N}_{pc}(E_1) = E_1 \setminus G = I_p$ est l'ensemble des nombres entiers naturels impairs premiers.

Or, $G = \{(2x + 3)(2y + 3), x, y \in \mathbb{N}\} = \{2(2xy + 3x + 3y + 3) + 3\}$

$= 2S(2, 1, 0) + 3.$

Donc $I_p = \{2z + 3;\ z \in \mathbb{N}\setminus S(2, 1, 0)\} = (2\mathbb{N} + 3) \setminus [2S(2, 1, 0) + 3].$

Par suite, l'ensemble I_p est infini (cas particulier du théorème d'Euclide). La démonstration algébrique en est automatiquement un cas particulier du théorème de Dirichlet.

3.3.4 APPLICATIONS

3.3.4.1 CONJECTURE DES NOMBRES PREMIERS JUMEAUX

Soit P_2 l'ensemble des paires des nombres entiers naturels premiers dont l'écart est deux. Il n'est pas encore établi que P_2 est infini. Nous nous proposons de l'établir.

La démonstration découle de la définition de l'ensemble I_p: 2n + 3 et 2n + 5 sont premiers

$\Leftrightarrow \forall x, y \in \mathbb{N}, n \neq 2xy + 3x + 3y + 3$ et $n \neq 2xy + 3x + 3y + 2.$

$\Leftrightarrow n \in [\mathbb{N}\setminus S(2, 1, 0)] \cap [\mathbb{N}\setminus S(2, 1, 1)] = \mathbb{N} \setminus [S(2, 1, 0) \cup S(2, 1, 1)].$

Ainsi, $P_2 = \{2n + 3, 2n + 5\}\ ;\ n \in \mathbb{N} \setminus [S(2, 1, 0) \cup S(2, 1, 1)].$

Dans ces conditions, l'ensemble P_2 est fini ou infini suivant que l'ensemble

$\mathbb{N} \setminus [S(2, 1, 0) \cup S(2, 1, 1)]$ est fini ou infini.

Théorème 8

L'ensemble P_2 est infini.

Démonstration

Supposons que l'ensemble P_2 est fini. Alors l'ensemble $N[S(2, 1, 0) \cup S(2, 1, 1)]$ est fini et, d'après le théorème 2,

$\exists r \in \mathbb{N} / \forall r' \in \mathbb{N}\ et\ r' \geq r, on\ ait\ r' \in S(2, 1, 0) \cup S(2, 1, 1) = \tau$.

Or, $r' \geq r \iff \exists u \in \mathbb{N} / r' = r + u \iff u = r' - r \in \mathbb{N}$.

Et, $r' \in \tau \Leftrightarrow \exists\, x, y \in \mathbb{N} / r' = 2xy + 3(x + y + 1) ou\, r' = 2xy + 3(x + y) + 2$.

Donc $u = 2xy + 3(x + y + 1) - r$ ou $u = 2xy + 3(x + y) + 2 - r$.

Par suite, les ensembles $\mathbb{N}_r = \{r' \in \mathbb{N} / r' \geq r\}$ et $\tau_r = \{r'' \in \tau / r'' \geq r\}$ vérifient $\mathbb{N}_r = \tau_r = \{r + u, u \in \mathbb{N}\}$.

Soient x_r et y_r des nombres entiers naturels tels que $r = 2x_r y_r + 3x_r + 3y_r + 3$ ou $r = 2x_r y_r + 3x_r + 3y_r + 2$. Posons $x = w + x_r$ et $y = v + y_r$. Alors,

$\forall u \in \mathbb{N}, u = 2(w + x_r)(v + y_r) + 3(w + x_r + v + y_r + 1) - r$ ou

$u = 2(w + x_r)(v + y_r) + 3(w + x_r + v + y_r) + 2 - r$;

i.e. $u = 2wv + (2y_r + 3)w + (2x_r + 3)v$; avec $ddc[2, (2y_r + 3)(2x_r + 3)] = 1$; ce qui contredit le théorème 6 pour a = 2.

D'où la supposition est fausse; l'ensemble $\mathbb{N} \setminus [S(2,1,0) \cup S(2,1,1)]$ est plutôt infini et il en est de même de l'ensemble P_2. CQFD

Corollaire

Si $2n + 3$ et $2n + 5$ sont premiers, alors il existe $z \in \mathbb{N}$ tel que $n = 3z + 1$ ou $n = 0$.

Démonstration

$2n + 3$ et $2n + 5$ sont premiers $\Rightarrow n \in \mathbb{N} \setminus [S(2,1,0) \cup S(2,1,1)] \Rightarrow n \in \mathbb{N}$ et

$n \notin S(2,1,0) \cup S(2,1,1)$.

Or, $S(2,1,0) \cup S(2,1,1) = \{2xy + 3(x + y + 1)\} \cup \{2xy + 3(x + y) + 2\}$

Donc $(3\mathbb{N} + 3) \cup (3\mathbb{N} + 2) \subset S(2,1,0) \cup S(2,1,1)$ (cas particuliers pour x = 0).

Par suite, $n \notin (3\mathbb{N} + 3) \cup (3\mathbb{N} + 2)$.

Un entier naturel qui n'est ni de la forme $3z + 3$ ni de la forme $3z + 2$, est de la forme

$3z + 1$ ou est nul (par définition de $\mathbb{N}_3$).

3.3.4.2 SUR LA CONJECTURE DE POLIGNAC

Soit P_{2j} l'ensemble des paires des entiers naturels premiers dont l'écart est $2j$ ($j \in \mathbb{N}^*$). Polignac ([3], p. 248) conjecture que P_{2j} est infini.

Nous venons de démontrer le cas où j = 1 (conjecture des nombres premiers jumeaux). Un raisonnement analogue permet d'écrire l'ensemble P_{2j} sous forme d'une réunion d'ensembles: il suffit de connaître les $\varphi(2j)$ premières paires; avec φ l'indicateur d'Euler. Il s'ensuit que la démonstration, que l'ensemble P_{2j} est infini, dépend de ses $\varphi(2j)$ premières paires; ce qui exige que j soit préalablement fixé: à chaque valeur de j correspond une démonstration. Néanmoins, les ensembles P_{2j} se notant sous la même forme, toutes ces démonstrations se ressemblent.

❖ **Ensembles** $P_{2j}; j \in \mathbb{N}^*$

- $j = 2 \Longrightarrow 2j = 4, \varphi(4) = 2\ et\ P_4 = P_4^1 \cup P_4^2$; avec

  $P_4^1 = \{4n + 7, 4n + 11\}; n \in S(4,1,1) \cap \{\mathbb{N} \setminus [S(4,2,1] \cup S(4,2,2)\}$.

  $P_4^2 = \{4n + 13, 4n + 17\}; n \in S(4,2,3) \cap \{\mathbb{N} \setminus [S(4,1,2] \cup S(4,1,3)\}$.
- $j = 3 \Longrightarrow 2j = 6, \varphi(6) = 2\ et\ P_6 = P_6^1 \cup P_6^2$; avec

  $P_6^1 = \{6n + 23, 6n + 29\}; n \in S(6,1,3) \cap \{\mathbb{N} \setminus [S(6,2,3] \cup S(6,2,4)\}$.

  $P_6^2 = \{6n + 31, 6n + 37\}; n \in S(6,2,5) \cap \{\mathbb{N} \setminus [S(6,1,4] \cup S(6,1,5)\}$.
- $j = 4 \Longrightarrow 2j = 8, \varphi(8) = 4\ et\ P_8 = P_8^1 \cup P_8^2 \cup P_8^3 \cup P_8^4$; avec

  $P_8^1 = \{8n + 89, 8n + 97\}$;

$n \in S(8,2,11) \cap S(8,3,11) \cap S(8,4,11) \cap \{\mathbb{N} \setminus [S(8,1,10] \cup S(8,1,11)\}$.

$P_8^2 = \{8n + 359, 8n + 367\}$;

$n \in S(8,1,44) \cap S(8,2,45) \cap S(8,3,45) \cap \{\mathbb{N} \setminus [S(8,4,44] \cup S(8,4,45)\}$.

$P_8^3 = \{8n + 389, 8n + 397\}$;

$n \in S(8,4,48) \cap S(8,1,48) \cap S(8,2,49) \cap \{\mathbb{N} \setminus [S(8,3,48] \cup S(8,3,49)\}$.

$P_8^2 = \{8n + 491, 8n + 499\}$;

$n \in S(8,3,61) \cap S(8,4,61) \cap S(8,1,61) \cap \{\mathbb{N} \setminus [S(8,2,61] \cup S(8,2,62)\}$;

…

❖ **Conséquence**

La conjecture de Polignac devient: « S'il existe au moins une paire des éléments de l'ensemble P_{2j} pour j fixé dans $\mathbb{N}^*$, alors l'ensemble P_{2j} est infini ».

❖ **Lemme**

Soient A et B deux parties infinies de $\mathbb{N}$ telles que $A \cap B \neq \emptyset$.

- $A \cap B \; est \; fini \Leftrightarrow \exists \, q \in \mathbb{N} \, / \, \forall q' \in N \; et \; q' \geq q, on \; ait \; q' \notin A \; ou \; q' \notin B.$
- $A \cap B \; est \; infini \Leftrightarrow \forall q \in \mathbb{N}, \exists q' \in \mathbb{N} \; et \; q' \geq q \, / \, q' \in A \; et \; q' \in B.$

Démonstration

Soient A et B deux parties infinies de $\mathbb{N}$. Alors $A \cap B$ est aussi une partie de $\mathbb{N}$.

Or, $A \cap B \neq \emptyset$. Donc, d'après le théorème 1, $A \cap B$ est fini si et seulement si $A \cap B$ est majoré. Aussi, $A \cap B$ est infini si et seulement si $A \cap B$ n'est pas majoré. En remplaçant « fini » par « majoré », « infini » par « n'est pas majoré » et en se servant de la définition de $A \cap B$, on trouve le lemme.

❖ **Démonstration pour j = 2**

Pour démontrer que l'ensemble P_4 est infini, il suffit de démontrer que l'un des ensembles P_4^i est infini. Faisons – le pour $i = 2$.

$S(4,2,3) = H(4,2) - 3 = \{4xy + 3x + 5y\}$.

$S(4,1,2) = H(4,1) - 2 = \{4xy + 5x + 5y + 3, 4xy + 3x + 3y - 1\}$.

$S(4,1,3) = H(4,1) - 3 = \{4xy + 5x + 5y + 2, 4xy + 3x + 3y - 2\}$.

Supposons que P_4^2 est fini. Alors, d'après le lemme,

$\exists q \in \mathbb{N} \, / \, \forall q' \in \mathbb{N} \; et \; q' \geq q, on \; ait \; q' \notin S(4,2,3) \; ou \; q' \notin \mathbb{N} \setminus [S(4,1,2) \cup S(4,1,3)]$. Faisons la disjonction des cas.

1) Supposons que $q' \in S(4,2,3)$ et $q' \notin \mathbb{N} \setminus [S(4,1,2) \cup S(4,1,3)]$. Alors $q' \in S(4,2,3)$ et $q' \in S(4,1,2) \cup S(4,1,3)$; i.e. $q' \in S(4,2,3) \cap S(4,1,2)$ ou $q' \in S(4,2,3) \cap S(4,1,3)$.

Ainsi $\exists x, y, u, v \in \mathbb{N}$ tels que $q' = 4xy + 3x + 5y$ et $q' = 4uv + 5u + 5v + 3$

ou $q' = 4xy + 3x + 5y$ et $q' = 4uv + 3u + 3v - 1$

ou $q' = 4xy + 3x + 5y$ et $q' = 4uv + 5u + 5v + 2$

ou $q' = 4xy + 3x + 5y$ et $q' = 4uv + 5u + 5v - 2$

Or, $q' \geq q$. Donc $\exists t \in \mathbb{N} \, / \, q' = q + t \; ; \; i.e. \; t = q' - q$

Soient $x_q, y_q, u_q, v_q \in \mathbb{N} / q = 4x_q y_q + 3x_q + 5y_q \; et \; q = 4u_q v_q + 5u_q + 5v_q + 3$

ou $q = 4x_q y_q + 3x_q + 5y_q \; et \; q = 4u_q v_q + 3u_q + 3v_q - 1$

ou $q = 4x_q y_q + 3x_q + 5y_q \; et \; q = 4u_q v_q + 5u_q + 5v_q + 2$

ou $q = 4x_q y_q + 3x_q + 5y_q \; et \; q = 4u_q v_q + 3u_q + 3v_q - 2$

Posons $x = X + x_q, y = Y + y_q, u = U + u_q$ *et* $v = V + v_q$ pour avoir $t = 4(x_qY + YX + Xy_q) + 3X + 5Y$ et $t = 4(u_qV + VU + Uv_q) + 5U + 5V$

ou $t = 4(x_qY + YX + Xy_q) + 3X + 5Y$ et $t = 4(u_qV + VU + Uv_q) + 3U + 3V$; i.e. $t = 4XY + (4x_q + 5)Y + (4y_q + 3)X$ et $t = 4UV + (4u_q + 5)V + (4v_q + 5)U$

ou $t = 4XY + (4x_q + 5)Y + (4y_q + 3)X$ et $t = 4UV + (4u_q + 3)V + (4v_q + 3)U$

ce qui contredit le théorème 6 (pour a = 4).

2) Supposons que $q' \notin S(4,2,3)$ *et* $q' \in \mathbb{N} \setminus [S(4,1,2) \cup S(4,1,3)]$. Alors

$q' \in \mathbb{N} \setminus S(4,2,3)$ *et* $q' \in \mathbb{N} \setminus [S(4,1,2) \cup S(4,1,3)]$; i.e.

$q' \in \mathbb{N} \setminus [S(4,2,3) \cup S(4,1,2) \cup S(4,1,3)]$; i.e. $q' \notin S(4,2,3) \cup S(4,1,2) \cup S(4,1,3)$.

Ainsi, $\forall x, y \in \mathbb{N}, q' \neq 4xy + 3x + 5y$ et $q' \neq 4xy + 5x + 5y + 3$ et

$q' \neq 4xy + 3x + 3y - 1$ et $q' \neq 4xy + 5x + 5y + 2$ et $q' \neq 4xy + 3x + 3y - 2$.

En appliquant le même raisonnement de la dernière partie de 1), on en déduit que $t \neq 4(x_qY + YX + Xy_q) + 3X + 5Y$ et $t \neq 4(x_qY + YX + Xy_q) + 5X + 5Y$ et $t \neq 4(x_qY + YX + Xy_q) + 3X + 3Y$; ce qui traduit, en particulier, que t ≠ 0 et contredit le fait que la propriété est vraie pour tout $q' \geq q$.

3) Supposons que $q' \notin S(4,2,3)$ et $q' \notin \mathbb{N} \setminus [S(4,1,2) \cup S(4,1,3)]$. Alors $q' \notin S(4,2,3)$ et $q' \in S(4,1,2) \cup S(4,1,3)$; i.e. $q' \in [S(4,1,2) \cup S(4,1,3)] \setminus S(4,2,3)$; ce qui contredit le fait que l'ensemble $[S(4,1,2) \cup S(4,1,3)] \cap S(4,2,3)$ est infini.

En effet, 4xy + 3x + 5y = 4uv + 5u + 5v + 3 devient, pour $y = 1$ et $v = 0$,

$7x + 5 = 5u + 3$; i.e. $5u - 7x = 2$; i.e. $u = 7k + 6$ *et* $x = 5k + 4$. Il s'ensuit que

$7x + 5 = 35k + 33 = 5u + 3$ appartient à cette intersection pour tout $k \in \mathbb{N}$.

D'où la supposition est fausse; P_4^2 est plutôt infini.

4 DISCUSSION DES RESULTATS

La formalisation algébrique du crible d'Eratosthène est possible. Elle permet d'isoler, dans l'ensemble $\mathbb{N}$, les nombres premiers pour mieux les étudier, c'est-à-dire d'établir de l'ordre dans l'ensemble $\mathbb{N}_p$ des nombres premiers par le désordre dans l'ensemble N_c des nombres entiers naturels composés. Elle consiste à écrire l'ensemble $\mathbb{N}_p$ comme la partie complémentaire, dans l'ensemble $\mathbb{N} \setminus \{0,1\}$, de l'ensemble $\mathbb{N}_c$: $\mathbb{N}_p = [\mathbb{N} \setminus \{0,1\}] \setminus \mathbb{N}_c$ (1). Par ricochets, elle consiste, plus généralement, à étudier, ensemble, les $\varphi(a)$ progressions arithmétiques et écrire l'ensemble $\mathbb{N}_{pc}(E_i)$ des nombres entiers naturels premiers contenus dans la progression arithmétique $E_i = \{ax + b_i\}$ sous la forme $\mathbb{N}_{pc}(E_i) = E_i \setminus \dot{E}_\iota$; $\dot{E}_\iota$ étant l'ensemble des produits $E_k E_l$ inclus dans E_i (théorème fondamental). Dans ce cas,

$\cup [\mathbb{N}_{pc}(E_i)] = \cup (E_i \setminus \dot{E}_\iota) = (\cup E_i) \setminus (\cup \dot{E}_\iota)$; $1 \leq i \leq \varphi(a)$ (2);
un résultat qui améliore (1) à partir du rang $n_a = \min_{1 \leq i \leq \varphi(a)} \{b_i\}$.

Une telle démarche est trop efficace pour unifier le théorème d'Euclide, le théorème de Dirichlet, le théorème de Green-Tao, la conjecture des nombres premiers jumeaux et le Phénomène de Biais de Tchebychev. D'une part, elle prouve automatiquement la conjecture des nombres premiers jumeaux et en élucide la généralisation (conjecture de Polignac) en les faisant passer de la théorie élémentaire à la théorie algébrique des nombres. D'autre part, elle constitue une nouvelle technique de détermination des nombres premiers, jumeaux ou non. Explicitement, deux résultats obtenus sont éclatants. Primo, le théorème de Green-Tao se démontre et le Phénomène de Biais de Tchebychev se résout, en quelques lignes, comme des corollaires de notre théorème fondamental. Secundo, trois problèmes, classiquement étudiés séparément, deviennent de même nature: la répartition des nombres premiers dans $\mathbb{N} \setminus \{0,1\}$;

La répartition des nombres premiers dans une progression arithmétique $ax + b$ (a et b étrangers) et la répartition des nombres premiers jumeaux dans $\mathbb{N} \setminus \{0,1\}$.

De cette manière, le théorème d'Euclide (pour le premier problème), le théorème de Dirichlet (pour le deuxième problème) et la conjecture des nombres premiers jumeaux (pour le troisième problème) se démontrent de la même manière. Le moyen utilisé est la condition pour qu'une partie non vide de $\mathbb{N}$ et sa partie complémentaire soient finies ou infinies.

La synthèse de l'article est présentée sous forme d'un schéma en annexe.

5 CONCLUSION

Désormais, des problèmes sur les nombres entiers naturels (premiers) peuvent être réétudiés et ramenés chaque fois autour de zéro. Ne serait-ce pas, ici, le fondement logique de la « Descente infinie » de Pierre De Fermat ? D'emblée, l'on ne saurait l'affirmer. Toutefois, en remettant l'étude des nombres entiers naturels à son stade primaire, cette recherche inaugure une nouvelle façon d'aborder des questions sur la primalité dans $\mathbb{N}$.

Un chercheur intéressé pourrait étudier

- Les propriétés de l'application

  $m_a: \mathbb{N}_a \longrightarrow \mathbb{N}: E_i \longrightarrow card\ \dot{E}_i\ (1 \leq i \leq \varphi(a))$

  et démontrer particulièrement que, $\forall a \in \mathbb{N}^*, card\{m_a\ [\ \mathbb{N}_a\ ]\} = \begin{cases} 1, & si\ a \in \{1,2\} \\ 2, & si\ a \in \mathbb{N}^* \setminus \{1,2\} \end{cases}$

  $m_a[\ \mathbb{N}_a]$ étant l'image directe de l'ensemble $\mathbb{N}_a$ par l'application m_a.

- L'ensemble des nombres premiers triplets $(p, p + 2, p + 6)$ ou $(p, p + 4, p + 6)$. Il se servirait, par exemple, de $P_2 \bigcap P_4$; avec P_2 et P_4 les ensembles des nombres premiers respectivement jumeaux (p, p + 2) et cousins (p, p+4).

- L'expression générale de l'ensemble P_{2j} $(j \in \mathbb{N}^*)$ en fonction de ses $\varphi(2j)$ premières paires; ce qui permettrait de généraliser la démonstration du théorème de Polignac. Il se servirait d'un pont entre les ensembles $\mathbb{N}_{pc}(E_i)$ et P_{2j}.

REFERENCES

[1] Yitang Zhang, « Bounded gaps between primes », *Annals of Mathematics,* Princeton University and the Institute for Advanced Study, 2013.

[2] Projet Polymath, Les Mathématiques.net (21.6.2023).

[3] Delahaye, J.P., Merveilleux nombres premiers, voyage au cœur de l'Arithmétique, Paris, Belin Pour la Science, 2000.

[4] Queysanne, M., *Algèbre M.P et Spéciales AA',* 7ème édition revue et augmentée, Paris, Armand Colin, 1964.

[5] François De Marçay, *Arithmétique dans $\mathbb{Z}$ et dans $\mathbb{Z}/n\mathbb{Z}$.*
[Online] Available: https://www.imo.universite-paris-saclay.fr (28 août 2023).

[6] Villemin, G., Nombres premiers – propriétés.
[Online] Available: http://villemin.gerard.fr/wwwgmm/Premier/propriet.htm (17 mai 2023).

[7] Ben J. Green et Terence Tao, « The primes contain arbitrarily long arithmetic progressions », *Annals of Mathematics,* vol. 167, arXiv math.NT/0404188, 481-547, 2008.

[8] Fiorilli, Daniel, Jouve et Florent, Nombres premiers et biais de Tchebychev, 2021.
[Online] Available: https://images.math.cnrs.fr (1er juillet 2023).

[9] Bouw I. I., Ozman E., Johnson-Leung J. et Newton R., *Women in Numbers Europe II. Contributions to number Theory and Arithmetic Geometry,* Vol. 11, Switzerland, Springer, 2018.

ANNEXE: SYNTHESE DE L'ARTICLE