

Résolution et application de l'équation diophantienne $AXY + BX + CY = D$ (A et BC étrangers)

[Resolution and Application of the Diophantine Equation $AXY + BX + CY = D$ (A and BC coprime)]

Mushiwalyahyage Zaluka¹, Déborah Amani Faraja², and Marie-Chantal Niyomanzi Sebutimbiri³

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

²Assistante, Ecole des Mines, Université Officielle de Bukavu (U.O.B), Bukavu, RD Congo

³Assistante, Institut Supérieur des Techniques médicales de Goma (ISTM, GOMA), Goma, RD Congo

Copyright © 2026 ISSR Journals. This is an open access article distributed under the **Creative Commons Attribution License**, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT: This paper deals with the Diophantine equation $axy + bx + cy = d$ (and bc are coprime). It revisits the old methods of solving this equation. It establishes a link between this solution and the characterization of the elements of the arithmetic progression $ax + b$ (and b are coprime). It provides a new method for solving this equation. It leads to two primality criteria and a commutative diagram characterizing odd natural numbers.

KEYWORDS: diophantine equation, coprime numbers, primality, commutative diagram, characterization.

RESUME: Cet article porte sur l'équation diophantienne $axy + bx + cy = d$ (a et bc étrangers). Il en repense les anciennes méthodes de résolution. Il établit un lien entre cette résolution et la caractérisation des éléments de la progression arithmétique $ax + b$ (a et b étrangers). Il en donne une nouvelle méthode de résolution. Il aboutit à deux critères de primalité et un diagramme commutatif de caractérisation des nombres entiers naturels impairs.

MOTS-CLEFS: équation diophantienne, nombres étrangers, primalité, diagramme commutatif, caractérisation.

1 INTRODUCTION

Les équations diophantiennes sont parmi les sujets les plus difficiles des mathématiques: on ne sait en traiter qu'un petit nombre et l'on a d'ailleurs montré que le cas général est indécidable (solution du deuxième problème de D. Hilbert); c'est-à-dire qu'aucune méthode générale algorithmique ne peut traiter toutes les équations diophantiennes ([3], p. 143). Cependant, l'importance en est indubitable. En effet, on peut montrer que des nombreuses questions d'Arithmétique (comme l'hypothèse de Goldbach, celle de Riemann,...) sont équivalentes à la non résolution d'une certaine équation diophantienne ([4], p. 115). Ainsi, autant ces questions sont actuelles, autant les équations diophantiennes le sont.

Parmi les équations diophantiennes les plus étudiées figurent l'équation de la forme $ax + by = c$ (1) et l'équation de la forme $ax^2 + bxy + cy^2 + dx + ey + f = 0$ (2). L'équation de la forme $axy + bx + cy + d = 0$ (3) est un cas particulier de l'équation (2). Ainsi, l'équation (3) n'est certes pas une nouveauté. Néanmoins, cet article relance son étude en établissant sa

relation avec la théorie de nombres; relation qui transparaît dans la formalisation algébrique du crible d'Eratosthène ([5], pp. 144 et 147) et qui oblige de revenir sur sa résolution.

La résolution de l'équation (2) distingue les cas elliptique, hyperbolique et parabolique ([1], p. 517). Selon cette classification, l'équation (3) se retrouve dans le cas hyperbolique et se réduit à l'équation diophantienne $AX^2 + BX + C = AY^2$ (4). Or, la résolution de l'équation (4) est une application de celle de l'équation diophantienne $XY = \alpha$ (5). Donc, par transitivité, l'équation (3) peut être résolue, directement, comme une équation réductible à l'équation (5). Malheureusement, ces deux méthodes (générale et particulière) de résolution de l'équation (3) posent problème: l'on recherche des solutions sans en avoir préalablement testé l'existence. L'application de la résolution de l'équation (4) à celle de l'équation (3), est une tentative d'un tel test. En repensant ces anciennes méthodes de résolution, cet article contribue à l'amélioration dudit test par une nouvelle méthode de résolution de l'équation (3). Une telle amélioration produit deux nouveaux critères de primalité dont les principes, quelques illustrations et explications constituent une partie importante de cet article.

2 MATERIEL ET METHODES

Nous écrivons l'équation (3) sous la forme générale $axy + bx + cy = d$ et, pour sa résolution, nous nous servons de deux outils. Le premier est le fait que l'équation (3) est du deuxième degré. Le second outil est la résolution de l'équation (1), dite équation de Bachet De Meziriac (a et b étrangers). D'une part, nous systématisons la résolution classique de l'équation (3). D'autre part, nous appliquons la résolution de l'équation (1) à celle de l'équation (3). La condition « a et b étrangers », dans l'équation (1), engendre la condition « (a et bc étrangers) » dans l'équation (3). Nous supposons, connue, la résolution des équations (1), (2), (5) ([6], pp. 4-24) et (4) ([1], p. 517).

Quant à l'application de l'équation (3), nous recherchons son importance dans l'arithmétique modulaire et l'appliquons à la caractérisation des nombres entiers naturels sous forme des critères de primalité. Ici, aussi, nous supposons, connus, les critères de primalité antérieurement existants et, sauf indication contraire, les intervalles sont inclus dans l'ensemble $\mathbb{N}$ des nombres entiers naturels.

3 RESULTATS

3.1 METHODES DE RESOLUTION

Nous proposons trois méthodes de résolution:

- L'application du principe de résolution de l'équation $XY = \alpha (\alpha \in \mathbb{Z})$;
- L'application du principe de résolution de l'équation $ax^2 + bx + c = ay^2$
($a \in \mathbb{Z}^*, b, c \in \mathbb{Z}$) ;
- L'application du principe de résolution de l'équation $ax + by = c$ (a et b étrangers).

Dans la première méthode, on recherche les solutions sans en connaître préalablement l'existence. Dans les deuxième et troisième méthodes, on teste l'existence de solutions avant de les déterminer. L'hypothèse (a et bc étrangers) intervient dans la dernière méthode.

3.1.1 ECRIRE L'ÉQUATION SOUS LA FORME

THÉORÈME 1.

$$axy + bx + cy = d \Leftrightarrow (ax + c)(ay + b) = ad + bc.$$

DÉMONSTRATION

$$axy + bx + cy = d \Leftrightarrow a^2xy + abx + acy = ad \text{ (Multiplication par } a)$$

$$\Leftrightarrow a^2xy + abx + acy + bc = ad + bc \text{ (Ajout de } bc \text{ aux deux membres)}$$

$$\Leftrightarrow ay(ax + c) + b(ax + c) = ad + bc \Leftrightarrow (ax + c)(ay + b) = ad + bc \text{ (Factorisation du premier membre).}$$

EXEMPLE

Résoudre, dans $\mathbb{Z} \times \mathbb{Z}$, l'équation $3xy + 2x + 4y = 5$.

SOLUTION

$$\begin{aligned} 3xy + 2x + 4y = 5 &\Leftrightarrow (3x + 4)(3y + 2) = 23 \\ &\Leftrightarrow \begin{cases} 3x + 4 = 23 \\ 3y + 2 = 1 \end{cases} \text{ ou } \begin{cases} 3x + 4 = 1 \\ 3y + 2 = 23 \end{cases} \text{ ou } \begin{cases} 3x + 4 = -23 \\ 3y + 2 = -1 \end{cases} \text{ ou } \begin{cases} 3x + 4 = -1 \\ 3y + 2 = -23 \end{cases} \\ &\Leftrightarrow x = -1 \text{ et } y = 7 \text{ ou } x = -9 \text{ et } y = -1 \\ S &= \{(-1, 7), (-9, -1)\} \end{aligned}$$

REMARQUE 1

Si en particulier $b = c$, alors l'équation $axy + bx + cy = d$ s'écrit sous la forme

$axy + b(x + y) = c$ (les lettres c et d étant muettes) et le principe de résolution reste le même.

- Multiplier l'équation par a : $axy + b(x + y) = c \Leftrightarrow a^2xy + ab(x + y) = ac$
- Ajouter b^2 aux deux membres: $a^2xy + ab(x + y) + b^2 = ac + b^2$
- Réduire à la forme $xy = \alpha$: $(ax + b)(ay + b) = ac + b^2$
- Résoudre.

EXEMPLES

Résoudre, dans $\mathbb{Z} \times \mathbb{Z}$, les équations suivantes

- $-5xy + 3x + 3y = -5 \Leftrightarrow (3 - 5x)(3 - 5y) = 34$.
 $34 = 1.34 = (-1).(-34) = 2.17 = (-2).(-17)$ et $S = \{(1, 4), (4, 1)\}$
- $2xy + x + y = 5 \Leftrightarrow (2x + 1)(2y + 1) = 11$.
 $11 = 1.11 = (-1).(-11)$ et $S = \{(5, 0), (0, 5), (-1, -6), (-6, -1)\}$

3.1.2 ECRIRE L'ÉQUATION $axy + bx + cy = d$ SOUS LA FORME $AX^2 + BX + C = AY^2$

THÉORÈME 2.

L'équation $axy + bx + cy = d$ admet de solution dans $\mathbb{Z} \times \mathbb{Z}$ si et seulement s'il existe $u, k, t \in \mathbb{Z}$ vérifiant simultanément les conditions suivantes:

- (1) $k^2 - u^2 = 4(ad + bc)$
- (2) $(at + b - c)^2 = u^2$
- (3) $(2ax + at + b + c)^2 = k^2$

Dans ces cas, $y = x + t$.

DÉMONSTRATION

Supposons que l'équation $axy + bx + cy = d$ admet une solution (x, y) . Alors $y - x \in \mathbb{Z}$; i.e. il existe $t \in \mathbb{Z}$ tel que $y - x = t$; i.e. $y = x + t$. L'équation devient :

$$\begin{aligned} ax(x + t) + bx + c(x + t) &= d \\ \Rightarrow ax^2 + (at + b + c)x &= d - ct \Rightarrow 4a^2x^2 + 4a(at + b + c)x = 4a(d - ct) \end{aligned}$$

$\Rightarrow (2ax + at + b + c)^2 = 4a(d - ct) + (at + b + c)^2$; ce qui n'est possible que s'il existe $k \in \mathbb{Z}$ tel que $4a(d - ct) + (at + b + c)^2 = k^2$;

i.e. $a^2t^2 + 2a(b - c)t = k^2 - 4ad - (b + c)^2$;

i.e. $(at + b - c)^2 = k^2 - 4ad - (b + c)^2 + (b - c)^2 = k^2 - 4(ad + bc)$; ce qui n'est possible que s'il existe $u \in \mathbb{Z}$ tel que $k^2 - 4(ad + bc) = u^2$; i.e. $k^2 - u^2 = 4(ad + bc)$.

Ainsi $(at + b - c)^2 = u^2$ et $(2ax + at + b + c)^2 = k^2$.

Réciproquement, supposons que les trois conditions sont simultanément remplies. Alors, en substituant (3) et (2) dans (1), on trouve

$$(2ax + at + b + c)^2 - (at + b - c)^2 = 4(ad + bc) \Rightarrow (ax + c)(ax + at + b) = ad + bc$$

$$\Rightarrow ax(x + t) + bx + c(x + t) = d \Rightarrow axy + bx + cy = d; \text{ avec } y = x + t: (x, y) \text{ vérifie l'équation } axy + bx + cy = d.$$

EXEMPLES

Résoudre dans $\mathbb{Z} \times \mathbb{Z}$, les équations suivantes:

a) $3xy + 2x + 4y = 5$

SOLUTION

$$a = 3, b = 2, c = 4 \text{ et } d = 5$$

- $k^2 - u^2 = 92 \Leftrightarrow u = -22 \text{ et } k = -24 \text{ ou } u = 22 \text{ et } k = 24$
- $(3t + 2 - 4)^2 = 22^2 \Leftrightarrow (3t - 24)(3t + 20) = 0 \Leftrightarrow t = 8.$
- $(6x + 3.8 + 2 + 4)^2 = 24^2 \Leftrightarrow (6x + 6)(6x + 54) = 0 \Leftrightarrow x = -1 \text{ ou } x = -9.$

$$x = -1 \Rightarrow y = 7 \text{ et } x = -9 \Rightarrow y = -1$$

$$S = \{(-1, 7), (-9, -1)\}$$

b) $2xy + x + y = 5$

SOLUTION

$$a = 2, b = 1, c = 1, d = 5$$

- $k^2 - u^2 = 44 \Leftrightarrow u = -10 \text{ et } k = -12 \text{ ou } u = 10 \text{ et } k = 12$
- $(2t + 1 - 1)^2 = 10^2 \Leftrightarrow t = 5 \text{ ou } t = -5$

$$1^\circ) t = 5 \Rightarrow (4x + 2.5 + 1 + 1)^2 = 12^2 \Leftrightarrow x = 0 \text{ ou } x = -6.$$

$$x = 0 \Rightarrow y = 5 \text{ et } x = -6 \Rightarrow y = -1.$$

$$2^\circ) t = -5 \Rightarrow (4x - 2.5 + 1 + 1)^2 = 12^2 \Leftrightarrow x = 5 \text{ ou } x = -1.$$

$$x = 5 \Rightarrow y = 0 \text{ et } x = -1 \Rightarrow y = -6.$$

$$S = \{(0, 5), (-6, -1), (5, 0), (-1, -6)\}$$

REMARQUE 2

Bien que multiplié par 4, l'entier $ad + bc$ joue le même rôle dans le théorème 2 que celui qu'il joue dans la première méthode de résolution: la résolution en dépend.

$$\text{Ainsi, } 4(ax + c)(ay + b) = k^2 - u^2$$

3.1.3 ECRIRE L'ÉQUATION $axy + bx + cy = d$ SOUS LA FORME $AX + BY = C$

A) FONDEMENT DE LA RÉOLUTION

La résolution de l'équation $axy + bx + cy = d$ repose sur le résultat suivant.

THÉORÈME 3.

Si la somme S et le produit P , de deux nombres, sont des nombres entiers et $S^2 - 4P$ est un nombre entier carré parfait, alors ces deux nombres sont aussi des nombres entiers.

DÉMONSTRATION

Soient S , P et t trois nombres entiers tels que $S^2 - 4P = t^2$.

$4P$ est pair $\Rightarrow S^2 - 4P$ et t sont de même parité que S . S et t de même parité $\Rightarrow S \pm t$ est pair $\Rightarrow x, y \in \mathbb{Z}$; avec $2x = S \pm t$ et $2y = S \mp t$.

B) RÉOLUTION

$$axy + bx + cy = d \quad (3)$$

$$\Leftrightarrow bc(axy + bx + cy) = bcd \Leftrightarrow a(bx)(cy) + bc(bx + cy) = bcd$$

Posons $S = bx + cy$ et $P = bx \cdot cy$ pour avoir $aP + bcS = bcd$ (3')

(3') est une équation linéaire du premier degré à deux inconnues S et P dont le principe de résolution est le même que celui de l'équation $ax + by = c$, auquel il faut ajouter les conditions d'existence des solutions. L'équation (3') s'appellera **équation résolvante**.

$$S, P \in \mathbb{Z} \text{ et } \Delta = S^2 - 4P, \text{ de sorte que } \exists t \in \mathbb{N} / \Delta = t^2 \Rightarrow 2bx = S \pm t \text{ et } 2cy = S \mp t \quad (6)$$

PROPOSITION 1. EXISTENCE DES SOLUTIONS DE L'ÉQUATION (3)

L'équation (3) est résoluble dans $\mathbb{Z} \times \mathbb{Z}$ si et seulement si les conditions suivantes sont simultanément remplies:

(i) $\exists t \in \mathbb{N} / S^2 - 4P = t^2$ (est un carré parfait)

(ii) $S \pm t \in 2b\mathbb{Z}$ et $S \mp t \in 2c\mathbb{Z}$

Il s'ensuit que pour résoudre l'équation (3):

- On résout l'équation (3'): on détermine P et S dépendamment d'un paramètre entier k (P et S existent, car a et bc sont étrangers);
- On calcule $\Delta = S^2 - 4P$;
- On détermine les valeurs de k pour lesquelles Δ vérifie (i) ;
- On choisit, parmi les valeurs de k , celles qui vérifient (ii) ;
- On détermine x et y pour les relations (6).

PROPOSITION 2

Soit (S_1, P_1) une solution particulière de l'équation (3'). $\Delta = S^2 - 4P$ est un carré parfait si et seulement si il existe $(k, t) \in \mathbb{Z} \times \mathbb{Z}$ tel que

$$(a^2k - at + aS_1 + 2bc)(a^2k + at + aS_1 + 2bc) = 4(abcS_1 + b^2c^2 + a^2P_1) \quad (7)$$

DÉMONSTRATION

Soit (S_1, P_1) une solution particulière de l'équation (3'). Alors sa solution générale est $(S_1 + ak, P_1 - bc k)$. Ainsi,

$$\Delta = S^2 - 4P = (S_1 + ak)^2 - 4(P_1 - bc k) = a^2 k^2 + 2(aS_1 + 2bc)k + S_1^2 - 4P_1$$

Il est un carré parfait si et seulement si il existe $t \in \mathbb{Z}$ tel que

$$a^2 k^2 + 2(aS_1 + 2bc)k + S_1^2 - 4P_1 = t^2 \quad (8)$$

L'équation (8) est un cas particulier des équations de la forme $ax^2 + bx + c = ay^2$ que nous savons résoudre: on la multiplie par a^2 , on ajoute $(aS_1 + 2bc)^2$ aux deux membres et on trouve la relation (7).

REMARQUE 3

Si dans la démonstration $S = S_1 - ak$ et $P = P_1 + bck$ (selon les remarques 2), alors la relation (7) s'écrit

$$(a^2 k - at - aS_1 - 2bc)(a^2 k + at - aS_1 - 2bc) = 4(abc S_1 + b^2 c^2 + a^2 P_1) \quad (7')$$

COROLLAIRE

L'ensemble des solutions de l'équation (3) est fini.

Evident: l'ensemble des solutions de l'équation (7) ou (7') est fini.

EXEMPLES

Résoudre, dans $\mathbb{Z} \times \mathbb{Z}$, les équations suivantes:

1°) $3xy + 2x + 4y = 5$: $a = 3$ et $bc = 8$

- Equation résolvante: $3P + 8S = 40$
- Solution particulière: $P_1 = 0$ et $S_1 = 5$
- Solution générale: $P = 8k$ et $S = 5 - 3k$
- $\Delta = t^2 \Leftrightarrow (9k - 3t - 31)(9k + 3t - 31) = 736$.

$$736 = 1.736 = (-1)(-736) = 2.368 = (-2)(-368) = 4.184 = (-4)(-184) \\ = 8.92 = (-8)(-92) = 16.46 = (-16)(-46) = 32.23 = (-32)(-23).$$

Après calculs tous faits, on trouve

$$(k, t) \in \{(24, 61), (24, -61), (-7, 30), (-7, -30), (9, 14), (9, -14), (0, 5), (0, -5)\}.$$

$$(s, t) \in \{(-67, 61), (-67, -61), (26, 30), (26, -30), (-22, 14), (-22, -14), (5, 5), (5, -5)\}.$$

$$(s + t, s - t) \in \{(-6, -128), (-128, -6), (-4, 56), (56, -4), (-8, -36), (-36, -8), (0, 10), (10, 0)\}.$$

$$2b\mathbb{Z} = 4\mathbb{Z} \text{ et } 2c\mathbb{Z} = 8\mathbb{Z}$$

$$x = -1 \text{ et } y = 7 \text{ ou } x = -9 \text{ et } y = -1 : S = \{(-1, 7), (-9, -1)\}$$

2°) $4xy + x + 3y = 10$: $a = 4$, $bc = 3$

- Equation résolvante: $4P + 3S = 30$
- Solution particulière: $P_1 = 3$ et $S_1 = 6$
- Solution générale: $P = 3 - 3k$ et $S = 6 + 4k$
- $\Delta = t^2$
 $\Leftrightarrow (16k - 4t + 30)(16k + 4t + 30) = 520 \Leftrightarrow (8k - 2t + 15)(8k + 2t + 15) = 130$.
 $130 = 1.130 = (-1)(-130) = 2.65 = (-2)(-65) = 5.26 = (-5)(-26) = 10.13 = (-10)(-13)$.

Les facteurs étant, chaque fois, des parités différentes, k ou t n'existe pas dans $\mathbb{Z}$.

$$S = \emptyset.$$

C) CAS PARTICULIER

Si en particulier $b = c$, alors l'équation (5) peut s'écrire sous la forme

$$axy + b(x + y) = c \quad (9)$$

Dans ce cas, la proposition 1 contient uniquement la première condition et le principe de résolution manque l'avant-dernière étape.

Les relations (6) deviennent $2x = S \pm t$ et $2y = S \mp t$ (6')

Et la condition (7) devient

$$(a^2k - at + as_1 + 2b)(a^2k + at + as_1 + 2b) = 4(abs_1 + b^2 + a^2P_1) \quad (10)$$

EXEMPLES

Résoudre, dans $\mathbb{Z} \times \mathbb{Z}$, les équations suivantes:

1°) $2xy + x + y = 5: a = 2, b = 1$

- Equation résolvante: $2P + S = 5$
- Solution particulière: $P_1 = 0$ et $S_1 = 5$
- Solution générale: $P = -k$ et $S = 5 + 2k$
- $\Delta = t^2 \Leftrightarrow (4k - 2t + 12)(4k + 2t + 12) = 44 : S = \{(5,0), (0,5), (-1, -6), (-6, -1)\}$

2°) $5xy + 3(x + y) = -5 : a = 5, b = 3$

- Equation résolvante: $5P + 3S = -5$
- Solution particulière: $P_1 = -1$ et $S_1 = 0$
- Solution générale: $P = -1 - 3k$ et $S = 5k$
- $\Delta = t^2 \Leftrightarrow (25k - 5t + 6)(25k + 5t + 6) = -64 : S = \{(1, -1), (-1, 1)\}$

D) RÉOLUTION DANS $\mathbb{N} \times \mathbb{N}$

Le principe de résolution de l'équation (5) ou (9) dans $\mathbb{N} \times \mathbb{N}$ est le même que celui dans $\mathbb{Z} \times \mathbb{Z}$ auquel il faut adjoindre la condition pour que $(x, y) \in \mathbb{N} \times \mathbb{N} : P \geq 0$ et

$$S \geq 0 \quad (11)$$

EXEMPLES.

1°) $3xy + 2x + 4y = 5: P = 8k$ et $S = 5 - 3k$.

$$P \geq 0 \text{ et } S \geq 0 \Leftrightarrow 8k \geq 0 \text{ et } 5 - 3k \geq 0 \Leftrightarrow k = 0 \text{ ou } k = 1$$

- $k = 0 \Rightarrow \Delta$ carré parfait, mais x et y n'existent pas
- $k = 1 \Rightarrow \Delta$ non carré parfait.

$$S = \emptyset$$

2°) $2xy + x + y = 5 : P = k$ et $S = 5 - 2k$.

$$P \geq 0 \text{ et } S \geq 0 \Leftrightarrow k \geq 0 \text{ et } 5 - 2k \geq 0 \Leftrightarrow k \in \{0, 1, 2\}.$$

$$\text{La seule valeur admissible est } k = 0: S = \{(5,0), (0,5)\}$$

3.2 IMPORTANCE DE L'EQUATION $axy + bx + cy = d$ (a et bc étrangers)

3.2.1 PROGRESSION ARITHMÉTIQUE ET CONGRUENCE MODULO a

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

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

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 $1, 2, \dots, a - 1$.

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

PROPOSITION 3

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

(1) $\text{Card } \mathcal{H}_a = \varphi(a)$; avec φ l'indicateur d'EULER.

(2) $(\mathcal{H}_a, \otimes)$ est un groupe commutatif

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

3.2.2 RESTRICTION À L'ENSEMBLE $\mathbb{N}$

Exploitions la multiplication des classes dans $\mathcal{H}_a$ en la particulierisant à l'ensemble

$\mathbb{N}_a = \{\dot{z} \in \mathbb{N} / \dot{z} \in \mathcal{H}_a\}$. Pour des raisons pratiques, remplaçons la classe de 1 par la classe de $a + 1$ (ces deux classes étant égales).

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

Il est évident que $E_i = \dot{b}_i$ ($1 < b_i \leq a + 1$), $E = \mathbb{N}_a$ et $\text{card } G = \frac{\varphi(a)[1+\varphi(a)]}{2}$ ([5], p. 143).

Exemples

- $a = 5 \Rightarrow E_1 = \{5x + 2\} = \dot{2}$, $E_2 = \{5x + 3\} = \dot{3}$, $E_3 = \{5x + 4\} = \dot{4}$ 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 $G = \{E_1 E_1, E_1 E_2, E_1 E_3, E_1 E_4, E_2 E_2, E_2 E_3, E_2 E_4, E_3 E_3, E_3 E_4, E_4 E_4\}$.
- $a = 6 \Rightarrow E_1 = \{6x + 5\} = \dot{5}$ et $E_2 = \{6x + 7\} = \dot{7} : \mathbb{N}_6 = \{\dot{5}, \dot{7}\} = \{E_1, E_2\} = E$ et $G = \{E_1 E_1, E_1 E_2, E_2 E_2\}$.
- $a = 2 \Rightarrow E_1 = \{2x + 3\} = \dot{3} : \mathbb{N}_2 = \{\dot{3}\} = E$ et $G = \{E_1 E_1\}$.

3.2.3 EQUATION $axy+bx+cy=d$ (a et bc étrangers)

Si on explicite G , on trouve que ses éléments sont de la forme:

$$(ax + b_i)(ay + b_j) = a(axy + b_j x + b_i y) + b_i b_j.$$

Or, $p. g. c. d(a, b_i) = 1$, $p. g. c. d(a, b_j) = 1$ et $b_i b_j > a$.

Donc $p. g. c. d(a, b_i b_j) = 1$ et il existe $c_{ij} \in \mathbb{N}$ et $d_k \in \{b_i\}$ tels que $b_i b_j = c_{ij} a + d_k$.

Par suite $(ax + b_i)(ay + b_j) = a(axy + b_j x + b_i y + c_{ij}) + d_k$ ([5], p. 147).

L'étude des conditions, pour qu'un nombre entier naturel appartenant à la progression arithmétique $an + d_k$ soit premier ou composé, conduit à l'étude des équations du type

$$axy + b_j x + b_i y + c_{ij} = n \Leftrightarrow axy + b_j x + b_i y = n - c_{ij}.$$

Ainsi, il ne s'agira plus seulement de résoudre l'équation $axy + bx + cy = d$, mais aussi et surtout d'avoir à l'esprit que la condition « a et bc étrangers » permet d'appliquer sa résolution à la caractérisation des nombres contenus dans une progression arithmétique $ax + b$ (a et b étrangers).

3.3 APPLICATION: CRITÈRES DE PRIMALITÉ

Si en particulier $a = 2$, $b = 3$ et $c = n - 3$, alors l'équation (9) devient

$$2xy + 3(x + y) = n - 3 \quad (9')$$

Or, d'après la première méthode de résolution, on a

$$2xy + 3(x + y) = n - 3 \Leftrightarrow (2x + 3)(2y + 3) = 2n + 3.$$

Donc les conditions d'existence des solutions de l'équation (9') dans $\mathbb{N} \times \mathbb{N}$ sont des critères de primalité:

- L'équation (9') admet de solution si et seulement si $2n + 3$ est composé;
- L'équation (9') n'admet pas de solution si et seulement si $2n + 3$ est premier.

Par suite, nous énonçons deux critères de primalité. Le premier est une application du théorème 2 (deuxième méthode de résolution) et, le second, une application de la proposition 1 et de la relation (11) (troisième méthode de la résolution).

3.3.1 ENONCÉ DES CRITÈRES

PROPOSITION 4

Le naturel $m = 2n + 3$ est composé si et seulement s'il existe $u, k, t, x \in \mathbb{Z}$ vérifiant simultanément les conditions suivantes:

- (1) $k^2 - u^2 = 8n + 12$
- (2) $u^2 = 4t^2$
- (3) $(4x + 2t + 6)^2 = k^2$

DÉMONSTRATION

Il suffit de prendre, dans le théorème 2, $a = 2$, $b = c = 3$ et $d = n - 3$ pour avoir la proposition 4.

COROLLAIRE

Le naturel $m = 2n + 3$ est premier si et seulement si pour tous $u, k, t, x \in \mathbb{Z}$,
 $k^2 - u^2 \neq 8n + 12$ ou $u^2 \neq 4t^2$ ou $(4x + 2t + 6)^2 \neq k^2$.

DÉMONSTRATION

Ce corollaire est la contraposée de la proposition 4.

PROPOSITION 5

Le naturel $m = 2n + 3$ est composé si et seulement s'il existe $k \in \mathbb{N}$ tel que l'on ait simultanément

- (a) $\frac{n}{3} \leq k \leq \frac{n-1}{2}$
- (b) $4k^2 - 4(n+2)k + (n+1)^2$ est un carré parfait

DÉMONSTRATION

Soit le naturel $m = 2n + 3$. Supposons que m est composé. Alors il existe $x, y \in \mathbb{N}$ tels que $2xy + 3(x + y) = n - 3$. En appliquant la condition (11) et la proposition 4 aux entiers $S = n - 1 - 2k$ et $P = 3k - n$, on trouve les conditions (a) et (b).

Réciproquement, supposons qu'il existe $k \in \mathbb{N}$ tel que les conditions (a) et (b) soient simultanément remplies. Alors $n \leq 3k$ et $2k \leq n - 1$ et il existe $t \in \mathbb{N}$ tel que

$$4k^2 - 4(n+2)k + (n+1)^2 = t^2; \text{ i.e. } 0 \leq 3k - n, 0 \leq n - 1 - 2k$$

$$\text{et } (n - 2k - 1)^2 - 4(3k - n) = t^2.$$

Posons $S = n - 2k - 1$ et $P = 3k - n$. Alors $S \in \mathbb{N}$, $P \in \mathbb{N}$ et $S^2 - 4P = t^2$. D'après le théorème 3, il existe $x, y \in \mathbb{N}$ tels que $x + y = S$ et $xy = P$. Dans ce cas, $2x = S \pm t$ et

$$2y = S \mp t; \text{ i.e. } 2x + 3 = S \pm t + 3 \text{ et } 2y + 3 = S \mp t + 3 \text{ de sorte que}$$

$$(2x + 3)(2y + 3) = (S + 3 \pm t)(S + 3 \mp t) = (s + 3)^2 - t^2$$

$$= (n - 2k + 2)^2 - (n - 2k - 1)^2 + 4(3k - n) = 2n + 3;$$

Ce qui traduit que m est composé

COROLLAIRE

Le naturel $m = 2n + 3$ est premier si seulement si pour tout naturel k vérifiant

$$\frac{n}{3} \leq k \leq \frac{n-1}{2}, 4k^2 - 4(n+2)k + (n+1)^2 \text{ n'est pas un carré parfait.}$$

EXEMPLES

a) $m = 1\,001$

- $n = \frac{m-3}{2} = \frac{1001-3}{2} = 499$
- $\frac{n}{3} \leq k \leq \frac{n-1}{2} \Rightarrow \frac{499}{3} \leq k \leq \frac{499-1}{2} \Leftrightarrow 167 \leq k \leq 249$
- $\Delta = 4k^2 - 2\,004k + 250\,000$

Tableau 1. Primalité de 1 001

k	167	...	227	228	229	...	249
Δ	26888	...	1208	1024	848	...	-992

Pour $k = 228$, $\Delta = 1024 = 32^2$. Ainsi, 1001 est un nombre composé

b) $m = 103$

- $n = \frac{m-3}{2} = \frac{103-3}{2} = 50$
- $\frac{50}{3} \leq k \leq \frac{49}{2} \Leftrightarrow 17 \leq k \leq 24$
- $\Delta = 4k^2 - 208k + 2\,601$

Tableau 2. Primalité de 103

k	17	18	19	20	21	22	23	24
Δ	221	153	93	41	-3	-39	-67	-87

Δ n'est un carré parfait pour aucune valeur de k . Ainsi, 103 est premier.

REMARQUES 4

— Pour l'équation $2xy + 3(x + y) = n - 3$, l'existence des solutions l'emporte sur leur détermination. C'est pourquoi l'application des méthodes de résolution est partielle.

- Etant des critères de primalité, les propositions 4 et 5 sont équivalentes.
- Avec la proposition 5, nous obtenons la suite de fonctions f_n définies de l'ensemble I_n vers $\mathbb{N}$ par

$$f_n(k) = 4k^2 - 4(n+2)k + (n+1)^2 ; \text{ avec } n \geq 3 \text{ et } I_n = \left[\frac{n}{3}, \frac{n-1}{2} \right] \quad (12)$$

3.3.2 PROPRIÉTÉS DE

Le cardinal de I_n est égal à la partie entière de $\frac{n+3}{6}$. Il croît avec n ; ce qui pose des problèmes de calcul dans l'application de la proposition 7 (test de primalité). Les propriétés de f_n résolvent légèrement ces problèmes. Elles sont évidentes: elles sont dues au fait que pour tout entier naturel $n \geq 3$, $f_n(k)$ est l'équation d'une « parabole »; courbe dont les caractéristiques analytiques sont bien connues.

PROPRIÉTÉ 1

La fonction f_n est décroissante sur $I_n : \forall n \in \mathbb{N} (n \geq 3), \forall k \in I_n, \left(\frac{n-3}{3}\right)^2 \geq f_n(k) \geq 6 - 2n$.

Cette propriété signifie qu'à la plus petite valeur de k correspond la plus grande valeur de $f_n(k)$ et vice versa.

Dans la suite, nous considérons l'ensemble $T_n = \left[0, \frac{n-3}{3}\right] \quad (13)$

PROPRIÉTÉ 2

$$f_n(k) \geq 0 \Leftrightarrow k \in \left[\frac{n}{3}, \frac{n+2-\sqrt{2n+3}}{2} \right] \quad (13')$$

Cette propriété permet de rejeter toutes les valeurs de k pour lesquelles $f_n(k) < 0$; ce qui réduit le nombre de valeurs à essayer dans l'application du critère. Ainsi, l'ensemble (13) a pratiquement la même importance que l'ensemble (13').

PROPRIÉTÉ 3

Soit $w = \text{card } I_n$. Pour tout $a \in [0, w]$, on a

$$f_n(k \pm a) = f_n(k) + f_{n_k}(a), \text{ où } f_{n_k}(a) = 4a[a \pm 2k \mp (n+2)] \quad (14)$$

Cette propriété signifie que, pour n donné, on n'est pas obligé de reprendre les calculs pour chaque valeur de k . On peut, plutôt, fixer une valeur de référence à laquelle on rattachera toutes les autres valeurs.

EXEMPLE

$$n = 50 \Rightarrow I_{50} = [17, 24]$$

$$f_{50}(17) = f_{50}(20 - 3) = f_{50}(20) + 4.3(3 - 2.20 + 50 + 2) = 41 + 12.15 = 221.$$

$$f_{50}(23) = f_{50}(20 + 3) = f_{50}(20) + 4.3(3 + 2.20 - 50 - 2) = 41 - 108 = -67.$$

PROPRIÉTÉ 4

Soient $n, m \in \mathbb{N}$. Si $n \in I_m$, alors pour tout a vérifiant $n \pm a = m$, on a

$$f_m(k) = f_n(k) + f_{n_a}(k), \text{ où } f_{n_a}(k) = a[a \pm 2(n+1) \mp 4k] \quad (15)$$

Cette propriété signifie que si une valeur de k est commune aux domaines de définition de deux fonctions f_n et f_m , on peut calculer l'image de k par l'une au moyen de l'image de k par l'autre. Elle concerne le test de primalité de plusieurs valeurs au même moment.

Si, de plus, il existe plusieurs valeurs de k dans $I_n \cap I_m$, alors la combinaison de (14) et (15) donne:

$$f_m(k \pm b) = f_n(k \pm b) + f_{n_a}(k - b) \quad (15')$$

EXEMPLE

$$I_{50} = [17, 24] \text{ et } I_{55} = [19, 27]$$

$$f_{55}(20) = f_{50+5}(20) = f_{50}(20) + 5[5 + 2(50 + 1) - 4.20] = 41 + 135 = 176$$

Pour simplifier les calculs dans la pratique du critère, chaque utilisateur peut se servir des propriétés de $f_n(k)$ comme il l'entend. Cependant, en associant les relations 12, 13 et 14, nous proposons que l'on commence par la plus grande valeur de k à laquelle on rattachera toutes les autres valeurs.

PROPRIÉTÉ 5

$$\text{Le symétrique de } I_n \text{ est } I'_n = \left[\frac{n+5}{2}, \frac{2n+6}{3} \right] \quad (16)$$

$$\text{Dans ce cas, } S' = 2k' - n - 5 \text{ et } P' = 2n - 3k' - 6, k' \in I'_n$$

$$\text{Par ailleurs, } \forall k \in I_n, \exists k' \in I'_n / k' = n - k + 2$$

Cette propriété est un résultat qui engendre une proposition équivalente à la proposition 5.

3.3.3 CONDITIONS POUR QUE SOIT UN CARRÉ PARFAIT

Nous voudrions expliciter le critère de primalité. Cette explicitation se présente sous deux formes: une version théorique et une version pratique. La première forme établit une relation entre les naturels k et n . Elle est qualifiée de théorique, car elle n'avance pas encore à grand-chose. La seconde forme donne une relation entre n et $f_n(k)$. Elle découle du critère. Elle est qualifiée de pratique, car elle s'apprête mieux aux applications. Nous avons certes prévenu que les intervalles sont inclus dans l'ensemble $\mathbb{N}$. Néanmoins, comme les deux versions utilisent le quantificateur existentiel, il n'y a pas de contraintes de respecter toute la rigueur des opérations dans l'ensemble $\mathbb{N}$.

THÉORÈME 4: VERSION THÉORIQUE

$$\exists t \in T_n / f_n(k) = t^2 \Leftrightarrow \exists b \in T_{n_k} / n = \frac{2b+3}{b+1}k + b;$$

$$\text{avec } T_{n_k} = \left[\frac{-n-3+\sqrt{n^2-6n+9+36k}}{6}, -1 + \sqrt{k} \right] \quad (17)$$

$$\text{Dans ce cas, } t = \frac{k}{b+1} - (b+1) \text{ ou } b = \frac{-t-2+\sqrt{t^2+4k}}{2} \quad (17')$$

DÉMONSTRATION

Supposons qu'il existe $t \in T_n$ tel que $f_n(k) = t^2$. Alors x et y existent dans $\mathbb{N}$. Ils sont les racines de l'équation $b^2 - Sb + P = 0$; avec $S = n - 2k - 1$ et $P = 3k - n$; i.e.

$$b^2 - (n - 2k - 1)b + 3k - n = 0 \Leftrightarrow b^2 + b - (b+1)n + (2b+3)k = 0$$

$$\Leftrightarrow n = \frac{2b+3}{b+1}k + b. \text{ Aussi si } t \in T_n, \text{ alors } b \in T_{n_k}.$$

Réciproquement, supposons qu'il existe $b \in T_{n_k}$ tel que $n = \frac{2b+3}{b+1}k + b$. Alors, en remplaçant n par cette valeur, on trouve: $f_n(k) = \left[\frac{k}{b+1} - (b+1) \right]^2$. En posant $t = \frac{k}{b+1} - (b+1)$, on obtient $f_n(k) = t^2$. En résolvant l'expression de t par rapport à b , on trouve $b = \frac{-t-2+\sqrt{t^2+4k}}{2}$ (l'autre valeur est rejetée; elle est négative). Aussi si $b \in T_{n_k}$, alors $t \in T_n$.

EXEMPLE

$$n = 21 \Rightarrow I'_n = I'_{21} = [7, 8] \quad T_n = T_{21} = [0, 6] \quad f_n(k) = f_{21}(k) = 4k^2 - 92k + 484$$

- $k = 7 \Rightarrow f_{21}(7) = 36 : t = 6 \in T_{21}$. Ainsi $T_{21_7} = [0, 1] : b = 0 \in T_{21_7}$ et

$$\frac{2b+3}{b+1}k + b = 21$$

- $k = 8 \Rightarrow f_{21}(8) = 4 : t = 2 \in T_{21}$. Ainsi $T_{21_8} = [1,1] : b = 1 \in T_{21_7}$ et $\frac{2b+3}{b+1}k + b = 21$

Aussi

- $k = 7 \Rightarrow 7 \cdot \frac{2b+3}{b+1} + b = 21 \Leftrightarrow 14b + 21 + b(b+1) = 21(b+1) \Leftrightarrow b^2 - 6b = 0$
 $\Leftrightarrow b = 0$ ou $b = 6 : 0 \in T_{21}(7)$ et $6 \notin T_{21}(7)$, de sorte que $t = \frac{7}{1} - 1 = 6 \in T_{21}$ et $f_{21}(7) = 36 = 6^2$.
- $k = 8 \Rightarrow 8 \cdot \frac{2b+3}{b+1} + b = 21 \Leftrightarrow b^2 - 4b + 3 = 0 \Leftrightarrow b = 1$ ou $b = 3 : 1 \in T_{21}(8)$ et $3 \notin T_{21}(8)$, de sorte que $t = \frac{8}{2} - 2 = 2 \in T_{21}$ et $f_{21}(8) = 4 = 2^2$.

NOTE 1

Pour n et k donnés, la recherche de b correspond automatiquement à la détermination partielle des solutions de l'équation $2xy + 3(x+y) = n-3$.

EXEMPLE

- $n = 21$ et $k = 7 \Rightarrow b = 0$ ou $b = 6$ traduit que (0,6) vérifie l'équation $2xy + 3(x+y) = 18$.
- $n = 21$ et $k = 8 \Rightarrow b = 1$ ou $b = 3$ traduit la même chose pour (1,3).
 Finalement, $S = \{(0,6), (6,0), (1,3), (3,1)\}$ et le naturel $2n + 3 = 45$ est composé.

THÉORÈME 5: VERSION PRATIQUE

$$\exists t \in \frac{T_n}{f_n(k)} = t^2 \Leftrightarrow \exists s \in \frac{\tau_n(t)}{n} = 2s^2 + 2(t+3)s + 3(t+1);$$

$$\text{avec } \tau_n(t) = \left[\frac{-3(t+2) + \sqrt{9t^2 + 12n}}{6}, \frac{-t-2 + \sqrt{t^2 + 2n-2}}{2} \right] \quad (18)$$

$$\text{Dans ce cas, } k = \frac{n+2-\sqrt{2n+3+t^2}}{2} = \frac{n+2s-t-1}{2} = s^2 + (t+2)s + t + 1$$

DÉMONSTRATION

Supposons qu'il existe $t \in T_n$ tel que $f_n(k) = t^2$. Alors $4k^2 - 4(n+2)k + (n+1)^2 = t^2$; i.e. $4k^2 - 4(n+2)k + (n+1)^2 - t^2 = 0$. $\Delta' = 8n + 12 + 4t^2$. Il est un carré parfait si et seulement s'il existe $l \in \mathbb{N}$ tel que $8n + 12 + 4t^2 = l^2$; i.e. $n = \frac{l^2 - 4t^2 - 12}{8} \quad (7)$

$$n \in \mathbb{N} \Leftrightarrow \exists s \in \frac{\mathbb{N}}{l} = 4s + 2(t+3) \quad (8). \text{ En substituant (8) dans (7), on a}$$

$$n = 2s^2 + 2(t+3)s + 3(t+1). \text{ Dans ce cas,}$$

$$k = \frac{n+2-\sqrt{2n+3+t^2}}{2} = \frac{n-2s-t-1}{2} = s^2 + (t+3)s + t + 1 \text{ (L'autre valeur de k n'appartient pas à } I_n). k \in I_n \Rightarrow s \in \tau_n(t).$$

Supposons qu'il existe $s \in \tau_n(t)$ tel que $n = 2s^2 + 2(t+3)s + 3(t+1)$. Alors en portant n dans $f_n(k)$, on a $f_n(k) = t^2$. Aussi $k \in I_n \Rightarrow 6 - 2n \leq 0 \leq t^2 \leq \left(\frac{n-3}{3}\right)^2; n \geq 3$ i.e. $t \in T_n$

REMARQUES 5

— Dans les énoncés des théorèmes 4 et 5, on peut ajouter aux premières propositions: il existe $k \in I_n$. Mais, ce n'est pas important, car l'existence de t équivaut celle de k.

— La relation (8) a été trouvée par induction. Cette technique a largement été exploitée par Archimède, Maurolico, Bachet de Méziriac et étendue par Jacques Bernoulli ([7], p. 229). Mais cette relation pouvait être contournée. En effet, en posant $s = x$ et $y = s + t$, l'équation $2xy + 3(x + y) = n - 3$ devient $n = 2s^2 + 2(t + 3)s + 3(t + 1)$; ce qui conduirait au même résultat, malheureusement, sans hypothèses supplémentaires.

— Grâce au théorème 5, on obtient une autre suite de fonctions h_t définies de $\mathbb{N}$ dans $\mathbb{N}$ par

$$h_t(s) = 2s^2 + 2(t + 3)s + 3(t + 1).$$

EXEMPLE

$$n = 21$$

$$\bullet \quad k = 7 \Rightarrow t = 6 : k = \frac{n-2s-t-1}{2} \Leftrightarrow s = 0.$$

$$\text{Dans ce cas, } 2s^2 + 2(t + 3)s + 3(t + 1) = 0 + 0 + 21 = 21$$

$$\bullet \quad k = 8 \Rightarrow t = 2 : k = \frac{n-2s-t-1}{2} \Leftrightarrow s = 1$$

$$\text{Dans ce cas, } 2s^2 + 2(t + 3)s + 3(t + 1) = 2 + 10 + 9 = 21$$

COROLLAIRE 1: RELATION ENTRE N, B, T ET S

$$\text{Dans les conditions des théorèmes 4 et 5, on a } n = 3(2s + t + 1) + 2(2s + t)b - 2b^2$$

DÉMONSTRATION

$$\text{D'après le théorème 4, } n = \frac{2b+3}{b+1}k + b. \text{ En tirant la valeur de } k, \text{ on a } k = \frac{b+1}{(2b+3)(n-b)}$$

$$\text{Or, d'après le théorème 5, } k = \frac{n-2s-t-1}{2}. \text{ Donc, en comparant les deux valeurs, on trouve la relation entre } n, b, t \text{ et } s.$$

COROLLAIRE 2: RELATION ENTRE B, T ET S

$$\text{Dans les conditions des théorèmes 4 et 5, on a } b^2 - (2s + t)b + s(t + s) = 0.$$

DÉMONSTRATION

La démonstration est immédiate. Il suffit de comparer les valeurs de n dans le théorème 4 et dans le corollaire 1.

COROLLAIRE 3: RELATION ENTRE B ET S

$$\text{Dans les conditions des théorèmes 4 et 5, } b = s$$

DÉMONSTRATION

$$\text{La première implication du théorème 4 donne } b^2 - (n - 2k - 1)b + 3k - n = 0 \quad (*)$$

$$\text{Le corollaire 2 donne } b^2 - (2s + t)b + s(t + s) = 0. \text{ En identifiant ces deux polynômes, on trouve:}$$

$$\begin{cases} 2s + t = n - 2k - 1 & (1) \\ s(s + t) = 3k - n & (2) \end{cases}$$

$$(1) \text{ donne } t = n - 2k - 1 - 2s \quad (3)$$

$$(3) \text{ dans } (2) \text{ donne } s^2 - (n - 2k - 1)s + 3k - n = 0 \quad (**)$$

$$\text{En identifiant } (*) \text{ et } (**), \text{ on tire } b = s.$$

NOTE 2.

On peut autrement démontrer le corollaire 3:

— En appliquant la note 1 et les remarques 5 (deuxième tiret):

$$b = x. \text{ Or, } x = s. \text{ Donc } b = s.$$

— Ou encore en démontrant l'équivalence $f_n(k) = t^2 \Leftrightarrow b = s$;

$$\text{avec } b = \frac{-t-2+\sqrt{t^2+4k}}{2} \text{ et } s = \frac{-t-3+\sqrt{t^2+2n+3}}{2}$$

COROLLAIRE 4

$2n + 3$ est premier si et seulement si $\forall t \in T_n, \forall s \in \tau_n(t), n \neq 2s^2 + 2(t+3)s + 3(t+1)$.

(C'est la contraposée du théorème 5)

NOTE 3

Le corollaire 4 signifie que pour tous $t \in T_n$ et $s \in \tau_n(t)$, il existe $v \in \mathbb{Z}^*$ tel que

$$n = 2s^2 + 2(t+3)s + 3(t+1) + v; \text{ i.e. } 2n + 3 = 4s^2 + 4(t+3)s + 6t + 9 + 2v.$$

Pour $2n + 3$ premier, les naturels $4, 4(t+3)$ et $6t + 9 + 2v$ sont étrangers et

$$\Delta' = 4(t^2 - 2v) \text{ est un carré parfait.}$$

EXEMPLE

$$n = 7 \Rightarrow 2n + 3 = 17 \text{ et } T_7 = [0,1]$$

- $h_0(s) = 2s^2 + 6s + 3 : h_0(0) = 3 \neq 7, h_0(1) = 11 \neq 7$ et $\forall s > 1, h_0(s) > 7$.
- $h_1(s) = 2s^2 + 8s + 6 : h_1(0) = 6 \neq 7$ et $\forall s > 0, h_1(s) > 7$.

D'où 17 est un naturel premier.

COROLLAIRE 5: CARACTÉRISATION DES NOMBRES ENTIERS NATURELS IMPAIRS

Soit un naturel $n \geq 3$. Considérons les ensembles et les fonctions suivants:

$$\mathbb{M} = \{t^2\}_{t \in T_n}; \mathbb{D}_n = \{2n + 3 + t^2\}_{t \in T_n}; z: \mathbb{D}_n \rightarrow \mathbb{M}; r \rightarrow z(r) = r;$$

$$q_t: I_n \rightarrow T_{n_k}: k \rightarrow q_t(k) = \frac{-t-2+\sqrt{t^2+4k}}{2}; z_n: T_n \rightarrow \mathbb{D}_n: t \rightarrow z_n(t) = 2n + 3 + t^2;$$

$$h_k: T_{n_k} \rightarrow T_n: b \rightarrow h_k(b) = \frac{k}{b+1} - (b+1) = h_b(k); g: T_n \rightarrow \mathbb{M}: t \rightarrow g(t) = t^2;$$

$$g_n: T_n \rightarrow I_n: t \rightarrow g_n(t) = \frac{n+2-\sqrt{2n+3+t^2}}{2}; w_k: T_{n_k} \rightarrow \mathbb{M}: b \rightarrow w_k(b) = [h_k(b)]^2 = w_b(k);$$

$$u_n: I_n \rightarrow \mathbb{D}_n: k \rightarrow u_n(k) = 2n + 3 + f_n(k); v_n: T_{n_k} \rightarrow \mathbb{D}_n: b \rightarrow v_n(b) = 2n + 3 + w_k(b)$$

Avec f_n des remarques 4; I_n de la relation (12); T_n de la relation (13) et T_{n_k} de la relation (17).

Alors nous obtenons les diagrammes commutatifs ci-après qui caractérisent les nombres entiers naturels impairs (cf. page suivante).

NOTE 4

Dans ces diagrammes, les flèches respectent la composition des relations (applications):

- $g = z \circ z_n = f_n \circ g_n$
- $z_n = u_n \circ g_n = v_n \circ q_t \circ g_n$
- $v_n = z_n \circ h_k = u_n \circ g_n \circ h_k$
- $u_n = v_n \circ g_t = z_n \circ h_k \circ q_t$
- $w_k = z \circ v_n = g \circ h_k = z \circ z_n \circ h_k = f_n \circ g_n \circ h_k$
- $f_n = z \circ u_n = z \circ v_n \circ q_t = z \circ z_n \circ h_k \circ q_t = w_k \circ q_t = g \circ h_k \circ q_t = f_n \circ g_n \circ h_k \circ q_t$

De cette façon, on retrouve le critère de primalité comme suit:

$$\mathbb{D}_n \cap \mathbb{M} \neq \emptyset \text{ et } g_n[T_n] \cap I_n \neq \emptyset \Leftrightarrow 2n + 3 \text{ est composé (19)}$$

$$\mathbb{D}_n \cap \mathbb{M} = \emptyset \text{ ou } g_n[T_n] \cap I_n = \emptyset \Leftrightarrow 2n + 3 \text{ est premier (19')}$$

Les relations (19) et (19') explicitent la caractérisation des nombres entiers naturels impairs sous-jacente dans les diagrammes 1 et 2.

COROLLAIRE 6: L'ENSEMBLE I_c DES NOMBRES ENTIERS NATURELS IMPAIRS COMPOSÉS

D'après le théorème 5, on a la relation (20):

$$I_c = \bigcup_{t \in \mathbb{N}} \{2h_t(s) + 3, s \in \mathbb{N}\} = \bigcup_{t \in \mathbb{N}} \{4s^2 + 4(t+3)s + 6t + 9, s \in \mathbb{N}\}$$

$$= \bigcup_{s \in \mathbb{N}} \{2h_s(t) + 3, t \in \mathbb{N}\} = \bigcup_{s \in \mathbb{N}} \{2(s+3)t + (2s+3)^2, t \in \mathbb{N}\} ;$$

$$\text{avec } h_t(s) = 2s^2 + 2(t+3)s + 3(t+1) = 2(s+3)t + (2s+3)^2 = h_s(t).$$

Diagramme 1. Caractérisation globale

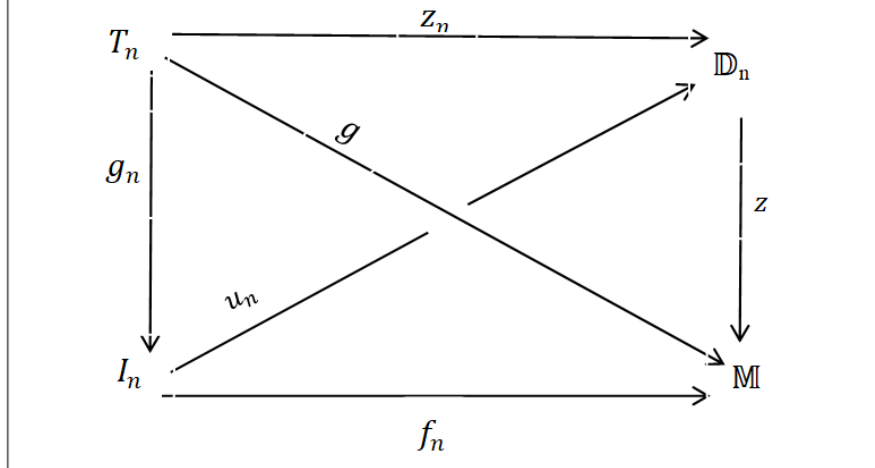
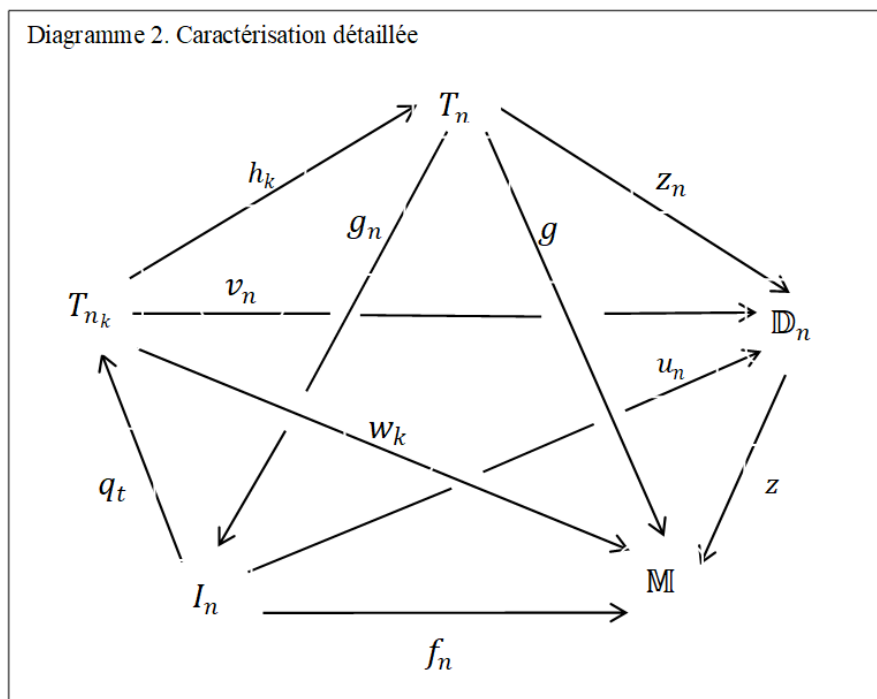


Diagramme 2. Caractérisation détaillée



COROLLAIRE 7: L'ENSEMBLE I_p DES NOMBRES ENTIERS NATURELS IMPAIRS PREMIERS

$$I_p = (2\mathbb{N} + 3) \setminus I_c \quad (20')$$

4 DISCUSSION

L'équation diophantienne $axy + bx + cy = d$ (a et bc étrangers) est, non seulement un cas particulier de l'équation diophantienne générale $ax^2 + bxy + cy^2 + dx + ey = f$, mais aussi et surtout une équation dont l'importance et l'application sont liées à l'étude de la primalité des nombres entiers naturels contenus dans une progression arithmétique $ax + b$ ($x \in \mathbb{N}$). Le cas particulier $a = 2$ et $b = 3$ fait le gros de cet article: l'étude de la primalité d'un nombre entier naturel impair $2n + 3$ (différent de l'unité) est équivalente à celle de l'équation $2xy + 3(x + y) = n - 3$. Par ailleurs, une famille des trinômes du second degré $2h_t(s) + 3 = 4s^2 + 4(t + 3)s + 6t + 9$ ou des binômes du premier degré

$h_s(t) = 2(s + 3)t + (2s + 3)^2$ devient trop suffisante pour engendrer l'ensemble I_c des nombres entiers naturels impairs composés. Bien que ce soit avec répétition, elle permet d'isoler les nombres entiers naturels impairs premiers par complémentarité dans $2\mathbb{N} + 3$:

$I_p = (2\mathbb{N} + 3) \setminus I_c$. D'une part, les corollaires 6 et 7 deviennent la forme algébrique du crible d'Eratosthène ([5], pp. 142 et 149), cette fois-ci, dans $2\mathbb{N} + 3$. D'autre part, le désordre dans l'ensemble I_c crée de l'ordre dans l'ensemble I_p ; un aspect qui, exploité, apporterait un plus à la théorie des nombres premiers.

Si $a > 2$, alors les corollaires 6 et 7 se généralisent dans $a\mathbb{N} + b$. Selon le paragraphe 3.2.3, on aura des familles d'équations $axy + b_jx + b_iy = n - c_{ij}$ et, par conséquent, plusieurs familles des trinômes du second degré ou des binômes du premier degré.

5 CONCLUSION

En théorie des nombres, l'existence de certains problèmes sans solutions exige de feindre d'ignorer les avancées scientifiques et retourner aux notions mathématiques classiques. C'est le cas de cet article dans lequel la résolution de l'équation $axy + bx + cy = d$ (a et bc étrangers) renforce l'étude des nombres premiers contenus dans une progression arithmétique $ax + b$ (a et b étrangers). Pour être utile, ladite résolution est améliorée et cette amélioration est passée par celle des conditions d'existence des solutions. Élémentaire soit-elle, l'application de la résolution de l'équation $ax + by = c$ à celle de l'équation $axy + bx + cy = d$ est une première et contribue à cette amélioration. Notre démarche rend, féconde, la résolution de l'équation $axy + bx + cy = d$ par la production de deux nouveaux critères de primalité; des critères

“polynômiaux” qui font intervenir des fonctions polynômes et qui conduisent, à leur tour, à un double diagramme commutatif, caractéristique des nombres entiers naturels impairs. Ces fonctions et ce diagramme sont aussi une nouveauté. Tous ces résultats enrichissent la théorie algébrique de nombres.

Quelques problèmes restent cependant ouverts. Nous en retenons:

1. L'étude, par une programmation, de la performance des nouveaux critères de primalité comparativement aux critères de primalité existants. Particulièrement, pour la fonction polynôme $f_n(k) = 4k^2 - 4(n+2)k + (n+1)^2$, l'algorithme ad hoc serait polynômial. Par ailleurs, la fonction $f_n(k)$ étant décroissante sur $I_n = \left[\frac{n}{3}, \frac{n-1}{2}\right]$, un tel algorithme contribuerait à la résolution du problème NP.
2. L'application de la résolution de l'équation $axy + bx + cy = d$ à la résolution de certains autres problèmes, ouverts, de la théorie de nombres comme la conjecture de Christian Goldbach, la valeur exacte de la fonction $\pi(x)$,...

REFERENCES

- [1] AVID, M. et COLLIOT-HELENE, J.L. « Diophante d'Alexandrie », in *Encyclopaedia Universalis*, corpus 7, Paris, 1995, 511-522.
- [2] DE MARÇAY, F. Arithmétique dans $\mathbb{Z}$ et dans $\mathbb{Z}/n\mathbb{Z}$, in <https://www.imo.universite-paris-saclay> 21 juin 2024.
- [3] DELAHAYE, J.P. *Merveilleux nombres premiers, voyage au cœur de l'Arithmétique*, Paris Belin Pour la Science, 2000.
- [4] KANTOR, J.M. « Les problèmes de David Hilbert », in *Encyclopaedia Universalis*, Corpus 11, Paris, 1995, 412-418.
- [5] MUSHIWALYAHYAGE ZALUKA, SAFARI MUKERU et AMANI FARAHA, D. « Formalisation algébrique du crible d'Eratosthène », *International Journal of Innovation and Scientific Research*, vol. 77, n° 1, février 2025, pp. 139-154.
- [6] NIYOMANZI SEBUTIMBILI, M.-CH. Résolution de l'équation diophantienne de la forme $axy + bx + cy + d = 0$, Mémoire de Licence, ISP/BUKAVU, Inédit, 2001.
- [7] TATON, R. *Histoire générale des sciences*, volumes 1-3, tomes 1-4, Paris, P.U.F, 1969.