Zeitschrift: L'Enseignement Mathématique
Band: 35 (1989)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: CONTRIBUTION À L'ÉTUDE D'UNE CONJECTURE DE THÉORIE DES NOMBRES PAR LE CODAGE ZBV
Kapitel: §1. Introduction
Autor: Grigorieff, Serge / Richard, Denis
DOI: https://doi.org/10.5169/seals-57370

§ 1. Introduction

1.1. La conjecture que nous allons étudier ici est due, selon R. Guy (cf. [GR], problem B 29) au logicien A. Woods et se formule ainsi:

Existe-t-il un entier k *tel que, pour tous entiers* x *et* y, *il y ait égalité entre* x *et* y *si et seulement si pour chaque* $i = 0, 1, 2, ..., k$ *les entiers* $x + i$ *et* $y + i$ *ont mêmes diviseurs premiers?*

Une telle constante k doit nécessairement être supérieure ou égale à 2: en effet, P. Erdös a remarqué que, pour tout n, les entiers $x = 2^n - 2$ et $y = 2^n(2^n-2)$ sont tels que x et y ont mêmes diviseurs premiers ainsi que $x + 1$ et $y + 1$. A la question soulevée par Erdös (cf. [GR], problem B 19) de trouver d'autres exemples qui ne soient pas de la forme précédente, la seule réponse apportée à ce jour l'a été par A. Makowski (cf. [MA]):

$$x = 75 = 3 \times 5^2 \quad \text{et} \quad y = 1215 = 3^5 \times 5$$

pour lesquels

$$x + 1 = 76 = 2^2 \times 19 \quad \text{et} \quad y + 1 = 1216 = 2^6 \times 19 .$$

1.2. La question d'A. Woods est un affaiblissement de la conjecture suivante, également due à P. Erdös (cf. [EP] ou [GR], problem B 35):

Il n'y a qu'un nombre fini d'entiers m, n, h, k *avec* $k \geqslant h \geqslant 3$ *et* $m \neq n$ *tels que les produits* $(m+1)(m+2)...(m+k)$ *et* $(n+1)(n+2)...(n+h)$ *aient les mêmes diviseurs premiers.*

Comme exemples de tels produits citons 2.3.4.5.6.7.8.9.10 et 14.15.16 ou 48.49.50, ou encore les produits 2.3.4.5.6.7.8.9.10.11 et 98.99.100.

1.3. Les deux conjectures précédentes sont liées à une autre, encore due à P. Erdös:

L'équation

$$\text{ppcm}\,[(n+1)(n+2)...(n+k)] = \text{ppcm}\,[(m+1)(m+2)...(m+h)]$$

ne possède qu'un nombre fini de solutions (m, n, h, k) *telles que* $h \geqslant 2$ *et* $m \geqslant n + k$.

1.4. Compte tenu de ce qui précède, la conjecture de A. Woods mérite d'être appelée conjecture d'Erdös-Woods, abrégée en conjecture de E-W dans la suite de l'article.

C'est en essayant de résoudre une question posée par J. Robinson en 1948 qu'A. Woods a formulé la conjecture E-W.

La question posée par J. Robinson — et que nous mentionnerons dans la suite sous le nom de problème de J. Robinson — est la suivante:

Peut-on définir, au premier ordre, toute l'arithmétique (c'est-à-dire tous les prédicats et fonctions usuels comme l'ordre naturel, l'addition, la multiplication, l'exponentiation, etc.) avec seulement la fonction successeur S *(c'est-à-dire* $x \mapsto x+1$*) et le prédicat de coprimarité* $x \perp y$ *(qui indique que* x *et* y *sont premiers entre eux)?*

1.5. A. Woods a montré que, de façon surprenante, *la conjecture de E-W et le problème de J. Robinson sont mathématiquement équivalents* (cf. 4.2 et 5.3). C'est la raison principale qui nous fait souhaiter retenir l'attention des théoriciens des nombres. Suite à cette équivalence, des avancées parallèles se font sur les deux versions de cette même question.

1.6. *Version Théorie des nombres*

Les premiers résultats remontent au siècle dernier:

— en 1897 C. Størmer (cf. [SC1] et [SC2] montra qu'*il n'y a qu'un nombre fini de couples* (x, y) *tels que* $x(x+1)$ *et* $y(y+1)$ *aient les mêmes diviseurs premiers fixés à l'avance*;

— en 1892 K. Zsigmondy (cf. [SH] ou [ZK] montra qu'*à l'exception de* 2 *et* 8, *un entier primaire* x *est caractérisé par le premier dont il est puissance et les diviseurs premiers de* $x+1$ (résultat retrouvé par Birkhoff et Vandiver en 1904 (cf. [BG & VH]).

On trouve ensuite les travaux de P. Erdös en 1980 (cf. [EP]), et, récemment (en 1986), ceux de D. Balasubramanian, T. N. Shorey et M. Waldschmidt (cf. [BD & ST & WM]).

Une synthèse des études menées sur la conjecture E-W avec des méthodes de théorie des nombres, ainsi que la contribution personnelle de M. Langevin écrite à l'occasion du colloque organisé pour fêter les 75 ans du professeur P. Erdös, sont à paraître dans [LM2].

1.7. *Version Logique*

Alors que les théoriciens des nombres attaquent la conjecture E-W en affinant des majorations ou minorations adéquates, le logicien tente « d'approcher le plus possible » le langage minimum considéré $(S\,;\perp)$.

— Il s'agit d'ajouter au successeur et à la coprimarité une relation ou fonction au pouvoir d'expression le plus restreint possible mais suffisant pour pouvoir définir *toute* l'arithmétique.

— On peut aussi remplacer le successeur par une relation plus forte (comme l'addition ou l'ordre naturel qui permettent de redéfinir la succession, la réciproque étant fausse),

ou bien renforcer la coprimarité par une relation (telle la multiplication ou la divisibilité) qui permette de redéfinir la première.

1.8. Le premier résultat remonte à A. Tarski ([TA]) qui montra que le langage du successeur et de la multiplication suffit à définir toute l'arithmétique.

J. Robinson (cf. [RJ]) prouva dans sa thèse (1948) que l'arithmétique du premier ordre est définissable par successeur et divisibilité.

Plus tard, en 1981, la thèse de A. Woods (cf. [WA]) établit la possibilité de définir l'arithmétique en termes d'ordre naturel et de coprimarité. Dans ce même travail, il montre, de plus, l'équivalence entre le problème de définissabilité posé par J. Robinson et la conjecture E-W.

Enfin, les travaux de [RD1], [RD2], [RD3], repris au § 5 ci-dessous, présentent la méthode de codage ZBV fondée sur le Théorème de Zsigmondy-Birkhoff-Vandiver (cf. [BG & VH], [SH] ou [ZK]). Cette méthode permet de prouver de nouveaux résultats et de retrouver nombre de ceux déjà connus.

Dans cet article nous étendons ces travaux et présentons des résultats originaux qui unifient tous ceux connus sur ce sujet.

1.9. Remarquons que des motivations mathématiques au départ très éloignées sur une même question peuvent conduire à des éclairages différents et mutuellement féconds. Par exemple, on trouvera dans les publications référencées [RJ] ou [RD2] des preuves du fait que les relations d'ordre naturel et de divisibilité sur les entiers suffisent à définir toute l'arithmétique, ce qui signifie que toute question de théorie des nombres possède une traduction canonique en termes de ces deux relations d'ordre.

Bien plus, il a été récemment prouvé par P. Cegielski (cf. [CP]) que l'axiomatique de G. Peano pour l'arithmétique du premier ordre peut être tout aussi bien remplacée par une axiomatisation comme théorie de deux ordres spécifiques: l'ordre naturel et celui de divisibilité.

Certains de ces axiomes expriment des propriétés caractéristiques de chacun de ces ordres, d'autres sont des théorèmes fondamentaux d'arithmétique

traduisant les liens entre ces deux ordres. Tous ces axiomes sont évidemment exprimés dans le langage réduit à ces deux seuls ordres.

1.10. On utilise, dans les méthodes logiques pour l'étude du problème de J. Robinson, des théorèmes classiques d'arithmétique: outre ceux mentionnés ci-dessus, d'autres résultats, par exemple ceux de Dirichlet, R. C. Carmichael (cf. [CR]), Størmer (cf. [SC1] et [SC2]), ou Schnirelman-Vaughan (cf. [SC] et [VR & RH]), reçoivent des applications à des questions difficiles de définissabilité.

1.11. La méthode de codage ZBV nous semble avoir un intérêt intrinsèque en logique et en informatique théorique (cf. [RD4]). Ainsi, les codages que nous présentons permettent d'interpréter les entiers premiers comme des mémoires abstraites de capacité arbitrairement grande.

1.12. PLAN DE L'ARTICLE

On rappelle au § 2 certains résultats de théorie des nombres fondamentaux pour l'étude de la conjecture E-W, et on développe quelques notions liées à la conjecture d'Erdös-Woods et utilisées dans la suite.

Le § 3 présente les notions logiques sur lesquelles s'appuient ce travail.

Le § 4 présente un survol de l'histoire de la définissabilité arithmétique et une synthèse des résultats obtenus sur le problème de J. Robinson (alias la conjecture d'Erdös-Woods). Il indique aussi la manière dont tous ces résultats peuvent être déduits de certains des théorèmes originaux (4.10, 6.2 et 6.5) de cet article.

Le § 5 est dédié à la preuve du Théorème 4.10: celui-ci donne une caractérisation en termes de définissabilité logique de la notion, purement arithmétique, de saturation pour l'équivalence « $x + i$ et $y + i$ ont mêmes diviseurs premiers pour $i \in A \subseteq \mathbf{Z}$ ». Cette preuve est basée sur les arguments de codage ZBV introduits en [RD1], ceux-ci sont entièrement repris et élargis.

Le § 6 étudie (Thms 6.2 et 6.5) le rôle de la relation d'égalité en face de la fonction successeur et de la relation de coprimarité. Le Théorème 6.2 est un résultat général sur la réduction de la question de définissabilité des opérations $+$ et $\times$ à celle de la seule relation d'égalité. Le Théorème 6.5 contraste avec le précédent en montrant que, toute difficile qu'elle semble à définir avec S et $\perp$, la relation d'égalité n'ajoute guère au pouvoir expressif de S et $\perp$ que la possibilité de se définir elle-même!

Les § 7, 8 et 9 présentent des résultats sur la définissabilité de l'arithmétique en termes du successeur, de la coprimarité et

de la fonction puissance,

ou du prédicat de résiduation quadratique,

ou de restrictions faibles soit de l'addition, soit de la multiplication, soit de la division.

L'article se conclut au § 10 sur des perspectives d'étude de la conjecture par les méthodes de codage, mais aussi sur une réflexion de logicien tentant de comprendre l'éventuel caractère « désespéré » de certaines conjectures arithmétiques comme celle qui nous intéresse.

§ 2. Préliminaires de théorie des nombres

2.1. On note $\mathbf{N}$, $\mathbf{Z}$, P les ensembles respectivement formés des entiers naturels, des entiers rationnels, et des nombres premiers.

L'ensemble des diviseurs premiers de x est appelé *support* de x et noté SUPP (x).

Un outil essentiel est le *Théorème de Dirichlet* sur l'infinitude des premiers dans les progressions arithmétiques $u(n) = an + b$, pour $a \perp b$. Joint au *Théorème des restes chinois*, il conduit à l'existence d'une infinité de solutions en entiers premiers des systèmes de congruences du type

$$z \equiv s_1 \pmod{t_1}, \ldots, z \equiv s_n \pmod{t_n}$$

où $t_1, \ldots, t_n$ sont deux à deux premiers entre eux et $0 < s_1 < t_1, \ldots, 0 < s_n < t_n$.

2.2. Un résultat constamment utilisé dans ce qui suit est le Théorème découvert par K. Zsigmondy en 1892, et redécouvert ensuite par Birkhoff et Vandiver en 1904, que nous appelons Théorème ZBV et que voici :

Théorème (Zsigmondy-Birkhoff-Vandiver). *Soient x et y des entiers premiers entre eux tels que $0 < y < x$. Pour tout $n > 0$, il existe au moins un diviseur premier de $x^n - y^n$ qui ne divise pas $x^m - y^m$ pour $0 < m < n$ (un tel diviseur est dit* primitif *pour $x^n - y^n$) excepté dans les cas suivants :*

i) $n = 1, x - y = 1$, *$x - y$ n'a alors aucun diviseur premier ;*

ii) $n = 2, x + y = 2^u$ *où* $u > 0$;

iii) $n = 6, x = 2, y = 1$.

2.3. L'analogue du Théorème ZBV à propos des formes $x^n + y^n$ a été démontré par R. Lucas et R. Carmichael (cf. [CR]).