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: §10. Conclusion
Autor: Grigorieff, Serge / Richard, Denis
DOI: https://doi.org/10.5169/seals-57370

Preuve. Si p est premier et $x \neq 0$, le nombre $p\mathrm{Quot}(x, p)$ est le plus grand entier divisible par p et inférieur ou égal à x. Ainsi, la fonction $(x, p) \mapsto p\mathrm{Quot}(x, p)$, de domaine $[\mathbf{N}\backslash\{0\}] \times P$ est définissable dans la structure $\langle \mathbf{N}; S, <, \perp \rangle$. Par ailleurs, pour $p \neq 3$, $\mathrm{Quot}_3(x, p)$ vaut

$$\mathrm{Reste}\,(p\mathrm{Quot}\,(x, p), 3) \quad \text{si} \quad 3 \text{ divise } p - 1\,,$$

$$\mathrm{Reste}\,[2 \times \mathrm{Reste}\,(p\mathrm{Quot}\,(x, p), 3), 3] \quad \text{si} \quad 3 \text{ divise } p - 2\,.$$

La Proposition 9.3 montre alors que la fonction Quot_3 est définissable avec $<, S$ et $\perp$.

Comme $<$ définit trivialement S et l'égalité, le langage $(S, \mathrm{Pred}, <, \perp)$ se ramène au langage $(<, \perp)$.

Problèmes. 1°) Le Théorème 9.4 est-il vrai pour $\alpha = 2$?

2°) La restriction de l'ordre $<$ à $\mathbf{N} \times P$ suffit-elle, avec S et $\perp$, à définir $+$ et $\times$? Une réponse positive est conséquence (par réduction immédiate au Corollaire ci-dessus) de la conjecture suivante d'Erdös: si $x < y$ et $x \cong_{\{0,1\}} y$ alors il existe un premier entre x et y.

§ 10. Conclusion

10.1. *Quelques perspectives*

Une stratégie possible pour résoudre la conjecture d'Erdös-Woods pourrait être de définir la fonction exponentielle dans le langage avec $S, \perp$ et la fonction carré, puis de définir la fonction carré avec S et $\perp$.

Une autre voie pourrait consister à déterminer, pour chaque entier x le support d'un entier $x + v$ éloigné de x.

On voit bien que la difficulté réside dans les liens cachés entre l'addition et le produit (ici la coprimarité). C'est ce qu'avaient remarqué certains théoriciens des modèles (par exemple, A. Ehrenfeucht et D. Jensen (cf. [EA & JD]) à propos de la reconstruction des modèles de l'arithmétique par amalgamation de structures additives et multiplicatives. Ce n'est d'ailleurs pas sans raison que ces derniers auteurs sont demandeurs de langages formés de deux ou trois prédicats (à l'exclusion de l'addition et la multiplication, bien évidemment) qui permettent de redéfinir l'arithmétique du premier ordre.

10.2. *Quelques remarques sur le caractère désespéré de certaines conjectures de théorie des nombres.*

On sait depuis les travaux de K. Gödel (1931) que la vérité arithmétique est au-delà du pouvoir démonstratif de toute théorie axiomatique:

L'ensemble des théorèmes de toute théorie non contradictoire qui contient l'arithmétique — et dont les axiomes sont « effectivement donnés » — ne recouvre pas l'ensemble des énoncés vrais de la structure $\langle \mathbf{N}; =, +, \times \rangle$.

A l'heure actuelle (plus précisément depuis les travaux de P. Cohen en 1963) ce résultat de Gödel n'a trouvé sa pleine concrétisation qu'en théorie des ensembles. Dans ce sujet, il y a maintenant pléthore de résultats logiques (aussi optimaux que déconcertants) des types (*) et (**) décrits ci-dessous:

Rappelons que si T est une théorie logique dans laquelle on peut interpréter l'arithmétique (par exemple toutes les formalisations classiques de la théorie des ensembles: Zermelo, Zermelo et Fraenkel, Gödel et Bernays, ...), il est possible de trouver un énoncé, que nous désignons par $\mathrm{NC}(T)$, exprimant le caractère non contradictoire de la théorie T.

Certains des résultats d'indépendance trouvés en théorie des ensembles sont du type suivant:

(*) Si la théorie des ensembles T n'est pas contradictoire, alors

— T ne prouve ni l'énoncé A ni l'énoncé $\neg A$ (négation de A);

— de plus, la théorie $T + \mathrm{NC}(T)$ prouve $\mathrm{NC}(T+A)$ et $\mathrm{NC}(T+\neg A)$.

Des exemples de tels énoncés A sont

— l'hypothèse du continu,

— l'assertion de la mesurabilité Lebesgue de tout ensemble de réels qui est PCA, c'est-à-dire projection du complémentaire de la projection d'un borélien, etc.

D'autres résultats d'indépendance sont du type plus subtil suivant:

(**) — La théorie $T + \mathrm{NC}(T)$ prouve $\mathrm{NC}(T+\neg A)$,

— si la théorie $T + \mathrm{NC}(T)$ n'est pas contradictoire alors elle ne prouve pas $\mathrm{NC}(T+A)$,

— ou bien T prouve $\neg A$, et, a fortiori, T prouve alors $\neg \mathrm{NC}(T+A)$), ou bien T ne prouve ni A ni $\neg A$.

Des exemples de tels énoncés A sont

— le problème d'Ulam sur l'existence d'un ensemble infini admettant un ultrafiltre non principal stable par intersections dénombrables,

— l'assertion de la mesurabilité Lebesgue de tout ensemble de réels qui est PCPCA, c'est-à-dire projection du complémentaire de la projection du complémentaire de la projection (sic) d'un borélien, etc.

10.3. Le pessimisme de spécialistes de théorie des nombres devant certaines conjectures qu'ils jugent désespérées (comme l'est la conjecture d'Erdös-Woods pour certains mathématiciens) pourrait être l'expression de leur intuition de résultats du type (*) ou (**).

Un argument logique montre que tout énoncé arithmétique de type universel, tel que le problème de Fermat $\forall n \forall x \forall y \forall z [n \leqslant 2 \vee x^n + y^n \neq z^n]$, qui n'est pas réfutable dans une théorie axiomatique T comme l'arithmétique du premier ordre de Peano est, en fait, vrai dans la structure **N**. En effet, A est alors vrai dans un modèle (standard ou non) de T et, comme **N** est isomorphe à un segment initial de ce modèle, l'énoncé A est également vrai dans **N**.

Il serait bien surprenant que la vérité d'un énoncé arithmétique soit établie par de telles méthodes, aussi est-ce plutôt à des résultats du type (**) (ou pire...) auxquels il faut s'attendre.

RÉFÉRENCES BIBLIOGRAPHIQUES

[BE] BETH, E. W. On Padoa's method in the theory of definition. *Indag. Math. 15* (1953), 330-339.

[BG & VH] BIRKHOFF, G. D. and H. S. VANDIVER. On the integral divisors of $a^n - b^n$. *Ann. of Math. 5* (1904), 173-180.

[CP] CEGIELSKI, P. Axiomatisation de l'arithmétique avec l'ordre naturel et la divisibilité. *Communication personnelle.*

[CR] CARMICHAEL, R. C. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. 15 (2)* (1913-1914), 30-69.

[DM] DAVIS, M. Hilbert's tenth problem is unsolvable. *American Math. Monthly 80* (1973), 233-269.

[EA & JD] EHRENFEUCHT, A. and D. JENSEN. Some problems in elementary arithmetics. *Fundamenta Mathematicae XCII* (1976), 223-245.

[EP] ERDÖS, P. How many pairs of products of consecutive integers have the same prime factors? *American Math. Monthly 87* (1982), 392-393.

[GR] GUY, R. K. Unsolved problems in Number Theory. *Problem book in mathematics, vol. 1.* Springer-Verlag (1981), 25-28.

[LM1] LANGEVIN, M. Plus grand facteur premier d'entiers voisins. *Comptes Rendus Acad. Sc. Paris 280* (1975), 1567-1570.

[LM2] —— Autour d'un problème d'Erdös et Woods. *Preprint.*