Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de 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
Autor: Grigorieff, Serge / Richard, Denis
Kapitel: §9. DÉFINISSABILITÉ PAR SUCCESSEUR, COPRIMARITÉ ET RESTRICTIONS DE L'ADDITION, DE LA MULTIPLICATION OU DE LA DIVISION
DOI: https://doi.org/10.5169/seals-57370

Puisque $p \equiv 5 \pmod 8$, l'entier $p-1$ est de la forme $p-1 = 4(2k+1)$. Puisque $\mathrm{ORD}(x, p)$ divise toujours $p-1$, l'équivalence (1) devient alors

(2) $(x, p) \in \mathrm{RES}$ si et seulement si 4 ne divise pas $\mathrm{ORD}(x, p)$.

Le point ii) du Corollaire 2.4 du Théorème ZBV montre que (2) peut aussi s'écrire

(3) $(x, p) \in \mathrm{RES}$ si et seulement si $\mathrm{SUPP}(x^4-1) \nsubseteq \mathrm{SUPP}[x^{\mathrm{ORD}(x, p)}-1]$.

Ceci prouve l'égalité

(4) $C \cap \mathrm{RES} = \{(x, p) \in C : \mathrm{SUPP}(x^4-1) \nsubseteq \mathrm{SUPP}[x^{\mathrm{ORD}(x, p)}-1]\}$.

Les résultats de 8.2 et 8.3 permettent alors de traduire cette égalité en une définition de la relation $C \cap \mathrm{RES}$ dans le langage $(S; \perp, \mathrm{PUIS})$.

Ceci achève la preuve de la Proposition 8.1 et donc du Théorème 8.1.

8.6. *Problème ouvert.* Peut-on remplacer dans le Théorème 8.1 le prédicat PUIS par la relation $y = x^2$?

§ 9. Définissabilité par successeur, coprimarité et restrictions de l'addition, de la multiplication ou de la division

9.1. Nous allons maintenant donner les prédicats les plus faibles que nous connaissions qui, joints au successeur et à la coprimarité, permettent de définir toute l'arithmétique.

Si $X \subseteq \mathbf{N}^2$, on note X-ADD et X-MULT les graphes des restrictions de l'addition et de la multiplication à X :

$$X\text{-ADD} = \{(x, y, z) : (x, y) \in X \quad \text{et} \quad z = x + y\} .$$

$$X\text{-MULT} = \{(x, y, z) : (x, y) \in X \quad \text{et} \quad z = xy\} .$$

Dans toute la suite, la première projection de X sera toujours égale à $\mathbf{N}$ tout entier. La relation d'égalité se définit alors facilement dans le langage réduit au seul prédicat X-ADD (resp. X-MULT) : $x = x'$ si et seulement si

$$\{(p, y) : (x, p, y) \in X\text{-ADD}\} = \{(p, y) : (x', p, y) \in X\text{-ADD}\} .$$

Les fonctions S et Pred sont donc définissables l'une à partir de l'autre avec X-ADD ou X-MULT.

Théorème. *Soit $X \subseteq \mathbf{N}^2$ une relation définissable dans la structure $\langle \mathbf{N}; +, \times; = \rangle$ et vérifiant la condition :*

(*) pour tout x il existe une infinité d'entiers primaires v tels que $(x, v) \in X$.

Les trois structures $\langle \mathbf{N}; S; \perp, X\text{-ADD}\rangle$, $\langle \mathbf{N}; S; \perp, X\text{-MULT}\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent alors les mêmes relations et fonctions.*

Preuve. Soit $\sigma = \{(x, v, p): (x, v) \in X,\ v$ est primaire, p premier, p divise $x + v\}$. Le Corollaire 2.8 assure que l'égalité $x = y$ équivaut à la condition

$$\mathrm{SUPP}(x+t) = \mathrm{SUPP}(y+t) \text{ pour une infinité d'entiers } t\,.$$

L'hypothèse faite sur X permet donc d'assurer que $x = y$ équivaut à

$$\{p: (x, v, p) \in \sigma\} = \{p: (y, v, p) \in \sigma\}\,.$$

Ceci donne une définition de la relation d'égalité dans la structure $\langle \mathbf{N}; \perp, \sigma\rangle$. Comme σ est incluse dans $\mathbf{N} \times PP \times P$, le Théorème 6.2 montre alors que $+$ et $\times$ sont aussi définissables dans la structure $\langle \mathbf{N}; S, \mathrm{Pred}; \perp, \sigma\rangle$.

Par ailleurs, l'égalité

$$\sigma = \{(x, v, p): \text{il existe } s \text{ tel que } (x, v, s) \in X\text{-ADD} \quad \text{et} \quad q \in \mathrm{SUPP}(s)\}$$

montre que la relation σ est définissable dans $\langle \mathbf{N}; S; \perp, X\text{-ADD}\rangle$. Comme Pred est définissable à partir de S et X-ADD, ceci prouve que $+$ et $\times$ sont aussi définissables dans $\langle \mathbf{N}; S; \perp, X\text{-ADD}\rangle$.

En ce qui concerne la structure $\langle \mathbf{N}; S; \perp, X\text{-MULT}\rangle$, on introduit la relation

$$\pi = \{(x, v, p): (x, v) \in X,\ v \text{ est primaire, } p \text{ premier, } p \text{ divise } xv + 1\}\,.$$

On raisonne alors de façon analogue en se servant du Corollaire 2 de 2.6 qui assure l'équivalence entre l'égalité $x = y$ et la condition

$$\mathrm{SUPP}(x) = \mathrm{SUPP}(y) \text{ et, pour une infinité d'entiers } t,$$
$$\mathrm{SUPP}(tx+1) = \mathrm{SUPP}(ty+1)\,.$$

Remarque. Considérons le cas où $X = \perp = \{(x, y): x$ et y sont premiers entre eux$\}$. On observe que l'ensemble $\{1\}$ et la relation $\perp$ se définissent très simplement dans la structure $\langle \mathbf{N}; |\rangle$ (où $|$ est le prédicat de divisibilité) par les formules

$$\forall t\ (x|t) \text{ et } \forall z\ [[(z|x) \wedge (z|y)] \to (z=1)]\,.$$

Par ailleurs, la relation $\perp$-MULT se confond avec le graphe de la fonction ppcm restreinte à cet ensemble $\perp$ et se définit donc aussi dans la structure $\langle \mathbf{N}; |\rangle$. On voit ainsi que le Théorème précédent contient le résultat de J. Robinson (cf. 4.5) selon lequel addition et multiplication sont $(S; |)$-définissables.

9.2. On obtient ci-dessous un renforcement important du Théorème 9.1.

THÉORÈME. *Il existe une fonction f, définissable dans la structure $\langle \mathbf{N}; S; \perp \rangle$ (resp. $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$), de domaine $\mathbf{N}$ et à valeurs dans l'ensemble des entiers premiers, et pour laquelle la propriété suivante est vraie. Si $X \subseteq \mathbf{N}^2$ est définissable dans la structure $\langle \mathbf{N}; +, \times; = \rangle$ et telle que*

(**) pour tout x il existe un entier primaire v tel que $v \geqslant f(x)$ et $(x, v) \in X$

alors les trois structures $\langle \mathbf{N}; S; \perp, X\text{-ADD} \rangle$, $\langle \mathbf{N}; S; \perp, X\text{-MULT} \rangle$ et $\langle \mathbf{N}; +, \times; = \rangle$ définissent les mêmes relations et fonctions.

Preuve. 1°) L'argument développé ci-dessous reprend la preuve du Corollaire 1 du Théorème de Størmer (cf. 2.6) en montrant que les notions introduites sont définissables dans les langages $(S; \perp)$ et $(\mathrm{Pred}; \perp)$.

Notons E et E' les ensembles

$$E = \{(x, q) \in \mathbf{N} \times P : \text{il existe } u, v \text{ tels que } u \cong_{\{0,1\}} x \quad \text{et} \quad v \cong_{\{0,1\}} x \quad \text{et} \quad u \neq v \quad \text{et} \quad q \in \mathrm{SUPP}(|u-v|)\},$$

$$E' = \{(x, y) \in \mathbf{N}^2 : \mathrm{SUPP}[y(y+1)] \subseteq \{q : (x, q) \in E\}\}.$$

D'après le Théorème de Størmer (cf. 2.6), l'ensemble $\{y : (x, y) \in E'\}$ est fini pour tout entier x. Soit $N(x)$ le plus grand élément de $\{y : (x, y) \in E'\}$. On définit la fonction f comme suit :

$$f(x) = \text{le plus petit entier premier supérieur à } N(x).$$

Les relations E, E' sont clairement saturées pour l'équivalence $\cong_{\{0,1\}}$. La définition de la fonction f à partir de E', et le fait qu'elle soit à valeurs dans les premiers, montre que son graphe est aussi saturé pour $\cong_{\{0,1\}}$. Le Théorème 4.10 assure alors que f est définissable dans $\langle \mathbf{N}; S; \perp \rangle$.

2°) La preuve du Corollaire 1 de 2.6 (appliquée avec l'ensemble fini $\{u : u \cong_{\{0,1\}} x\}$ comme ensemble A) montre que les trois conditions suivantes sont équivalentes :

i) $x = y$,

ii) $x \cong_{\{0,1\}} y$ et $\mathrm{SUPP}(x+m) = \mathrm{SUPP}(y+m)$ et $\mathrm{SUPP}(x+m+1) = \mathrm{SUPP}(y+m+1)\}$ pour un $m \geqslant f(x)$,

iii) $x \cong_{\{0,1\}} y$ et $\mathrm{SUPP}(mx+1) = \mathrm{SUPP}(my+1)$ pour un $m \geqslant f(x)$.

Posons, de façon semblable à ce qui a été fait plus haut,

$$\sigma = \{(x, v, p) : (x, v) \in X, v \text{ est primaire, } p \text{ premier, } p \text{ divise } x + v\},$$

$$\sigma' = \{(x, v, p) : (x, v) \in X,\ v \text{ est primaire, } p \text{ premier, } p \text{ divise } x + v + 1\},$$

$$\pi = \{(x, v, p) : (x, v) \in X,\ v \text{ est primaire, } p \text{ premier, } p \text{ divise } xv + 1\}.$$

L'hypothèse faite sur X permet de traduire les conditions ii) et iii) en des définitions de la relation d'égalité dans les structures $\langle \mathbf{N}; \perp, \sigma, \sigma' \rangle$ et $\langle \mathbf{N}; \perp, \pi \rangle$. Commme σ, σ' et π sont incluses dans $\mathbf{N} \times PP \times P$, le Théorème 6.2 montre que $+$ et $\times$ sont aussi définissables dans $\langle \mathbf{N}; S, \text{Pred}; \perp, \sigma, \sigma' \rangle$ et $\langle \mathbf{N}; S, \text{Pred}; \perp, \pi \rangle$. On achève la preuve, commme précédemment, en observant σ et σ' sont définissables à partir de S et X-ADD, et que π l'est à partir de S et X-MULT.

3°) Pour obtenir une fonction f ayant la même propriété et définissable avec Pred et $\perp$, on remplace $\cong_{\{0,1\}}$ par $\cong_{\{-1,0\}}$ dans la définition de E, et le produit $y(y+1)$ par $y(y-1)$ dans la définition de E'.

On raisonne enfin à l'aide de la condition iii)bis suivante du Corollaire 1 de 2.6:

iii)bis $x \cong_{\{-1,0\}} y$ et $\text{SUPP}(mx-1) = \text{SUPP}(my-1)$ pour un $m \geqslant f(x)$.

9.3. Nous considérons maintenant des prédicats qui sont des affaiblissements de la division euclidienne.

Avant de prouver le Théorème 9.4 ci-dessous, dont le Théorème de Woods cité en 4.6 est corollaire, nous mentionnons d'abord un fait simple.

PROPOSITION. *Pour tout entier premier* π, *la fonction* $z \mapsto \text{Reste}(z, \pi)$, *de domaine* $\mathbf{N}$ *est définissable dans les structures*

$$\langle \mathbf{N}; S; \perp \rangle \quad \textit{et} \quad \langle \mathbf{N}; \text{Pred}; \perp \rangle.$$

Preuve. La relation $y = \text{Reste}(x, \pi)$ est équivalente à chacune des conditions:

$$[y=0 \text{ et } \pi|x] \text{ ou } [y=1 \text{ et } \pi|S^{\pi-1}(x)] \text{ ou } \ldots \text{ ou } [y=\pi-1 \text{ et } \pi|S(x)],$$

et

$$[y=0 \text{ et } \pi|x] \text{ ou } [y=1 \text{ et } x \geqslant 1 \text{ et } \pi|\text{Pred}(x)] \text{ ou } \ldots$$
$$\text{ou } [y=\pi-1 \text{ et } x \geqslant \pi-1 \text{ et } \pi|\text{Pred}^{\pi-1}(x)].$$

Comme $\pi \mid z$ s'écrit $\neg(\pi \perp z)$ et que les singletons sont définissables dans les langages $(S, \perp)$ et $(\text{Pred}, \perp)$ (cf. 5.4 et 5.6), ces conditions se traduisent dans ces langages.

9.4. Rappelons que Quot et Reste désignent les fonnctions quotient et reste de la division euclidienne.

Soit $\alpha \geqslant 2$; on note Quot_α et Reste_α les graphes des fonctions partielles

$$(x, p) \mapsto \text{Reste}\big(\text{Quot}(x, p), \alpha\big) \quad \text{et} \quad (x, p) \mapsto \text{Reste}\big(\text{Reste}(x, p), \alpha\big)$$

de domaine $[\mathbf{N}\backslash\{0\}] \times [P\backslash\{\alpha\}]$.

Remarque. 1°) Ces fonctions sont une vue modulo un entier fixé de la restriction de la division au cas des diviseurs premiers; elles sont évidemment définissables à partir des fonctions Quot et Reste.

2°) En contraste avec le théorème ci-dessous, les graphes des fonctions $(x, y) \mapsto \text{Reste}(x+y, \alpha)$ et $(x, y) \mapsto \text{Reste}(xy, \alpha)$, de domaine $\mathbf{N}\backslash\{0\}] \times \mathbf{N}$, sont définissables dans les langages $(S, \perp)$ et $(\text{Pred}, \perp)$.

Ceci résulte de la Proposition 9.3, du calcul évident du reste de la somme et d'un produit, et de ce que les graphes de $+$ et $\times$ restreintes à $\{0, ..., \alpha - 1\}^2$ sont définissables dans $(S, \perp)$ et $(\text{Pred}, \perp)$.

THÉORÈME. *Soit* $\alpha \geqslant 3$. *Les structures*

$$\langle \mathbf{N}; S; \perp, \text{Quot}_\alpha\rangle, \quad \langle \mathbf{N}; \text{Pred}; \perp, \text{Quot}_\alpha\rangle, \quad \langle \mathbf{N}; \text{Pred}; \perp, \text{Reste}_\alpha\rangle$$
$$\textit{et} \quad \langle \mathbf{N}; +, \times; =\rangle$$

définissent les mêmes relations et fonctions.

Preuve. Les conditions $\text{ii})_\alpha$ et $\text{iii})_\alpha$ de la Proposition 2.14 montrent que l'égalité $x = y$ équivaut à chacune des conditions

(*) x et y ont même parité et $\text{Reste}_\alpha(x, p) = \text{Reste}_\alpha(y, p)$ pour tout premier $p \neq \alpha$;

(**) x et y ont même parité et $\text{Quot}_\alpha(x, p) = \text{Quot}_\alpha(y, p)$ pour tout premier $p \neq \alpha$.

Comme l'égalité restreinte à l'ensemble fini fixé $\{0, ... \alpha - 1\}$ (dans lequel les fonctions Quot_α et Reste_α prennent leurs valeurs) est définissable dans chacun des langages $(S, \perp)$ et $(\text{Pred}, \perp)$ (cf. Remarque 5.5), on voit que la condition (*) (resp. (**)) se traduit dans les langages $(S; \perp, \text{Quot}_\alpha)$ et $(S; \perp, \text{Reste}_\alpha)$ (resp. $(\text{Pred}; \perp, \text{Quot}_\alpha)$ et $(\text{Pred}; \perp, \text{Reste}_\alpha)$).

Comme Quot_α et Reste_α sont inclus dans $\mathbf{N} \times P \times \{0, ..., \alpha - 1\}$, on conclut grâce au Théorème 6.2.

COROLLAIRE (Woods). *Les structures* $\langle \mathbf{N}; <, \perp\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent les mêmes relations et fonctions.*

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.