L'Enseignement Mathématique, t. 35 (1989), p. 125-189

CONTRIBUTION À L'ÉTUDE D'UNE CONJECTURE DE THÉORIE DES NOMBRES PAR LE CODAGE ZBV

par Serge GRIGORIEFF et Denis RICHARD

ABSTRACT. In [RJ] J. Robinson asked whether first order arithmetic over the set **N** of non negative integers is definable in terms of the successor function S and the coprimeness predicate $\perp$ (where $a \perp b$ iff a and b have no common prime divisor). It turns out that this question is equivalent to the following conjecture of number theory: Is there an integer k such that for every pair (x, y) of integers, the equality $x = y$ holds if and only if $x + i$ and $y + i$ have the same prime divisors for $0 \leqslant i \leqslant k$? This conjecture, due to A. Woods, is itself closely linked to some open questions proposed by P. Erdös (see [EP]). From the results in [RJ], [WA] and [RD], first order arithmetic is expressible in terms of the successor function S, the coprimeness predicate $\perp$ and anyone of the predicates of the following list:

$$x < y; x + y = z; x \mid y \,(x \text{ divides } y); x \times y = z;$$
$$y = m^x \text{ (for any fixed } m \geqslant 2)\,.$$

This paper intends

1°) to present some number theoretical results which are pertinent tools to develop methods essentially relevant to mathematical logic;

2°) to give a survey of the history of arithmetical definability;

3°) to present some results about J. Robinson's question which unify all previously known ones;

4°) to add to the previous list new predicates such as RES(x, p) (which means that p is prime and x is a quadratic residue modulo p), POW(y, x) (which means that y is a power of x) and weak restrictions of addition, multiplication and division.

Ce travail a bénéficié du soutien du PRC Mathématiques et Informatique du CNRS, France.

§ 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 **N**, **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]).

THÉORÈME (Lucas-Carmichael). *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* caractéristique *pour* $x^n + y^n$*) excepté dans le cas où* $n = 3, x = 2$ *et* $y = 1$.

Ce théorème est, en fait, corollaire de ZBV puisque tout diviseur primitif de $x^{2n} - y^{2n}$ est diviseur caractéristique de $x^n + y^n$.

2.4. Si p est premier, nous notons $\mathrm{ORD}(x, p)$ l'ordre de x modulo p, c'est-à-dire le plus petit α tel que $x^\alpha \equiv 1 \pmod{p}$.

Il est clair que p divise (resp. est diviseur primitif de) $x^\alpha - 1$ si et seulement si α est multiple de (resp. est égal à) $\mathrm{ORD}(x, p)$.

Les Théorèmes ZBV et LC, joints au fait simple suivant lequel le pgcd des entiers $x^n - 1$ et $x^m - 1$ est $x^{\mathrm{pgcd}(n, m)} - 1$, montrent le résultat suivant:

COROLLAIRE. *Pour tout entier* $x > 1$ *et tous entiers* α *et* β*:*

i) *L'égalité* $\mathrm{SUPP}(x^\alpha - 1) = \mathrm{SUPP}(x^\beta - 1)$ *équivaut à*
($\alpha = \beta$ ou bien x est de la forme $2^u - 1$ avec $u > 1$ et α et β éléments de $\{1, 2\}$).

ii) *L'inclusion* $\mathrm{SUPP}(x^\beta - 1) \subseteq \mathrm{SUPP}(x^\alpha - 1)$ *équivaut à*
($\beta \mid \alpha$ ou x est de la forme $2^u - 1$ avec $u > 1$ et $\beta = 2$).

iii) *Un entier* p *est diviseur primitif de* $x^\alpha - 1$ *si et seulement si*
p divise $x^\alpha - 1$ et, ou bien $\alpha = 1$,
ou bien $\mathrm{SUPP}(x^\alpha - 1) \subset_{\neq} \mathrm{SUPP}(x^\beta - 1)$ pour tout $\beta \neq \alpha$ tel que p divise $x^\beta - 1$.

iv) *L'égalité* $\mathrm{SUPP}(x^\alpha + 1) = \mathrm{SUPP}(x^\beta + 1)$ *équivaut à*
($\alpha = \beta$ ou bien $x = 2$ et α et β sont éléments de $\{1, 3\}$).

Preuve. Cf. les Corollaires 1.7, 1.8 et 1.9 de [RD1] pages 223-224.

2.5. Le Théorème suivant remonte à C. Størmer (1897, cf. [SC1] et [SC2]).

THÉORÈME (Størmer). *Soient* $p_1, ..., p_n$ *des premiers distincts,* $K, \alpha_1, ..., \alpha_n$ *des entiers strictement positifs. Pour* $1 \leqslant i \leqslant n$, *posons* $\varepsilon_i = 1$ *si* α_i *est impair et* $\varepsilon_i = 2$ *si* α_i *est pair. Posons aussi* $D = K \cdot p_1^{\varepsilon_1} \cdot \ldots \cdot p_n^{\varepsilon_n}$.

Si $x^2 - 1 = K \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ *alors* x *est la solution fondamentale de l'équation de Pell-Fermat* $x^2 - Dy^2 = 1$.

Si $x(x+1) = K \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ *alors* $2x + 1$ *est la solution fondamentale de l'équation de Pell-Fermat* $x^2 - 4Dy^2 = 1$.

COROLLAIRE.

i) *Si* E *est un ensemble de* n *entiers premiers distincts, il y a au plus* 2^n *entiers* x *tels que* $\mathrm{SUPP}[x(x+1)] \subseteq E$.
Ainsi, pour tout entier a, *l'ensemble* $ST(a)$ *des entiers* b *tels que*

$$\mathrm{SUPP}(a) = \mathrm{SUPP}(b) \quad et \quad \mathrm{SUPP}(a+1) = \mathrm{SUPP}(b+1)$$

est lui aussi fini.

ii) *Les entiers naturels* x *et* y *sont égaux si et seulement si les conditions suivantes sont simultanément satisfaites:*

1) $\mathrm{SUPP}(x-1) = \mathrm{SUPP}(y-1)$ *et* $\mathrm{SUPP}(x+1) = \mathrm{SUPP}(y+1)$;

2) *pour tout premier* p *et tout* $i \in \{-1, +1\}$, *les valuations de* p *dans les décompositions primaires de* $x + i$ *et de* $y + i$ *ont la même parité.*

2.6. COROLLAIRE 1. *Soit* A *un ensemble fini d'entiers positifs de même support. Il existe un entier* $N(A)$ *tel que, pour tous* x *et* y *dans* A, *les conditions suivantes soient équivalentes:*

i) $x = y$,

ii) *Il existe* $m > N(A)$ *tel que*

$$\mathrm{SUPP}(x+m) = \mathrm{SUPP}(y+m) \quad et$$
$$\mathrm{SUPP}(x+m+1) = \mathrm{SUPP}(y+m+1),$$

iii) *Il existe* $m > N(A)$ *tel que*

$$\mathrm{SUPP}(mx+1) = \mathrm{SUPP}(my+1).$$

iii)bis *Il existe* $m > N(A)$ *tel que*

$$\mathrm{SUPP}(mx-1) = \mathrm{SUPP}(my-1).$$

Preuve. Soit E l'ensemble fini

$$E = \{q \in \mathbf{N}: \text{il existe } (u, v) \in A \times A \text{ tel que } u \neq v \text{ et } q \in \mathrm{SUPP}(|u-v|)\}.$$

Le Théorème de Størmer assure que l'ensemble

$$\{z \in \mathbf{N}: [\mathrm{SUPP}[z(z+1)] \subseteq E\}$$

est fini, majoré par un entier $N(A)$.

Soient x et y des éléments distincts de A, avec $x < y$. Nous montrons que si l'une des conditions ii) ou iii) est vérifiée alors l'entier m est majoré par $N(A)$.

Supposons que l'on ait

$$\mathrm{SUPP}(x+m) = \mathrm{SUPP}(y+m) \quad \text{et} \quad \mathrm{SUPP}(x+m+1) = \mathrm{SUPP}(y+m+1).$$

Tout diviseur premier q de $x+m$ ou de $x+m+1$ divise alors $y-x$. Ainsi, l'entier $(x+m)(x+m+1)$ a un support inclus dans E et donc — par définition de $N(A)$ — l'entier $x+m$ est majoré par $N(A)$. En particulier, m est majoré par $N(A)$.

Supposons maintenant que l'on ait $\mathrm{SUPP}(mx+1) = \mathrm{SUPP}(my+1)$. Tout diviseur premier q de $mx+1$ divise alors $m(y-x)$ et donc aussi $y-x$. Ainsi, l'entier $mx(mx+1)$ a encore un support inclus dans E et l'entier mx est donc majoré par $N(A)$. En particulier, l'entier m est majoré par $N(A)$.

Le cas où $\mathrm{SUPP}(mx-1) = \mathrm{SUPP}(my-1)$ est analogue.

COROLLAIRE 2. *Soient x et y des entiers positifs ou nuls. Les conditions suivantes soient équivalentes:*

i) $x = y$,

ii) *x et y ont le même support et, pour une infinité d'entiers m, on a*

$$\mathrm{SUPP}(x+m) = \mathrm{SUPP}(y+m) \quad \textit{et}$$
$$\mathrm{SUPP}(x+m+1) = \mathrm{SUPP}(y+m+1),$$

iii) *x et y ont le même support et, pour une infinité d'entiers m, on a*

$$\mathrm{SUPP}(mx+1) = \mathrm{SUPP}(my+1).$$

2.7. Il est intéressant de remarquer que, sans utiliser le Théorème de Stømer, un autre résultat du même type peut être prouvé en se servant du Théorème de Dirichlet.

PROPOSITION. *Soit A un ensemble fini d'entiers. Pour chaque x de A, il existe des entiers premiers p arbitrairement grands tels que*

$$\mathrm{SUPP}(px+1) \cap \Big[\bigcup_{y \in A\setminus\{x\}} \mathrm{SUPP}(py+1)\Big] \subseteq \{2\}.$$

Preuve. Soit d le produit des entiers premiers ne divisant pas x et appartenant à la réunion des $\mathrm{SUPP}(|y-z|)$ avec y et z dans A. Soit x' tel que $xx' \equiv 1 \pmod d$. On sait qu'il existe des entiers p arbitrairement grands tels que $p \equiv x' \pmod d$, c'est-à-dire tels que $\mathrm{SUPP}(px-1)$ contienne $\mathrm{SUPP}(d)$. Il nous suffit de montrer que, pour de tels p, on a, pour tout y de $A\setminus\{x\}$

$$\mathrm{SUPP}(px+1) \cap \mathrm{SUPP}(py+1) \subseteq \{2\}.$$

Soit q un diviseur premier de $px + 1$ et $py + 1$. Comme $q \neq p$ et q divise $p \mid x - y \mid$, alors q divise $\mid x - y \mid$. N'étant pas dans SUPP(x), il divise d. Par suite, q divise $px - 1$; comme q divise aussi $px + 1$, on a $q = 2$.

2.8. L'étude des suites d'entiers de même support remonte au moins à G. Pòlya qui prouva un résultat amélioré depuis par M. Langevin (cf. [LM1]).

THÉORÈME.

i) (G. Pòlya) *Si* $(a_n)_{n\in\mathbf{N}}$ *est une suite strictement croissante d'entiers positifs de même support alors la suite* $(a_{n+1}-a_n)_{n\in\mathbf{N}}$ *tend vers l'infini.*

ii) (M. Langevin) *Si* $0 < x < y$ *et* SUPP(x) = SUPP(y), *alors*

$$\mid y - x \mid > [\mathrm{Log}\,(x+y)]^{1/6}.$$

Ce résultat permet d'améliorer la condition ii) du Corollaire 2 de 2.6 en montrant que la donnée d'une infinité de supports du type SUPP$(x+i)$ caractérise x.

COROLLAIRE. *Soient* x *et* y *des entiers de* $\mathbf{Z}$.

Si pour une infinité d'entiers $m \in \mathbf{N}$ *on a* SUPP$(|x+m|)$ = SUPP$(|y+m|)$ *alors* $x = y$.

Preuve. Supposons que l'ensemble

$$I = \{i \in \mathbf{N} : \mathrm{SUPP}\,(|x+i|) = \mathrm{SUPP}\,(|y+i|)\}$$

soit infini et que l'on ait $x < y$. Observant qu'un diviseur premier de $x + i$ et $y + i$ divise $y - x$, on constate que SUPP$(|x+i|) \subseteq$ SUPP$(y-x)$. Le principe des tiroirs montre qu'il existe une partie X de SUPP$(y-x)$ telle que l'ensemble $J = \{i \in \mathbf{N} : \mathrm{SUPP}\,(|x+i|) = \mathrm{SUPP}\,(|y+i|)\}$ soit infini. On définit par récurrence une suite strictement croissante d'entiers positifs, tous de support X comme suit:

$a_0 = x+i$ et $a_1 = y+i$ où i est minimum dans J tel que $x+i>0$;

$a_{2n} = x+j$ et $a_{2n+1} = y+j$ où j est minimum dans J tel que $x+j>a_{2n-1}$.

La preuve s'achève en remarquant que $(a_{2n+1}-a_{2n})_{n\in\mathbf{N}}$ est constante de valeur $y - x$ et donc ne tend pas vers l'infini avec n, ce qui contredit le Théorème de Pòlya.

2.9. Nous mentionnons enfin un résultat qui souligne la portée de la conjecture E-W sur $\mathbf{N}$.

En formalisant la négation de cette conjecture, on obtient la formule suivante:

$$\forall k\ \exists x\ \exists y > x\ \forall i \leqslant k \quad [\mathrm{SUPP}(x+i) = \mathrm{SUPP}(y+i)]\,.$$

Il est intéressant de constater que l'énoncé

$$\forall k\ \exists x\ \exists y > x\ \forall i \leqslant k \quad [\mathrm{SUPP}(x+i) \subseteq \mathrm{SUPP}(y+i)]\,,$$

obtenu en remplaçant l'égalité par l'inclusion est facilement prouvable.

PROPOSITION. *Pour tout* $k > 0$, *pour tout* $x \in \mathbf{N}$ *il existe* $y > x$ *tel que*

$$\mathrm{SUPP}(x+i) \subseteq \mathrm{SUPP}(y+i) \quad \textit{pour tout} \quad i \in \{0, 1, ..., k\}\,.$$

Preuve. On considère le plus grand entier premier p qui divise $(x+k)!$. Un y convenable est alors donné par les conditions $y > x$ et $y \equiv x \pmod{\pi}$, où π est le produit des entiers premiers $q < p$.

Remarque. La condition $y > x$ est ici essentielle. En effet, M. Langevin a montré que si pour tout x assez grand il existe $y < x$ tel que $\mathrm{SUPP}(x+i) \subseteq \mathrm{SUPP}(y+i)$ pour tout $i \in \{0, 1, 2\}$ alors la conjecture d'Oesterlé-Masser est fausse (cf. [LM2]).

2.10. L'étude de la conjecture d'Erdös-Woods introduit naturellement la notion suivante:

Définition. Soit A une partie de $\mathbf{Z}$. On note $\cong_A$ la relation d'équivalence sur $\mathbf{Z}$ définie comme suit:

$x \cong_A y$ si et seulement si $\mathrm{SUPP}(|x+i|) = \mathrm{SUPP}(|y+i|)$ pour tout $i \in A$.

Notons $[x]_A$ la classe de x pour $\cong_A$. Le Fait suivant est immédiat.

FAIT. 1°) *Si* $A \subseteq B$ *alors* $\cong_A$ *est moins fine que* $\cong_B$.
La relation $\cong_\emptyset$ *est l'équivalence grossière.*
2°) *Si* $t \in \mathbf{Z}$, $x \in \mathbf{Z}$, $y \in \mathbf{Z}$, $A + t = \{x + t : x \in A\}$, $-A = \{-x : x \in A\}$, *alors* $x \cong_{A+t} y$ *si et seulement si* $x + t \cong_A y + t$ *(i.e.* $[x]_{A+t} = ([x+t]_A) - t$*);* $x \cong_{-A} y$ *si et seulement si* $-x \cong_A -y$ *(i.e.* $[x]_{-A} = -[-x]_A$*).*
3°) *Si* $x \in \mathbf{Z}$ *alors* $[x]_{\{-x\}} = [x]_{\{-x+1\}} = \{x\}$.

Remarque. 1°) La conjecture d'Erdös-Woods exprime alors simplement qu'*il existe une constante* k *telle que la trace sur* $\mathbf{N}$ *de la relation* $\cong_{\{0, 1, ..., k\}}$ *soit la relation d'égalité.*

2°) La conjecture d'Erdös-Woods équivaut aussi aux assertions suivantes:

(E-W)bis *Il existe une constante* k *telle que la trace sur* $\mathbf{N}$ *de la relation* $\cong_{\{-k,\ldots,0\}}$ *soit la relation d'égalité.*

(E-W)ter *Il existe une constante* k *telle que la trace sur* $\mathbf{N}$ *de la relation* $\cong_{\{-k,\ldots,k\}}$ *soit la relation d'égalité.*

Seules les implications (E-W)ter $\Rightarrow$ (E-W) et (E-W)ter $\Rightarrow$ (E-W)bis sont non triviales.

La première résulte facilement de l'égalité $[x]_{\{0,\ldots,2k\}} = [x+k]_{\{-k,\ldots,k\}} - k$. La seconde résulte de l'égalité $[x]_{\{-2k,\ldots,0\}} = [x-k]_{\{-k,\ldots,k\}} + k$ pour $x \geqslant k$, et des égalités $[x]_{\{-2k,\ldots,0\}} = \{x\}$ pour $x < k$.

2.11. Le Corollaire 2.8 et le théorème de Stømer 2.6 se traduisent par le théorème suivant:

THÉORÈME.

i) *Si* A *est infini alors* $\cong_A$ *est la relation d'égalité sur* $\mathbf{Z}$.

ii) *Les classes d'équivalence de* $\cong_A$ *sont finies dès que* A *contient deux entiers successifs de* $\mathbf{Z}$.

iii) *Si* A *contient un segment* $\{i,\ldots,i+k\}$ *de* $\mathbf{Z}$, $x \cong_A y$ *et* $x \neq y$ *alors*

$$|x-y| \geqslant \prod_{p\in P,\, p|(x+i)\ldots(x+i+k)} p \quad \geqslant \quad \prod_{p\leqslant k+1,\, p\in P} p \ .$$

Preuve. i) Supposons $A \cap \mathbf{N}$ infini et $x \cong_A y$.

Soit $m \in \mathbf{N}$ tel que $x+m > 0$ et $y+m > 0$. Comme $(A-m) \cap \mathbf{N}$ est aussi infini et que $x+m \cong_{A-m} y+m$, le Corollaire 2.8 assure l'égalité $x+m = y+m$ et donc $x = y$. Dans le cas où $A \cap (\mathbf{Z}\backslash\mathbf{N})$ est infini on considère $\cong_{-A}$ et on conclut à l'aide du point 2 du Fait 2.10.

ii) Notons $[x]_A$ la classe de x pour $\cong_A$.

Le théorème de Stømer montre que les traces de $[x]_{\{0,1\}}$ et $[x]_{\{-1,0\}}$ sur $\mathbf{N}$ et $\mathbf{Z}\backslash\mathbf{N}$ sont finies. D'après le point 2 du Fait 2.10 on a $[x]_{\{0,1\}} = ([x]_{\{0,1\}} \cap \mathbf{N}) \cup (-([-x]_{\{-1,0\}} \cap \mathbf{N}))$, égalité qui montre le caractère fini des classes de $\cong_{\{0,1\}}$. On conclut la preuve de ii) à l'aide du point 2 du Fait 2.10, en considérant les $\cong_{A+t}$.

iii) Il suffit d'observer que si p divise $x+j$ il divise aussi $y+j$ et donc $x-y$.

2.12. Les points i) et iv) du Corollaire 2.4 se traduisent par le théorème suivant:

THÉORÈME. *Les restrictions à l'ensemble PP des entiers primaires des relations* $\cong_{\{0,1,2\}}$, $\cong_{\{-2,-1,0\}}$ *et* $\cong_{\{-1,0,1\}}$ *coïncident avec la relation d'égalité. Les parties des* PP^k, $k > 0$, *sont donc saturées pour les relations d'équivalence* $\cong_A$ *telles que A contienne* $\{0,1,2\}$ *ou bien* $\{-2,-1,0\}$ *ou bien* $\{-1,0,1\}$.

Preuve. Le point iv) du Corollaire 2.4 montre que la seule classe de $\cong_{\{0,1\}}$ dont la trace sur *PP* n'est pas réduite à un seul élément est celle de 2 dont la trace est $\{2,8\}$. Comme $\mathrm{SUPP}(2+2) = \{2\}$ et $\mathrm{SUPP}(8+2) = \{2,5\}$, on voit que $2 \not\cong_{\{0,1,2\}} 8$.

Le point i) du Corollaire 2.5 montre que les seules classes de $\cong_{\{-1,0\}}$ dont les traces sur *PP* ne sont pas réduites à un seul élément sont les classes $\{p, p^2\}$ où p est un entier premier de Mersenne, i.e. de la forme $p = 2^u - 1$. Comme $p^2 + 1 = (2^u-1)^2 + 1 = 2[2^u(2^{u-1}-1)+1]$, on voit que $\mathrm{SUPP}(p^2+1) \neq \{2\}$ tandis que $\mathrm{SUPP}(p+1) = \mathrm{SUPP}(2^u) = \{2\}$, d'où $p \not\cong_{\{-1,0,1\}} p^2$. Comme $p - 2 = 2^u - 3$ et $p^2 - 2 = (2^u-3)(2^u+1) + 2$, ces entiers sont impairs et premiers entre eux, d'où $p \not\cong_{\{-2,-1,0\}} p^2$.

Le Fait 2.10 donne le corollaire suivant de ce Théorème:

COROLLAIRE. *Soit* $n > 0$. *Sur l'ensemble* $PP + [0,n] = \{x + s : x \in PP$ *et* $0 \leqslant s \leqslant n\}$ *la relation* $\cong_{\{-n-1,\ldots,-1,0\}}$ *coïncide avec la relation d'égalité.*

Sur l'ensemble $PP + [-n,0] = \{x + s : x \in PP$ *et* $-n \leqslant s \leqslant 0$ *et* $x + s \geqslant 0\}$ *la relation* $\cong_{\{0,1,\ldots,n+1\}}$ *coïncide avec la relation d'égalité.*

Sur l'ensemble $PP + [-n,n]$ *la relation* $\cong_{\{-n,\ldots,0,\ldots,n\}}$ *coïncide avec la relation d'égalité.*

Les parties des $(PP+[0,n])^k$ *(resp.* $(PP+[-n,0])^k$, *resp.* $(PP+[-n,n])^k$*) où* $k > 0$, *sont donc saturées pour les relations d'équivalence* $\cong_A$ *telles que A contienne* $\{-n-1,\ldots,0\}$ *(resp.* $\{0,\ldots,n+1\}$, *resp.* $\{-n,\ldots,0,\ldots,n\}$*).*

Remarques. 1°) Soit U l'ensemble

$$U = \{-56, -26, -20, -14, -11, -10, -6, -5, -4, 0, 1, 4, 10, 16, 46\}.$$

On peut montrer (en utilisant le Théorème ZBV) que la restriction de $\cong_{\{0,1,m\}}$ à l'ensemble *PP* des entiers primaires coïncide avec la relation d'égalité si et seulement si $m \notin U$.

2°) Les cas d'exception du Théorème ZBV étant liés aux premiers de Mersenne, il semble plus difficile de déterminer les m pour lesquels la relation $\cong_{\{0,-1,m\}}$, restreinte à *PP*, coïncide avec l'égalité: ce sont les m tels que, pour tout Mersenne p on ait $\mathrm{SUPP}(p+m) \neq \mathrm{SUPP}(p^2+m)$.

Outre la valeur $m = -2$ vue dans le Théorème précédent, on peut montrer que c'est le cas des entiers $m = \pm q^{\alpha} - 1$, où q est un premier non Mersenne, $m \notin \{-p^2 - p : p$ est Mersenne et $p^2 + p - 1$ est premier$\}$ et $m \notin \{-6, -5\}$ (à cause de $p = 3$). Les exemples de tels m entre -20 et 22 sont

$$-20, -18, -17, -14, -12, -10, -9, -8, -5, -4, -3, 1, 2, 4,$$
$$6, 8, 10, 12, 15, 16, 18, 22 .$$

On peut aussi montrer qu'en revanche, outre 0 et -1, les valeurs suivantes de m ne conviennent pas:

— les entiers $-57, -27, -21, -15, -12, -11, -7, -6, -5, 3, 9, 15, 45$ (à cause de $p = 3$),

— les entiers $-2695, -385, -343, -336, -133, -105, -91, -70, -63, -56, -55, -43, -35, -31, -28, -25, -21, -13, 5, 7, 14, 35, 49, 140, 252, 287, 329, 2639$ (à cause du Mersenne 7),

De façon générale, pour chaque Mersenne p, ne conviennent pas:

— les entiers $m = r(p-1) - p$, où SUPP $[(r(r+p)] \subseteq$ SUPP $(p-1)$, entiers qui sont premiers avec p. En particulier, pour $r = -1, -p-1, -p+1$ on obtient $-p^2 - p + 1, -p^2 + p - 1$ et $-2p + 1$).

— les entiers $m = p[r(p-1)-1]$ où SUPP $[(r(r+1)] \subseteq$ SUPP $[p(p-1)]$. En particulier, on peut prendre $r = -9, -4, -3, -2, 1, 2, 3, 8, p, -p, p-1, -p-1, p^2-1, -p^2$, d'où les valeurs suivantes de m:

$$-p[p^2(p-1)+1], -p^3, -p[p(p-1)+1], -p(9p-8), -p(4p-3),$$
$$-p(3p-2), -p(2p-1), -p(p+2), -p(p+1), p, p^2, p(p-2), p(2p-3),$$
$$p(3p-4), p(8p-9), p(2p-3), p[p(p-1)+1], p^2(p-2)+1, p[(p+1)(p-1)^2-1] .$$

etc.

2.13. Le symbole de Legendre qui indique qu'un entier x est résidu quadratique modulo un entier premier p est noté $\left(\frac{x}{p}\right)$.

Nous aurons besoin au § 7 du lemme suivant, combinaison du *critère d'Euler* (qui caractérise les résidus quadratiques modulo les premiers) et du Théorème de Dirichlet:

LEMME. *Soit x un entier impair et p un diviseur premier de x. Il existe un entier premier q, qui ne divise pas x, tel que* $\left(\frac{p}{q}\right) = -1$

et $\left(\frac{p'}{q}\right) = +1$ *pour tout* $p' \in \mathrm{SUPP}(x)\backslash\{p\}$.

Par suite, $\left(\frac{x}{q}\right) = (-1)^{\alpha}$, *où* α *est l'exposant de* p *dans la décomposition primaire de l'entier* x.

Preuve. Soit s l'un des $(p-1)/2$ entiers qui ne sont pas résidus quadratiques modulo l'entier p. Considérons le système de congruences suivant:

$$z \equiv 1 \pmod 4, \quad z \equiv 1 \pmod{x/p^{\alpha}}, \quad z \equiv s \pmod p.$$

Le Théorème des restes chinois et le Théorème de Dirichlet montrent qu'il existe un entier premier $q > x$ solution de ce système.

Soit $p' \in \mathrm{SUPP}(x)\backslash\{p\}$. Comme $q > x$, on a $q \neq p'$. D'autre part, puisque $q \equiv 1 \pmod 4$, on voit que l'entier $(q-1)(p'-1)/4$ est pair pour tout $p' \in \mathrm{SUPP}(x)\backslash\{p\}$. La loi de réciprocité quadratique assure donc

$$\left(\frac{p'}{q}\right) = \left(\frac{q}{p'}\right).$$

La condition $q \equiv s \pmod p$ conduit à $\left(\frac{q}{p}\right) = \left(\frac{s}{p}\right) = -1$ puisque s n'est pas un résidu quadratique modulo p. Ainsi, on a $\left(\frac{p}{q}\right) = -1$. La condition $q \equiv 1 \pmod{p'}$ nous assure que $\left(\frac{p'}{q}\right) = \left(\frac{q}{p'}\right) = +1$. Le caractère multiplicatif du symbole de Legendre montre alors que:

$$\left(\frac{x}{q}\right) = \left(\frac{p^{\alpha}}{q}\right) \times \left(\frac{x/p^{\alpha}}{q}\right) = (-1)^{\alpha},$$ ce qui achève la démonstration.

2.14. Nous aurons besoin au § 9 de caractériser l'égalité en termes de division vue modulo un entier fixé. Si $v > 0$, nous notons $\mathrm{Quot}(u, v)$ et $\mathrm{Reste}(u, v)$ les quotient et reste de la division euclidienne de u par v.

LEMME. *Soient* x, y, α *des entiers positifs ou nuls. Si* $\alpha \geqslant 3$ *et* $y - x \geqslant 2$ *alors il existe un entier premier* $p \neq \alpha$ *tel que* $p\mathrm{Quot}(x, p) \not\equiv p\mathrm{Quot}(y, p) \pmod{\alpha}$.

Preuve. 1°) Des inégalités $\mathrm{Quot}(t, p) \leqslant t/p < \mathrm{Quot}(t, p) + 1$ on déduit

$$|\mathrm{Quot}(y, p) - \mathrm{Quot}(x, p)| - 1 < |y - x|/p < |\mathrm{Quot}(y, p) - \mathrm{Quot}(x, p)| + 1.$$

On a donc

$$|\operatorname{Quot}(y,p) - \operatorname{Quot}(x,p)| - 1 \leqslant \operatorname{Quot}(|y-x|,p) < |\operatorname{Quot}(y,p) - \operatorname{Quot}(x,p)| + 1,$$

d'où

$$\operatorname{Quot}(|y-x|,p) = |\operatorname{Quot}(y,p) - \operatorname{Quot}(x,p)| + \varepsilon, \quad \text{où} \quad \varepsilon \in \{-1, 0\}.$$

2°) Nous traitons d'abord le cas où $y - x \geqslant 8$. Nous utiliserons le Théorème de Tchebycheff sur l'existence d'un premier strictement compris entre x et $2x$ (ceci pour $x \geqslant 2$).

Si $y - x \geqslant 8$ alors il existe des premiers p et q tels que $(y-x)/4 < q < (y-x)/2 < r < y - x$. On a donc $2 < (y-x)/q < 4$, $1 < (y-x)/r < 2$, d'où $\operatorname{Quot}(y-x, q) = 1$ et $\operatorname{Quot}(y-x, r) = 3$.

Le point 1°) montre alors que

$$\operatorname{Quot}(y,r) - \operatorname{Quot}(x,r) = 1 - \varepsilon \in \{1, 2\}$$
$$\text{et} \quad \operatorname{Quot}(y,q) - \operatorname{Quot}(x,q) = 1 - \varepsilon \in \{3, 4\}.$$

3°) On déduit de ce qui précède que

$$q\operatorname{Quot}(x,q) - q\operatorname{Quot}(y,q) \in \{3q, 4q\} \quad \text{et} \quad r\operatorname{Quot}(x,r) - r\operatorname{Quot}(y,r) \in \{r, 2r\}$$

Observons que $\{2, 3, 4, q, 2q, 3q, 4q\} \cap \{2, r, 2r\} = \{2\}$ car r et q sont premiers et $2 < q < r$. Comme $\alpha \neq 2$, on voit que les deux cas suivants sont exhaustifs.

1er cas : $\alpha \notin \{2, 3, 4, q, 2q, 3q, 4q\}$.

L'entier α ne divise alors ni $3q$ ni $4q$. On peut choisir pour p l'entier q puisque $q \neq \alpha$ et $q\operatorname{Quot}(y,q) - q\operatorname{Quot}(x,q) \not\equiv 0 \pmod{\alpha}$.

2e cas : $\alpha \notin \{2, r, 2r\}$.

L'entier α ne divise alors ni r ni $2r$. On peut choisir pour p l'entier r puisque $r \neq \alpha$ et $r\operatorname{Quot}(y,r) - r\operatorname{Quot}(x,r) \not\equiv 0 \pmod{\alpha}$.
Ceci achève la preuve dans l'hypothèse $y - x \geqslant 8$.

4°) Supposons maintenant $y = x + 2$. Comme $\alpha \geqslant 3$ on a $2\operatorname{Quot}(y,2) - 2\operatorname{Quot}(x,2) = 2 \not\equiv 0 \pmod{\alpha}$ et on peut prendre pour p l'entier 2.

5°) Supposons maintenant $y = x + i$, i premier, $i \geqslant 3$ (ce qui règlera les cas $y - x = 3, 5, 7$). On a alors $i\operatorname{Quot}(y,i) - i\operatorname{Quot}(x,i) = i$.
Si $\alpha \neq i$ alors on peut choisir pour p l'entier i.
Si $\alpha = i$ alors $2\operatorname{Quot}(y,2) - 2\operatorname{Quot}(x,2) \in \{2[i/2], 2([i/2]+1)\}$, ensemble

qui ne contient pas i car i est un premier impair. Ainsi, on peut choisir pour p l'entier 2.

6°) Supposons maintenant $y = x + 4$. On a alors

$$2\text{Quot}(y, 2) - 2\text{Quot}(x, 2) = 4 .$$

Si $\alpha \neq 4$ alors on peut choisir pour p l'entier 2 (car on a toujours $\alpha \neq 2$).
Si $\alpha = 4$ alors $3\text{Quot}(y, 3) - 3\text{Quot}(x, 3) \in \{3, 6\}$, ensemble qui ne contient pas 4. On peut alors choisir pour p l'entier 3.

7°) Supposons enfin $y = x + 6$. On a alors $2\text{Quot}(y, 2) - 2\text{Quot}(x, 2) = 6$ et $5\text{Quot}(y, 5) - 5\text{Quot}(x, 5) \in \{5, 10\}$. Comme $\alpha \neq 2$, α ne peut pas diviser 6 et l'un d'entre 5 et 10. Ainsi, on peut donc prendre pour p l'une au moins des valeurs 2 ou 5.

Le Lemme précédent permet d'établir le résultat suivant :

PROPOSITION. *Soient* x, y, α *des entiers positifs ou nuls.*

1°) *Les conditions suivantes sont équivalentes :*

i) $x = y$.

ii)$_\alpha$ (*où* $\alpha \geqslant 3$) $\text{Reste}(x, p) \equiv \text{Reste}(y, p) \pmod{\alpha}$ *pour tout premier* $p \neq \alpha$.

iii)$_\alpha$ (*où* $\alpha \geqslant 3$) $\text{Quot}(x, p) \equiv \text{Quot}(y, p) \pmod{\alpha}$ *pour tout premier* $p \neq \alpha$ *et* $|y - x| \neq 1$.

iv)$_\alpha$ (*où* $\alpha \geqslant 3$) $p\text{Quot}(x, p) \equiv p\text{Quot}(y, p) \pmod{\alpha}$ *pour tout premier* $p \neq \alpha$ *et* $|y - x| \neq 1$.

Preuve de la Proposition.

1°) Le Lemme précédent se traduit immédiatement par l'implication iv)$_\alpha \Rightarrow$ i).

2°) Observons que si $p > z$ alors $\text{Reste}(z, p) = z$. Ainsi, considérant un premier p supérieur à α, x et y, on voit que ii)$_\alpha$ implique $x \equiv y \pmod{\alpha}$.

3°) L'égalité $x = p\text{Quot}(x, p) + \text{Reste}(x, p)$ montre immédiatement que si

$$x \equiv y \pmod{\alpha} \quad \text{et} \quad \text{Reste}(x, p) \equiv \text{Reste}(y, p) \pmod{\alpha}$$

alors

$$p\text{Quot}(x, p) \equiv p\text{Quot}(y, p) \pmod{\alpha} .$$

Par ailleurs, la condition $x \equiv y \pmod{\alpha}$ implique $|y - x| \neq 1$.
Ceci montre que ii)$_\alpha \Rightarrow$ iv)$_\alpha$.

4°) On conclut en remarquant que les implications i) $\Rightarrow$ ii)$_\alpha$, i) $\Rightarrow$ iii)$_\alpha$, iii)$_\alpha \Rightarrow$ iv)$_\alpha$ sont toutes triviales.

Remarques. 1°) La restriction $|y - x| \neq 1$, triviale dans ii)$_\alpha$, ne peut être omise dans iii)$_\alpha$. En fait, les conditions suivantes sont équivalentes:

A) $y = x + 1$ et $p\mathrm{Quot}(x, p) \equiv p\mathrm{Quot}(y, p) \pmod{\alpha}$ pour tout premier $p \neq \alpha$;

B) $(x, y) = (0, 1)$ ou bien α est premier et $(x, y) = (\alpha^k - 1, \alpha^k)$ pour un $k \geqslant 1$.

2°) Le statut des assertions ii)$_2$, iii)$_2$ et iv)$_2$ reste ouvert. On note cependant qu'elles ne sont équivalentes à i) puisque

$$\mathrm{Quot}(0, p) = \mathrm{Quot}(2, p) = 0 \text{ pour tout premier } p \neq 2.$$
$$\mathrm{Reste}(0, p) \equiv \mathrm{Reste}(2, p) \pmod{2} \text{ pour tout premier } p.$$

§ 3. Préliminaires de logique

3.1. Les *langages formels logiques* que nous considérerons sont ceux, dits *du premier ordre*, qui ne comportent qu'un seul type de variables. Dans le cadre arithmétique auquel nous nous intéressons, ces variables sont alors destinées à varier sur l'ensemble **N** des seuls entiers naturels et non sur les ensembles, relations ou fonctions sur **N**.

Ainsi, les formules ne permettent de traduire que les seules quantifications sur les entiers et non sur les relations ou fonctions comme il est usuel et tacite de le faire en mathématiques (en particulier dans les définitions par induction).

Un langage logique du premier ordre L est caractérisé par une liste de symboles spécifiques à chacun desquels est attaché un caractère relationnel ou fonctionnel ainsi qu'une arité (i.e. le nombre des arguments). En pratique, on désignera un langage L par la simple liste de ses symboles spécifiques fonctionnels puis relationnels, omettant d'expliciter les arités (rendues évidentes par le contexte).

A partir des variables on construit les termes de L par « composition » des symboles fonctionnels. Par « application » des symboles relationnels aux termes, on obtient les formules atomiques. Les opérations de négation, conjonction, implication et quantifications appliquées aux formules atomiques donnent enfin les formules de L.

3.2. Soit $L = (f_1, ..., f_m; R_1, ..., R_n)$ un langage du premier ordre.

Une *structure* $\Omega = \langle X; \varphi_1, ..., \varphi_m; \rho_1, ..., \rho_n \rangle$ du langage L est la donnée

— d'un ensemble de base X,

— de fonctions $\varphi_1, ..., \varphi_m$ sur X qui interprètent les symboles fonctionnels du langage L (en respectant le nombre d'arguments de ces symboles),

— de relations $\rho_1, ..., \rho_n$ sur X qui interprètent les symboles relationnels du langage L (en respectant le nombre d'arguments de ces symboles).

Une relation ρ à k arguments sur X est dite *Ω-définissable* lorsqu'il existe une formule $F(x_1, ..., x_k)$ du langage L pour laquelle on a l'équivalence suivante :

un k-uplet $(a_1, ..., a_k)$ *d'éléments de* X *est dans* ρ *si structure* Ω *satisfait la formule* F *au point* $(a_1, ..., a_k)$.

Une fonction est dite *Ω-définissable* lorsque son graphe est une relation *Ω-définissable*.

3.3. *Remarque.* Par un abus commode et usuel, on confond souvent une structure de base $\mathbf{N}$ avec le langage associé $L = (f_1, ..., f_m; R_1, ..., R_n)$.

En particulier, les symboles du langage logique pour les prédicats et fonctions *(syntaxe)* d'une telle structure sont alors confondus avec ceux désignant les relations et fonctions qui les interprètent dans $\mathbf{N}$ *(sémantique)*.

Ainsi, les lettres S, $+$, $\times$, $=$, $\perp$, $|$ désignent tant les fonctions successeur, addition et multiplication, les relations d'égalité, de coprimarité et de divisibilité que les symboles de fonctions et de relations associés dans un langage formel logique.

Les expressions « *le langage* $(\varphi_1, ..., \varphi_m; \rho_1, ..., \rho_n)$ *définit...* » et « *la structure* $\langle \mathbf{N}; \varphi_1, ..., \varphi_m; \rho_1, ..., \rho_n \rangle$ *définit...* » sont donc synonymes.

3.4. *Remarques.* 1°) Il est important d'observer que nous considérons aussi des structures qui peuvent ne pas contenir la relation d'égalité (et donc des langages sans symbole d'égalité). C'est le cas de la structure $\langle \mathbf{N}; S; \perp \rangle$, notée aussi $(S; \perp)$, qui est le sujet principal d'intérêt de ce travail.

2°) Toute structure doit cependant contenir au moins une relation afin qu'il y puisse être défini quelque chose. En termes de langage, on voit que, sans symbole relationnel, le discours logique ne permet pas d'exprimer des propriétés et de décrire des relations et fonctions sur une structure mais ne peut que se borner à nommer des objets de celle-ci. Autrement dit, sans symbole relationnel il n'y a que des termes et pas de formules.

3.5. Une fonction φ et la relation $Gr(\varphi)$ constituée par son graphe ne sont pas, en général, équivalentes quant au pouvoir de définissabilité. Tout ce qui

est définissable dans la structure $\langle X ; \varphi_1, ..., \varphi_m ; \rho_1, ..., \rho_n, Gr(\varphi)\rangle$ l'est aussi dans la structure $\langle X ; \varphi_1, ..., \varphi_m, \varphi ; \rho_1, ..., \rho_n\rangle$. Si cette dernière structure permet de définir la relation d'égalité alors la réciproque est vraie. Dans le cas général, elle est fausse. Par exemple, considérant le graphe de la multiplication, on voit que :

— l'égalité est définissable dans toute structure $\langle \mathbf{N} ; Gr(\times), ...\rangle$ par la formule

$$\forall u \forall v [Gr(\times)(x, u, v) \leftrightarrow Gr(\times)(y, u, v)] .$$

— mais elle ne l'est pas dans la structure $\langle \mathbf{N} ; \times ; \perp\rangle$ (cf. l'exemple 3.9 ci-dessous).

3.6. La classe des relations définissables dans une structure peut aussi se définir en termes ensemblistes à l'aide des notions introduites ci-dessous.

On note $\mathrm{Proj}_{p,\{i_1,...,i_q\}}$ la fonction projection $(x_1, ..., x_p) \mapsto (x_{i_1}, ..., x_{i_q})$ de X^p dans X^q, où $1 \leqslant i_1 < ... < i_q \leqslant p$.

Si σ est une fonction de $\{1, 2, ..., q\}$ dans $\{1, 2, ..., p\}$, on appelle fonction de brassage la fonction $f_\sigma : (x_1, ..., x_p) \mapsto (x_{\sigma(1)}, ..., x_{\sigma(q)})$ qui envoie X^p dans X^q. Ces fonctions de brassage permettent d'ajouter de nouvelles variables (cas où $q \leqslant p$ et σ est l'injection canonique de $\{1, 2, ..., q\}$ dans $\{1, 2, ..., p\}$), de démultiplier certaines variables (cas où $q > p$), de permuter les variables (cas où $p = q$ et σ est une permutation de $\{1, 2, ..., p\}$), ou encore d'identifier certaines variables (cas où σ n'est pas injective).

PROPOSITION. 1°) *La classe des relations définissables dans une structure* Ω *de base* X *est la plus petite classe* $\mathfrak{R}$ *de relations sur* X *telle que :*

i) *Les relations* $\rho_1, ..., \rho_n$ *sont dans* $\mathfrak{R}$, *ainsi que toutes leurs images réciproques par les fonctions qui sont des composées des fonctions* $\varphi_1, ..., \varphi_m$ *et des fonctions de brassage.*

ii) *La classe* $\mathfrak{R}$ *est stable par les opérations booléennes.*

iii) *La classe* $\mathfrak{R}$ *est stable par image directe des fonctions projections.*

2°) *Cette classe* $\mathfrak{R}$ *est stable par image réciproque des fonctions qui sont des composées des fonctions* $\varphi_1, ..., \varphi_m$ *et des fonctions de brassage.*

Les conditions i) à iii) traduisent la construction des formules du langage L :

— les formules atomiques correspondent à la condition i),

— les connecteurs des formules correspondent aux opérations booléennes,

— toute quantification existentielle correspond à une projection.

3.7. *Remarque.* Cette caractérisation ensembliste de la notion de définissabilité dans une structure Ω se simplifie dans le cas où la relation d'égalité sur X est Ω-définissable; on peut alors remplacer la condition i) par la condition plus simple suivante:

i*) *Les relations* $\rho_1, ..., \rho_n$ *et les graphes des fonctions* $\varphi_1, ..., \varphi_m$ *sont tous dans* $\mathfrak{R}$, *ainsi que leurs produits par des* X^k.

3.8. Une méthode commode, dite de Beth & Padoa (cf. [BE]), pour montrer des résultats de non-définissabilité est fondée sur le résultat suivant, dû à Svenonius (cf. [PB] p. 241).

PROPOSITION. *Soit* $\Omega = \langle \mathbf{N}; \varphi_1, ..., \varphi_m; \rho_1, ..., \rho_n, \rho \rangle$ *une structure du langage* $L = (f_1, ..., f_m; R_1, ..., R_n, R)$.

1°) *Les trois conditions suivantes sont équivalentes:*

i) *La relation* ρ *n'est pas définissable (par une formule du langage réduit* $L\backslash\{R\}$*) dans la structure réduite* $\langle \mathbf{N}; \varphi_1, ..., \varphi_m; \rho_1, ..., \rho_n \rangle$.

ii) *Il existe une structure* $\Theta = \langle X; \psi_1, ..., \psi_m; \tau_1, ..., \tau_n, \tau \rangle$ *et une fonction* ξ *de* X *dans* X *telles que*

— *les deux structures* Ω *et* Θ *vérifient exactement les mêmes énoncés du langage* L;

— *la fonction* ξ *ne respecte pas la relation* τ *mais respecte les relations* τ_i *et leurs images réciproques par les fonctions qui sont des composées des fonctions* ψ_j *et des fonctions de brassage (cf. 3.6) (c'est le cas, par exemple, si* ξ *respecte les relations* τ_i *et les fonctions* ψ_j*).*

iii) *Il existe une structure* $\Theta = \langle X; \psi_1, ..., \psi_m; \tau_1, ..., \tau_n, \tau \rangle$ *et une bijection* ξ *de* X *dans* X *telles que*

— *les deux structures* Ω *et* Θ *vérifient exactement les mêmes énoncés du langage* L;

— *la fonction* ξ *respecte les relations* τ_i *et les fonctions* ψ_i *mais pas la relation* τ.

(i.e. ξ *est un automorphisme de la structure réduite*

$$\Theta = \langle X; \psi_1, ..., \psi_m; \tau_1, ..., \tau_n \rangle$$

mais pas de la structure Θ*).*

2°) *Dans le cas où la relation* ρ_i *est la relation d'égalité sur* $\mathbf{N}$, *alors*

on peut aussi faire en sorte que la relation τ_i *précédente soit la relation d'égalité sur* X.

Remarque. Si ρ est l'égalité sur $\mathbf{N}$, alors ou bien ξ n'est pas injective, ou bien la relation τ de la condition iii) n'est pas l'égalité sur X.

Exemples. 1°) On voit que le langage réduit à l'égalité et à la multiplication ne définit pas l'ordre (ni — a fortiori — l'addition) sur $\mathbf{N}$ en considérant

— la structure $\Theta = \langle \mathbf{N}; \times; =, < \rangle$

— et la bijection ξ de $\mathbf{N}$ sur $\mathbf{N}$ définie comme suit: $\xi(x)$ s'obtient à partir de x en échangeant, dans la décomposition de Gauss, les exposants de 2 et 3 et en laissant inchangés les autres.

2°) On voit que le langage réduit à l'égalité et au successeur ne définit pas l'ordre en considérant

— la structure $\Theta = \langle X; f, =, < \rangle$ suivante du langage $(S; =, <)$ où

$$X = \{ \sum_{0 \leqslant i \leqslant n} 2^{-i} : n \in \mathbf{N} \} \cup \{ 2 + \sum_{-\infty < i \leqslant n} 2^{-|i|} : n \in \mathbf{Z} \} \cup \{ 5 + \sum_{-\infty < i \leqslant n} 2^{-|i|} : n \in \mathbf{Z} \},$$

$=$ et $<$ sont les relations d'égalité et d'ordre usuelles sur les réels,

$$f : X \mapsto X, \quad f(a + \sum_{i \leqslant n} 2^{-|i|}) = a + \sum_{-i \leqslant n+1} 2^{-|i|}$$

où $(a, n) \in [\{1\} \times \mathbf{N}] \cup [\{2\} \times \mathbf{Z}] \cup [\{5\} \times \mathbf{Z}]$

(cette structure Θ satisfait les mêmes énoncés que $\langle \mathbf{N}; S, =, < \rangle$);

— et l'involution σ qui échange $2 + \Sigma$ avec $5 + \Sigma$ et laisse invariants les autres points de X.

3°) On voit que le langage réduit à la multiplication et à la coprimarité ne définit pas l'égalité en considérant

— la structure $\Theta = \langle \mathbf{N}; \times; =, \perp \rangle$

— et la fonction ξ de $\mathbf{N}$ sur $\mathbf{N}$ définie comme suit: $\xi(x)$ est le produit des facteurs premiers de x, i.e. ξ réduit à 1 les exposants des primaires dans la décomposition de Gauss de x.

3.9. Contrairement à ce qu'on peut penser a priori, il n'est pas toujours trivial de montrer que la relation d'égalité est définissable dans une structure (cf. 4.8 et le § 5).

Par exemple, la définissabilité de l'égalité dans chacune des structures $\langle \mathbf{N}; +; \perp \rangle$, $\langle \mathbf{N}; S, \times; \perp \rangle$ et $\langle \mathbf{N}; \mathrm{Pred}, \times; \perp \rangle$ (où Pred est la fonction prédécesseur, qui vaut 0 en 0) nécessite les équivalences suivantes (conséquences non triviales des Corollaires de 2.8 et 2.6) entre les conditions:

i) x et y sont égaux;

ii) pour tout $m \geqslant 0$, on a $\mathrm{SUPP}(x+m) = \mathrm{SUPP}(y+m)$;

iii) $\mathrm{SUPP}(x) = \mathrm{SUPP}(y)$ et, pour tout $m \geqslant 0$, on a $\mathrm{SUPP}(mx+1) = \mathrm{SUPP}(my+1)$;

iv) $\mathrm{SUPP}(x) = \mathrm{SUPP}(y)$, x et y sont simultanément nuls ou non nuls, et, pour tout $m \geqslant 0$, on a $\mathrm{SUPP}[\mathrm{Pred}(mx-1] = \mathrm{SUPP}[\mathrm{Pred}(my-1)]$;

Ces conditions se traduisent par des formules des langages $(+; \perp)$ et $(S, \times; \perp)$:

$$\forall i \forall p \, \{[p \perp (x+i)] \leftrightarrow [p \perp (y+i)]\},$$

$$\forall p \, [(p \perp x) \leftrightarrow (p \perp y)] \wedge \forall m \forall p \, \{[p \perp S(m \times x)] \leftrightarrow [p \perp S(m \times y)]\},$$

$$A(x, y) \wedge \forall p \, [(p \perp x) \leftrightarrow (p \perp y)] \wedge \forall m \forall p \, \{[p \perp \mathrm{Pred}(m \times x)] \leftrightarrow [p \perp \mathrm{Pred}(m \times y)]\}$$

où A est la formule [Zéro $(x) \leftrightarrow$ Zéro (x)], Zéro (x) étant la formule $\forall u(x \times u = x)$.

3.10. Pour conclure cette revue des notions de Logique utilisées dans cette étude, nous précisons la notion — usuelle mais implicite en général — d'*extension par définitions* d'une structure (ou d'un langage).

Soit Ω une structure de base $\mathbf{N}$ du langage L et soient $\psi_1, ..., \psi_p$ des relations sur $\mathbf{N}$ et $\tau_1, ..., \tau_q$ des fonctions sur $\mathbf{N}$ qui sont définissables dans la structure Ω (par des formules du langage L).

Il est commode de considérer

— la structure Ω' obtenue en rajoutant à Ω ces relations et fonctions ψ_i et τ_j;

— le langage L' associé à Ω', obtenu en rajoutant au langage L de nouveaux symboles de relation et fonction $R_1, ..., R_p$ et $f_1, ..., f_p$.

PROPOSITION. *A toute formule* $F(x_1, ..., x_k)$ *du langage* L' *on peut associer une formule du langage* L, *notée* $\mathrm{Trad}[F](x_1, ..., x_k)$, *de sorte que la relation sur* $\mathbf{N}$ *définie par* $F(x_1, ..., x_k)$ *dans la structure* Ω' *coïncide avec celle définie dans la structure* Ω *par* $\mathrm{Trad}[F](x_1, ..., x_k)$.

Remarque. Comme il a déjà été dit en 3.3, nous utiliserons — abusivement — souvent les notations ψ_i et τ_j au lieu de R_i et f_j.

§ 4. Autour du problème de J. Robinson

4.1. Rappelons, avant d'en venir aux premiers résultats concernant le problème de JR, dans quelle problématique logique celui-ci s'est posé.

Ce problème relève de l'étude du pouvoir d'expression des langages faibles de l'arithmétique du premier ordre de $\mathbf{N}$ et de $\mathbf{Z}$. Il s'agit de savoir ce qui peut s'exprimer dans les structures arithmétiques formées de prédicats et fonctions dont la portée est — a priori — réduite.

4.2. Le premier résultat spectaculaire dans ce domaine de la définissabilité remonte à la thèse du logicien K. Gödel :

Théorème (Gödel, 1931). *La classe des fonctions et relations qui sont définissables dans la structure* $\langle \mathbf{N}; +, \times; = \rangle$ *par des formules du premier ordre du langage associé* $(+, \times; =)$ *est stable par le procédé de construction par récurrence.*

Ce résultat permet de voir que toutes les fonctions et relations arithmétiques de la pratique mathématique sont définissables (au premier ordre) à partir de l'addition, la multiplication et l'égalité.

Ainsi,

La structure $\langle \mathbf{N}; +, \times; = \rangle$ *est la structure logique essentielle de l'arithmétique ;* l'objet de l'étude des langages faibles est donc de déterminer la part de cette structure que l'on peut retrouver à partir d'eux.

Remarque. Pour saisir la portée du résultat de Gödel, il convient d'observer que le procédé de construction par récurrence

— n'est pas une définition explicite d'une fonction f à partir d'autres fonctions,

— mais une caractérisation d'une fonction f comme l'unique solution d'un système d'équations fonctionnelles.

Pour traduire une telle caractérisation en termes de formule logique il est nécessaire — a priori — d'utiliser des quantifications portant sur les fonctions et non sur les entiers seulement.

On pourra aussi se rendre compte de la force de ce résultat en essayant de définir directement l'exponentielle ou l'énumération des entiers premiers par des formules du premier ordre du langage $(+, \times; =)$.

4.3. Ce résultat de K. Gödel a reçu sa forme optimale dans la solution du 10-ième problème de Hilbert, achevée en 1972 (cf. [DM]) et due à

J. Robinson, M. Davis, H. Putnam et Y. Matijacevitch. Ils montrèrent que toute partie récursive (c'est-à-dire algorithmiquement reconnaissable) de $\mathbf{N}^k$ est diophantienne et peut donc être définie par une formule du type suivant:

$$\exists y_1 \ldots \exists y_n [P(y_1, \ldots, y_n, x_1, \ldots, x_k) = Q(y_1, \ldots, y_n, x_1, \ldots, x_k)]$$

où P et Q sont des polynômes à coefficients dans $\mathbf{N}$.

4.4. Bien entendu, des langages trop réduits ne permettent pas en général de retrouver toutes les relations et fonctions usuelles de l'arithmétique. Ainsi, comme il a été vu en 3.8,

— l'égalité et le successeur ne suffisent pas à définir l'ordre,

— l'égalité et l'ordre ne suffisent pas à définir l'addition,

— l'égalité et l'addition ne suffisent pas à définir la multiplication,

— l'égalité et la multiplication ne suffisent pas à définir l'addition (ni même l'ordre).

En revanche, l'équivalence:

$$(xz-1)(yz-1) = [z^2(xy+1)] + 1 \quad \text{si et seulement si} \quad z = 0 \text{ ou } x + y = z$$

montre que l'on peut définir l'addition avec le successeur en plus de l'égalité et de la multiplication, résultat observé par A. Tarski (cf. [TA]).

Une formule convenable du langage $(S, \times ; =)$ est

$$[\{\text{Zéro}(x) \cdot \text{Zéro}(y)\} \leftrightarrow \text{Zéro}(z)] \wedge [S(x \times z) \times S(y \times z) = S[(z \times z) \times S(x \times y)]]$$

où Zéro(x) est la formule $\forall u(x \times u = x)$.

4.5. Le premier résultat d'importance relatif aux langages plus réduits que le langage $(+, \times ; =)$ a été obtenu par J. Robinson dans sa thèse, publiée en 1949 (cf. [RJ]):

L'addition et la multiplication sont définissables dans la structure $\langle \mathbf{N}; S; | \rangle$.

Bien sûr, l'égalité est déjà définissable de façon triviale dans la structure $\langle \mathbf{N}; | \rangle$ par la formule $(x|y) \wedge (y|x)$. Ainsi,

THÉORÈME (J. Robinson, 1948). *Les structures* $\langle \mathbf{N}; S; | \rangle$ *et* $\langle \mathbf{N}; +, \times ; = \rangle$ *définissent les mêmes relations et fonctions.*

Preuve (esquissée). L'argument de J. Robinson est fondé sur l'équivalence suivante (elle-même conséquence simple du Théorème de Dirichlet, cf. 2.2): $z = xy$ si et seulement si pour tout premier p ne divisant ni x

ni y, il existe x' et y', premiers entre eux et premiers avec x et y et vérifiant les équations de congruence

$$xx' \equiv -1 \pmod{p}, \quad yy' \equiv -1 \pmod{p} \quad \text{et} \quad zx'y' \equiv 1 \pmod{p}.$$

Comme la fonction ppcm est définissable dans la structure $\langle \mathbf{N}; | \rangle$ et donne le produit de deux entiers premiers entre eux, on voit simplement que cette condition permet de définir la multiplication avec S et $|$. On conclut à l'aide de 4.4.

J. Robinson montre aussi que l'ensemble $\mathbf{N}$ est définissable en termes d'addition et de multiplication dans le corps $\mathbf{Q}$ des rationnels (c'est-à-dire que le fait, *pour un rationnel, d'être un entier naturel* est définissable au premier ordre dans le langage de l'arithmétique sur $\mathbf{Q}$). Ce dernier résultat est central dans l'étude des théories indécidables.

Dans ce même travail, et dans le but de trouver d'autres axiomatiques naturelles de l'arithmétique, J. Robinson pose la question qui nous intéresse ici :

PROBLÈME (J. Robinson). *Peut-on définir l'addition et la multiplication en termes d'égalité, successeur et coprimarité ?*

4.6. Les premiers résultats sur le problème de J. Robinson figurent dans la thèse d'A. Woods (cf. [WA]) soutenue en 1981. Celui-ci montre que

THÉORÈME (A. Woods, 1981). *Les structures* $\langle \mathbf{N}; <, \perp \rangle$ *et* $\langle \mathbf{N}; +, \times; = \rangle$ *définissent les mêmes relations et fonctions.*

On a vu (cf. 3.10) que l'égalité est définissable dans les structures $\langle \mathbf{N}; +; \perp \rangle$ et $\langle \mathbf{N}; S, \times; \perp \rangle$. Comme l'addition est définissable dans la structure $\langle \mathbf{N}; S, \times; = \rangle$ (cf. 4.4) et que la relation d'ordre $x < y$ est définissable dans la structure $\langle \mathbf{N}; +; = \rangle$ (par la formule $\exists i[(x+i)=y \wedge \neg(i+i=i)]$), on déduit le résultat suivant :

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

Remarque. 1°) En revanche, la structure $\langle \mathbf{N}; \times; =, \perp \rangle$ ne permet pas de définir l'addition. Ceci résulte de l'exemple 1 de 3.8 puisque la relation $\perp$ est déjà définissable dans la structure $\langle \mathbf{N}; \times; = \rangle$ et n'apporte donc rien de plus.

2°) Comme l'égalité est aussi définissable dans la structure $\langle \mathbf{N}; \mathrm{Pred}, \times ; \perp \rangle$ — où Pred est la fonction prédécesseur, qui vaut 0 en 0 — (cf. 3.9), cette structure permet de définir S et est donc passible du même Corollaire ci-dessus.

4.7. Dans le même travail, A. Woods relie ces problèmes de définissabilité logique à des problèmes ouverts d'arithmétique.

Il prouve aussi que, dans le problème de J. Robinson, l'égalité est superfétatoire (cf. 4.12 pour une preuve de ces résultats).

THÉORÈME (A. Woods). *Les assertions suivantes sont équivalentes:*

i) *Le problème de J. Robinson admet une réponse positive: on peut définir l'addition et la multiplication en termes d'égalité, coprimarité et fonction successeur.*

i)′ *On peut définir l'ordre* ou *l'addition* ou *la multiplication en termes d'égalité, coprimarité et fonction successeur.*

ii) *On peut définir l'égalité, l'addition et la multiplication en termes de coprimarité et fonction successeur.*

ii)′ *On peut définir l'ordre* ou *l'addition* ou *la multiplication en termes de coprimarité et fonction successeur.*

iii) *On peut définir l'égalité en termes de coprimarité et fonction successeur.*

iv) *La conjecture d'Erdös-Woods.*

Remarque. Comme S est une injection, il est équivalent de dire que S et $\perp$ définissent l'égalité ou de dire qu'ils définissent le graphe de S: en effet, $x = y$ si et seulement s'il existe z tel que (x, z) et (y, z) soient tous deux dans $Gr(S)$.

4.8. Rappelons la différence — quant au pouvoir de définissabilité — entre une fonction et la relation constituée par son graphe. Ainsi,

— La relation d'égalité est trivialement définissable à partir de chacun des *graphes* $Gr(S)$ et $Gr(\mathrm{Pred})$ des fonctions S et Pred par les formules suivantes:

$$\exists z[Gr(S)(x, z) \wedge Gr(S)(y, z)] \quad \text{et} \quad \exists z[Gr(\mathrm{Pred})(z, x) \wedge Gr(\mathrm{Pred})(z, y)] .$$

— La relation d'égalité n'est pas — a priori — définissable à partir de la relation $\perp$ et des *fonctions* S et Pred (cf. le Théorème ci-dessous).

— En présence de la relation d'égalité chacune des deux fonctions S et Pred permet de définir les deux graphes de S et de Pred.

Sans égalité il n'en est plus — a priori — de même.

Cependant, le Théorème de Woods reste valable en remplaçant la fonction S par Pred ou bien par S et Pred (cf. 4.12 pour une preuve).

THÉORÈME. *Les assertions du* Théorème 4.7 *sont également équivalentes aux suivantes :*

ii)bis *On peut définir l'égalité, l'addition et la multiplication en termes de coprimarité et fonction prédécesseur.*

ii)ter *On peut définir l'égalité, l'addition et la multiplication en termes de coprimarité et fonctions successeur et prédécesseur.*

Les versions ii)'bis, ii)'ter de ii)'.

iii)bis *On peut définir l'égalité en termes de coprimarité et fonction prédécesseur.*

iii)ter *On peut définir l'égalité en termes de coprimarité et fonctions successeur et prédécesseur.*

4.9. D'autres travaux récents sur le problème de J. Robinson figurent dans [RD1] :

THÉORÈME (D. Richard, 1985). *Toute relation définissable dans la structure* $\langle \mathbf{N}; +, \times, = \rangle$ et qui ne porte que sur les seuls entiers primaires *est également définissable dans la structure* $\langle \mathbf{N}; S; \perp \rangle$.

4.10. Le résultat suivant (dont la preuve est l'objet de 4.11 et du § 5 ci-dessous) est une version plus forte du Théorème 4.9, s'exprimant en termes des équivalences $\cong_A$ introduites en 2.10.

THÉORÈME. *Soit* ρ *une relation définissable dans la structure* $\langle \mathbf{N}; +, \times, = \rangle$.

1°) ρ *est définissable dans la structure* $\langle \mathbf{N}; S; \perp \rangle$ *si et seulement si elle est saturée par une relation* $\cong_A$, *où* A *est un ensemble* fini *d'entiers positifs ou nuls.*

2°) ρ *est définissable dans la structure* $\langle \mathbf{N}; \text{Pred}; \perp \rangle$ *si et seulement si elle est saturée par une relation* $\cong_A$, *où* A *est un ensemble* fini *d'entiers négatifs ou nuls.*

3°) ρ *est définissable dans la structure* $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$ *si et seulement si elle est saturée par une relation* $\cong_A$, *où* A *est un ensemble* fini *d'entiers de* $\mathbf{Z}$.

N.B. Comme toute relation sur les primaires est saturée pour $\cong_{\{0,1,2\}}$ et $\cong_{\{-2,-1,0\}}$ (cf. le Théorème 2.12), le Théorème 4.9, et son analogue relatif au langage $(S, \mathrm{Pred}; \perp)$, apparaît comme un corollaire de celui-ci.

4.11. La Proposition suivante donne le sens le plus facile à établir des équivalences du Théorème 4.10.

PROPOSITION. *Soit* ρ *une relation définissable dans* $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$ *(resp.* $\langle \mathbf{N}; S; \perp \rangle$, *resp.* $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$*); il existe une partie finie* A *de* $\mathbf{Z}$ *(resp. de* $\mathbf{N}$, *resp. de* $-\mathbf{N}$*) telle que* ρ *soit* $(\cong_A)$*-saturée.*

Preuve. Nous prouvons le cas de la définissabilité dans $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$, les deux autres sont analogues (en fait, plus simples).

Soit $\mathfrak{R}$ la famille des relations ρ pour lesquelles il existe une partie finie A de $\mathbf{Z}$ telle que ρ soit $(\cong_A)$-saturée. Il est clair que $\mathfrak{R}$ est stable par opérations booléennes et par projections (opérations qui correspondent aux connecteurs logiques et aux quantifications). Tout revient donc à montrer que $\mathfrak{R}$ contient les images réciproques de la relation $\perp$ par les fonctions composées des fonctions S et Pred avec les fonctions de brassage (cf. 3.6). (En termes logiques, ceci revient à montrer que $\mathfrak{R}$ contient les relations définies par les formules atomiques.) Comme $\mathrm{Pred} \circ S$ est l'identité, toute composée des fonctions S et Pred est de la forme $S^i \circ \mathrm{Pred}^j$. Il est à noter que $[S^i \circ \mathrm{Pred}^j](n) = i$ si $n \leqslant j$ et $[S^i \circ \mathrm{Pred}^j](n) = n + (i-j)$ si $n > j$; on ne peut donc pas simplifier cette fonction.

On voit facilement que, posant $A_{i,j} = \{-j, ..., 0\} \cup \{i-j\}$, si $x \cong_{A_{i,j}} y$ alors

— si $x \leqslant j$ ou $y \leqslant j$ alors $A_{i,j}$ contient $-x$ ou $-y$ et donc $x = y$ (cf. Fait 2.10, 3°)),

— $x + (i-j) \cong_{\{0\}} y + (i-j)$.

Il en résulte que $\mathrm{SUPP}[[S^i \circ \mathrm{Pred}^j](x)] = \mathrm{SUPP}[[S^i \circ \mathrm{Pred}^j](y)]$. Toute composée des fonctions S et Pred avec les fonctions de brassage (cf. 3.6) est de la forme $(x_1, ..., x_p) \mapsto (S^{i_1}[\mathrm{Pred}^{j_1}(x_{\sigma(1)})], ..., S^{i_q}[\mathrm{Pred}^{j_q}(x_{\sigma(q)})])$, où $\sigma : \{1, ..., q\} \mapsto \{1, ..., p\}$.

Il est clair que l'image réciproque de la relation $\perp$ par une telle fonction (nécessairement à valeurs dans $\mathbf{N}^2$, i.e. $q = 2$) est une relation $\cong_A$ saturée, où $A = A_{i_1, j_1} \cup A_{i_2, j_2}$.

Remarque. La preuve précédente montre, en fait, que si $p \geqslant 0$, $q \geqslant 0$ et si les termes figurant dans une formule $F(x, x_1, ..., x_k)$ et dans lesquels intervient effectivement la variable x sont tous de la forme $S^i[\mathrm{Pred}^j(x)]$ avec $j \leqslant p$ et $i - j \leqslant q$, alors la relation définie dans la structure $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$ par la formule $F(x, x_1, ..., x_k)$ est saturée en sa première variable pour la relation $\cong_{\{-p, ..., 0, ..., q\}}$ (i.e. si $\mathrm{SUPP}(a+i) = \mathrm{SUPP}(b+i)$ pour tout i dans $\{-p, ..., 0, ..., q\}$, alors, pour tout p-uplet $(c_1, ..., c_k)$, la structure $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$ satisfait la formule F au point $(a, c_1, ..., c_k)$ si et seulement si elle la satisfait au point $(b, c_1, ..., c_k)$).

4.12. *Preuve des Théorèmes 4.7 et 4.8*

Les résultats de Woods mentionnés en 4.6 (qui, ici, sont obtenus au § 9) montrent l'équivalence de i), ii), ii)bis, ii)ter) avec leurs versions primées.

On montre les implications

$$\begin{array}{ccccccc} & & & & \text{iii)} & \leftarrow & \text{ii)} \quad \rightarrow \text{ii)ter} \\ & & & & \downarrow & & \Uparrow \\ \text{ii)ter} & \rightarrow & \text{i)} & \Rightarrow & \text{iii)ter} & \Rightarrow & \text{iv)} \\ & & & & \uparrow & & \Downarrow \\ & & & & \text{iii)bis} & \leftarrow & \text{ii)bis} \quad \rightarrow \text{ii)ter} \end{array}$$

1°) Les implications notées par des flèches simples sont triviales.

2°) i) $\Rightarrow$ iii)ter est prouvée plus loin, c'est le Corollaire 6.6.

3°) iv) $\Rightarrow$ ii) et iv) $\Rightarrow$ ii)bis se prouve à l'aide du Théorème 4.10 (dont la preuve est donnée au § 5).

Appliquant la Remarque 2.10, la conjecture d'Erdös-Woods montre l'existence de k tel que les restrictions à $\mathbf{N}$ de $\cong_{\{0, ..., k\}}$ et $\cong_{\{-k, ..., 0\}}$ coïncident avec l'égalité. Toute relation sur $\mathbf{N}$ est alors — trivialement — saturée à la fois pour $\cong_{\{0, ..., k\}}$ et $\cong_{\{-k, ..., 0\}}$. Le Théorème 4.10 montre donc que toute relation est définissable avec S et $\perp$ ou bien Pred et $\perp$; c'est en particulier le cas de $=$, $+$ et $\times$.

4°) iii)ter $\Rightarrow$ iv) est une autre application du Théorème 4.10 (en fait, de sa partie facile qu'est la Propriété 4.11): si l'égalité est $(S, \mathrm{Pred}; \perp)$-définissable alors elle est saturée pour un certain $\cong_{\{-k, ..., k\}}$, ce qui implique (cf. Remarque 2.10) la conjecture d'Erdös-Woods.

Remarque. L'implication iv) ⇒ iii) peut se voir directement (sans passer par le Théorème 4.10). La conjecture d'Erdös-Woods, si elle est vraie, fournit la définition simple suivante de l'égalité dans le langage $(S; \perp)$:

$$\forall z[[z \perp x \leftrightarrow z \perp y] \wedge [z \perp S(x) \leftrightarrow z \perp S(y)] \wedge \ldots \wedge [z \perp S^k(x) \leftrightarrow z \perp S^k(y)]] .$$

Cette conjecture d'Erdös-Woods montre l'équivalence de l'égalité $x = y$ avec la condition suivante:

$x \geqslant k$ et $y \geqslant k$ et $\mathrm{SUPP}(x-i) = \mathrm{SUPP}(y-i)$ pour tout $i \in \{0, 1, \ldots, k\}$, ou bien x et y sont tous deux inférieurs à k et égaux.

Désignant par $\mathrm{Egal}_n(x)$ une formule qui définit $\{n\}$ dans la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$, on déduit alors de la condition précédente une définition simple de l'égalité dans la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$:

$$[\mathrm{Egal}_1(x) \leftrightarrow \mathrm{Egal}_1(y)] \wedge \ldots \wedge [\mathrm{Egal}_k(x) \leftrightarrow \mathrm{Egal}_k(y)]$$
$$\wedge \forall z[[z \perp x \leftrightarrow z \perp y] \wedge \ldots \wedge [z \perp \mathrm{Pred}^k(x) \leftrightarrow z \perp \mathrm{Pred}^k(y)]] .$$

4.13. Mentionnons enfin le résultat suivant qui étend à **Z** le Théorème 4.9 ci-dessus:

THÉORÈME. *Toute relation ou fonction arithmétique définie sur l'ensemble* ZPP *des primaires de* **Z** *et de leurs opposés est* $(S; \perp)$*-définissable.*

Remarquons que contrairement à ce qui peut sembler à première vue, le passage de **N** à **Z** n'a rien d'automatique. La preuve de ce résultat constitue d'ailleurs l'objet principal de l'article [RD2].

La difficulté principale est ici de reconnaître le signe d'un élément de ZPP. En particulier, on ne sait pas distinguer avec le langage $(S; \perp)$ si un diviseur premier de $x - 1$ divise $|x| - 1$ ou $|x| + 1$.

On peut voir (cf. [RD2]) que le Théorème précédent implique le Théorème 4.9. Il a aussi les Corollaires suivants.

1°) Une généralisation du Théorème de Woods:

L'arithmétique de **Z** (i.e. l'addition et la multiplication) est $(S; \perp)$-définissable sur **Z** si et seulement s'il existe un entier k (nécessairement $\geqslant 2$) tel que tout entier x de **Z** soit uniquement déterminé par les supports des entiers $x + 1, x + 2, \ldots, x + k$.

2°) La définissabilité de l'arithmétique de **Z** par successeur et divisibilité (question posée par J. Robinson dans l'article où elle prouve le résultat analogue sur **N**). Une preuve directe du même résultat se trouve aussi en [RD3].

3°) Des résultats nouveaux de définissabilité de l'addition et de la multiplication à partir de $(S, +; \perp)$ ou de $(<, \perp)$ sur $\mathbf{Z}$.

Il est à noter que S n'est pas définissable par addition et coprimarité sur $\mathbf{Z}$: en effet, $x \mapsto (-x)$ est un automorphisme de $\mathbf{Z}$ qui respecte $+$ et $\perp$ mais pas S.

§ 5. La méthode de codage ZBV et le problème de J. Robinson

5.1. *La méthode de codage* ZBV

Les Théorèmes ZBV et LC (cf. 2.2 et 2.3) et leur Corollaire 2.4 permettent des codages qui s'avèrent particulièrement performants dans l'étude du pouvoir de définissabilité des langages $(S; \perp)$ et $(\mathrm{Pred}; \perp)$.

La méthode de codage ZBV *consiste à considérer comme codes d'un entier x les supports ou bien les diviseurs primitifs des formes du type $p^x \pm 1$, où p est premier.*

On ramène ainsi certaines questions arithmétiques à la théorie des ensembles finis *de nombres premiers; en particulier, à des questions sur leur combinatoire.*

Par ailleurs, chaque ensemble fini de nombres premiers (ou fonction de domaine fini entre nombres premiers) est lui-même codable (de multiples façons) par un seul nombre premier via la méthode indiquée en 2.1 combinant le Théorème de Dirichlet et le Théorème des restes chinois. Un tel code joue alors le rôle de mémoire dans laquelle est stocké l'ensemble fini de premiers (ou la fonction) considéré(e).

5.2. Avant de passer à des applications de la méthode ZBV, nous montrons quelques résultats simples sur la mise en place dans la structure $\langle \mathbf{N}; \perp \rangle$ d'éléments d'une théorie des ensembles finis par le biais des supports d'entiers: l'ensemble de base est P, *chaque partie finie X de P est codée par les entiers ayant X pour support.*

La relation d'inclusion entre parties finies de P se traduit sur leurs codes par la relation $\mathrm{SUPP}(x) \subseteq \mathrm{SUPP}(y)$.

Comme cette inclusion entre supports a lieu si et seulement si tout entier premier avec y est premier avec x, on voit qu'elle se traduit dans la structure $\langle \mathbf{N}; \perp \rangle$ par la formule $\forall z[(z \perp y) \rightarrow (z \perp x)]$, notée $\mathrm{SUPP}(x) \subseteq \mathrm{SUPP}(y)$.

A partir de cette relation, on peut définir la relation d'égalité entre supports et les opérations ensemblistes d'union, intersection et différence des

supports. On obtient ainsi l'algèbre ensembliste élémentaire sur les parties finies de P.

5.3. On remarque ensuite qu'un entier x est primaire si et seulement si son support est inclus dans celui de tout entier non premier avec lui.

On en déduit alors des formules qui définissent dans $\langle \mathbf{N}; \perp \rangle$ l'ensemble PP des primaires et la relation $\{(x, y) : x$ et y sont des puissances d'un même premier$\}$. Notées respectivement $PP(x)$ et $PP(x, y)$, ce sont

$$\forall y\{[\neg(y \perp x)] \to \mathrm{SUPP}(x) \subseteq \mathrm{SUPP}(y)\} \quad \text{et} \quad PP(x) \wedge PP(y) \wedge \neg(x \perp y) \ .$$

On observe enfin que les ensembles $\{1\}$ et $\{0\}$ sont $\langle \mathbf{N}; \perp \rangle$-définis par les formules suivantes, notées respectivement $\mathrm{Egal}_1(x)$ et $\mathrm{Egal}_0(x)$:

$$\forall y(y \perp x) \quad \text{et} \quad \forall y[(y \perp x) \to \mathrm{Egal}_1(y)] \ .$$

On utilisera donc (cf. la Proposition 3.10) les constantes 0 et 1 dans le cadre de tout langage contenant $\perp$.

Remarque. L'exemple 1 de 3.8 permet de voir que les singletons $\{0\}$ et $\{1\}$ sont les seuls à pouvoir être définis dans $\langle \mathbf{N}; \perp \rangle$.

5.4. On peut définir très simplement le singleton $\{n\}$, $n \geqslant 2$, (et donc aussi toute relation finie) dans la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$ par la formule $\mathrm{Egal}_1[\mathrm{Pred}^{n-1}(x)]$, notée $\mathrm{Egal}_n(x)$.

On utilisera donc toutes les constantes entières dans le cadre du langage $\langle \mathrm{Pred}; \perp \rangle$.

5.5. Nous montrons maintenant des applications simples — et fondamentales — de la méthode ZBV.

Le Théorème 2.12 montre que pour des entiers primaires x et y, les trois conditions $x = y$, $x \cong_{\{0,1,2\}} y$, $x \cong_{\{-2,-1,0\}} y$ sont équivalentes.
On en déduit des définitions de l'égalité restreinte au domaine PP dans les structures $\langle \mathbf{N}; S; \perp \rangle$ et $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$, notées toutes deux $x =_{PP} y$:

$$PP(x, y) \wedge \mathrm{SUPP}[S(x)] = \mathrm{SUPP}[S(y)] \wedge \mathrm{SUPP}[S^2(x))] = \mathrm{SUPP}[S^2(y))] \ ,$$

$$PP(x, y) \wedge \mathrm{SUPP}[\mathrm{Pred}(x)] = \mathrm{SUPP}[\mathrm{Pred}(y)] \wedge \mathrm{SUPP}[\mathrm{Pred}^2(x))] = \mathrm{SUPP}[\mathrm{Pred}^2(y))] \ .$$

A partir de ces formules, on obtient une définition dans $\langle \mathbf{N}; S; \perp \rangle$ de la restriction à PP de la fonction prédécesseur par la formule, notée $\mathrm{Pred}_{PP}(x, y)$:

$$[\mathrm{Egal}_0(x) \to \mathrm{Egal}_0(y)] \wedge \{[\neg(\mathrm{Egal}_0(x)] \to [x =_{PP} S(y)]\}$$

On obtient aussi une définition dans $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$ de la restriction à PP de la fonction successeur par la formule, notée $S_{PP}(x, y)$: $\neg(\mathrm{Egal}_0(y)] \wedge [x =_{PP} \mathrm{Pred}(y)]\}$.

Remarques. 1°) Soit $n > 0$. La formule

$$PP(x) \vee PP[S(x)] \vee \ldots \vee PP[S^n(x)]$$

définit l'ensemble $PP + [-n, 0]$ dans $\langle \mathbf{N}; S; \perp \rangle$. L'application du Corollaire 2.12 montre — comme plus haut — que l'égalité et la fonction prédécesseur restreintes à cet ensemble sont définissables avec S et $\perp$.

2°) De façon analogue, avec Pred et $\perp$, c'est l'ensemble $PP + [0, n]$ qui est définissable, ainsi que l'égalité et la fonction successeur restreintes à celui-ci.

5.6. On peut maintenant définir les singletons dans $\langle \mathbf{N}; S; \perp \rangle$.
Soit $n \geqslant 2$ et soit p un premier plus grand que n. La condition $x = n$ équivaut à

$$(p-n)\text{-ième successeur de } x = (p-1)\text{-ième successeur de } 1\,,$$

relation qui ne fait intervenir que la seule restriction de l'égalité à PP.

Ainsi, l'ensemble $\{n\}$ est défini dans $\langle \mathbf{N}; S; \perp \rangle$ par la formule $S^{p-n}(x) =_{PP} S^{p-1}(1)$, notée $\mathrm{Egal}_n(x)$. On utilisera donc toutes les constantes entières dans le cadre du langage $(S; \perp)$.

5.7. Nous définissons maintenant (à la suite de [RD1]) *l'ensemble P des nombres premiers* dans chacun des langages $(S; \perp)$ et $(\mathrm{Pred}; \perp)$.

Le point ii) du Corollaire 2.4 montre que l'ensemble X des primaires x tels que $\mathrm{SUPP}(x-1) \subseteq \mathrm{SUPP}(y-1)$ pour tout primaire y de même base que x est égal à

$$X = P \cup \{(2^u-1)^2 : u \geqslant 2 \text{ et l'entier } 2^u - 1 \text{ est premier}\}\,.$$

Cet ensemble X se définit dans $\langle \mathbf{N}; S; \perp \rangle$ par la formule $X(x)$ suivante:

$$PP(x) \wedge \forall y \forall u \forall v \{[PP(x, y) \wedge \mathrm{Pred}_{PP}(x, u) \wedge \mathrm{Pred}_{PP}(y, v)] \to \mathrm{SUPP}(u) \subseteq \mathrm{SUPP}(v)\}$$

Comme $(2^u-1)^2 + 1 = 2[2^u(2^{u-1}-1)+1]$, l'entier $(2^u-1) + 1$ est une puissance de 2 mais pas $(2^u-1)^2 + 1$. On voit ainsi que P se définit à

partir de X comme suit: $P = \{x \in X$: s'il existe $y \in X$, y de même base que x et $y \neq x$ alors $x + 1$ est une puissance de $2\}$
On en déduit alors une définition, notée $P(x)$, dans $\langle \mathbf{N}; S; \perp \rangle$ de l'ensemble P:

$$X(x) \wedge \{[\exists z[X(z) \wedge (z \neq_{PP} x) \wedge PP(x, z)]] \rightarrow PP(S(x), 2)]\} .$$

Grâce au prédicat S_{PP}, ces définitions se transfèrent simplement de la structure $\langle \mathbf{N}; S; \perp \rangle$ à la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$ donnant les formules, notées également $X(x)$ et $P(x)$:

$$PP(x) \wedge \forall y\{PP(x, y) \rightarrow \mathrm{SUPP}\,[\mathrm{Pred}(x)] \subseteq \mathrm{SUPP}\,[\mathrm{Pred}(u)]\} .$$

$$X(x) \wedge \{[\exists z[X(z) \wedge (z \neq_{PP} x) \wedge PP(x, z)]] \rightarrow \exists t\,[S_{PP}(x, t) \wedge PP(t, 2)]\} .$$

5.8. La possibilité de définir P par l'adjonction à $\perp$ de S ou bien Pred permet de développer considérablement la théorie des parties finies de P mise en place en 5.2 par le biais des supports d'entiers:

Toute la combinatoire ensembliste sur les supports s'exprime dans chacun des langages $(S; \perp)$ *et* $(\mathrm{Pred}; \perp)$.

La relation d'appartenance, traduite sur les codes par la relation $p \in \mathrm{SUPP}\,(x)$, est définie dans chacune des structures $\langle \mathbf{N}; S; \perp \rangle$ et $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$ par la formule $P(p) \wedge \neg(p \perp x)$.

Nous montrons ci-dessous comment élargir le codage des parties finies de P à un *codage des relations et fonctions sur ces parties finies.*

Pour $k \geqslant 1$ fixé, on note $(A_\alpha)_{1 \leqslant \alpha \leqslant K}$ une énumération des suites de $k + 1$ parties de $\{1, 2, ..., k\}$. Soit π un entier premier plus grand que K. Soient $x_1, ..., x_k$ des entiers.
A tout $(p_1, ..., p_k) \in \mathrm{SUPP}\,(x_1) \times ... \times \mathrm{SUPP}\,(x_k)$ on associe — à l'aide du Théorème de Dirichlet (cf. 2.1) — l'ensemble infini $X_{p_1, ..., p_k}$ des entiers premiers $z > \pi$ qui vérifient les équations de congruences:

$z \equiv i \pmod{p_i}$ pour les i tels que $p_i > k + 1$, $p_i \neq \pi$ et $p_i \neq p_j$ pour tous les $j < i$,

$z \equiv k + 1 \pmod{q}$ si $q \in [\mathrm{SUPP}(x_1) \cup ... \cup \mathrm{SUPP}(x_k)] \setminus \{1, ..., k+1, p_1, ..., p_k, \pi\}$,

$z \equiv \alpha \pmod{\pi}$ si A_α est $(\{i: p_i = 2\}, ..., \{i: p_i = k + 1\}, \{i: p_i = \pi\})$.

On voit simplement que les $X_{p_1, ..., p_k}$ sont deux à deux disjoints.

Les Pred-codes d'une relation ρ sur $\mathrm{SUPP}\,(x_1) \times ... \times \mathrm{SUPP}\,(x_k)$ sont alors les entiers dont les supports coupent les seuls $X_{p_1, ..., p_k}$ tels que $(p_1, ..., p_k) \in \rho$. Les Pred-codes d'une fonction sont ceux de son graphe.

Les S-codes d'une relation sont définis de façon similaire avec les ensembles $Y_{p_1, \ldots, p_k}$ obtenus en remplaçant dans la définition de $X_{p_1, \ldots, p_k}$ les restes de congruences par leurs opposés.

PROPOSITION. *Les relations*

« $(p_1, \ldots, p_k)$ appartient à la relation S-codée par x sur $\mathrm{SUPP}(x_1) \times \ldots \times \mathrm{SUPP}(x_k)$ »,

« $(p_1, \ldots, p_k)$ appartient à la relation Pred-codée par x sur $\mathrm{SUPP}(x_1) \times \ldots \times \mathrm{SUPP}(x_k)$ »

sont respectivement définissables dans les structures $\langle \mathbf{N}; S; \perp \rangle$ *et* $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$.

Preuve. La définition des $X_{p_1, \ldots, p_k}$ se traduit simplement en une définition avec Pred et $\perp$ de la relation $\{(x_1, \ldots, x_k, p_1, \ldots, p_k, z) : z \in X_{p_1, \ldots, p_k}\}$. D'où l'assertion relative aux Pred-codes. Celle pour les S-codes se déduit de même.

Les notions ensemblistes usuelles se traduisent alors en propriétés sur les S-codes ou Pred-codes définissables avec S et $\perp$, ou Pred et $\perp$.

En particulier, la notion d'injection entre supports d'entiers conduit à la définissabilité de toute l'arithmétique sur les cardinalités des supports.

Notant $|X|$ le nombre d'éléments de X, on retrouve ainsi un résultat de Woods:

COROLLAIRE (Woods). 1°) *Les images réciproques par la surjection* $x \mapsto |\mathrm{SUPP}(x)|$ *de* $\mathbf{N} \backslash \{0\}$ *sur* $\mathbf{N}$ *des relations* $\leqslant$, $=$ *et des graphes de l'addition et de la multiplication sont définissables dans les structures* $\langle \mathbf{N}; S; \perp \rangle$ *et* $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$.

2°) *La théorie* $Th(\mathbf{N}; S; \perp)$ (ensemble des énoncés s'écrivant avec le successeur et la coprimarité pour seuls symboles de fonction et prédicat) *est indécidable.*

Remarque. La partie 2°) de ce Corollaire signifie que la vérité arithmétique des énoncés avec successeur et coprimarité est aussi compliquée que celle de tous les énoncés de l'arithmétique. C'est une condition évidemment nécessaire à une réponse positive à la conjecture d'Erdös-Woods d'après le théorème cité en 4.7.

5.9. Une autre application simple du Théorème ZBV permet de définir une fraction de la fonction exponentielle.

La caractérisation donnée par le point iii) du Corollaire 2.4 de la notion de diviseur primitif se traduit directement par des formules des langages $(S; \perp)$ et (Pred; $\perp$), notées toutes deux PRIMITIF (p, u).

Si p et q sont des nombres premiers distincts, l'entier $q^{\mathrm{ORD}(q, p)}$ est la seule puissance u de q telles que p soit diviseur primitif de $u - 1$. Cette condition s'exprime immédiatement avec la formule PRIMITIF (p, u), d'où le résultat suivant.

PROPOSITION. *On peut définir avec* S *et* $\perp$, *ou bien* Pred *et* $\perp$, *la relation ternaire*

$$\{(p, q, u): p \text{ et } q \text{ sont premiers distincts et } u = q^{\mathrm{ORD}(q, p)}\}.$$

5.10. Les deux propositions qui suivent sont des résultats techniques utiles en 5.11. Soient p^α un primaire de base p et x un entier tels que:

— $\mathrm{SUPP}(x) \subseteq \mathrm{SUPP}(p^\alpha - 1)$,

— l'ensemble $\mathrm{SUPP}(x)$ contient exactement un diviseur primitif de tout $p^\beta - 1$ qui admet un diviseur primitif et vérifie l'inclusion $\mathrm{SUPP}(p^\beta - 1) \subseteq \mathrm{SUPP}(p^\alpha - 1)$.

Le point ii) du Corollaire 2.5 montre que

— si p^α n'est pas le carré d'un premier de Mersenne $p = 2^u - 1$ et si $p \neq 2$ ou bien $p = 2$ mais $\mathrm{SUPP}(2^6 - 1) = \{3, 7\} \nsubseteq \mathrm{SUPP}(p^\alpha - 1)$, alors le cardinal de $\mathrm{SUPP}(x)$ est le nombre des diviseurs de α,

— si $p = 2$ et $\mathrm{SUPP}(2^6 - 1) = \{3, 7\} \subseteq \mathrm{SUPP}(p^\alpha - 1)$, alors le cardinal de $\mathrm{SUPP}(x)$ est le nombre des diviseurs de α diminué de 1,

— si p est de la forme $2^u - 1$ et $p^\alpha = p^2$, alors $|\mathrm{SUPP}(x)| = 1$ tandis que le nombre des diviseurs de α est 2.

Toutes les clauses précédentes sont exprimables avec S et $\perp$, ou Pred et $\perp$. A l'aide du Corollaire 5.8, ceci conduit à:

PROPOSITION 1. *On peut définir avec* S *et* $\perp$, *ou bien* Pred *et* $\perp$, *la relation*

$$\{(u, x): u \text{ est primaire et } |\mathrm{SUPP}(x)| \text{ est le nombre des diviseurs de la valuation de } u\}.$$

En particulier, on peut aussi exprimer dans ces langages la relation

$$\{(u, v): u \text{ et } v \text{ sont primaires et leurs valuations ont le même nombre des diviseurs}\}.$$

On peut alors montrer la Proposition suivante.

PROPOSITION 2. *On peut définir avec* S *et* $\perp$, *ou bien* Pred *et* $\perp$, *la relation*

$$\{(p, q,) : p \text{ et } q \text{ sont premiers et distincts et } \mathrm{ORD}(q, p) = p - 1\}.$$

Preuve. Comme pour tout r l'entier $\mathrm{ORD}(r, p)$ est toujours un diviseur de $p - 1$, on voit que l'égalité $\mathrm{ORD}(q, p) = p - 1$ équivaut à la condition « *pour tout premier* r *l'entier* $\mathrm{ORD}(r, p)$ *n'a pas plus de diviseurs que* $\mathrm{ORD}(q, p)$ ».

Cette dernière condition peut aussi s'écrire

« *pour tout premier* r *la valuation de* $r^{\mathrm{ORD}(r, p)}$ *n'a pas plus de diviseurs que celle de* $q^{\mathrm{ORD}(q, p)}$ ».

Sous cette forme, la traduction dans les langages avec S ou Pred est une application immédiate de la Proposition 1 et de celle de 5.9.

5.11. La Proposition 2 précédente permet de définir maintenant une partie importante de la fonction exponentielle. La preuve qui suit reprend et simplifie celle de [RD1].

PROPOSITION. *On peut définir avec* S *et* $\perp$, *ou bien* Pred *et* $\perp$, *la restriction de la fonction* $(p, q) \mapsto q^{p-1}$ *à l'ensemble* $\{(p, q,) : p$ *et* q sont premiers et distincts$\}$.

Preuve. Compte tenu de la Proposition 2 de 5.10, il suffit de définir q^{p-1} lorsque p et q sont des premiers distincts tels que $\mathrm{ORD}(q, p) < p - 1$.

Soit w une puissance de q telle que $\mathrm{SUPP}(q^{\mathrm{ORD}(q, p)} - 1) \subseteq \mathrm{SUPP}(w - 1)$ (c'est-à-dire de la forme $q^{k \times \mathrm{ORD}(q, p)}$). On pose

$$X_w = \{q^\alpha : \mathrm{SUPP}(q^{\mathrm{ORD}(q, p)} - 1) \subseteq \mathrm{SUPP}(q^\alpha - 1) \subseteq \mathrm{SUPP}(w - 1)\},$$

$$D(X_w) = \{r : r \neq p \text{ et } r \text{ est diviseur primitif d'un } q^\alpha - 1 \text{ où } q^\alpha \in X\},$$

$$\Sigma(X_w) = \{z : z \text{ est premier, } \mathrm{ORD}(z, p) = p - 1 \text{ et } z \equiv q \pmod r \text{ pour tout } r \in D(X_w)\}.$$

Le théorème de Dirichlet (cf. 2.2) (et le fait que la condition $\mathrm{ORD}(z, p) = p - 1$ soit impliquée par toute équation de congruence $z \equiv g \pmod p$, où g est un entier tel que $\mathrm{ORD}(g, p) = p - 1$) montre que l'ensemble $\Sigma(X_w)$ est infini.

La définition de $\Sigma(X_w)$ montre que si $z \in \Sigma(X_w)$ alors $\mathrm{ORD}(z, p) = \mathrm{ORD}(g, p) = p - 1$ et $\mathrm{ORD}(z, r) = \mathrm{ORD}(q, r)$. Ainsi, p est diviseur primitif de z^{p-1} et tout diviseur primitif de $q^\alpha - 1$ qui est différent de p est aussi primitif pour $z^\alpha - 1$ (et donc non primitif pour les $z^\beta - 1$ où $\alpha \neq \beta$). En particulier,

— si $\alpha \neq p - 1$ alors $q^\alpha - 1$ n'a aucun diviseur primitif différent de p et qui soit primitif pour $z^{p-1} - 1$;

— si $q^{p-1} \in X$ et s'il existe un diviseur primitif de $q^{p-1} - 1$ alors celui-ci est différent de q et tel que $\mathrm{SUPP}(u-1) = \mathrm{SUPP}(q-1)$;

3°) il existe un primaire w de base q tel que $\mathrm{SUPP}(q^{\mathrm{ORD}(q,p)}-1) \subseteq \mathrm{SUPP}(w-1)$ et u admet un diviseur primitif différent de p en commun avec $z^{p-1} - 1$ pour tout z de $\Sigma(X_w)$.

On conclut la preuve en observant que ces conditions sont simplement exprimables dans les langages $(S; \perp)$ et $(\mathrm{Pred}; \perp)$.

COROLLAIRE. *La restriction de la fonction* $x \mapsto 5^x$ *à l'ensemble* P *est définissable dans la structure* $\langle \mathbf{N}; S; \perp \rangle$.

Preuve. Le Corollaire 2.4 montre que 5^{n+1} est le seul primaire 5^α tel que $\mathrm{SUPP}(5^\alpha - 5) = \{5\} \cup \mathrm{SUPP}(5^n - 1)$.

Cette condition permet donc de définir la fonction $5^n \mapsto 5^{n+1}$ de domaine $5^{\mathbf{N}}$ dans la structure $\langle \mathbf{N}; S; \perp \rangle$. On conclut avec la Proposition précédente, appliquée à $q = 5$.

5.12. PROPOSITION. *La fonction* $x \mapsto 5^x$ *transforme la structure*

$$\langle \mathbf{N}; +; \times, = \rangle$$

en une structure $\langle 5^{\mathbf{N}}; \mathrm{NA}, \mathrm{NM}; =_{PP} \rangle$ *qui est entièrement définissable dans la structure* $\langle \mathbf{N}; S; \perp \rangle$.

En particulier, les structures $\langle \mathbf{N}; S, x \mapsto 5^x; \perp \rangle$ *et* $\langle \mathbf{N}; +, \times; = \rangle$ *définissent les mêmes relations et fonctions.*

Preuve. On a déjà vu que la fonction $5^n \mapsto 5^{n+1}$ de domaine $5^{\mathbf{N}}$, notée NS (pour Nouveau Successeur) est $(S, \perp)$-définissable.

Le même Corollaire 2.4 définit aussi directement la relation NDIV (pour Nouvelle DIVisibilité) formée des couples $(5^n, 5^m)$ tels que n divise m.

Cette fonction et cette relation sont les images, par l'application $x \mapsto 5^x$, de la fonction successeur et de la relation de divisibilité.

Ainsi, on peut définir, au sein de la structure $\langle \mathbf{N}; S; \perp \rangle$, une nouvelle structure $\langle 5^{\mathbf{N}}; \mathrm{NS}; \mathrm{NDIV} \rangle$ qui est isomorphe, via $x \mapsto 5^x$, à la structure $\langle \mathbf{N}; S; | \rangle$.

Le Théorème de J. Robinson (cf. 4.5) assure que l'addition et la multiplication sont définissables dans $\langle \mathbf{N}; S; | \rangle$. Les formules qui définissent l'addition et la multiplication usuelles sur les entiers à partir de S et $|$ permettent alors de définir dans la structure $\langle 5^{\mathbf{N}}; \mathrm{NS}; \mathrm{NDIV} \rangle$, et donc à fortiori dans $\langle \mathbf{N}; S; \perp \rangle$, les fonctions, notées NA et NM (pour nouvelles addition et multiplication), qui sont les images des fonctions $+$ et $\times$ par l'isomorphisme $x \mapsto 5^x$.

Remarques. 1°) Le choix de la base 5 (plutôt que 2 ou 3) permet d'éviter les exceptions au Théorème ZBV et à son Corollaire 3.4, lesquelles ne concernent en effet que les bases 2 et $2^u - 1$.

2°) J. P. Jones nous a signalé l'article [RR] dans lequel R. M. Robinson utilise également les modèles internes sur les puissances d'un premier fixé. Il démontre que ceux-ci sont $(S; |)$-définissables.

3°) La $(S; \perp)$-définissabilité de la fonction $x \mapsto 5^x$, de domaine $\mathbf{N}$, reste un problème ouvert (car équivalent à la conjecture E-W).

5.13. On peut maintenant prouver une partie essentielle du Théorème annoncé en 4.10.

PROPOSITION. *Soit* ρ *une relation définissable dans la structure* $\langle \mathbf{N}; +, \times, = \rangle$. *La relation* $\mathrm{Sat}(\rho)$ *obtenue en saturant* ρ *par la relation* $\cong_{\{0\}}$, *(où* $x \cong_{\{0\}} y$ *signifie* $\mathrm{SUPP}(x) = \mathrm{SUPP}(y)$*) est définissable dans les structures* $\langle \mathbf{N}; S; \perp \rangle$ *et* $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$.

Preuve. Soit $F(x_1, ..., x_k)$ une formule qui définit ρ dans $\langle \mathbf{N}; +; \times, = \rangle$. L'isomorphisme $\mathrm{Exp}_5 : x \mapsto 5^x$ entre $\langle \mathbf{N}; +; \times, = \rangle$ et $\langle 5^{\mathbf{N}}; \mathrm{NA}, \mathrm{NM}; =_{PP} \rangle$ transforme ρ en l'ensemble $5^\rho = \{(5^{x_1}, ..., 5^{x_k}) : (x_1, ..., x_k) \in \rho\}$, et cette image est la partie de $5^{\mathbf{N}^k}$ définie dans la structure $\langle 5^{\mathbf{N}}; \mathrm{NA}, \mathrm{NM}; =_{PP} \rangle$ par la même formule $F(x_1, ..., x_k)$. Comme cette structure est définissable dans $\langle \mathbf{N}; S; \perp \rangle$ et $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$, on voit que 5^ρ est aussi définissable avec $\perp$ et S ou Pred. Notons SUPP la fonction support, qui envoie $\mathbf{N} \setminus \{0\}$ dans l'ensemble $\mathscr{P}_f(P)$ des parties finies de P. L'isomorphisme Exp_5 transforme SUPP en la fonction NSUPP (nouveau support) qui envoie $5^{\mathbf{N} \setminus \{0\}}$ dans l'ensemble $\mathscr{P}_f(5^P)$ des parties finies de 5^P de sorte que, notant EXP_5 la restriction à $\mathscr{P}_f(P)$ de l'extension de Exp_5 aux parties, le diagramme (1) soit commutatif:

Diagramme (1)

$$\begin{array}{ccc} \mathscr{P}_f(P) & \xrightarrow[\mathrm{EXP}_5]{} & \mathscr{P}_f(5^P) \\ {\scriptstyle \mathrm{SUPP}}\uparrow & & \uparrow{\scriptstyle \mathrm{NSUPP}} \\ \mathbf{N}\backslash\{0\} & \xrightarrow[\mathrm{Exp}_5]{} & 5^{\mathbf{N}}\backslash\{1\} \end{array}$$

On observe que

$$\begin{aligned} \mathrm{Sat}(\rho) &= \mathrm{SUPP}^{-1}[\mathrm{SUPP}(\rho)] \\ &= [\mathrm{EXP}_5 \circ \mathrm{SUPP}]^{-1}[\mathrm{EXP}_5 \circ \mathrm{SUPP}](\rho) \\ &= [\mathrm{EXP}_5 \circ \mathrm{SUPP}]^{-1}[\mathrm{NSUPP} \circ \mathrm{Exp}_5](\rho) \\ &= [\mathrm{EXP}_5 \circ \mathrm{SUPP}]^{-1}[\mathrm{NSUPP}](5^\rho) \end{aligned}$$

Chacune des fonctions intervenant dans cette dernière égalité est $(S; \perp)$ et $(\mathrm{Pred}; \perp)$ définissable :

— c'est évident pour la fonction SUPP,

— ceci résulte de la Proposition 5.12 pour EXP_5 (extension aux parties de la *restriction aux premiers* de Exp_5),

— la fonction NSUPP, définissable dans $\langle 5^{\mathbf{N}}; \mathrm{NA}, \mathrm{NM}; =_{PP}\rangle$ l'est aussi avec $(S; \perp)$ ou $(\mathrm{Pred}; \perp)$.

La définissabilité de $\mathrm{Sat}(\rho)$ avec $(S; \perp)$ ou $(\mathrm{Pred}; \perp)$ résulte alors de celle de 5^ρ.

5.14. On peut enfin prouver le Théorème annoncé en 4.10.

THÉORÈME. *Soit* A *un ensemble d'entiers de* $\mathbf{Z}$. *Soit* ρ *une relation définissable dans la structure* $\langle \mathbf{N}; +, \times, =\rangle$, *incluse dans* $\mathbf{N}^k$, *et saturée par la restriction à* $\mathbf{N}$ *de la relation d'équivalence* $\cong_A$ *(où* $x \cong_A y$ *signifie* $\mathrm{SUPP}(|x+i|) = \mathrm{SUPP}(|y+i|)$ *pour tout* $i \in A$, *cf. 2.11).*

i) *Si* A *est fini alors* ρ *est définissable dans la structure* $\langle \mathbf{N}; S, \mathrm{PRED}; \perp\rangle$.

ii) *Si* A *est fini et formé d'entiers tous positifs ou nuls, alors* ρ *est définissable dans la structure* $\langle \mathbf{N}; S; \perp\rangle$.

iii) *Si* A *est fini et formé d'entiers tous négatifs ou nuls, alors* ρ *est définissable dans la structure* $\langle \mathbf{N}; \mathrm{Pred}; \perp\rangle$.

Preuve. 1°) Le cas $A = \{0\}$ est réglé par la Proposition 5.13. Le cas où A est vide est trivial car ρ est alors égal à $\mathbf{N}^k$ tout entier.

Si $a \in \mathbf{Z}$ on désigne par T_a la translation $x \mapsto \mathrm{Sup}(x+a, 0)$ de $\mathbf{N}$ dans $\mathbf{N}$. Si $A = \{a_1, ..., a_n\}$, on note T_A l'application $x \mapsto (T_{a_1}(x), ..., T_{a_n}(x))$ de $\mathbf{N}$ dans $\mathbf{N}^n$.

Si $B \subseteq \mathbf{Z}$, (la trace de) l'équivalence $\cong_B$ sur $\mathbf{N}$ s'étend de façon évidente sur $\mathbf{N}^n$. Pour toute relation τ sur $\mathbf{N}$ on note $\mathrm{Sat}_{\cong_B}(X)$ la relation obtenue en saturant τ pour (la restriction à $\mathbf{N}$ de) l'équivalence $\cong_B$.
Nous considérons d'abord le cas où $A = \{a_1, ..., a_n\} \subseteq \mathbf{N}$.

2°) Remarquons que si x et y sont dans $\mathbf{N}$ alors $T_A(x) \cong_B T_A(y)$ si et seulement si $x \cong_{A+B} y$, où $A + B = \{a + b : a \in A \text{ et } b \in B\}$. En particulier, $T_A(x) \cong_{\{0\}} T_A(y)$ si et seulement si $x \cong_A y$.

On observe enfin que, pour toute partie ρ de $\mathbf{N}^k$, on a

$$\begin{aligned}\mathrm{Sat}_{\cong_A}(\rho) &= \{(y_1, ..., y_k) : \text{il existe } (x_1, ..., x_k) \in \rho \text{ tel que } y_i \cong_A x_i \\ &\qquad \text{pour } 1 \leqslant i \leqslant k\} \\ &= \{(y_1, ..., y_k) : \text{il existe } (x_1, ..., x_k) \in \rho \text{ tel que } T_A(y_i) \cong_{\{0\}} T_A(x_i) \\ &\qquad \text{pour } 1 \leqslant i \leqslant k\} \\ &= [(T_A, ..., T_A)]^{-1}[\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)(\rho)]] \\ &\qquad (\text{où } (T_A, ..., T_A)(\rho) \text{ est incluse dans } \mathbf{N}^{n \times k}).\end{aligned}$$

3°) Si ρ est définissable dans la structure $\langle \mathbf{N}; +, \times; = \rangle$ alors la relation $\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)(\rho)]$ l'est aussi; étant $\cong_{\{0\}}$ saturée, elle est également (d'après la Proposition 5.13) définissable dans la structure $\langle \mathbf{N}; S; \perp \rangle$.

Par ailleurs, si $a \in \mathbf{N}$, l'application T_a n'est autre que l'itérée d'ordre a de la fonction S. La fonction T_A est donc une composée d'itérées de la fonction S avec la fonction de brassage $x \mapsto (x, ..., x)$ de $\mathbf{N}$ dans $\mathbf{N}^n$.

D'après la Proposition 3.6, la famille des relations définissables dans $\langle \mathbf{N}; S; ... \rangle$ est stable par image réciproque par T_A (en termes logiques, si $F(x_1, ..., x_n)$ définit τ dans $\langle \mathbf{N}; S; ... \rangle$ alors $[(T_A, ..., T_A)]^{-1}(\tau)\, y$ est défini par la formule $F[S^{a_1}(x), ..., S^{a_n}(x)]$).

Remarque. Rappelons que l'application S n'est pas — à priori — $(S; \perp)$-définissable (cf. 3.5), il en est donc de même de T_A.

Il en résulte que l'ensemble $[(T_A, ..., T_A)]^{-1}[\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)(\rho)]]$, c'est-à-dire $\mathrm{Sat}_{\cong_A}(\rho)$, est définissable dans la structure $\langle \mathbf{N}; S; \perp \rangle$. Si ρ est saturée pour $\cong_A$ alors $\rho = \mathrm{Sat}_{\cong_A}(\rho)$ et est donc $(S; \perp)$-définissable. Ceci achève la preuve de l'assertion ii) du Théorème.

4°) Considérons maintenant le cas où $A = \{a_1, ..., a_n\}$ est formé d'éléments tous négatifs ou nuls. Soit m le plus grand entier positif ou nul tel que $-m$ soit dans A. On note M le saturé de $\{0, ..., m\}$ pour $\cong_A$:

$$M = \{x \in \mathbf{N} : \text{il existe } i \in \{0, ..., m\} \text{ tel que } x \cong_A i\}.$$

Si $a \leqslant 0$ alors la fonction T_a est constante de valeur 0 sur $\{0, ..., a\}$ et sa restriction à $\mathbf{N}\backslash\{0, ..., a\}$ est injective et d'image $\mathbf{N}\backslash\{0\}$. On voit ainsi que si $x > m$ alors $T_A^{-1}(x)] = \{x\}$.

De même, si $x > m$ et $y > m$ (en particulier si x et y sont dans $\mathbf{N}\backslash M$) alors, comme plus haut, $T_A(x) \cong_{\{0\}} T_A(y)$ si et seulement si $x \cong_A y$.

On remarque que pour toute partie τ de $\mathbf{N}^p$ on a

$$\begin{aligned}(\mathbf{N}\backslash M)^p \cap \mathrm{Sat}_{\cong_A}(\tau) &= \mathrm{Sat}_{\cong_A}[(\mathbf{N}\backslash M)^p \cap \tau] \\ &= \{(y_1, ..., y_p) \in (\mathbf{N}\backslash M)^p : \text{il existe } (x_1, ..., x_p) \in (\mathbf{N}\backslash M)^p \cap \tau \\ &\quad \text{tel que } y_i \cong_A x_i \text{ pour } 1 \leqslant i \leqslant p\} \\ &= \{(y_1, ..., y_p) \in (\mathbf{N}\backslash M)^p : \text{il existe } (x_1, ..., x_p) \in (\mathbf{N}\backslash M)^p \cap \tau \\ &\quad \text{tel que } T_A(y_i) \cong_{\{0\}} T_A(x_i) \text{ pour } 1 \leqslant i \leqslant p\} \\ &= [(T_A, ..., T_A)]^{-1}[\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)((\mathbf{N}\backslash M)^p \cap \tau)]] .\end{aligned}$$

5°) Si τ est définissable dans $\langle \mathbf{N}; +, \times; = \rangle$ alors la relation

$$\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)((\mathbf{N}\backslash M)^p \cap \tau)]$$

(qui est incluse dans $\mathbf{N}^{n \times k}$) l'est aussi. Etant $\cong_{\{0\}}$ saturée, elle est également (d'après la Proposition 5.13) définissable dans la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$.

D'autre part, si $a \leqslant 0$, l'application T_a n'est autre que l'itérée d'ordre $|a|$ de la fonction Pred. Comme en 3°), on voit que la famille des relations définissables dans $\langle \mathbf{N}; \mathrm{Pred}; ... \rangle$ est stable par image réciproque par T_A.

Ainsi,

$$[(T_A, ..., T_A)]^{-1}[\mathrm{Sat}_{\cong_{\{0\}}}[(T_A, ..., T_A)((\mathbf{N}\backslash M)^p \cap \tau)]] ,$$

c'est-à-dire $(\mathbf{N}\backslash M)^p \cap \mathrm{Sat}_{\cong_A}(\tau)$, est définissable dans la structure $\langle \mathbf{N}; \mathrm{Pred}; \perp \rangle$.

Ceci prouve que

si $\tau \subseteq \mathbf{N}^p$ *est saturée pour* $\cong_A$ *alors* $(\mathbf{N}\backslash M)^p \cap \tau$ *est* (Pred; $\perp$)-*définissable.*

6°) Soit ρ une partie de $\mathbf{N}^k$.

Si $I = \{i_1, ..., i_t\}$, où $i_1 < ... < i_t$, est incluse dans $\{1, ..., k\}$, on note Proj_I la fonction $(x_1, ..., x_k) \mapsto (x_{i_1}, ..., x_{i_t})$ de $\mathbf{N}^k$ sur $\mathbf{N}$.

Si $\tau \subseteq \mathbf{N}^t$, on note $\mathrm{Ext}_I(\tau)$ l'ensemble

$$\begin{aligned}\mathrm{Ext}_I(\tau) = \{(x_1, ..., x_k) : \mathrm{Proj}_I[(x_1, ..., x_k)] \in \tau \quad \text{et} \quad x_i \in M \\ \text{pour tout } i \in \{1, ..., k\}\backslash I\} .\end{aligned}$$

Comme M est saturée pour $\cong_A$, on voit que pour toute partie ρ de $\mathbf{N}^k$ on a

$$(*) \qquad \mathrm{Sat}_{\cong_A}(\rho) = \bigcup_{I \subseteq \{1,\ldots,k\},\, p=|I|} \mathrm{Ext}_I[(\mathbf{N}\backslash M)^p \cap \mathrm{Proj}_I[\mathrm{Sat}_{\cong_A}(\rho)]] .$$

On note $K_{i,a}$ l'ensemble $K_{i,a} = \{x > m : \mathrm{SUPP}(x+a) = \mathrm{SUPP}(|i+a|)\}$. Il est clair que si $-m \leqslant a \leqslant 0$ l'ensemble $K_{i,a}$ est (Pred ; $\perp$)-définissable. Comme $M = [M \cap \{0, 1, ..., m\}] \cup [\bigcup_{1 \leqslant i \leqslant m} \bigcap_{a \in A} K_{i,a}]$, on en déduit que M est (Pred ; $\perp$)-définissable.

Il en résulte que si X est (Pred ; $\perp$)-définissable alors il en est de même des $\mathrm{Ext}_I(X)$.

7°) On peut maintenant achever la preuve du point iii) du Théorème. Si ρ est saturée pour $\cong_A$ alors les $\mathrm{Proj}_I[\mathrm{Sat}_{\cong_A}(\rho)]$ le sont aussi. Le point 5°) montre que les $(\mathbf{N}\backslash M)^p \cap \mathrm{Proj}_I[\mathrm{Sat}_{\cong_A}(\rho)]$ sont (Pred ; $\perp$)-définissables, il en résulte que les $\mathrm{Ext}_I[(\mathbf{N}\backslash M)^p \cap \mathrm{Proj}_I[\mathrm{Sat}_{\cong_A}(\rho)]]$ le sont aussi, et donc également ρ.

8°) Dans le cas général où A comprend des éléments positifs et d'autres négatifs, on raisonne comme dans les points 4°) à 7°). Cependant, la fonction T_A est, dans ce cas, une composée d'itérées des deux fonctions S et Pred avec la fonction de brassage $x \mapsto (x, ..., x)$ de $\mathbf{N}$ dans $\mathbf{N}^n$. C'est donc alors la famille des relations définissables dans $\langle \mathbf{N} ; S, \mathrm{Pred} ; ... \rangle$ qui est stable par image réciproque par T_A. D'où la nécessité (à priori) d'introduire le langage $(S, \mathrm{Pred} ; \perp)$.

§ 6. L'ÉGALITÉ ET LE PROBLÈME DE J. ROBINSON

6.1. Le résultat ci-dessous — à priori technique — s'avère être un outil performant dans l'étude du rôle de l'égalité en face de S et $\perp$.

Définition. Soit A une partie finie de $\mathbf{Z}$. Une relation ρ, incluse dans $\mathbf{N}^{k+1}$, est dite *quasi-saturée* pour $\cong_A$ si elle est saturée en toutes ses variables sauf peut-être la première, c'est-à-dire que lorsque $x_i \cong_A y_i$ pour $1 \leqslant i \leqslant k$, alors les $(k+1)$-uplets $(z, x_1, ..., x_k)$ et $(z, y_1, ..., y_k)$ sont simultanément dans ρ ou hors de ρ.

Exemple. D'après la Proposition 2.13, toutes les parties de $\mathbf{N} \times PP^k$ (où PP est l'ensemble des primaires) sont quasi-saturées pour $\cong_A$ si A contient $\{0, 1, 2\}$ ou $\{-2, -1, 0\}$.

LEMME. *Soit A une partie finie de $\mathbf{Z}$. Soient $\rho_1, ..., \rho_p, \theta$ des relations définissables dans la structure $\langle \mathbf{N} ; +, \times ; = \rangle$ et chacune quasi-*

saturée pour $\cong_A$. *On suppose que* θ *est incluse dans* $\mathbf{N}^2$ *et que la deuxième projection* Δ *de* θ *(i.e.* $\Delta = \{x_0$: il existe x tel que $(x, x_0) \in \theta\}$*) est une partie de* $\mathbf{N}$ *définissable dans* $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$.

Si τ *est une relation définissable dans* $\langle \mathbf{N}; S, \mathrm{Pred}; \perp, \rho_1, ..., \rho_p \rangle$ *et incluse dans* $\mathbf{N}^n$, *alors les relations*

$$\tau' = \{(x_0, x_1, ..., x_{n-1}) : \text{ il existe } x \text{ tel que } (x, x_0) \in \theta \text{ et } (x, x_1, ..., x_{n-1}) \in \tau\},$$

$$\tau'' = \{(x_0, x_1, ..., x_{n-1}) : x_0 \in \Delta \text{ et, pour tout } x, \text{ si } (x, x_0) \in \theta \text{ alors } (x, x_1, ..., x_{n-1}) \in \tau\}$$

sont également définissables dans la structure $\langle \mathbf{N}; S, \mathrm{Pred}; \perp, \rho_1, ..., \rho_p \rangle$ *(c'est-à-dire sans faire intervenir la relation* θ*).*

Preuve. 1°) Le fait que Δ soit la deuxième projection de θ et la quasi-saturation de θ pour $\cong_A$ montrent que Δ est $(\cong_A)$-saturé. Comme, relativement à τ' et τ'', la variable x_0 varie dans Δ, on voit que τ' et τ'' sont $(\cong_A)$-saturées par rapport à x_0.

2°) Si X est une partie de $\mathbf{Z}$, posons $T_{i,j}(X) = \{-j, ..., 0\} \cup [X + \{i-j\}]$. Si $u \cong_{T_{i,j}(X)} v$ alors (cf. la preuve de 4.11) on voit facilement que

— si $x \leqslant j$ ou $y \leqslant j$ alors $T_{i,j}(X)$ contient $-x$ ou $-y$ et donc $x = y$,

— $x + (i-j) \cong_X y + (i-j)$.

Il en résulte que $S^i[\mathrm{Pred}^j(u)] \cong_X S^i[\mathrm{Pred}^j(v)]$.

3°) Par récurrence sur la complexité de la formule $F(x_0, x_1, ..., x_{n-1})$ qui définit τ dans $\langle \mathbf{N}; S, \mathrm{Pred}; \perp, \rho_1, ..., \rho_p \rangle$, on construit des formules F' et F'' qui définissent τ' et τ'' dans cette même structure.

L'étape d'induction, c'est-à-dire l'introduction des connecteurs et quantificateurs (qui, en termes ensemblistes (cf. 3.6), correspond aux opérations booléennes et aux projections) est évidente: si $D(x_0)$ définit Δ avec S, Pred et $\perp$, alors

$$(\exists x_i F)' \text{ est } \exists x_i(F'), (F \vee G)' \text{ est } F' \vee G', (\neg F)' \text{ est } \neg(F'') \wedge D(x_0);$$

$$(\forall x_i F)'' \text{ est } \forall x_i(F''), (F \wedge G)'' \text{ est } F'' \wedge G'', (\neg F)'' \text{ est } \neg(F') \wedge D(x_0).$$

L'étape initiale de la récurrence concerne les formules atomiques, c'est-à-dire les relations τ qui sont images réciproques des relations $\perp, R_1, ..., R_p$ par les composées des fonctions S et Pred avec les fonctions de brassage. Les termes du langage $(S, \mathrm{Pred}; \perp, R_1, ..., R_p)$ se ramènent (après simplification des $\mathrm{Pred} \circ S$) à ceux de la forme $t(x) = S^i[\mathrm{Pred}^j(x)]$ où x est une variable. D'où les différents cas considérés ci-dessous.

4°) *Cas où* F *est* $t(x_0) \perp u(x_0)$

Dans ce cas τ' et τ'' ne comportent qu'un seul argument et le point 1°) montre qu'elles sont $(\cong_A)$-saturées et donc, d'après le Théorème 4.10, définissables dans la structure $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$.

5°) *Cas où* F *est* $t_0(x_0) \perp t_1(x_1)$

Si le terme $t_1(x_1)$ est $S^i[\mathrm{Pred}^j(x_1)]$ alors la $(\cong_{\{0\}})$-saturation de $\perp$ implique la $(\cong_{T_{i,j}(\{0\})})$-saturation par rapport à x_1 de la relation τ et donc aussi de τ' et τ''. Compte tenu de 1°), les relations τ' et τ'' sont $(\cong_{T_{i,j}(\{0\})A})$-saturées, et donc (Théorème 4.10) définissables dans $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$.

6°) *Cas où* $F(x_0, x_1, ..., x_{n-1})$ *est* $R_\alpha(t_1[x_{\sigma(1)}], ..., t_{k_\alpha}[x_{\sigma(k_\alpha)}])$, *où* $1 \leqslant \alpha \leqslant p - 1$, $\sigma: \{1, ..., k_\alpha\} \to \{0, ..., n-1\}$ *et* $\sigma(1) = 0$.

Si $t_{i_r, j_r}(x_{\sigma(r)})$ est $S^{i_r}[\mathrm{Pred}^{j_r}(x_{\sigma(i)})]$, on pose $B = T_{i_1, j_1}(A) \cup ... \cup T_{i_{k_\alpha}, j_{k_\alpha}}(A)$. De la $(\cong_A)$-quasi-saturation de l'interprétation ρ_α de R_α, on déduit la $(\cong_B)$-saturation de τ par rapport aux variables x_i telles que $i \neq \sigma(1) = 0$, et donc aussi le même résultat relatif à τ' et τ''. Le point 1°) assure alors que τ' et τ'' sont $(\cong_{B \cup A})$-saturées et donc (Théorème 4.10) définissables dans $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$.

7°) *Cas où* $F(x_0, x_1, ..., x_{n-1})$ *est* $R_\alpha(t_1[x_{\sigma(1)}], ..., t_{k_\alpha}[x_{\sigma(k_\alpha)}])$, *où* $1 \leqslant \alpha \leqslant p - 1$, $\sigma: \{1, ..., k_\alpha\} \to \{0, ..., n-1\}$ *et* $\sigma(1) \neq 0$.

Soit B défini comme au point 6°). On pose

$$\lambda = \{(z, x_0): \text{il existe } x \text{ tel que } z \cong_B x \text{ et } (x, x_0) \in \theta\}.$$

Comme θ est $(\cong_A)$-quasi-saturée, λ est $(\cong_{B \cup A})$-saturée et donc (Théorème 4.10) définissable dans $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$. La $(\cong_A)$-quasi-saturation de ρ_α montre la $(\cong_B)$-saturation de τ par rapport aux variables x_i telles que $i \neq \sigma(1)$, en particulier celles telles que $\sigma(i) = 0$ (car $\sigma(1) \neq 0$). On a donc

$$\begin{aligned}
\tau' &= \{(x_0, x_1, ..., x_{n-1}): \text{il existe } x \text{ tel que } (x, x_0) \in \theta \text{ et } (y_1, ..., y_{k_\alpha}) \in \rho_\alpha \text{ où} \\
&\qquad y_i \text{ vaut } t_i[x_{\sigma(i)}] \text{ si } \sigma(i) \neq 0 \text{ et vaut } t_i[x] \text{ si } \sigma(i) = 0\}, \\
&= \{(x_0, x_1, ..., x_{n-1}): \text{il existe } z \text{ tel que } (z, x_0) \in \lambda \text{ et } (y_1, ..., y_{k_\alpha}) \in \rho_\alpha \text{ où} \\
&\qquad y_i \text{ vaut } t_i[x_{\sigma(i)}] \text{ si } \sigma(i) \neq 0 \text{ et vaut } t_i[z] \text{ si } \sigma(i) = 0\}. \\
\tau'' &= \{(x_0, x_1, ..., x_{n-1}): x_0 \in \Delta \text{ et pour tout } x, \text{ si } (x, x_0) \in \theta \text{ alors} \\
&\qquad (y_1, ..., y_{k_\alpha}) \in \rho_\alpha \text{ où } y_i \text{ vaut } t_i[x_{\sigma(i)}] \text{ si } \sigma(i) \neq 0 \text{ et vaut} \\
&\qquad t_i[x] \text{ si } \sigma(i) = 0\}, \\
&= \{(x_0, x_1, ..., x_{n-1}): x_0 \in \Delta \text{ et pour tout } z, \text{ si } (z, x_0) \in \lambda \text{ alors} \\
&\qquad (y_1, ..., y_{k_\alpha}) \in \rho_\alpha \text{ où } y_i \text{ vaut } t_i[x_{\sigma(i)}] \text{ si } \sigma(i) \neq 0 \text{ et vaut} \\
&\qquad t_i[z] \text{ si } \sigma(i) = 0\}.
\end{aligned}$$

Ces égalités donnent des définitions de τ' et τ'' à partir de Δ, λ et ρ_α, et donc (puisque Δ et λ sont définissables avec S, Pred et $\perp$) des définitions de τ' et τ'' dans $\langle \mathbf{N}; S, \text{Pred}; \perp, \rho_\alpha \rangle$.

6.2. Le résultat suivant est une extension du Théorème de Woods sur l'équivalence du Problème de Robinson et de la $(S; \perp)$-définissabilité de l'égalité.

THÉORÈME. *Soient* $\rho_1, ..., \rho_p, \varphi_1, ..., \varphi_q$ *des relations et fonctions définissables dans* $\langle \mathbf{N}; +, \times; = \rangle$. *On suppose que* $\rho_1, ..., \rho_p$ *et les graphes de* $\varphi_1, ..., \varphi_q$ *sont quasi-saturés pour* $\cong_A$ *où* A *est une partie finie de* $\mathbf{Z}$ *(c'est le cas, en particulier, si ces relations et graphes sont inclus dans un produit* $\mathbf{N} \times [PP^k + B]$ *où* B *est une partie finie de* $\mathbf{Z}$*).*

Si l'égalité est définissable dans $\langle \mathbf{N}; S, \text{Pred}, \varphi_1, ..., \varphi_q; \perp, \rho_1, ..., \rho_p \rangle$ *(resp.* $\langle \mathbf{N}; S, \varphi_1, ..., \varphi_q; \perp, \rho_1, ..., \rho_p \rangle$, *resp.* $\langle \mathbf{N}; \text{Pred}, \varphi_1, ..., \varphi_q; \perp, \rho_1, ..., \rho_p \rangle$*) alors cette structure définit les mêmes relations et fonctions que* $\langle \mathbf{N}; +, \times; = \rangle$.

Preuve. Appliquons le Lemme 6.1 avec les relations ρ_i et les graphes des φ_j, et, pour τ la relation d'égalité, pour θ le graphe de la fonction $x \mapsto 5^x$ (graphe qui est bien quasi-saturé puisque son second argument est toujours un primaire). On observe que τ' est l'image de θ par la fonction de brassage $(x, y) \mapsto (y, x)$. La $\langle \mathbf{N}; S, \text{Pred}; \perp, \rho_1, ..., \rho_p, Gr(\varphi_1), ... Gr(\varphi_q) \rangle$-définissabilité de τ', et donc de θ, permet de conclure à celle de $+$ et $\times$, grâce à la Proposition 5.12.

On achève la preuve en observant que la définissabilité de l'égalité dans la structure $\langle \mathbf{N}; S, \text{Pred}, \varphi_1, ..., \varphi_q; \perp, \rho_1, ..., \rho_p \rangle$ montre l'équivalence de cette structure et de $\langle \mathbf{N}; S, \text{Pred}; \perp, \rho_1, ..., \rho_p, Gr(\varphi_1), ... Gr(\varphi_q) \rangle$.

On remarque enfin que si l'égalité est définissable avec les ρ_i, φ_j, $\perp$ et S sans l'aide de Pred (resp. avec Pred sans l'aide de S) alors la fonction Pred (resp. S) l'est aussi.

Remarque. Considérant pour ρ la relation d'égalité, on voit que la condition de quasi-saturation des ρ_α ne peut pas être levée dans le Lemma 6.1 ni dans le présent Théorème (sauf si la conjecture d'Erdös-Woods est vraie !).

6.3. Une application simple du Théorème 6.2 est la suivante :

THÉORÈME. *Soit* J *une injection de domaine* $\mathbf{N}$ *à valeurs dans les primaires et définissable dans* $\langle \mathbf{N}; +, \times; = \rangle$.

Les trois structures $\langle \mathbf{N}; S, J; \perp \rangle$, $\langle \mathbf{N}; \mathrm{Pred}, J; \perp \rangle$ *et* $\langle \mathbf{N}; +, \times; = \rangle$ *définissent les mêmes relations et fonctions.*

Preuve. La relation d'égalité est définissable dans la structure $\langle \mathbf{N}; S, J; \perp \rangle$ par la formule $J(x) =_{PP} J(y)$ (cf. 5.5 pour la définition de $=_{PP}$). On conclut en appliquant le Théorème 6.2 avec pour ρ le graphe de J (qui est quasi-saturé car à valeurs dans les primaires).

6.4. Une autre application simple du Théorème 6.2 est la suivante:

Soit EXP la relation binaire $\mathrm{EXP} = \{(x, y)$: il existe $a \geqslant 0$ tel que $y = a^x\}$.

THÉORÈME. *Les trois structures* $\langle \mathbf{N}; S; \perp, \mathrm{EXP} \rangle$, $\langle \mathbf{N}; S; \perp, \mathrm{EXP} \rangle$ *et* $\langle \mathbf{N}; +, \times; = \rangle$ *définissent les mêmes relations et fonctions.*

Preuve. On considère seulement le cas $(S; \perp, \mathrm{EXP})$. Soit A l'ensemble $A = \mathrm{EXP} \cap [\mathbf{N} \times PP] = \{(x, p^x)$: $x \in \mathbf{N}$ et $p \in P\}$. On observe que l'égalité $x = y$ équivaut à l'existence d'un z tel que (x, z) et (y, z) soient dans A. L'égalité est donc définissable dans la structure $\langle \mathbf{N}; S; \perp, A \rangle$.

Comme A est incluse dans $\mathbf{N} \times PP$, elle est quasi-saturée pour $\cong_{\{0,1,2\}}$, et le Théorème 6.2 montre que $+$ et $\times$ sont définissables dans la structure $\langle \mathbf{N}; S; \perp, A \rangle$. On conclut en remarquant que la relation A est elle-même définissable dans la structure $\langle \mathbf{N}; S; \perp, \mathrm{EXP} \rangle$ par la formule $PP(y) \wedge \mathrm{EXP}(x, y)$.

6.5. Le Théorème ci-dessous est un fait curieux que l'on peut énoncer ainsi:

bien qu'il apparaisse difficile de la définir avec successeur et coprimarité, la relation d'égalité n'a pourtant pas un pouvoir de définissabilité important, sa contribution — en face de S *et* $\perp$ *— se limite à se définir elle-même ainsi que le graphe des itérés de* S *et elle n'est pas en mesure d'utiliser la puissance des quantifications!*

THÉORÈME. *Toute formule du langage* $(S, \mathrm{Pred}; =, \perp)$ *équivaut à une combinaison booléenne de formules du langage* $(S, \mathrm{Pred}; \perp)$ *— formules sans égalité — et de formules du type* $x = S^i(y)$ *(resp.* $x = \mathrm{Pred}^i(y)$*) — formules sans quantificateur —.*

En termes ensemblistes, la classe des relations $\langle \mathbf{N}; S, \mathrm{Pred}; =, \perp \rangle$*-définissables coïncide avec la classe des relations obtenues par combinaisons booléennes*

— *des relations définissables dans la structure* $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$,

— *des graphes des itérées de la fonction successeur (resp. prédécesseur) et leurs images réciproques par les fonctions* $f_{p,\alpha,\beta}: (x_1, ..., x_p) \mapsto (x_\alpha, x_\beta)$ *où* $1 \leqslant \alpha \leqslant p, 1 \leqslant \beta \leqslant p, \alpha \neq \beta$.

Preuve. 1°) On commence par montrer que toute formule du langage $(S, \mathrm{Pred}; =, \perp)$ équivaut à une formule de ce même langage dont les sous-formules atomiques sont particulièrement simples. C'est l'objet des points 2°) à 4°).

2°) Si t_1 et t_2 sont des termes, les formules $t_1 \perp t_2$ et $t_1 = t_2$ sont équivalentes à

$$\exists z_1 \exists z_2 [(z_1 = t_1) \wedge (z_2 = t_2) \wedge (z_1 \perp z_2)] \quad \text{et} \quad \exists z_1 \exists z_2 [(z_1 = t_1) \wedge (z_2 = t_2) \wedge (z_1 = z_2)] .$$

Toute formule est donc équivalente à une autre dans laquelle les sous-formules atomiques sont toutes de la forme $t = x$ ou $x \perp y$ où t est un terme et x, y sont des variables.

3°) Comme $\mathrm{Pred} \circ S$ est l'identité, on peut se ramener au cas où tous les termes sont de la forme $S^i[\mathrm{Pred}^j(z)]$ où z est une variable.

4°) On a déjà vu (cf. 5.3) que tout singleton, et donc toute relation finie ou cofinie, est définissable avec $\perp$ et S ou Pred.

Comme $S^i[\mathrm{Pred}^j(z)]$ vaut i si $z \leqslant j$ et vaut $z + i - j$ si $z \geqslant j$, la formule $S^i[\mathrm{Pred}^j(z)] = x$ est équivalente à :

$$\begin{aligned}
&[(x = z) \wedge (z \geqslant j)] \vee [(x = i) \wedge (z \leqslant j)] && \text{si} \quad i = j , \\
&[(x = \mathrm{Pred}^{j-1}(z)) \wedge (z \geqslant j)] \vee [(x = i) \wedge (z \leqslant j)] && \text{si} \quad i < j , \\
&[(x = S^{i-j}(z)) \wedge (z \geqslant j)] \vee [(x = i) \wedge (z \leqslant j)] && \text{si} \quad i > j .
\end{aligned}$$

Ces formules sont de la forme $[(t = x) \wedge A(x)] \vee B(x, z)$ où A et B sont écrites avec Pred et $\perp$, et t est un terme du type $S^k(z)$ ou $\mathrm{Pred}^k(z)$.

Notons enfin que la formule $x = x$ est toujours vraie et équivaut à $\neg(x \perp x)$; si $k \neq 0$, la formule $x = S^k(x)$ est toujours fausse et équivaut à $(x \perp x) \wedge \neg(x \perp x)$, la formule $x = \mathrm{Pred}^k(x)$ équivaut à $x = 0$.

On voit donc que

(*) *Toute formule est équivalente à une formule dont les sous-formules atomiques sont toutes de la forme* $x = S^k(y)$ *ou* $x = \mathrm{Pred}^k(y)$ *ou encore* $x \perp z$, *où* x, y *sont des variables distinctes,* z *une variable et* $k \geqslant 0$.

5°) Notons enfin que la formule $x = S^k(y)$ est équivalente à $(y = \mathrm{Pred}^k(x)) \wedge (x \geqslant k)$, laquelle est de la forme $(y = \mathrm{Pred}^k(x)) \wedge A(x)$, où A est écrite avec Pred et $\perp$ (et sans égalité).

De même, la formule $x = \mathrm{Pred}^k(y)$ est équivalente à $(y = S^k(x)) \vee [(x = 0) \wedge (y \leqslant k)]$, de la forme $(y = \mathrm{Pred}^k(x)) \wedge B(x, y)$ où B est écrite sans égalité. Ainsi, on peut donc échanger les sous-formules $x = \mathrm{Pred}^k(y)$ et $y = S^k(x)$, modulo l'introduction d'autres sous-formules du langage $(\mathrm{Pred}, \perp)$ ou $(S, \perp)$.

6°) Le point 5°) montre qu'il suffit, pour prouver le Théorème, de pouvoir associer à toute formule $F(x_1, ..., x_p)$ du langage $(S, \mathrm{Pred}; =, \perp)$ une formule *équivalente* $F'(x_1, ..., x_p)$ qui est combinaison booléenne de formules du langage $(S, \mathrm{Pred}, \perp)$ et de formules du type $S^i(x) = y$ ou $\mathrm{Pred}^i(x) = y$, où x, y sont des variables. Les points 2°) à 4°) montrent que l'on peut se restreindre aux formules $F(x_1, ..., x_p)$ du langage $(S, \mathrm{Pred}; =, \perp)$ qui ont la propriété (*).

La construction procède alors par récurrence sur la complexité de F.

7°) L'initialisation de la récurrence indiquée en 6°) est l'étude du cas des formules atomiques. Puisque F vérifie (*), les seuls cas à étudier sont $x = S^k(y)$, $x = \mathrm{Pred}^k(y)$ et $x \perp y$; il est évident qu'il suffit de prendre alors F' égale à F.

8°) L'étape d'induction de cette récurrence concerne l'introduction des connecteurs et du quantificateur existentiel.

Le passage aux connecteurs est évident: $(\neg F)'$ est $\neg(F')$, etc.

Le passage au quantificateur existentiel est l'objet des points ci-dessous.

9°) Soit $F(x_1, ..., x_p, x_{p+1})$ une formule du langage $(S, \mathrm{Pred}, =, \perp)$ pour laquelle est déjà construite la formule équivalente F' de la forme indiquée en 6°). On cherche à construire $[\exists x_{p+1} F(x_1, ..., x_p, x_{p+1})]'$.

Utilisant 5°) pour les sous-formules $\mathrm{Pred}^k(x_i) = x_j$, $S^k(x_{p+1}) = x_j$ et $\mathrm{Pred}^k(x_{p+1}) = x_j$ de F', on voit que F', et donc aussi F, équivaut à une combinaison booléenne de formules du langage $(S, \mathrm{Pred}, \perp)$ et de formules des types $S^k(x_i) = x_j$, $S^k(x_i) = x_{p+1}$ et $\mathrm{Pred}^k(x_i) = x_{p+1}$, où $i \leqslant p$ et $j \leqslant p$.

Rappelons que toute combinaison booléenne de formules se ramène à une disjonction de conjonctions de ces formules et de leurs négations. D'autre part, toute conjonction $(t_1 = x_{p+1}) \wedge R(t_2, x_{p+1})$ équivaut à

$$(t_1 = x_{p+1}) \wedge R(t_2, t_1).$$

Enfin, toute conjonction $(t_1 \neq x_{p+1}) \wedge (t_2 \neq x_{p+1})$ équivaut à

$$[(t_1 \neq x_{p+1}) \wedge (t_1 = t_2)] \vee [(t_1 \neq x_{p+1}) \wedge (t_2 \neq x_{p+1}) \wedge (t_1 \neq t_2)].$$

Ceci montre que *la formule* F', et donc aussi F, *équivaut à la disjonction d'une famille de formules* $H_\alpha(x_1, ..., x_p) \wedge F_\alpha(x_1, ..., x_p, x_{p+1})$, $\alpha \in A$ (A *fini*),

où H_α *est une conjonction de formules* $S^k(x_i) = x_j, i \leqslant p, j \leqslant p,$ *et de leurs négations, et chacune des* F_α *est de l'une des deux formes suivantes:*

$$G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge [(s_\alpha = x_{p+1})]$$

ou $$G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge [\bigwedge_{u \in U_\alpha} (t_u \neq x_{p+1})] \wedge [\bigwedge_{u \in U_\alpha, v \in U_\alpha, u \neq v} (t_u \neq t_u)]$$

où G_α *est une formule du langage* $(S, \mathrm{Pred}, \perp)$, s_α *et* t_u *sont des termes de la forme* $S^k(x_i)$ *ou* $\mathrm{Pred}^k(x_i)$, *avec* $i \leqslant p$.

10°) Comme la quantification existentielle commute avec la disjonction, la formule $\exists x_{p+1} F$ équivaut à la disjonction des $\exists x_{p+1}(H_\alpha \wedge F_\alpha)$. La construction de $[\exists x_{p+1} F]'$ peut ainsi être ramenée à celle des $[\exists x_{p+1}(H_\alpha \wedge F_\alpha)]'$ (dont ce sera la disjonction).

Comme $H_\alpha(x_1, ..., x_p)$ ne dépend pas de x_{p+1}, la formule $\exists x_{p+1}(H_\alpha \wedge F_\alpha)$ équivaut à $H_\alpha(x_1, ..., x_p) \wedge \exists x_{p+1} F_\alpha$. La construction de $[\exists x_{p+1}(H_\alpha \wedge F_\alpha)]'$ peut ainsi être ramenée à celle de $[\exists x_{p+1} F_\alpha]'$ (dont ce sera la conjonction avec H_α).

11°) Le cas où F_α est de la forme $G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge [(s_\alpha = x_{p+1})]$ est trivial: la formule $\exists x_{p+1} F_\alpha$ équivaut alors à $G_\alpha(x_1, ..., x_p, s_\alpha)$, laquelle est de la forme demandée en 6°) et peut être prise pour $[\exists x_{p+1} F_\alpha]'$.

12°) Etudions maintenant le cas où F_α est de la forme

$$G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge [\bigwedge_{u \in U_\alpha} (t_u \neq x_{p+1})] \wedge [\bigwedge_{u \in U_\alpha, v \in U_\alpha, u \neq v} (t_u \neq t_u)]$$

D'après la Proposition 4.11 il existe une partie finie A de $\mathbf{Z}$ telle que la relation définie par la formule G_α soit $(\cong_A)$-saturée. La relation $\cong_A$ est évidemment définissable dans le langage $(S, \mathrm{Pred}, \perp)$. Pour tout entier $k \geqslant 1$, l'ensemble $\{x \in \mathbf{N}$: la classe de x pour $\cong_A$ contient exactement k éléments$\}$ est $(\cong_A)$-saturé. Le Théorème 4.10 assure donc qu'il est définissable par une formule, notée $EQ_k(x)$, du langage $(S, \mathrm{Pred}, \perp)$. Si X est un ensemble fini nous notons $|X|$ le nombre de ses éléments. On considère les formules θ, $\varphi_{u,X}$ et $\psi_{u,X}$ suivantes, où $u \in U_\alpha$ et $X \subseteq U_\alpha$:

$$\bigwedge_{v \in U_\alpha} (x_{p+1} \ncong_A t_v),\ (x_{p+1} \cong_A t_u)] \wedge [\bigwedge_{v \in X} (t_v \cong_A t_u)] \wedge [\bigwedge_{w \notin X} (t_w \ncong_A t_u)] \wedge EQ_{|X|}(t_u)$$

et

$$(x_{p+1} \cong_A t_u)] \wedge [\bigwedge_{v \in X} (t_v \cong_A t_u)] \wedge [\bigwedge_{w \notin X} (t_w \ncong_A t_u)] \wedge \neg EQ_{|X|}(t_u).$$

La disjonction de ces formules, quand u varie dans U_α et X dans les parties de U_α, est une tautologie.

La construction de $[\exists x_{p+1} F_\alpha]'$ peut ainsi être ramenée à celle des $[\exists x_{p+1}(F_\alpha \wedge \theta)]'$, $[\exists x_{p+1}(F_\alpha \wedge \varphi_{u,X})]'$, $[\exists x_{p+1}(F_\alpha \wedge \psi_{u,X})]'$ (dont ce sera la disjonction).

13°) On observe que les clauses $t_u \neq x_{p+1}$ de F_α sont trivialement impliquées par θ et peuvent donc être supprimées dans la formule $F_\alpha \wedge \theta$. Cette dernière équivaut donc à $G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge L_\alpha$ où L_α est la conjonction des $t_u \neq t_v$ (où ne figure pas x_{p+1}). Ainsi, $\exists x_{p+1}(F_\alpha \wedge \theta)$ équivaut à $L_\alpha \wedge \exists x_{p+1} G_\alpha$. Il est clair que cette dernière formule est de la forme demandée en 6°) et peut être prise pour $[\exists x_{p+1}(F_\alpha \wedge \theta)]'$.

14°) On observe que la formule $F_\alpha \wedge \varphi_{u,X}$ est toujours fausse car $\varphi_{u,X}$ implique que la classe de t_u pour $\cong_A$ est l'ensemble des t_v, $v \in X$, et donc que x_{p+1} est égal à l'un d'eux, ce qui contredit une des clauses de F_α. On peut donc prendre pour $[\exists x_{p+1}(F_\alpha \wedge \varphi_{u,X})]'$ une formule comme $x_1 \neq x_1$.

15°) La relation définie par G_α étant $(\cong_A)$-saturée et $\psi_{u,X}$ impliquant $x_{p+1} \cong_A t_u$, les formules $G_\alpha(x_1, ..., x_p, x_{p+1}) \wedge \psi_{u,X}$ et $G_\alpha(x_1, ..., x_p, t_u) \wedge \psi_{u,X}$ sont équivalentes. Notons $\rho_{u,X}$ la conjonction des clauses $t_v \cong_A t_u$, $t_w \not\cong_A t_u$ et $\neg EQ_{|X|}(t_u)$ de $\psi_{u,X}$ ($v \in X$ et $w \notin X$). Cette formule assure que la classe de t_u pour $\cong_A$ contient un élément z différent des t_v, $v \in X$. Un tel élément z est nécessairement également différent des t_w, $w \notin X$ (lesquels ne sont pas dans la classe de t_u). Ainsi, $\rho_{u,X}$ implique $\exists z[(z \cong_A t_u) \wedge \bigwedge_{v \in U_\alpha} (t_v \neq z)]$.

Observons que $F_\alpha \wedge \psi_{u,X}$ est équivalente à une formule de la forme

$$M_\alpha(x_1, ..., x_p) \wedge [(x_{p+1} \cong_A t_u)] \wedge \bigwedge_{v \in U_\alpha} (t_v \neq x_{p+1})],$$

où M_α, qui contient $\rho_{u,X}$, est la conjonction d'une formule du langage $(S, \mathrm{Pred}, \perp)$ et des $t_u \neq t_v$ (où ne figure pas x_{p+1}).

On voit donc que $\exists x_{p+1}(F_\alpha \wedge \psi_{u,X})$ équivaut à $M_\alpha(x_1, ..., x_p)$, laquelle peut donc être prise pour $[\exists x_{p+1}(F_\alpha \wedge \psi_{u,X})]'$.

Fin de la preuve du Théorème 6.5.

6.6. Une application du Théorème 6.5 permet d'obtenir l'implication i) ⇒ iii)ter du Théorème 4.8 (et ce, de façon tout à fait constructive).

COROLLAIRE. *Si* $+$ *et* $\times$ *sont définissables dans la structure* $\langle \mathbf{N}; S, \mathrm{Pred}; =, \perp \rangle$ *alors l'égalité l'est dans* $\langle \mathbf{N}; S, \mathrm{Pred}; \perp \rangle$.

Preuve. Le Théorème 6.5 montre que si la relation d'ordre $x < y$ est définissable avec $S, \mathrm{Pred}, =$ et $\perp$, elle l'est par une formule qui, mise sous forme de disjonction de conjonctions, a la forme suivante

$$\bigvee_{\alpha\in A}[F_\alpha(x,y)\wedge[\bigwedge_{i\in I_\alpha}(y\neq x+i)]\wedge[\bigwedge_{j\in J_\alpha}(x\neq y+j)]\wedge[\bigwedge_{k\in K_\alpha}(y=x+k)]\wedge[\bigwedge_{l\in L_\alpha}(x=y+1)]]$$

où F_α est une formule ne faisant pas intervenir l'égalité.

Si K_α ou L_α contient plus d'un élément alors la clause associée à α est impossible et peut donc être supprimée. Si L_α n'est pas vide ou si K_α contient 0 alors la clause associée à α contredit la condition $x < y$ et peut donc être supprimée. Si $K_\alpha = \{k\}, k \geqslant 1$, alors la sous-formule $y = x + k$ implique $x < y$; ainsi, la clause associée à α peut, toute entière, être remplacée par $y = x + k$.

Ceci permet de définir $x < y$ sous la forme suivante:

$$[\bigvee_{k\in K}y=x+k]\vee\bigvee_{\alpha\in A}[F_\alpha(x,y)\wedge[\bigwedge_{i\in I_\alpha}(y\neq x+i)]\wedge[\bigwedge_{j\in J_\alpha}(x\neq y+j)]].$$

Soit M le supremum des éléments des J_α.
Puisque la clause associée à α implique $x < y$, on voit que $F_\alpha(x, y)$ implique $(x<y)\vee[\bigvee_{i\in I_\alpha}(y=x+i)]\vee[\bigvee_{j\in J_\alpha}(x=y+j)]]$, qui implique aussi $x \leqslant y + M$.
Si $F(x, y)$ est la disjonction des $F_\alpha(x, y)$, on voit donc que

$$x < y \Rightarrow F(x,y) \Rightarrow x \leqslant y + M,$$

d'où $x = y \Rightarrow F(x, y+1) \wedge F(y, x+1) \Rightarrow |x - y| \leqslant M + 1$.

Le point iii) du Théorème 2.11 permet alors de conclure que l'égalité $x = y$ est définie par la formule $F(x, y+1) \wedge F(y, x+1) \wedge E(x, y)$ où $E(x, y)$ est la formule, écrite avec S et $\perp$ qui définit la relation $x \cong_{\{0,\ldots,k\}} y$, où k est un premier supérieur à M.

§ 7. Définissabilité par successeur, coprimarité et résiduation quadratique

7.1. Désignons par RES et T les relations binaires

RES $= \{(x, p) \in \mathbf{N} \times P$: x est résidu quadratique modulo le premier $p\}$,

$T = \{(x, p) \in \mathbf{N} \times P$: x est impair et l'exposant (peut-être nul) du premier p dans la décomposition primaire de x est pair$\}$.

Le Théorème de Størmer (cf. Corollaire 2.5, point ii) se traduit par le lemme suivant:

LEMME. *L'égalité des entiers impairs x et y équivaut à la condition suivante (où ε vaut, au choix, 1 ou bien -1):*

$\mathrm{SUPP}(x) = \mathrm{SUPP}(y)$ *et* $\mathrm{SUPP}(x+2\varepsilon) = \mathrm{SUPP}(y+2\varepsilon)$ *et, pour tout p premier et tout $i \in \{0, 2\}$, les couples $(x+\varepsilon i, p)$ et $(y+\varepsilon i, p)$ sont simultanément dans T ou hors de T.*

7.2. THÉORÈME. *Les structures* $\langle \mathbf{N}; S; \perp, T\rangle$, $\langle \mathbf{N}; \mathrm{Pred}; \perp, T\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent les mêmes relations et fonctions.*

Preuve. Le Lemme 7.1 fournit des définitions dans les langages $(\mathrm{Pred}; \perp, T\rangle$ et $(S; \perp, T)$ de la relation d'égalité restreinte aux entiers impairs. On en déduit simplement des définitions dans ces langages de la relation d'égalité tout entière. On conclut enfin en appliquant le Théorème 6.2 puisque, la seconde variable de T variant dans P, la relation T est quasi-saturé (cf. Exemple 6.1).

7.3. Nous allons maintenant définir la relation T dans le langage $(S; \perp, \mathrm{RES})$.

PROPOSITION. *La relation T est définissable dans les structures* $\langle \mathbf{N}; S; \perp, \mathrm{RES}\rangle$ *et* $\langle \mathbf{N}; \mathrm{Pred}; \perp, \mathrm{RES}\rangle$.

Preuve. Soient x un entier impair différent de 1 et p un diviseur premier de x. Le Lemme 2.13 montre que l'exposant de p dans x est pair si et seulement s'il existe un entier premier q ne divisant pas x et tel que les conditions suivantes soient simultanément satisfaites:

$$\left(\frac{x}{q}\right) = +1 \quad \text{et} \quad \left(\frac{p}{q}\right) = -1 \quad \text{et} \quad \left(\frac{p'}{q}\right) = +1$$

$$\text{pour tout} \quad p' \in \mathrm{SUPP}(x)\backslash\{p\}\,.$$

Comme l'égalité sur les premiers s'exprime dans les langages $(\mathrm{Pred}; \perp)$ et $(S; \perp)$ (cf. 5.5) cette caractérisation s'écrit dans $(\mathrm{Pred}; \perp, T, \mathrm{RES})$ et dans $(S; \perp, T, \mathrm{RES})$.

COROLLAIRE. *Les structures* $\langle \mathbf{N}; S; \perp, \mathrm{RES}\rangle$, $\langle \mathbf{N}; \mathrm{Pred}; \perp, \mathrm{RES}\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent les mêmes relations et fonctions.*

7.4. L'analyse de la preuve précédente et de celle du Lemme 2.3 suggère qu'on peut remplacer RES par diverses restrictions. Nous utiliserons au § 8 la restriction suivante de la relation RES:

$$\text{RRES} = \text{RES} \cap \mathbf{N} \times [8\mathbf{N}+5]$$
$$= \{(x, p) \in \mathbf{N} \times P : p \equiv 5 \pmod 8 \text{ et } x \text{ est résidu quadratique modulo } p\}$$

L'intérêt de restreindre RES à $8\mathbf{N} + 5$ tient à ce que $q - 1$ est de la forme $4(2k+1)$ lorsque q est lui-même de la forme $8k + 5$.

Le Corollaire 7.3 précédent s'adapte simplement :

THÉORÈME. *Les structures* $\langle \mathbf{N}; S; \perp, \text{RRES}\rangle$, $\langle \mathbf{N}; \text{Pred}; \perp, \text{RRES}\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent les mêmes relations et fonctions.*

Preuve. En changeant, dans la preuve du Lemme 2.13, l'équation $z \equiv 1 \pmod 4$ en $z \equiv 5 \pmod 8$, on peut supposer que l'entier premier q obtenu dans ce lemme satisfait l'équation $q \equiv 5 \pmod 8$.

Ceci permet alors de remplacer RES par RRES dans la traduction utilisée dans la preuve de la Proposition 7.3.

§ 8. DÉFINISSABILITÉ PAR SUCCESSEUR, COPRIMARITÉ ET LA RELATION BINAIRE « y EST UNE PUISSANCE DE x »

8.1. Nous considérons maintenant la relation binaire

$$\text{PUIS} = \{(x, y) : \text{il existe } n \geqslant 1 \text{ tel que } y = x^n\}.$$

Remarquons que la relation d'égalité se définit facilement dans le langage réduit au seul prédicat PUIS par la formule $\text{PUIS}(x, y) \wedge \text{PUIS}(y, x)$. Les fonctions S et Pred sont donc définissables l'une à partir de l'autre avec PUIS.

THÉORÈME. *Les deux structures* $\langle \mathbf{N}; S; \perp, \text{PUIS}\rangle$ *et* $\langle \mathbf{N}; +, \times; =\rangle$ *définissent les mêmes relations et fonctions.*

Remarque. Bien sûr, le Théorème 6.2 n'est pas directement applicable car PUIS n'est pas — a priori — quasi-saturé pour un $\cong_A$.

Ce Théorème est un corollaire immédiat du Théorème 7.4 et de la Proposition suivante, dont la preuve est l'objet des alinéas 8.2 à 8.5 ci-dessous.

PROPOSITION. *La relation* RRES *est définissable dans* $\langle \mathbf{N}; S; \perp, \text{PUIS}\rangle$.

8.2. Le Corollaire 2.4 (point ii) du Théorème ZBV montre que l'égalité $y = x^2$ équivaut à la condition

(*) $x = y = 0$ ou $x = y = 1$ ou bien y est une puissance de x et $y \neq x$ et $\text{SUPP}(y-1) = \text{SUPP}(x^2-1)$.

Comme $\text{SUPP}(x^2-1) = \text{SUPP}(x+1) \cup \text{SUPP}(x-1)$, on peut exprimer dans le langage $(S, \text{Pred}; \perp)$ la relation $\text{SUPP}(y-1) = \text{SUPP}(x^2-1)$.

Comme Pred est exprimable avec S et PUIS, on voit que (*) donne une définition de la fonction $x \mapsto x^2$ dans le langage $(S; \perp, \text{PUIS})$.

8.3. Si p est premier et ne divise pas x, nous notons $\text{ORD}(x, p)$ l'ordre de x modulo p.

Rappelons que $x^\alpha = x^{\text{ORD}(x,p)}$ si et seulement si p est diviseur primitif de $x^\alpha - 1$. La caractérisation donnée par le point iii) du Corollaire 2.4 de la notion de diviseur primitif donne alors une définition de la fonction $(x, p) \mapsto x^{\text{ORD}(x,p)}$ sur le domaine $\{(x, p): x \geqslant 2,\ p$ est premier et ne divise pas $x\}$ dans le langage $(\text{Pred}; =, \perp, \text{PUIS})$ et donc aussi dans $(S; \perp, \text{PUIS})$.

8.4. Soient A et B les relations suivantes:

$A = \{(x, p): p$ est premier et divise x, ou $x \leqslant 1\}$,

$B = \{(x, p): x \geqslant 2,\ p$ est premier et ne divise pas x, et $p \equiv 5 \pmod 8\}$.

On observe que l'on a l'égalité

$$\text{RRES} = [A \cap [\mathbf{N} \times (P \cap 8\mathbf{N}+5)]] \cup [B \cap \text{RES}].$$

La relation A est évidemment $(S; \perp)$-définissable, l'ensemble $P \cap 8\mathbf{N} + 5$, inclus dans P, l'est aussi (Théorème 4.8 ou 4.9). Ainsi, le premier terme de cette union est $(S; \perp)$-définissable.

Le même argument montre que la relation B est $(S; \perp)$-définissable.

8.5. Nous montrons que $B \cap \text{RES}$ est $(S; \perp, \text{PUIS})$-définissable.
Soit (x, p) dans B, le critère d'Euler sur les résidus quadratiques montre que

(1) $(x, p) \in \text{RES}$ si et seulement si $x^{(p-1)/2} \equiv 1 \pmod p$
si et seulement si $\text{ORD}(x, p)$ divise $(p-1)/2$.

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 $\mathrm{SUPP}(x^4-1) \not\subseteq \mathrm{SUPP}[x^{\mathrm{ORD}(x, p)}-1]$.

Ceci prouve l'égalité

(4) $C \cap \mathrm{RES} = \{(x, p) \in C : \mathrm{SUPP}(x^4-1) \not\subseteq \mathrm{SUPP}[x^{\mathrm{ORD}(x, p)}-1]\}$.

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 Stømer (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 Stømer (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

$$\mathrm{Reste}\big(p\mathrm{Quot}(x, p), 3\big) \quad \text{si} \quad 3 \text{ divise } p - 1,$$
$$\mathrm{Reste}\big[2 \times \mathrm{Reste}\big(p\mathrm{Quot}(x, p), 3\big), 3\big] \quad \text{si} \quad 3 \text{ divise } p - 2.$$

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 $\mathbf{N}$. En effet, A est alors vrai dans un modèle (standard ou non) de T et, comme $\mathbf{N}$ est isomorphe à un segment initial de ce modèle, l'énoncé A est également vrai dans $\mathbf{N}$.

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.*

[MA] MAKOWSKI, A. On a problem of Erdös. *Enseignement mathématique (2) 14* (1968), 193.

[PB] POIZAT, B. *Cours de Théorie des Modèles. Nur Al-Mantiq Wal-Ma'rifah*, 1985.

[RD1] RICHARD, D. All arithmetical sets of powers of primes are first order definable in terms of the successor function and the coprimeness predicate. *Journal of Discrete Math. 53* (1985), 221-247.

[RD2] —— Definability by successor and coprimeness in the set of arbitrary integers. *The Journal of Symbolic Logic* (à paraître).

[RD3] —— Answer to a problem raised by J. Robinson. *The Journal of Symbolic Logic 50* (1985), 135-143.

[RD4] —— L'intuition-machine en codage logique. *Actes des journées mathématiques et informatique, PRC du CNRS*, Paris 11-12 mars 1987, édité par B. Courcelle (Université de Bordeaux), 51-57.

[RD5] —— Définissabilité en arithmétique et méthode de codage ZBV appliquée à des langages avec successeur et coprimarité. *Thèse de Doctorat d'Etat*, Lyon 20 juin 1985, N° d'ordre 85-16.

[RH & VR] REISEL, H. and R. C. VAUGHAN. On sums of primes. *Arkiv für Matematik 21* (1983), 45-74.

[RJ] ROBINSON, J. Definability and decision problems in arithmetic. *The Journal of Symbolic Logic* (1949), 98-114.

[RR] ROBINSON, R. M. Undecidable rings. *Trans. of the Amer. Math. Soc. 70* (1951), 137-159.

[SC1] STØRMER, C. Quelques théorèmes sur l'équation de Pell $x^2 - dy^2 = \pm 1$. *Skrifter Videnskabs-selskabet (Christiana), I, Mat. Naturw. Kl., 2* (1887), 3-48.

[SC2] —— Solution d'un problème curieux qu'on rencontre dans la théorie élémentaire des logarithmes. *Nyt Tidsskrift for Mat., XIX, B* (1908), 1-7.

[SH] SHAPIRO, H. *Introduction to the theory of numbers.* Wiley-Interscience Publication (1982), 217-227.

[SL] SCHNIRELMAN, L. Über additive Eigenschaften von Zahlen. *Math. Ann. 107* (1933), 649-690.

[TA] TARSKI, A. On essential undecidability. *The Journal of Symbolic Logic, 14* (1949), 76-77.

[WA] WOODS, A. Some problems in logic and number theory and their connections. *Thesis*, University of Manchester (1981), 51-70, 121-122.

[ZK] ZSIGMONDY, K. Zur Theorie der Potenzreste. *Monatshefte math. Phys. 3* (1892), 265-284.

(Reçu le 30 juillet 1987)

Denis Richard
I.U.T.
Université de Clermont-Ferrand I
Ensemble universitaire des Cézeaux
B.P. 29
73170 Aubière (France)

Serge Grigorieff
U.F.R. d'Informatique
Université Paris VII
2, place Jussieu
75251 Paris Cedex 05 (France)