E.N.S. LYON - MMA 1

Rapport de stage

Problèmes de décidabilité et de définissabilité
Arithmétique de Peano
Arithmétiques faibles

Annie Chateau
Sous la direction de
Serge Grigorieff
U.F.R. d'Informatique
Université Paris VII
2, place Jussieu
75251 Paris Cedex 05

16 Juin - 8 Juillet et 18 Août - 8 Septembre 1997

Table des matières

Remerciements

Je remercie Serge Grigorieff pour ses conseils fort utiles et pour m'avoir fait entrevoir de multiples aspects intéressants de cette partie trop peu connue des mathématiques qu'est la logique.

Je remercie également zephir, titus, neron, wojcek, perrache, lapin et dragon pour leur soutien matériel au cours de ce stage.

Introduction

On a considéré dans ce stage des problèmes liés à l'arithmétique. Il se trouve que la logique mathématique contient des notions fort utiles, comme celle de définissabilité, qui apporte un élan non négligeable à la compréhension de problèmes traités plus classiquement. Nous n'aurons pas ici à utiliser des outils analytiques usuels, mais les outils plus élémentaires de la théorie des nombres.

1 Définissabilité au premier ordre

1.1 Formules du premier ordre - Exemple

On se restreindra dans toute la suite, sauf mention contraire, à des formules du premier ordre, à savoir que les quantificateurs universel et existentiel $\forall$ et $\exists$ ne porteront que sur des entiers et non sur des fonctions, ensembles ou relations.

Il est important de bien faire la distinction entre ces deux classes d'objets. Nous verrons un peu plus loin que c'est nécessaire à l'utilisation des outils logiques. Se restreindre au premier ordre garantit en quelque sorte que l'on puisse se référer à un cadre de théorie de la démonstration essentiel pour la logique, même si les mathématiciens non logiciens se passent fort bien de ce cadre. En effet de nombreux énoncés mathématiques font intervenir des quantifications sur des fonctions ou des structures plus compliquées, ce que nous ne ferons pas ici.

Fort heureusement, cette restriction aux quantifications du premier ordre n'est pas aussi réductrice qu'on pourrait le croire. En effet il est curieusement possible de définir de nombreuses fonctions usuelles au premier ordre alors qu'il est plus naturel de le faire au second ordre.
Prenons un exemple parlant : la fonction exponentielle $x \mapsto 2^x$.
On la définit usuellement comme étant l'unique fonction qui vérifie les propriétés suivantes :

$$\begin{cases} f(0) = 1 \\ f(1) = 2 \\ \forall x \forall y f(x+y) = f(x) \times f(y) \end{cases}$$

mais en fait, cela revient à la définir dans la structure standard sur les entiers, à savoir $< \mathbb{N}, +, \times, = >$ par la formule :

$$\exists! f (f(0) = 1) \wedge (f(1) = 2) \wedge \forall x \forall y (f(x+y) = f(x) \times f(y))$$

La quantification porte sur une fonction : c'est une formule au second ordre. Essayons maintenant de la définir au premier ordre dans la même structure

standard sur les entiers. C'est bien plus compliqué !
Cela fait intervenir la fonction de Gödel, qui est très utile dans de nombreux problèmes de codage de suites finies d'entiers. Elle est définie comme suit :

$$\beta : \mathbb{N}^3 \to \mathbb{N}$$
$$(x, y, z) \mapsto x \bmod (1 + (z + 1) \times y)$$

Cette fonction possède la propriété remarquable suivante : Pour toute suite finie d'entiers $(\alpha_0 \dots \alpha_p)$ il existe des entiers c et d tels que $\forall i \in \{0 \dots p\}$, $\beta(c, d, i) = \alpha_i$
De plus, elle se définit facilement au premier ordre. (voir Annexe A).
L'exponentielle $z = 2^x$ est alors définie par la formule :

$$\exists c \exists d ((\beta(c, d, 0) = 1) \wedge (\forall i\, 0 < i \leq x\, \beta(c, d, i) = 2 \times \beta(c, d, i - 1)) \wedge (z = \beta(c, d, x))))$$

Les quantificateurs ne portent plus que sur des variables : c'est bien une formule au premier ordre.

1.2 Définissabilité en logique : quelques notions

Il est important de bien préciser la notion de définissabilité, et notamment le cadre où l'on se place.

1.2.1 Langages et structures

Un langage est un ensemble de symboles, ici ce sont :
- Zéro, symbole de constante ;
- $\oplus$ et $\otimes$, symboles de fonctions ;
- $\simeq$, symbole de relation ;
- les opérateurs logiques usuels : $\neg$ non, $\wedge$ et, $\vee$ ou, $\to$ implique, $\leftrightarrow$ équivaut, $\forall$ quel que soit, $\exists$ il existe.

Structure sur un langage $\mathcal{L}$:

On appelle structure sur un langage $\mathcal{L}$ ou $\mathcal{L}$-structure :
- un ensemble appelé domaine. Ici le domaine sera l'ensemble des entiers naturels $\mathbb{N}$;
- des symboles interprétant les symboles de fonctions et de relations du langage. Ici Zéro sera interprété comme $0 \in \mathbb{N}$, $\oplus$, $\otimes$, $\simeq$ comme les fonctions d'addition et de multiplication usuelles sur $\mathbb{N}$ et la relation d'égalité usuelle.

  Généralement on note $\bar{c}$ l'interprétation du symbole c.

Comme par la suite on s'intéressera à des interprétations naturelles des symboles de fonctions et des prédicats (symboles de relations), on les confondra dans les notations, et il sera sous-entendu que le domaine est $\mathbb{N}$.

1.2.2 Theories et modèles

Les termes du langage sont obtenus à partir des symboles de constantes et de fonctions :

- c symbole de constante est un terme ;
- si f est un symbole de fonction d'arité k et que t_1,...,t_k sont des termes, alors
  f(t_1,...,t_k) est un terme ;

Les formules du langage sont obtenues par induction sur les formules atomiques de la forme : R t_1 ... t_k où R est un prédicat d'arité k et t_1,...,t_k des termes du langage :

- les formules atomiques sont des formules ;
- si F est une formule, ¬F est une formule ;
- si F et G sont des formules, F∧G, F∨G, F→G, et F↔G sont des formules ;
- si F est une formule, ∀xF[x] et ∃xF[x] sont des formules.

Notion de satisfaisabilité : Une $\mathcal{L}$-structure $\mathcal{M}$ satisfait une formule atomique du langage $\mathcal{L}$, R t_1 ... t_k si, pour tout i, les variables libres de t_i sont dans $\{x_0, \ldots, x_n\}$, et il existe des valeurs $a_0, \ldots, a_n$ des variables $x_0, \ldots, x_n$ telles que :
$(\bar{t_1}(a_0, \ldots, a_n), \ldots, \bar{t_k}(a_0, \ldots, a_n)) \in \bar{R}$.
On note : $\mathcal{M}$,$\{a_1, \ldots, a_n\}$⊨F$(x_1, \ldots, x_n)$ pour exprimer que la structure $\mathcal{M}$ satisfait la formule F en $(a_1, \ldots, a_n)$.
On étend cette notion à toutes les formules du langages par induction sur la structure de la formule :

- $\mathcal{M}\models$ F∧G ssi $\mathcal{M}\models$ F et $\mathcal{M}\models$ G ;
- $\mathcal{M}\models$ F∨G ssi $\mathcal{M}\models$ F ou $\mathcal{M}\models$ G ;
- $\mathcal{M}\models$ ¬F ssi $\mathcal{M}\not\models$ F ;
- $\mathcal{M}\models$ ∀xF[x] ssi pour toute valeur a de x prise dans le domaine, $\mathcal{M}\models$ F[a] ;
- $\mathcal{M}\models$ ∃xF[x] ssi il existe une valeur a de x prise dans le domaine telle que $\mathcal{M}\models$ F[a].

Théorie d'un langage :
Il s'agit d'un ensemble de formules closes, c'est-à-dire sans variables libres.

Notion de modèle : Soit T une théorie du langage $\mathcal{L}$. $\mathcal{M}$ une $\mathcal{L}$-structure de domaine D est un modèle de T ssi $\mathcal{M}$ satisfait toutes les formules de T. On note : $\mathcal{M}\models$T.

1.2.3 Définissabilité et synonymie

Soit $\mathcal{L}$ un langage et $\mathcal{M}$ une $\mathcal{L}$-structure. On dit qu'une relation R d'arité n est $\mathcal{L}$-définissable dans $\mathcal{M}$ s'il existe une formule ϕ du premier ordre à n variables libres de $\mathcal{L}$ telle que :
R=$\{(a_1, \ldots, a_n) \in D^n \backslash\ \mathcal{M}\models \phi(a_1, \ldots, a_n)\}$.

Une fonction f est définissable dans $\mathcal{M}$ si son graphe $\{(x, f(x))\}_{x\in D}$ est $\mathcal{L}$-définissable dans $\mathcal{M}$.

Synonymie :
Deux langages $\mathcal{L}$ et $\mathcal{L}'$ sont synonymes sur une $\mathcal{L}\cup\mathcal{L}'$-structure $\mathcal{M}$ si $\mathcal{L}$ et $\mathcal{L}'$ définissent exactement les mêmes fonctions et relations : on peut définir les fonctions et relations de $\mathcal{L}$ dans $\mathcal{L}'$ et inversement.

1.3 Arithmétique de Peano

1.3.1 Axiomes de base

On s'intéresse au langage $\mathcal{L}_0$: {0,S,×,+,=} et à une $\mathcal{L}_0$-structure où S est interprétée comme la fonction successeur $x \mapsto x+1$, + et × par les fonctions usuelles, et = par la relation d'égalité usuelle.
On considère une théorie notée $\mathcal{P}$, qui détermine l'arithmétique de Peano, formée de :

- un ensemble de sept axiomes de base, $\mathcal{P}_0$:

$$\begin{aligned}
&A_1 : \forall v_0 \neg S v_0 = 0\\
&A_2 : \forall v_0 \exists v_1 (\neg v_0 = 0 \rightarrow S v_1 = v_0)\\
&A_3 : \forall v_0 \forall v_1 (S v_0 = S v_1 \rightarrow v_0 = v_1)\\
&A_4 : \forall v_0 (v_0 + 0 = v_0)\\
&A_5 : \forall v_0 \forall v_1 (v_0 + S v_1 = S(v_0 + v_1))\\
&A_6 : \forall v_0 (v_0 \times 0 = 0)\\
&A_7 : \forall v_0 \forall v_1 (v_0 \times S v_1 = (v_0 \times v_1) + v_0)
\end{aligned}$$

- un schéma d'axiomes d'induction (SI) formé des formules de la forme : pour n entier et $F[v_0, \ldots, v_n]$ une formule de $\mathcal{L}_0$ telle que $v_0, \ldots, v_n$ soient exactement les variables libres de F :

$$\forall v_1 \ldots \forall v_n ((F[0, v_1, \ldots, v_n] \wedge \forall v_0 (F[v_0, \ldots, v_n] \rightarrow F[S v_0, v_1, \ldots, v_n])) \rightarrow \forall v_0 F[v_0, \ldots, v_n])$$

On peut également définir une théorie au second ordre en remplaçant (SI) par une unique formule :

$$\forall X(((0 \in X) \wedge \forall x(x \in X \rightarrow Sx \in X)) \rightarrow \forall x(x \in X))$$

où X est une variable parcourant l'ensemble des parties de $\mathbb{N}$.
Mais comme précisé précédemment, nous ne nous intéresserons qu'à la théorie de Peano au premier ordre.

1.3.2 Résumé

A partir de maintenant, on travaillera sur la $\mathcal{L}_0$-structure $< \mathbb{N}, +, \times, =>$ qui est un modèle de $\mathcal{P}$. Remarquons que la fonction successeur est directement définissable en termes d'addition par la formule :

$$\forall x \forall y \exists \rho(((x = Sy) \leftrightarrow (x = y + \rho)) \wedge Un(\rho))$$

où $Un(\rho)$ est la formule $\forall t(t \times \rho = t)$ (exprime que $\rho = 1$).
ce qui permet bien à la structure $< \mathbb{N}, +, \times, =>$ d'être un modèle de $\mathcal{P}$ (à une expansion par définition près comme disent les logiciens).
Revenons maintenant un instant à la raison pour laquelle il est indispensable de travailler au premier ordre :
On dit qu'une théorie est cohérente s'il n'existe pas de formule F du langage associé qui soit telle que l'on ait simultanément : T⊢F et T⊢ ¬F. (T⊢F signifie qu'il existe une preuve formelle de F à partir des axiomes de T en utilisant des règles de déduction). Or le théorème de complétude (Gödel - 1930) assure que toute théorie cohérente admet un modèle. (cf. [3], Tome 1. Chapitre 4)
Au second ordre, le théorème de complétude est faux, on ne peut donc pas considérer de modèle de Peano au second ordre dans le cadre qui nous intéresse.

2 La conjecture d'Erdös - Woods

2.1 Présentation

Il peut arriver curieusement que la logique intervienne dans des problèmes purement arithmétiques. C'est le cas de la conjecture suivante, due à A.Woods :

> " 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,...,k, les entiers x+i et y+i ont les mêmes diviseurs premiers ?"

Cette conjecture est un affaiblissement de la conjecture due à P.Erdös :

> " Il n'y a qu'un nombre fini d'entiers m, n, h, k avec k≥h≥3 et m≠n tels que les produits (m+1)(m+2)...(m+k) et (n+1)(n+2)...(n+h) aient les mêmes diviseurs premiers."

C'est pourquoi la première conjecture est appelée conjecture d'Erdös-Woods.
Or elle est équivalente à un problème de définissabilité soulevé par J.Robinson, en les termes suivants :

> " Peut-on définir au premier ordre toute l'arithmétique (prédicats et fonctions usuelles +, ×, Exp, ...) avec seulement la fonction successeur S et le prédicat de coprimarité ⊥ (x⊥y ssi x et y sont premiers entre eux) ?¿ ¿

Une évolution parallèle de l'étude de cette conjecture entre théorie des nombres et logique est d'autant plus intéressante qu'elle permet de jeter des ponts entre ces deux disciplines a priori fort distinctes : la théorie des nombres apporte à la logique des outils puissants pour démontrer des synonymies et des propriétés intéressantes, tandis que la logique apporte un éclairage nouveau sur certains aspects de la théorie des nombres...

2.2 Quelques résultats à propos d'Erdös-Woods

Il serait long de mentionner dans un souci d'exhaustivité tous les résultats utilisés jusqu'à ce jour dans l'étude de la conjecture d'Erdös-Woods, mais certains dépassent largement ce cadre et méritent d'être mentionnés.

2.2.1 Théorie des nombres

Pour commencer, voici quelques notations qui pourront s'avérer utiles par la suite :
On notera SUPP(x) l'ensemble des diviseurs premiers de x. Rappelons au passage qu'un entier est primaire si SUPP(x) est un singleton. (x est une puissance d'un nombre premier).
On notera ORD(x,p) le plus petit nombre u tel que $x^u \equiv 1\ [p]$.
On aura également besoin de la relation d'équivalence suivante : pour A une partie de $\mathbb{Z}$ donnée, $x \cong_A y$ ssi pour tout entier i dans A, $SUPP(\mid x+i \mid) = SUPP(\mid y+i \mid)$.

Outils

Théorème 1 (Dirichlet) *il existe une infinité de nombres premiers dans les progressions arithmétiques $u_n = an + b$ pour $a \perp b$.*

Théorème 2 (Restes chinois) *Soient $(b_0, \ldots, b_n)$ des entiers premiers entre eux et $(\alpha_0, \ldots, \alpha_n)$ des entiers, alors il existe $a \in \mathbb{N}$ tel que $\forall i \in \{0 \ldots n\}, a \equiv \alpha_i [b_i]$.*

Théorème 3 *Il y a équivalence entre les propositions suivantes :*
i). $x = y$
ii). Pour une infinité d'entiers z, $SUPP(x+z) = SUPP(y+z)$

<u>*Dem*</u> : voir Annexe A

Les théorèmes les plus importants dans l'étude de la conjecture d'Erdös-Woods sont, entre autres :
- Le théorème de Zsigmondy-Birkhoff-Vandiver :

Théorème 4 (ZBV) *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 <u>primitif</u> 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).$n = 6$, $x = 2$, $y = 1$.

- Le théorème de Lucas-Carmichael :

Théorème 5 (LC) *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 un corollaire du précédent puisque tout diviseur primitif de $x^{2n} - y^{2n}$ est diviseur caractéristique pour $x^n + y^n$.

- Le théorème de Størmer :

Théorème 6 (Størmer) *Soient $p_1, \ldots, p_n$ des entiers premiers distincts, soient K, $\alpha_1, \ldots, \alpha_n$ des entiers strictement positifs. Pour $1 \leq i \leq n$, posons $\varepsilon_i = 1$ si α_i est impair et $\varepsilon_i = 2$ si α_i est pair. On pose aussi D=$K.p_1^{\varepsilon_1}, \ldots, p_n^{\varepsilon_n}$.*
Si $x^2 - 1 = K.p_1^{\alpha_1}, \ldots, p_n^{\alpha_n}$ alors x est la solution fondamentale de l'équation de Pell-Fermat $x^2 - Dy^2 = 1$.
Si $x(x+1) = K.p_1^{\alpha_1}, \ldots, p_n^{\alpha_n}$ alors x est la solution fondamentale de l'équation de Pell-Fermat $x^2 - 4Dy^2 = 1$.

(sur les équations de Pell-Fermat, voir Annexe A).

- Un autre résultat intéressant, corollaire du théorème de Størmer :

Théorème 7 *Soient x et y des entiers positifs ou nuls. Il y a équivalence entre :*
i). x=y
ii). SUPP(x)=SUPP(y) et, pour une infinité d'entiers m, on a :

$$\begin{cases} SUPP(x+m) = SUPP(y+m) \\ SUPP(x+m+1) = SUPP(y+m+1) \end{cases}$$

iii). SUPP(x)=SUPP(y) et, pour une infinité d'entiers m, on a

$$SUPP(mx+1) = SUPP(my+1).$$

Retour à Erdös-Woods

Nous allons voir comment faire un lien entre ces notions et la conjecture d'Erdös-Woods. Il suffit de passer par la relation d'équivalence $\cong_A$ définie précédemment. En effet la conjecture d'Erdös-Woods équivaut à l'existence d'un entier k tel que la trace sur $\mathbb{N}$ de $\cong_{\{0,\ldots,k\}}$ (ou de $\cong_{\{-k,\ldots,0\}}$, ou de $\cong_{\{-k,\ldots,k\}}$) soit la relation d'égalité.

Cette notion permet de voir que si l'on se restreint aux entiers primaires, la conjecture est vraie pour k=2.

Théorème 8 (restriction aux entiers primaires) *Les restrictions à l'ensemble PP des entiers primaires des relations $\cong_{\{0,1,2\}}$, $\cong_{\{-2,-1,0\}}$, $\cong_{\{-1,0,1\}}$ coïncident avec la relation d'égalité.*

(Démonstration en Annexe A.4).

Il est même possible d'étendre ce résultat "autour" des entiers primaires :

Corollaire 1 *Soit $n > 0$.*
Sur l'ensemble $PP + [0, \dots, n] = \{x + s/x \in PP, s \in \{0, \dots, n\}\}$ la relation $\cong_{\{-n-1,\dots,-1,0\}}$ coïncide avec la relation d'égalité. (respectivement $\cong_{\{0,1,\dots,n+1\}}$ sur $PP + [-n, \dots, 0]$ et $\cong_{\{-n,\dots,0,\dots,n\}}$ sur $PP + [-n, \dots, n]$)

2.2.2 Logique

On va retrouver le résultat précédent, en se servant cette fois d'outils empruntés à la logique mathématique. Il s'agit maintenant de travailler sur le problème de J.Robinson :

> " Peut-on définir l'addition et la multiplication en terme d'égalité, successeur et coprimarité ?".

Lien avec Erdös-Woods

L'équivalence entre le problème de J.Robinson et la conjecture est due à A.Woods :

Théorème 9 (équivalence E-W - J.Robinson avec égalité) *Les propositions suivantes sont équivalentes :*
i). On peut définir l'addition et la multiplication en termes d'égalité, coprimarité et fonction successeur.
ii). On peut définir l'ordre ou l'addition ou la multiplication en termes d'égalité, coprimarité et fonction successeur.
iii). La conjecture d'Erdös-Woods.

Ce théorème est lui-même équivalent au suivant :

Théorème 10 (équivalence E-W - J.Robinson sans égalité) *Les propositions suivantes sont équivalentes :*
i). On peut définir 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 terme de successeur et de coprimarité.
iv). La conjecture d'Erdös-Woods.

Les équivalences entre les points 9.i, 9.ii, 10.i et 10.ii relèvent de problèmes de synonymie (voir plus loin). Pour les autres équivalences, on se sert du théorème suivant :

Théorème 11 (définissabilité et saturation) *si ρ est une relation définissable dans la structure $< \mathbb{N}, +, \times, => $:*
ρ est définissable dans la structure $< \mathbb{N}, S, \perp >$ ssi elle est saturée pour une relation $\cong_A$, où A est un ensemble fini d'entiers positifs ou nuls.

(Une relation saturée pour $\cong_A$ est une partition de classes de $\cong_A$).
Quelques morceaux de démonstration du théorème 10 :
10.iii).⇒10.iv). : si l'égalité est (S,⊥)-définissable, alors elle est saturée pour un certain $\cong_{\{0,\ldots,k\}}$, ce qui implique Erdös-Woods.
10.iv).⇒10.iii). : l'égalité est définissable dans $< \mathbb{N}, S, \perp >$ si E-W est vraie :

$$\forall z((z \perp x \leftrightarrow z \perp y) \wedge (z \perp Sx \leftrightarrow z \perp Sy) \wedge \ldots \wedge (z \perp S^k x \leftrightarrow z \perp S^k y))$$

10.iv).⇒10.i). repose également sur le théorème précédent.

On mentionnera enfin le théorème suivant, qui établit l'équivalence en restriction aux primaires entre les structures $< \mathbb{N}, S, \perp >$ et $< \mathbb{N}, +, \times, => $:

Théorème 12 (D.Richard - 1985) *Toute relation définissable dans la structure $< \mathbb{N}, +, \times, => $ et qui ne porte que sur les entiers primaires est également définissable dans la structure $< \mathbb{N}, S, \perp >$.*

Ce théorème est le pendant logique du théorème 8.

Intervention de la méthode de codage ZBV

On va définir peu à peu les relations et fonctions qui seront utiles pour établir l'équivalence au point de vue pouvoir de définissabilité entre les structures $< \mathbb{N}, S, \perp, >$ et l'image de $< \mathbb{N}, =, +, \times >$ par l'isomorphisme $x \mapsto 5^x$.
La méthode complète figure dans [1], il n'est donc fait mention ici que des étapes principales.

Etablissement d'une structure ensembliste sur les premiers

On considère l'ensemble P des nombres premiers, et une structure sur ses parties finies : on code une partie finie de P par les entiers ayant cette partie comme support.

- la relation d'inclusion entre deux parties se traduit par l'inclusion des supports de leurs codes : $SUPP(x) \subseteq SUPP(y)$, autrement dit dans le langage $<\perp>$ par la formule : $\forall z((z \perp y) \rightarrow (z \perp x)$;

- la relation d'égalité entre ensembles, les opérateurs d'union, intersection et différence en découlent simplement ; (voir annexe B)
- on peut définir ensuite l'ensemble des primaires (un primaire est un entier caractérisé par l'inclusion de son support dans celui de tout entier non premier avec lui), par l'intermédiaire des formules PP(x) (x est primaire) et PP(x,y) (x et y sont primaires d'un même premier) :
  $\forall y((\neg(x \perp y)) \rightarrow SUPP(x) \subseteq SUPP(y))$ et
  $PP(x) \wedge PP(y) \wedge \neg(x \perp y)$;
- les constantes 1 et 0 peuvent être également définies dans ce même langage : $EGAL_1(x) \leftrightarrow \forall y(y \perp x)$ et
  $EGAL_0(x) \leftrightarrow \forall y((y \perp x) \rightarrow EGAL_1(y))$.

Définition des fonctions et relations restreintes

On traite en parallèle les cas des langages $< S, \perp >$ et $< Pred, \perp >$.

1. L'égalité restreinte à PP : On a vu que l'égalité sur les primaires était équivalente aux relations $\cong_{\{0,1,2\}}$ et $\cong_{\{-2,-1,0\}}$. On se sert de cette propriété pour définir l'égalité dans les langages $< S, \perp >$ et $< Pred, \perp >$, restreinte aux primaires (notée $=_{PP}$) :
   $$PP(x,y) \wedge SUPP(Sx) = SUPP(Sy) \wedge SUPP(S^2x) = SUPP(S^2y)$$
   $$PP(x,y) \wedge SUPP(Pred(x)) = SUPP(Pred(y)) \wedge SUPP(Pred^2(x)) = SUPP(Pred^2(y))$$
2. Les restrictions de Pred et S : on définit les restrictions des fonctions Pred et S ($Pred_{PP}$ et S_{PP}) puis les ensembles $PP + [-n, \ldots, 0]$ dans $< \mathbb{N}, S, \perp >$ et $PP + [0, \ldots, n]$ dans $< \mathbb{N}, Pred, \perp >$;
3. Les singletons : Dans $< Pred, \perp >$, ils sont définis par la formule
   $EGAL_1(Pred^{n-1}(x))$ et dans $< S, \perp >$ par la formule
   $S^{p-n}(x) =_{PP} S^p(1)$, où p est un premier plus grand que x. On notera dans les deux cas $EGAL_n(x)$ la formule définissant l'ensemble {n} ;
4. L'ensemble P : il se définit d'après les théorèmes 4 et 5 et grâce à l'intermédiaire de l'ensemble des primaires x tels que $SUPP(x-1) \subseteq SUPP(y-1)$ pour tout primaire y de même base.
   Le fait de pouvoir exprimer P enrichit la théorie des parties finies de P. Cela permet également d'exprimer un codage des relations et fonctions sur les parties finies de P, qui mène à l'indécidabilité de la théorie $< \mathbb{N}, S, \perp >$; (voir Annexe B)
5. Un petit bout d'exponentielle : on peut définir dans $< S, \perp >$ ou $< Pred, \perp >$ la relation $\{(p, q, u) : p$ et q sont premiers distincts, et $u = q^{ORD(q,p)}\}$;

6. La fonction $x \mapsto 5^x$: sa restriction à l'ensemble P est définissable dans la structure $< \mathbb{N}, S, \perp >$. (voir Annexe B et [1])

Isomorphisme de structures $x \mapsto 5^x$

On déplace le problème de J.Robinson vers la fonction $x \mapsto 5^x$ par le biais du théorème suivant :

Théorème 13 *La fonction $x \mapsto 5^x$ transforme la structure $< \mathbb{N}, +, \times, = >$ en une structure $< 5^{\mathbb{N}}, NA, NM, =_{PP} >$ qui est entièrement définissable dans la structure $< \mathbb{N}, S, \perp >$.*
En particulier, les structures $< \mathbb{N}, S, x \mapsto 5^x, \perp >$ et $< \mathbb{N}, +, \times, = >$ définissent les mêmes relations et fonctions.

Dem :
Les images par la fonction $x \mapsto 5^x$ de la fonction successeur et de la relation de divisibilité sont définissables dans $< S, \perp >$: se sont respectivement la fonction $5^n \mapsto 5^{n+1}$ de domaine $5^{\mathbb{N}}$ (notée NS) et la relation $\{(5^n, 5^m) \backslash n \mid m\}$ (notée NDIV).
On définit alors dans la structure $< \mathbb{N}, S, \perp >$ une structure $< 5^{\mathbb{N}}, NS, NDIV >$ isomorphe à la structure $< \mathbb{N}, S, | >$. Comme dans cette structure l'addition et la multiplication sont définissables (résultat obtenu pa r J.Robinson, voir 2), on peut, en transposant les formules correspondantes, définir dans $< 5^{\mathbb{N}}, NS, NDIV >$ des fonctions NA et NM qui sont images des fonctions + et $\times$ par l'isomorphisme $x \mapsto 5^x$.
On a donc une équivalence entre la validité de la conjecture d'Erdös-Woods et la $< S, \perp >$-définissabilité de la fonction $x \mapsto 5^x$ de domaine $\mathbb{N}$.

3 Problèmes de définissabilité et de synonymie

Dans cette section, on s'attachera surtout à présenter une vue d'ensemble des outils utilisés sans rentrer dans des détails de calculs parfois subtils, et quelques résultats intéressants dans le cadre de l'arithmétique de Peano et des arit hmétiques voisines définies sur des sous-langages ou des langages synonymes.

3.1 Préliminaires de calculabilité

La notion de calculabilité, très importante dans le domaine de l'informatique théorique, peut être utile dans le cas qui nous intéresse afin de comprendre les différents types de fonctions et relations accessibles au sein de l'arithmétique de Peano. Elle permet de faire une distinction entre différents problèmes via une certaine mesure de complexité, la récursivité.

3.1.1 Récursivité

Il existe plusieurs notion de récursivité, qui semblent recouvrir le même ensemble d'objets. La notion la plus couramment rencontrée est celle de récursivité définie à partir de fonctions de base, composition et récurence.

Fonctions récursives primitives et prédicats récursifs primitifs

Les fonctions récursives primitives font partie de l'ensemble $\{\mathbb{N}^k \to \mathbb{N}/k \geq 0\}$. Elles sont définies à partir des fonctions de bases, qui sont :
- la fonction **0**
- les fonctions de projection $\pi_j^k : (n_1, \dots, n_k) \mapsto n_j$
- la fonction successeur **S** : $\lambda n.n + 1$

Les deux schémas de construction sont :
- la composition : si g est une fonction d'arité l et $h_1, \dots, h_l$ d'autres fonctions d'arité k, la composée de g par $h_1, \dots, h_l$ est la fonction : $(n_1, \dots, n_k) \mapsto g(h_1(n_1, \dots, n_k), \dots, h_l(n_1, \dots, n_k))$;
- la récurrence : si g et h sont des fonctions d'arités respectives k et $k+2$, alors la fonction f d'arité $k+1$ est définie par récurrence à partir de g et h si : $f(n_1, \dots, n_k, 0) = g(n_1, \dots, n_k)$ et $f(n_1, \dots, n_k, m+1) = h(n_1, \dots, n_k, m, f(n_1, \dots, n_k, m))$.

Exemples de fonctions primitives récursives : les fonctions constantes, $+$, $\times$, les fonctions puissances n^m, la fonction factorielle,...
Les prédicats récursifs primitifs sont ceux dont la fonction caractéristique (fonction qui prend la valeur 1 en les points appartenant au prédicat et 0 sinon) est primitive récursive.
Exemple de prédicats primitifs récursifs : $n < m$, $n = m$,...

Fonctions semi-récursives, schéma μ, ensembles récursifs

Il existe une classe de fonctions qui recouvre celle des fonctions récursives primitives, les fonctions semi-récursives, construites comme les premières et avec le schéma de minimisation non borné ou schéma μ :
on considère un prédicat primitif récursif $p(n_1, \dots, n_k, m)$ et la fonction f d'arité k est définie à partir de p par le schéma μ si : $f(n_1, \dots, n_k) = \mu z p(n_1, \dots, n_k, z) =$ le plus petit z tel que $p(n_1, \dots, n_k, z)$ est vrai, 0 sinon.

Lien avec la calculabilité

Les problèmes de calculabilité font intervenir les machines de Turing (déterministes) :

$$\mathcal{M} = (Q, \Gamma, \Sigma, \delta, s, B, F)$$

où :

- Q est un ensemble fini d'états ;
- Γ est l'alphabet utilisé sur le ruban ;
- $\Sigma \subseteq \Gamma$ est l'alphabet utilisé pour le mot d'entrée ;
- $s \in Q$ est l'état initial ;
- $F \subseteq Q$ est l'ensemble des états finaux ;
- $B \in \Gamma - \Sigma$ est le symbole "blanc" ;
- $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{\leftarrow, \rightarrow\}$ est la fonction de transition qui permet de passer d'une configuration a une autre.

On dit alors qu'un langage est récursif s'il vérifie cette propriété :
" La machine atteint un état final accepteur pour tout mot du langage et un état final non accepteur pour tout mot qui n'est pas dans le langag".
Et un langage est dit récursivement énumérable s'il vérifie la propriété
" La machine atteint un état final accepteur pour tout mot du langage, et soit s'arrête sur un état final non accepteur, soit ne s'arrête pas, pour un mot qui n'est pas dans le langage".

Or les fonctions récursives sont calculables par machines de Turing et inversement, grâce à un encodage possible des nombres entiers en chaînes de caractères et inversement. (Pour une démonstration, voir [7], pages 172 à 179).
Ces deux notions sont intimement liées, c'est le résultat énoncé par la thèse de Church.

Récursivité au sens d'Herbrand-Gödel

Une autre définition de la récursivité est due à Gödel d'après une idée de Herbrand. Elle fait intervenir des systèmes d'équation. On définit des termes par :
- Les variables sont des termes ;
- 0 est un terme ;
- Si t est un terme, alors $\mathbf{S}t$ est un terme ;
- si $t_1, \ldots, t_n$ sont des termes et que f_j^n est un symbole de fonction, alors $f_j^n(t_1, \ldots, t_n)$ est un terme.

On définit également les nombres dans ce langage comme termes : $\bar{0}$ est $\mathbf{0}$, $\overline{n+1}$ est $\mathbf{S}\bar{n}$.
Une équation est une formule $r = s$ où r et s sont des termes.
Un système d'équations est une suite finie d'équations dont la dernière est de la forme : $f_j^n(t_1, \ldots, t_n) = s$. f_j^n est alors appelé symbole principal du système.
On dispose de deux règles d'inférence qui donnent la notion de preuve d'une équation à partir d'un système. On dit qu'une fonction $\phi(x_1, \ldots, x_n)$ est calculable dans un système d'équations $\mathcal{E}$ si et seulement si le symbole principal de $\mathcal{E}$ est un symbole de fonction d'arité n, f_j^n, tel que

pour tous entiers $k_1, \ldots, k_n, p$, on ait :
$\mathcal{E} \vdash f_j^n(\bar{k_1}, \ldots, \bar{k_n}) = p$ si et seulement si $\phi(k_1, \ldots, k_n) = p$.
On dit alors qu'une fonction est calculable au sens de Herbrand-Gödel si et seulement si on peut trouver un système d'équations dans lequel elle est calculable au sens précédent.
Cette troisième définition de fonctions calculables est équivalente aux deux précédentes. Pour une démonstration détaillée, se référer à [5].

3.1.2 Décidabilité - Théorème d'incomplétude de Gödel

Dans cette partie seront traitées les notions de décidabilité appliquées à l'arithmétique, notamment le caractère indécidable de $\mathcal{P}$.

Décidabilité

On va parler de décidabilité d'une théorie (en l'occurence celle de $< \mathbb{N}, +, \times, => $) : il s'agit de savoir s'il existe un algorithme qui permette de répondre à la question "est-ce-que la formule X est un théorème dans la stru cture concernée ?" pour toute formule X.

Le thorme d'incompltude

La complétude d'une théorie est la propriété qui consiste en l'identification des formules vraies et des formules prouvables dans la structure concernée.
On distingue deux résultats classiques concernant la théorie $\mathcal{P}$: le théorème d'indécidabilité dû à Gödel et Rosser (1936) et le théorème d'incomplétude dû à Gödel (1931). Le second est plus faible que le premier, mais c'est celui auquel nous nous intéresserons de plus près.

Théorème 14 (indécidabilité) *Si la théorie $\mathcal{P}$ est cohérente, elle contient une formule F qui n'est ni prouvable, ni réfutable dans $\mathcal{P}$.*

Théorème 15 (incomplétude) *Si la théorie $\mathcal{P}$ est cohérente, elle contient une formule vraie qui n'est pas démontrable dans $\mathcal{P}$.*

Il existe un second théorème d'incomplétude également dû à Gödel (1931) qui explique l'hypothèse restrictive des deux précédents sur la cohérence de $\mathcal{P}$:

Théorème 16 (incomplétude - bis) *Il existe une formule arithmétique exprimant la cohérence de $\mathcal{P}$, qui n'est pas démontrable dans $\mathcal{P}$.*

Il existe des démonstrations de la cohérence de $\mathcal{P}$, mais en se plaçant dans un système plus complexe, ou en changeant la notion de preuve.
Il existe de nombreuses variantes de la preuve du theorème 15, mais elles reposent généralement sur un codage des formules. On peut travailler sur les fonctions et relations récursives primitives comme dans [8], ou sur les fonctions et relations arithmétiques comme ci-dessous.

Une démonstration possible

Cette démonstration (détaillée en [6]) se fonde sur l'idée suivante : on choisit un langage synonyme de $< +, \times, =>$, on lui rajoute un symbole bizarre # et on lui adjoint d'autres symboles pour obtenir un nombre de symboles égal à un nombre premier, par exemple 13.(pour des raisons de commodité)

Au préalable, quelques définitions :

- les numéraux : $\overline{n}$ est le terme $S^n(0)$;
- une relation Arithmétique ou une fonction Arithmétique est une relation ou une fonction définissable dans le langage $< +, \times, = , Exp >$;
- une relation arithmétique ou une fonction arithmétique est une relation ou une fonction définissable dans le langage $< +, \times, =>$. On a vu en 1.1 que cela était équivalent. Or pour plus de simplicité on a besoin de travailler sur la notion Arithmétique. On va donc prouver l'incomplétude de Peano avec exponentielle, ce qui sera équivalent avec l'incomplétude de Peano tout court ;
- la concaténation en base 13 : si $x = x_k \dots x_0$ et $y = y_l \dots y_0$ sont deux nombres $n_x = x_0 \times 1 + x_1 \times 13^1 + \dots + x_k \times 13^k$ et $n_y = y_0 \times 1 + y_1 \times 13^1 + \dots + y_l \times 13^l$, exprimés en base 13, le nombre $x *_{13} y$ est $x_k \dots x_0 y_l \dots y_0$. Cette fonction de concaténation est Arithmétique ;
- numérotation des formules : à chaque symbole du langage choisi, on associe un chiffre en base 13, et pour toute formule, le numéro qui lui est associé est obtenu en “lisant” les chiffres dans l'ordre d'apparition des symboles. Ainsi en notant E_n la formule de numéro n, on a $E_x E_y = E_{x *_{13} y}$. Enfin en choisissant pour le symbole représentant la fonction successeur le numéro 0, on a un codage simple des numéraux (le numéro de Gödel de $\overline{n}$ est 13^n) ;

Voici certaines propriétés utiles pour une numérotation de Gödel :

1. Il existe une fonction arithmétique $(x, y) \mapsto x \circ y$ telles que pour toute expression X et Y de numéros de Gödel respectifs x et y, $x \circ y$ est le numéro de Gödel de l'expression XY (ici c'est donc la concaténation en base 13).
2. Pour tout entier n, le numéro de Gödel du numéral $\overline{n}$ est une fonction arithmétique de n (ici la fonction $n \mapsto 13^n$).

La démonstration repose dès lors sur deux résultats importants :

Théorème 17 (Tarski) *L'ensemble T des numéros de Gödel des énoncés vrais du langage n'est pas Arithmétique.*

Théorème 18 *Les ensembles P et R des numéros de Gödel des formules respectivement prouvables et réfutables de Peano sont Arithmétiques.*

On appelera “énoncé de Gödel d'un ensemble A” une formule X telle que :
– soit X est vraie et son numéro de Gödel est dans A ;
– soit X est fausse et son numéro de Gödel n'est pas dans A.
Le premier résultat peut se ramener au suivant :

Lemme 1 *Tout ensemble Arithmétique possède un énoncé de Gödel.*

Pour arithmétiser la syntaxe de Peano avec exponentielle, nous avons besoin de pouvoir coder les suites d'expressions. Le symbole bizarre # intervient alors : le numéro de Gödel de la suite $(X_{x_1}, \dots X_{x_n})$ est alors le numéro de Gödel de l'expression $\#E_{x_1}\# \dots \#E_{x_n}\#$. On peut alors coder successivement de manière Arithmétique le fait pour une expression E_x d'être une v ariable, un terme, une formule atomique, une formule, un axiome, une formule déduite à partir d'une autre par une règle donnée, une preuve, prouvable, réfutable. Ce qui donne finalement le deuxième résultat.
La conjonction des deux résultats montre bien que les énoncés vrais ne sont pas identifiables aux énoncés prouvables dans Peano.
Pour une démonstration détaillée, des extensions et autres considérations sur le même sujet, voir [6].

3.1.3 Toute relation récursivement énumérable est diophantienne. 10^e problème de Hilbert

Equations diophantiennes

Une équation diophantienne est une équation de la forme $P(x_0, \dots, x_{n-1}) = 0$, où $P(x_0, \dots, x_{n-1})$ est un polynôme à coefficients entiers. C'est le cas par exemple des équations de Pell-Fermat (voir Annexe A), o u des équations de Fermat $x^n + y^n = z^n$.
Pour chacun des domaines D= $\mathbb{N}^*$, $\mathbb{N}$, $\mathbb{Z}$, on peut rechercher des solutions dans D d'une équation diophantienne. En fait cela revient au même de rechercher des solutions dans l'un quelconque de ces domaines, étant don né que l'on peut ramener chacun de ces problèmes à l'un des autres. En outre, pour D= $\mathbb{Q}$, la classe des équations admettant des solutions dans ce domaine est contenue dans la classe des équations admettant des solutions dans $\mathbb{Z}$.

Le dixième problème de Hilbert

Le dixième problème de Hilbert consiste en la décidabilité des classes d'équations ayant des solutions dans un domaine donné. En l'occurrence, il s'agit de savoir s'il existe un algorithme qui, prenant une équation diophantienne en entr 'ee, détermine si elle possède des solutions dans $\mathbb{N}$ en un temps fini.

Ce problème a une réponse négative : un tel algorithme n'existe pas. ce résultat a été obtenu par M.Davis, H.Putnam et J.Robinson à partir des années soixantes sous une forme affaiblie, et par Y.Matiassevich vers 1970.

Lien entre caracères diophantien et récursif

Les deux preuves de l'insolvabilité du dixième problème de Hilbert évoquées ci-dessus font appel aux relations récursivement énumérables :

Théorème 19 (Davis-Putnam-Robinson) *Toute relation récursivement énumérable est exponentiellement diophantienne.*

Ce théorème peut s'exprimer de manière plus explicite sont la forme : pour toute relation récursivement énumérable $R \in \mathbb{N}^n$, il existe un polynôme exponentiel P tel que $R(a_0, \ldots, a_{n-1})$ est définie par :

$$\exists x \forall y \leq x \exists x_0 \leq x \ldots \exists x_{n-1} \leq x (P(a_0, \ldots, a_{n-1}, x, y, x_0, \ldots, x_{n-1}) = 0)$$

Un polynôme exponentiel est un élément de l'ensemble EP défini par induction de la manière suivante : les variables et les entiers naturels sont dans EP, si P et Q sont dans EP, alors P+Q et P×Q sont dans EP, si n est un entier positif et X et Y des variables, alors n^Y et X^Y sont dans EP.

Associé au fait que la relation $z = x^y$ est diophantienne, ce théorème prouve l'équivalence entre relations récursivement énumérables et relations diophantiennes (car une relation diophantienne est récursivement énumérable). Or il n' existe pas d'algorithme qui, prenant une relation récursivement énumérable et un uplet de valeurs, peut déterminer si la relation est vraie sur cette entrée, d'où l'indécidabilité du dixième problème de Hilbert.

Remarque : on a ici une démarche analogue à celle utilisée dans la preuve de l'incomplétude de Peano : on étudie ce qui se passe en présence de l'exponentielle, puis on se ramène au cas plus général en focalisant l'étude su r celle-ci. C'est également un peu une des démarches adoptées en ce qui concerne Erdös-Woods, puisqu'on a prouvé la conjecture à un isomorphisme exponentiel près, et que le point manquant pour prouver la conjecture dans le cas généra l est la $< S, \perp >$-définissabilité de la fonction $x \mapsto 5^x$.

3.2 Les arithmétiques faibles

On appelle arithmétique faible une $\mathcal{L}$-structure, où $\mathcal{L}$ est soit une restriction de $\mathcal{L}_0$, soit une restriction d'un de ses langages synonymes.

3.2.1 Presburger, $\mathcal{L}= \{+, 0\}$

On s'intéresse à la théorie du langage $< +, <, = >$. Cette théorie est décidable, résultat prouvé par Presburger (1929) et Skolem (1930).

La méthode utilisée est celle de l'élimination des quantificateurs : pour une théorie T d'un langage $\mathcal{L}$, une élimination de quantificateurs pour T est une façon d'associer à chaque formule ϕ de $\mathcal{L}$ une formule ψ de $\mathcal{L}$ sans quantificateurs, telle que $T \vdash \phi \leftrightarrow \psi$.
Généralement, on étend le langage $\mathcal{L}$ et on prouve le résultat pour le langage étendu $\mathcal{L}$'.
Dans le cas de l'addition, Skolem et Presburger se sont intéressés à la théorie de $< \mathbb{Z}, <, +, 0, 1 >$, où $\mathbb{N}$ est définissable aisément par la formule : $(v_0 = 0) \vee (0 < v_0)$.

Pour trouver une élimination de quantificateurs, il suffit en fait de se restreindre à certaines formules, de la forme : $\exists v_i \bigwedge_i \phi_j v_i$, où ϕ_j est une formule atomique ou la négation d'une formule atomique.

La méthode de Skolem fait intervenir le langage étendu par les fonctions q$\cdot$ (multiplication par le rationnel q), pour q$\in \mathbb{Q}$, et la fonction partie entière supérieure. Pour plus de détails, voir [2].
L'obtention d'une telle élimination permet de conclure sur la décidabilité de la théorie Th$< \mathbb{Z}, <, +, 0, 1 >$ et par conséquent de celle de Th$< \mathbb{N}, <, +, 0, 1 >$: si on a une formule ϕ, on lui associe une formule équivalente ψ sans quantificateurs pour laquelle on sait déterminer son caractère vrai ou faux.

3.2.2 Skolem-Mostowski, $\mathcal{L}= \{\times, 1\}$

De même que la théorie de $< \mathbb{N}, +, 0 >$, celle de $< \mathbb{N}^*, \times, 1 >$ est décidable. Ce résultat, annoncé par Skolem en 1930, a été prouvé par Mostowski en 1952.
En fait, Mostowski ramène la décidabilité de Th$< \mathbb{N}^*, \times, 1 >$ à celle de Th$< \mathbb{N}, +, 0 >$ en s'intéressant au problème plus général de ramener la décidabilité d'un produit de structures à cel les des structures facteurs du produit.

Par le biais du théorème fondamental de l'arithmétique (décomposition unique en facteurs premiers), on peut ramener $< \mathbb{N}^*, \times, 1 >$ à un produit particulier de copies de $< \mathbb{N}, +, 0 >$:
On appelle $p_0, \ldots, p_n, \ldots$ les nombres premiers dans l'ordre croissant et on considère deux nombres entiers x et y. Si $x = p_0^{n_0} \ldots p_k^{n_k} \ldots$ et $y = p_0^{m_0} \ldots p_k^{m_k} \ldots$, alors le produit est $xy = p_0^{n_0+m_0} \ldots p_k^{n_k+m_k} \ldots$.

<u>Puissance directe faible :</u> Soit $\mathcal{M}$ une $\mathcal{L}$-structure de domaine A, et avec $\mathcal{L}$ ne comprenant qu'un symbole de constante c_0, interprété par a dans $\mathcal{M}$ ($a = (c_0)^{\mathcal{M}}$). On appelle puissance directe faible de $\mathcal{M}$ une $\mathcal{L}$-structure $\mathcal{B}$ de domaine B telle que :

- B= { suites de A stationnant sur a à partir d'un certain rang }

$= \{F : \mathbb{N} \to A / \exists x_0 \in \mathbb{N}, \forall x > x_0 (Fx = a)\}$;
- l'interprétation de c_0 est la suite constante de valeur a : $(c_0)^{\mathcal{B}} = (a)_{n\in\mathbb{N}}$;
- si f_i^n est un symbole de fonction d'arité n : $(f_i^n)^{\mathcal{B}}(F_0, \dots, F_n) = F$, où $F(m) = (f_i^n)^{\mathcal{M}}(F_0(m), \dots, F_n(m))$;
- si R_i^n est un prédicat d'arité n : $(R_i^n)^{\mathcal{B}}(F_0, \dots, F_n)$ ssi $\forall m (R_i^n)^{\mathcal{M}}(F_0(m), \dots, F_n(m))$.

Mostowski observa que $< \mathbb{N}^*, \times, 1 >$ est la puissance directe faible de $< \mathbb{N}, +, 0 >$, avec 0 devenant 1, + devenant $\times$. (et $<$ devenant la relation de divisibilité $|$)
Le caractère décidable de Th$< \mathbb{N}^*, \times, 1 >$ est alors mis en évidence par le théorème suivant :

Théorème 20 (Mostowski) *Si T est une théorie décidable avec une unique constante, les théories des puissances directes faibles de modèles de T sont décidables.*

D'autres résultats ont été obtenus ultérieurement, notamment une élimination de quantificateurs explicitée par P.Cegielski en 1980 :

Théorème 21 (Cegielski) *Th*$< \mathbb{N}^*, \times, 1 >$ *admet une élimination de quantificateurs pour le langage étendu par les symboles de fonction I, T,* $SP_n(n \geq 0)$, *et les symboles de relation unaires* $E_n(n \geq 1)$.

où les symboles de fonction et les prédicats ci-dessus sont définis comme suit :
- $Prem(v_0) : \forall v_1 (v_1 \mid v_0 \to (v_1 = 1) \vee (v_1 = v_0)) \wedge \neg(v_0 = 1)$;
- $I((p_{i_0})^{n_0} \dots (p_{i_{k-1}})^{n_{k-1}}) = (p_{i_0})^{n_0+1} \dots (p_{i_{k-1}})^{n_{k-1}+1}$;
- $V(p, x)$ est la valuation p-adique de x (exposant de p dans la décomposition de x en facteurs premiers) ;
- $T(v_1, v_2) = v_3 : \forall v_1 \forall v_2 \exists v_3 \forall v_0 ((Prem(v_0) \to ((v_0 \mid v_1) \to V(v_0, v_3) = V(v_0, v_2))) \wedge (\neg(v_0 \mid v_1) \to V(v_0, v_3) = 1))$;
- nième puissance : $v_0 \mid_n v_1 : \exists v_2 (v_1 = (v_2)^n \times v_0)$;
- $SP_n : V(p, x) \mid_n V(p, y)$ ssi $V(p, SP_n(x, y)) = p$;
- $E_n(v_0) : \exists v_0 \dots \exists v_{n-1} (\bigwedge_{1 \leq i < j \leq n} v_i \neq v_j \wedge \bigwedge_{i \leq n} (Prem(v_i) \wedge (v_i \mid v_0)))$.

Pour plus de détails, consulter le [2].

3.2.3 Outils de définissabilité - Théorème de Svénonius

Les arithmétiques faibles, en tant que restrictions de l'arithmétique de $< \mathbb{N}, +, \times, = >$, amènent à se poser la question des outils de la définissabilité :

Montrer le caractère définissable

Il existe peu de méthodes pour démontrer qu'une fonction ou une relation est définissable dans un langage. La plus simple et la plus couramment utilisée est d'exhiber une formule explicite.
exemple : la définition de $<$ à partir du langage $< +, = >$:

$\forall v_0 \forall v_1((v_0 < v_1) \leftrightarrow (\exists v_2(v_1 = v_0 + v_2)))$

Montrer le caractère non définissable

On dispose pour cela d'un outil puissant, le théorème de Svenonius, utilisé dans la méthode de Beth et Padoa :

Théorème 22 (Svenonius) *Soit* $\Omega = < \mathbb{N}; \phi_1, \dots, \phi_m; \rho_1, \dots, \rho_n, \rho >$ *une structure du langage* $\mathcal{L} = (f_1, \dots, f_m; R_1, \dots, R_n)$*.*
1). Les trois conditions suivantes sont équivalentes :
i). La relation ρ *n'est pas définissable (par une formule du langage réduit* $\mathcal{L} \backslash \{R\}$*) dans la structure réduite* $< \mathbb{N}; \phi_1, \dots, \phi_m; \rho_1, \dots, \rho_n >$*.*
ii). Il existe une structure $\Theta = < X; \psi_1, \dots, \psi_m; \tau_1, \dots, \tau_n, \tau >$ *et une fonction* ξ *de* X *dans* X *telles que :*
- *les deux structures* Ω *et* Θ *vérifient exactement les mêmes énoncés du langage* $\mathcal{L}$ *;*
- *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. (Si* σ *est une fonction de* $\{1, 2, \dots, q\}$ *dans* $\{1, 2, \dots, p\}$*, on appelle fonction de brassage la fonction* $f_\sigma : (x_1, \dots, x_p) \mapsto (x_{\sigma(1)}, \dots, x_{\sigma(q)})$ *qui envoie* X^p *dans* X^q*. Les fonctions de brassage permettent d'ajouter de nouvelles variables, de les démultiplier, de les permuter ou de les identifier).*

iii). Il existe une structure $\Theta = < X; \psi_1, \dots, \psi_m; \tau_1, \dots, \tau_n, \tau >$ *et une bijection* ξ *de* X *dans* X *telles que :*
- *les deux structures* Ω *et* Θ *vérifient exactement les mêmes énoncés du langage* $\mathcal{L}$ *;*
- *la fonction* ξ *ne respecte pas la relation* τ *mais respecte les relations* τ_i *et les fonctions* ψ_j*.*
  (ξ *est donc un automorphisme de la structure réduite* $< X; \psi_1, \dots, \psi_m; \tau_1, \dots, \tau_n >$*, mais pas de la structure* Θ*).*

2). Dans le cas où la relation ρ_i *est la relation d'égalité sur* $\mathbb{N}$*, alors on peut aussi faire en sorte que la relation* τ_i *précédente soit la relation d'égalité sur* $\mathbb{N}$*.*

Exemples :

1. L'ordre n'est pas défini dans le langage $<=, \times>$:
   On considère la structure $\Theta = < \mathbb{N}, \times, =, < >$ et la bijection ξ de $\mathbb{N}$ dans $\mathbb{N}$ définie de la manière suivante :
   à un entier x on associe ξ(x) obtenu en échangeant les exposants de 2 et 3 dans la décomposition en facteurs premiers de x.

2. L'égalité n'est pas définie dans le langage $<\perp, \times>$:
   On considère la structure $\Theta = < \mathbb{N}, \times, =, \perp >$ et la fonction ξ

définie de la manière suivante :
à un entier x on associe ξ(x) le produit des facteurs premiers de x. (on réduit à 1 les exposants non nuls de la décomposition de x en facteurs premiers)

3. L'ordre n'est pas défini dans le langage $<=, S >$:
voir [1].

3.3 Langages synonymes de $< +, \times, =>$

3.3.1 Exemples

On utilisera la convention suivante dans ce paragraphe : " $\mathcal{A}\subseteq$ " désignera la définition du langage étudié dans le langage $< +, \times, =>$ et " $\subseteq\mathcal{A}$" la définition des fonctions et relations du langage $< +, \times, =>$ dans le langage étudié.

1. Le langage de l'exponentielle $< Exp, =>$
$\mathcal{A}\subseteq$: On a vu en 1.1 (preuve en Annexe A) la définition de la fonction exponentielle à l'aide de $+$ et $\times$;
$\subseteq\mathcal{A}$: On se sert de la caractérisation des opérations d'addition et de multiplication par les formules suivantes :

$$\begin{cases} t^{x\times y} = (t^x)^y \\ t^{(u^{(x+y)})} = (t^{(u^x)})^{u^y} \end{cases}$$

On en déduit des formules définissant dans $< Exp, =>$ les graphes de la multiplication et de l'addition :
$\forall t(Exp(t,z) = Exp(Exp(t,x),y))$
et $\forall t\forall u(Exp(t, Exp(u,z)) = Exp(Exp(t, Exp(u,x)), Exp(u,y)))$;

2. L'ordre de divisibilité et la fonction successeur
$\mathcal{A}\subseteq$:| est défini à l'aide de $\times$ par la formule : $\neg(Zero(x)) \rightarrow \exists u(y = x \times u)$ $(x \mid y)$, où Zero(x) est la formule $\forall t(t \times x = x)$;
S est définie par la formule $\exists t((y = x + t) \wedge Un(t))$, où Un(t) est la formule $\forall u(u \times t = u)$;
$\subseteq\mathcal{A}$: Procédons par étapes :
On peut simplement définir dans le langage $< S, |>$ la constante Zero, la constante Un, l'égalité, la coprimarité et la fonction Pred, dont nous aurons besoin par la suite, respectivement par les formules :

$$\begin{cases} Zero(x) \ : \ \forall y(y \mid x) \\ Un(x) \ : \ \neg(Zero(x)) \wedge \forall y(x \mid y) \\ x = y \ : \ ((x \mid y) \wedge (y \mid x) \vee (Zero(x) \wedge Zero(y))) \\ x \perp y \ : \ \forall k(((k \mid x) \vee (k \mid y)) \rightarrow ((k \mid x) \leftrightarrow \neg(k \mid y))) \\ y = Pred(x) \ : \ (Zero(x) \rightarrow Zero(y)) \wedge (\neg Zero(x) \rightarrow S(y) = x) \end{cases}$$

On s'intéresse ensuite à la multiplication, que l'on ramène à la multiplication de deux nombres premiers par le lemme suivant : (démonstration en Annexe C)

Lemme 2 *Il y a équivalence entre les propositions suivantes :*
i). $z = x \times y$
ii). Pour tout nombre premier p ne divisant ni x ni y, il existe des entiers x' et y' premiers entre eux et avec x, y, et z, tels que :

$$\begin{cases} xx' \equiv -1\ [p] \\ yy' \equiv -1\ [p] \\ zx'y' \equiv 1\ [p] \end{cases}$$

Ramener le problème à la multiplication de deux nombres premiers entre eux permet d'utiliser la notion de ppcm (le produit de deux nombres premiers entre eux est égal à leur ppcm) qui est définissable dans $< S, | >$ par la formule z=ppcm(x,y) :
$(x \mid z) \wedge (y \mid z) \wedge \forall k((x \mid k) \wedge (y \mid k) \rightarrow (z \mid k))$. On a également besoin de définir ce qu'est un nombre premier : Premier(p) est $\forall u((u \mid p) \rightarrow ((u = p) \vee Un(u)))$.
Il ne reste plus alors qu'à traduire calmement la partie ii). du lemme pour obtenir la définition de $\times$:
$z = x \times y$ est $(\forall p(Premier(p) \wedge \neg(p \mid x) \wedge \neg(p \mid y)) \rightarrow \exists x'\exists y'(((x' \perp x) \wedge (x' \perp y) \wedge (x' \perp z) \wedge (x' \perp y') \wedge (y' \perp x) \wedge (y' \perp y) \wedge (y' \perp z)) \bigwedge ((p \mid S(ppcm(x, x'))) \wedge (p \mid S(ppcm(y, y'))) \wedge (p \mid Pred(ppcm(z, ppcm(x', y')))))))) \vee (Zero(z) \leftrightarrow (Zero(x) \vee Zero(y)))$;
L'addition découle facilement de la multiplication une fois que l'on dispose du résultat suivant :

$$z = 0\, ou\, z = x + y \Leftrightarrow (x \times z + 1) \times (y \times z + 1) = (z^2 \times (x \times y + 1)) + 1$$

La formule définissant l'addition est alors z=x+y : $(Zero(z) \rightarrow Zero(x) \wedge Zero(y)) \wedge (S(x \times z) \times S(y \times z) = S(z \times z \times S(x \times y)))$;

3. L'ordre naturel et l'ordre de divisibilité
   $\mathcal{A}\subseteq$: $<$ est défini à l'aide de $+$ par la formule : $\exists u(y = x + u)$ $(x < y)$
   la définition de $|$ est la même que précédemment ;
   $\subseteq\mathcal{A}$: il suffit de définir la fonction successeur dans le langage $<|, <>$ pour se ramener au cas précédent :
   on a vu qu'on pouvait définir l'égalité uniquement à l'aide de $|$, on peut donc à nouveau s'en servir : $y = Sx$ est définie par $\neg(x = y) \wedge (x < y) \wedge \forall u((x < u) \rightarrow ((y < u) \vee (y = u))$.
   On peut voir une démonstration directe de la synonymie entre les langages $<|, <>$ et $< +, \times, =>$ dans [4] (IV-2) ;
4. Le langage de la fonction β de Gödel $< \beta, =>$
   $\mathcal{A}\subseteq$: voir en Annexe A

$\subseteq\mathcal{A}$: on va se ramener au langage $<|,<>$ dont on vient de prouver la synonymie avec $<+,\times,=>$. On va pour se faire définir successivement les constantes Zero et Un, la fonction successeur, puis les relations d'ordre et de divisibilité.
La constante Zero : 0 est le seul entier u tel que tout entier vérifie $x \equiv u\,[1+u]$, c'est-à-dire $\beta(x,0,u)=u$, et comme on a d'autre part pour tous x et y on a $\beta(x,y,0)=0$, on peut caractériser 0 comme le seul entier u vérifiant : pour tous x et y, $\beta(x,y,u)=u$, ce qui se traduit par la formule $\forall x\forall y(\beta(x,y,u)=u)$.
La constante Un : on a l'équivalence $\beta(x,y,z)=x \Leftrightarrow x<1+(1+y)\times z$. Donc 1 est le seul entier u non nul tel que pour tous y et z$\neq 0$ on ait $\beta(u,y,z)=u$, d'où la formule définissant Un : $\neg Zero(u) \wedge \forall y\ forallz(\neg Zero(z) \rightarrow (\beta(u,y,z)=u))$;
La fonction successeur : on remarque que $\beta(x,u,1)$ est le reste de x par u+2, et $\beta(x,0,v)$ le reste de x par v+1. Cela permet de déduire une formule définissant la fonction successeur : $v=S(u)$ est $\forall x(\beta(x,u,1)=\beta(x,0,v))$; L'ordre naturel : l'équivalence $\beta(x,0,z)=x \Leftrightarrow x<1+z$ permet de définir l'ordre naturel par la formule $u<v : \beta(S(u),0,v)=S(u)$;
L'ordre de divisibilité : l'équivalence $\beta(x,0,z)=0 \Leftrightarrow 1+z \mid x$ permet de définir l'ordre de divisibilité par la formule $y \mid x : \exists z((y=S(z)) \wedge (\beta(x,0,z)=0))$.
Les langages du quotient euclidien, du reste et du complément au reste peuvent être traités de manière analogue (voir Annexe C) ;

5. La relation de coprimarité et l'addition
   $\mathcal{A}\subseteq$: Pour définir la relation $u \perp v$, on utilise le fait que les supports de u et de v sont disjoints :
   $\forall k((\exists x((u=x\times k)\vee(v=x\times k))) \rightarrow (\exists y(u=y\times k) \leftrightarrow \forall z\neg(v=z\times k)))$.
   $\subseteq\mathcal{A}$: On procède par étapes, en définissant l'égalité, la constante Un, la relation d'ordre naturel, le successeur, le caractère premier, la multiplication restreinte aux premiers, et enfin la multiplication, grâce au théorème de Schnirelman-Vaughan :

   Théorème 23 (SV) *Tout entier supérieur ou égal à 2 est la somme d'au plus 19 nombres premiers.*

   Pour le détail des étapes, voir en Annexe C. Pour une deuxième démonstration, voir [4] (IV-17).
6. L'ordre naturel et la relation de coprimarité
   $\mathcal{A}\subseteq$: L'ordre naturel et la coprimarité ont déjà été traités précédemment ;
   $\subseteq\mathcal{A}$: On se ramène au cas précédent en définissant l'addition.
   On va utiliser pour cela le fait suivant : On note C(x,p) le quotient de x par p, multiplié par p.

   Lemme 3 (caractérisation de l'addition) *x+y est le plus petit entier z tel que*

$z \equiv x + y\,[6]$ et pour tout entier p premier différent de 11, on a : $C(x,p) + C(y,p) - C(z,p) \equiv ip\,[11]$ où i vaut 0 ou -1.

(Pour une démonstration du lemme, voir en Annexe C)
On notera A(x,y,z) la relation décrite précédemment.
L'égalité $u = v$ est définie par : $\forall z((z < u) \leftrightarrow (z < v))$;
Les relations de congruence modulo 6 et 11 : notée respectivement CONG6(i,x) et CONG11(j,x) (x est congru à i modulo 6 et j modulo 11 respectivement), elles se fondent sur le fait que la relation $u \equiv v\,[k]$ équivaut à $k \mid (u + (k - v))$, d'où :
CONG6(i,x) est $\neg(2 \perp S^{6-i}(x)) \wedge \neg(3 \perp S^{6-i}(x))$
CONG11(j,x) est $\neg(11 \perp S^{11-j}(x))$
Remarque : on a vu précédemment que la fonction successeur était définissable à l'aide de $<$ et $=$, donc ces congruences sont bien exprimées dans le langage $<\perp, <>$. Le caractère premier d'un entier est exprimé dans ce même langage, en Annexe C.3.
La relation $v = C(u,p)$: quand p est premier, C(u,p) est le plus grand entier inférieur ou égal à u qui ne soit pas premier avec p, d'où la formulation de la relation dans le langage $<\perp, <>$: $Premier(p) \wedge (v \leq u) \wedge \neg(p \perp v) \wedge \forall w(((w \leq u) \wedge \neg(w \perp v)) \rightarrow (w \leq v))$.
Les relations $z \equiv x+y\,[6]$ et $x+y-z \equiv -t\,[11]$: $z \equiv x+y\,[6]$ s'exprime comme l'union pour j,k,l dans $\{0, \dots, 5\}$ tels que $j + k \equiv l\ [6]$ des relations $x \equiv j\ [6]$ et $y \equiv k\ [6]$ et $z \equiv l\ [6]$ d'où la formule pour définir cette relation :

$$\bigvee_{\substack{j,k,l \in \{0,\dots,5\} \\ \text{tels que } j+k \equiv l\,[6]}} (CONG6(j,x) \wedge CONG6(k,y) \wedge CONG6(l,z))$$

De même la relation $x + y - z \equiv -t\,[11]$ s'exprime par la formule :

$$\bigvee_{\substack{j,k,l,m \in \{0,\dots,10\} \\ \text{tels que } j+k-l \equiv -t\,[11]}} (CONG11(j,x) \wedge CONG11(k,y) \wedge CONG11(l,z) \wedge CONG11(m,t))$$

On peut alors définir la relation A(x,y,z) par la formule :
$(z \equiv x + y\ [6]) \wedge \forall p((Premier(p) \wedge \neg(p = 11)) \rightarrow \exists u \exists v \exists w \exists t((u = C(x,p)) \wedge (v = C(y,p)) \wedge (w = C(z,p)) \wedge ((t = 0) \vee (t = p)) \wedge (u+v-w \equiv -t\,[11])))$.
Et on a enfin la formule permettant de définir l'addition $z = x + y$:
$A(x,y,z) \wedge \forall t(A(x,y,t) \rightarrow (z \leq t))$;

7. La relation de coprimarité, la multiplication et la fonction successeur
   $\mathcal{A} \subseteq$: Déjà vu en ce qui concerne la fonction successeur et la relation de coprimarité ;
   $\subseteq \mathcal{A}$: On se ramène au cas précédent en rappelant que l'addition est définissable à partir du successeur et de la multiplication. (Voir le cas du langage $< S, | >$)

3.3.2 Cas de $< S, \perp >$

La fonction successeur et la relation de coprimarité sont bien évidemment définissables dans le langage standard de l'arithmétique, mais le problème réciproque est encore ouvert puisqu'équivalent à la conjecture d'Erdös-Woods (voir la partie logique de l'étude de la conjecture en 2.2.2). Une condition nécessaire à la synonymie avec $< +, \times, = >$ est remplie par le langage $< S, \perp >$: la théorie de ce langage est aussi indécidable que celle du langage $< +, \times, = >$ (voir en Annexe B.2). D'autre part on peut se ramener à des problèmes équivalents qui permettront peut-être de résoudre la conjecture en considérant des extensions du langage $< S, \perp >$, qui sont synonymes de $< +, \times, = >$: on peut alors étudier le caractère définissable des relations et fonctions que l'on rajoute dans $< S, \perp >$. (voir en Annexe B.4).

4 Extensions

4.1 Une illustration de l'incomplétude

Peu de théorèmes sont connus comme étant non prouvables dans Peano mais vrais, c'est-à-dire prouvés dans des systèmes plus compliqués que l'arithmétique du premier ordre. L'un d'eux est issu de la théorie des groupes finis, il s'agit du théorème de Schur-Zassenhaus :

Théorème 24 (Schur-Zassenhaus) *Soit G un groupe fini et H un sous-groupe distingué de G. Si $\mid H \mid$ et $\mid G/H \mid$ sont premiers entre eux, et si l'un des deux groupes H ou G/H est résoluble, alors H possède un complément dans G : il existe un sous-goupe H' de G tel que :*

$$\begin{cases} H' \cap H = \emptyset \\ G = H \cdot H' \end{cases}$$

Pour plus de détail sur ce sujet, se référer à [9].

4.2 Définissabilité des entiers dans $\mathbb{Q}$

Un résultat très remarquable de Julia Robinson est la définissabilité des entiers dans l'ensemble des nombres rationnels, ou plus exactement de $\mathbb{Z}$ dans $\mathbb{Q}$.

Remarque : La définissabilité des entiers naturels dans $\mathbb{Z}$ s'obtient facilement à partir du fait que tout entier positif est la somme de quatre carrés (résultat dû à Lagrange. Pour une dḿonstration, voir [2], II.3.8) : on peut alors définir l'appartenance à $\mathbb{N}$ dans la structure $< \mathbb{Z}, +, \times, = >$ par la formule Nat(x) : $\exists v_0 \exists v_1 \exists v_2 \exists v_3 (x = v_0 \times v_0 + v_1 \times v_1 + v_2 \times v_2 + v_3 \times v_3)$.

La définissabilité de $\mathbb{Z}$ dans $< \mathbb{Q}, +, \times, = >$ repose sur l'étude des relations de la forme :

$\varphi(a, b, t) \ : \ \exists X \exists Y \exists Z (X^2 + aY^2 = bZ^2 + abt^2 + 2)$.
La formule $x \in \mathbb{Z}$ est vraie si et seulement si

$$< \mathbb{Q}, 0, 1, +, \times, => \models \forall a \forall b((\varphi(a, b, 0) \wedge \forall t(\varphi(a, b, t) \rightarrow \varphi(a, b, t{+}1))) \rightarrow \varphi(a, b, x))$$

si le sens direct est facile à établir en tant qu'expression du principe de récurrence, lequel est vrai dans $< \mathbb{Z}, 0, 1, +, \times, =>$, le sens réciproque est beaucoup plus délicat et fait appel au théorème de Hasse-Minkowski :

Théorème 25 (Hasse-Minkowski) *Un polynôme quadratique homogène à n variables et à coefficients entiers admet une solution non nulle dans $\mathbb{Q}$ si et seulement s'il admet une solution non nulle dans $\mathbb{R}$ et dans tous les corps p-adiques pour p premier.*

Il s'agit alors de montrer que pour tout entier p premier, il existe a et b dans $\mathbb{Q}$ tels que l'ensemble $\{t \backslash \mathbb{Q} \models \varphi(a, b, t)\}$ contient 0, est stable par la fonction $t \mapsto t{+}1$, et est inclus dans l'ensemble des rationnels à dénominateur premier avec p.

Conclusion

Dans ce stage ont été abordées certaines notions fondamentales en logique mathématique telle la définissabilité, les isomorphismes de structures, les synonymies entre différents langages. Mais l'on a surtout vu qu'un problème ouvert, tel la conjecture d'Erdös-Woods, ouvre de nombreuses portes vers d'autres domaines des mathématiques que la logique.
D'autre part il est intéressant de constater la puissance des théorèmes employés, tel le théorème de Störmer ou le théorème ZBV. On est en droit de se demander si la résolution des chaînons manquants dans Erdös-Woods, en vue d'infirmer ou de confirmer la conjecture, ne fait pas elle aussi appel à des résultats de théorie des nombres ou d'analyse aussi fins et complexes.

A Résultats de théorie des nombres : extensions-démonstrations

A.1 La fonction β de Gödel

On rappelle la propriété remarquable de la fonction de Gödel : "Pour toute suite finie d'entiers $(\alpha_0 \ldots \alpha_p)$ il existe des entiers c et d tels que $\forall i \in \{0 \ldots p\}$, $\beta(c,d,i) = \alpha_i$"

Dem :

On choisit un entier m supérieur à n+1 et tel que d=m! soit supérieur à tous les α_i.

Les entiers γ_i =d(i+1) + 1 sont premiers entre eux car si u est un nombre premier tel que $u \mid \gamma_i$ et $u \mid \gamma_j$, avec $i > j$, alors $u \mid \gamma_i - \gamma_j = m!(i-j)$, donc u est inférieur à $\max\{\gamma_k\}_{k \in \{0,\ldots,n\}}$ donc à m, ce qui est impossible puisque u doit diviser m!(i+1) +1.

On peut donc appliquer le théorème chinois des restes pour en déduire l'existence d'un entier c qui convienne.

Remarque : On peut définir la fonction β dans le langage de l'arithmétique par la formule :

$$B[v_0, v_1, v_2, v_3] = \exists v_4 (v_3 = (v_4 \times S(v_2 \times Sv_1)) + v_0) \wedge (v_0 < S(v_2 \times Sv_1))$$

Définition de l'exponentielle :

Rappelons la formule qui définit l'exponentielle dans le langage $< +, \times, = >$ par l'intermédiaire de la fonction β (ici présentée par la relation B définie ci-dessus). :

$$\exists c \exists d (B(c,d,0,1) \wedge (\forall i 0 < i \leq x \exists \gamma B(c,d,i,2 \times \gamma) \wedge B(c,d,i-1,\gamma)) \wedge B(c,d,x,z)))$$

Dem : Soit t, k, y des entiers tels que $k > 2^t$ et $y = k!$. Montrons qu'il existe un entier x tel que pour tout i inférieur à t, $\beta(x,y,t) = 2^i$: on le montre par récurrence sur t.

· t=0 : on prend $x = 1$.

· "t"⇒"t+1" : il existe un entier c tel que $\forall i \in [1..t-1]$, $\beta(c,y,i+1) \equiv 2 \times \beta(c,y,i) \bmod (a_i)$. a_{t+1} et $a_1 \ldots a_t$ sont premiers entre eux, donc d'après Bezout, il existe deux entiers relatifs u et v tels que : $ua_{t+1} + va_1 \ldots a_t = 1$. On pose alors $x = (2c - c)ua_{t+1} + c + pa_1 \ldots a_{t+1} = (c - 2c)va_1 \ldots a_t + pa_1 \ldots a_{t+1}$ avec p assez grand pour que x soit positif.

A.2 Caractérisation d'un entier par support

On démontre ici le théorème 3, dont on rappelle l'énoncé :

Il y a équivalence entre les propositions suivantes :

i). $x = y$

ii). Pour une infinité d'entiers z, $SUPP(x+z) = SUPP(y+z)$
Pour ce faire, on a besoin d'un lemme dû à G.Polyà :

Lemme 4 (Polyà) *Si $(a_n)_{n\in\mathbb{N}}$ est une suite strictement croissante d'entiers strictement positifs, alors $(a_{n+1} - a_n)_{n\in\mathbb{N}} \to +\infty$.*

<u>*Dem*</u> : Soit $\{p_1, \ldots, p_k\}$ le support d'une telle suite.
$a_n = p_1^{\alpha_1^n} p_2^{\alpha_2^n} \ldots p_k^{\alpha_k^n}$. On a alors :
$a_{n+1} - a_n = a_n \times (\prod_{i=1\ldots k} p_i^{\alpha_i^{n+1}-\alpha_i^n} - 1)$. Or $\prod_{i=1\ldots k} p_i^{\alpha_i^{n+1}-\alpha_i^n} > 1$ car la suite est strictement croissante. De plus $(a_n)_{n\in\mathbb{N}} \to \infty$ en croissant strictement. D'où le résultat souhaité.
<u>*Dem*</u>(théorème) :
i). $\Rightarrow$ ii). : c'est trivial
i). $\Leftarrow$ ii). : On suppose que $x < y$ et que $I = \{i \in \mathbb{N} \backslash SUPP(x+i) = SUPP(y+i)\}$ est infini.
$p \in SUPP(x+i) = SUPP(y+i) \Rightarrow p \mid (x+i) - (y+i) = x - y$, donc $SUPP(x+i) = SUPP(y+i) \subset SUPP(\mid x-y \mid)$ qui est fini. Il existe donc un sous-ensemble X de $SUPP(\mid x-y \mid)$ tel que $J = \{i \in I \backslash SUPP(x+i) = SUPP(y+i) = X\}$ est infini.
On définit par récurrence une suite strictement croissante d'entiers strictement positifs de même support X :

$$\begin{cases} a_0 = x+i & \text{i le plus petit élément de J tel que} \\ a_1 = y+i & x+i > 0 \end{cases}$$

$$\begin{cases} a_{2n} = x+j & \text{j le plus petit élément de J tel que} \\ a_{2n+1} = y+i & x+j > a_{2n-1} \end{cases}$$

On a alors d'après le lemme précédent $(a_{2n+1} - a_{2n}) \to \infty$ or c'est une suite constante égale à x-y : il y a contradiction.

A.3 Les équations de Pell-Fermat

Une équation de Pell-Fermat associée à un paramètre d, qui est un entier strictement positif non carré parfait, se présente sous la forme :

$$x^2 - dy^2 = 1$$

Si cette équation a une solution non triviale, elle en admet une infinité, qui sont dans l'ensemble $\{x + y\sqrt{d}\}_{(x,y)\in\mathbb{N}^2}$, et définies par une solution fondamentale de la forme $x_0 + y_0\sqrt{d}$. Pour simplifier, on se place dans $\mathbb{N}^2$, la solution fondamentale est alors décrite par (x_0, y_0) est l'ensemble des solutions est : $\{(x_n, y_n)\}_{n\in\mathbb{N}}$, telles que $x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^n$. Par un souci de simplification encore une fois, on appelle solution fondamentale l'entier x_0. (y_0 s'en déduit facilement par l'équation).
<u>*Dem :*</u>
On a $x^2 = 1 + dy^2$. Donc sur l'ensemble des solutions, x et y croissent en même temps, ce qui assure l'existence d'une solution minimale telle que $x_0 > 1$ et $y_0 > 0$.

On note $\delta = x_0 + y_0\sqrt{d}$.
Alors $1 = \delta^0 < \delta < \delta^2 < \ldots < \delta^n < \ldots$ est un ensemble de solutions :
en effet, l'ensemble des solutions est stable par multiplication : soient $a = x + y\sqrt{d}$ et $b = u + v\sqrt{d}$ deux solutions, alors $a \times b$ est aussi une solution : $a \times b = (xu + dyv) + (xv + uy)\sqrt{d}$. On a :

$$(xu+dyv)^2 - d(xv+uy)^2 = x^2u^2 + d^2y^2v^2 + 2dxuyv - dx^2v^2 - du^2y^2 - 2dxvuy$$

$$= x^2(u^2 - dv^2) - dy^2(u^2 - dv^2) = x^2 - dy^2 = 1$$

Réciproquement : si (x,y) est une solution : il existe un entier n tel que $\delta^n \leq x + y\sqrt{d} \leq \delta^{n+1}$
on multiplie cette inéquation par le nombre $x_n - y_n\sqrt{d}$:

$$1 \leq (x + y\sqrt{d})(x_n - y_n\sqrt{d}) \leq x_0 + y_0\sqrt{d}$$

or, par stabilité de l'ensemble des solutions par multiplication, et minimalité de la solution $x_0 + y_0\sqrt{d}$, on en déduit que $(x + y\sqrt{d})(x_n - y_n\sqrt{d}) = 1$, d'où $x + y\sqrt{d} = x_n + y_n\sqrt{d}$.

A.4 Preuve de la conjecture E-W sur les primaires

On va commencer par démontrer deux résultats intermédiaires :

Corollaire 2 (de Lucas-Carmichael) *$SUPP(x^\alpha + 1) = SUPP(x^\beta + 1)$ équivaut à $\alpha = \beta$ ou $x = 2$ et α et β dans $\{1, 3\}$.*

Dem :
Si $\alpha > \beta$, alors $x^\alpha + 1$ admet un diviseur premier caractéristique, ce qui entraîne $SUPP(x^\alpha + 1) \neq SUPP(x^\beta + 1)$.On se trouve donc dans un cas d'exception : $x = 2$, $\alpha = 3$, $\beta = 1$, et de manière analogue pour $\alpha < \beta$.

Corollaire 3 (de ZBV) *$SUPP(x^\alpha - 1) = SUPP(x^\beta - 1)$ équivaut à $\alpha = \beta$ ou $x = 2^u - 1, u \geq 2$ et α et β dans $\{1, 2\}$.*

Dem :
si $\alpha > \beta$, alors $x^\alpha - 1$ a un diviseur premier primitif, d'où $SUPP(x^\alpha - 1) \neq SUPP(x^\beta - 1)$. On est donc dans un cas d'exception :
$\cdot x = 2^u - 1, \alpha = 2, \beta = 1, u > 0$
$\cdot x = 2, \alpha = 6$
or dans ce dernier cas, on a :
$2^1 - 1 = 1$, donc de support $\{1\}$
$2^2 - 1 = 3$, donc de support $\{3\}$
$2^3 - 1 = 8$, donc de support $\{7\}$
$2^4 - 1 = 15$, donc de support $\{3, 5\}$
$2^5 - 1 = 31$, donc de support $\{31\}$
$2^6 - 1 = 63$, donc de support $\{3, 7\}$

ils sont tous de supports différents...
On raisonne de manière analogue pour $\alpha < \beta$.

On peut maintenant en déduire le résultat voulu :
La seule classe de $\cong_{\{0,1\}}$ dont la trace sur PP n'est pas réduite à un seul élément est celle de 2.
Comme $SUPP(2+2) = \{2\}$ et $SUPP(2^3+2) = \{2,5\}$, on a $2 \ncong_{\{0,1,2\}} 8$.
De même les seules classes de $\cong_{\{-1,0\}}$ dont les traces sur PP ne sont pas réduites à un seul élément sont de la forme $\{p, p^2\}$, où p est un premier de Mersenne : $p = 2^u - 1$. Comme $p^2+1 = (2^u-1)^2+1 = 2(2^u(2^{u-1}-1)+1)$, on a $SUPP(p^2+1) \neq \{2\}$ alors que $SUPP(p+1) = \{2\}$, d'où $p \ncong_{\{-1,0,1\}} p^2$.
Comme $p - 2 = 2^u - 3$, $p^2 - 2 = (2^u - 3)(2^u + 1) + 2$ sont deux entiers impairs et premiers entre eux (si $d \mid 2^u - 3$ et $d \mid p^2 - 2$, alors $d \mid 2$), on a $p \ncong_{\{-2,-1,0\}} p^2$.

B Résultats de définissabilité : autour d'Erdös-Woods

B.1 Compléments sur la structure ensembliste sur les parties finies de P

Structure ensembliste sur les parties finies des entiers : opérations élémentaires

On a vu qu'on pouvait définir l'inclusion de deux supports $SUPP(x) \subseteq SUPP(y)$. On définit maintenant :

- L'égalité : $SUPP(x) = SUPP(y)$ est $(SUPP(x) \subseteq SUPP(y)) \wedge (SUPP(y) \subseteq SUPP(x))$;
- L'union : $SUPP(z) = SUPP(x) \cup SUPP(y)$ est $(SUPP(x) \subseteq SUPP(z)) \wedge (SUPP(y) \subseteq SUPP(z)) \wedge \forall t((SUPP(x) \subseteq SUPP(t)) \wedge (SUPP(y) \subseteq SUPP(t)) \rightarrow (SUPP(z) \subseteq SUPP(t)))$;
- L'intersection : $SUPP(z) = SUPP(x) \cap SUPP(y)$ est $(SUPP(z) \subseteq SUPP(x)) \wedge (SUPP(z) \subseteq SUPP(y)) \wedge \forall t((SUPP(t) \subseteq SUPP(x)) \wedge (SUPP(t) \subseteq SUPP(y)) \rightarrow (SUPP(t) \subseteq SUPP(z)))$;
- La différence : $SUPP(z) = SUPP(x) - SUPP(y)$ est $(SUPP(y) \subseteq SUPP(x)) \wedge (SUPP(z) \subseteq SUPP(x)) \wedge \forall u(SUPP(z) \cap SUPP(y) \subseteq SUPP(u)) \wedge \forall t(((SUPP(t) \subseteq SUPP(x)) \wedge \forall u(SUPP(t) \cap SUPP(y) \subseteq SUPP(u))) \rightarrow (SUPP(t) \subseteq SUPP(z)))$.

La définition de l'ensemble des nombres premiers dans $< S, \perp >$

On passe par l'intermédiaire de l'ensemble

$X = \{x$ primaire $\backslash SUPP(x-1) \subseteq SUPP(y-1)$ pour tout primaire y de même base que $x\}$.

En effet, d'après le théorème ZBV, cet ensemble n'est autre que l'ensemble
$P \cup \{(2^u-1)^2 \backslash u \geq 2$ et $2^u - 1$ premier $\}$. Il faut donc se débarasser du deuxième ensemble pour obtenir P. Cela se fait en remarquant que $(2^u - 1) + 1$ est une puissance de 2, mais pas $(2^u-1)^2 + 1 = 2(2^u(2^{u-1} - 1) + 1)$. D'où
$P = \{x \in X \backslash$ s'il existe un y, de même base que x, différent de x, dans X, alors $x + 1$ est une puissance de 2 $\}$.
Exprimer $x \in X$ dans le langage $< S, \perp >$ est possible grâce à la formule $X(x)$:

$$PP(x) \wedge \forall y \forall u \forall v((PP(x,y) \wedge S_{PP}(u,x) \wedge S_{PP}(v,y)) \rightarrow (SUPP(u) \subseteq SUPP(v))).$$

Enfin l'ensemble des nombres premiers est défini par la formule d'appartenance $x \in P$ ou encore $P(x)$:

$$X(x) \wedge ((\exists z(X(z) \wedge \neg(z =_{PP} x) \wedge PP(x,z))) \rightarrow PP(S(x), 2)).$$

Un codage des relations et fonctions sur les parties finies de P

On va se servir de certaines relations de congruence liées au théorème de Dirichlet (théorème 1).
Soit ρ une relation d'arité $k \geq 1$.
On va tout d'abord considérer l'énumération des suites de k+1 parties de l'ensemble $\{1, \ldots, k\}$: $\{A_\alpha\}_{\alpha \in \{1,\ldots,K\}}$. Soit π un entier plus grand que K. Soient $x_1, \ldots, x_k$ des entiers.
A tout k-uplet $(p_1, \ldots, p_k) \in SUPP(x_1) \times \ldots \times SUPP(x_k)$, on associe un ensemble infini de nombres premiers supérieurs à π, $X_{p_1 \ldots p_k}$, de manière à ce que ces différents ensembles $X_{p_1 \ldots p_k}$ soi ent deux à deux disjoints.
Les S-codes obtenus pour la relation ρ sont alors les entiers dont les supports ne coupent que les $X_{p_1 \ldots p_k}$ tels que $(p_1, \ldots, p_k) \in \rho$. Les S-codes d'une fonction sont définis comme étant ceux de son graphe.
On peut même définir cette notion dans le langage du successeur et de la coprimarité :

Théorème 26 *"$(p_1, \ldots, p_k)$ appartient à la relation S-codée par x sur $SUPP(x_1) \times \ldots \times SUPP(x_k)$" est définissable dans la structure $< \mathbb{N}, S, \perp >$.*

Dem : La définition de $X_{p_1,\ldots,p_k}$ se traduit par la définition de la relation
$\{(x_1, \ldots, x_k, p_1, \ldots, p_k, z) \backslash z \in X_{p_1 \ldots p_k}\}$. Or on sait exprimer dans $< S, \perp >$ l'appartenance à un support, et les relations de congruence devant être vérifiées par un $z \in X_{p_1 \ldots p_k}$:

$z \equiv i\,[p_i]$ pour les i tels que $p_i > k+1, p_i \neq \pi$ et $p_i \neq p_j$ pour tous les $j < i$,
$z \equiv k+1\,[q]$ si $q \in (\bigcup_{s=1\ldots k} SUPP(x_s)) \backslash \{1, \ldots k+1, p_1, \ldots, p_k, \pi\}$,
$z \equiv \alpha\,[\pi]$ si A_α est $(\{i \backslash p_i = 2\}, \ldots, \{i \backslash p_i = k+1\}, \{i \backslash p_i = \pi\})$.

B.2 L'indécidabilité de Th($< \mathbb{N}, S, \perp >$)

On va se ramener à l'indécidabilité de l'arithmétique par la surjection $x \mapsto \mid SUPP(x) \mid$ (où $\mid X \mid$ est le nombre d'éléments de l'ensemble X). Le résultat est dû à Woods, dans le corollaire du théorèm e précédent :

Corollaire 4 (Woods)
1). Les images réciproques par la surjection $x \mapsto \mid SUPP(x) \mid$ de $\mathbb{N} \backslash \{0\}$ sur $\mathbb{N}$ des relations $\geq, =$ et des graphes de l'addition et de la multiplication sont définissables dans la structure $< \mathbb{N}, S, \perp >$.
2). La théorie $Th(\mathbb{N}, S, \perp)$ est indécidable.

Le deuxième point est une condition nécessaire à l'équivalence entre les structures $< \mathbb{N}, S, \perp >$ et $< \mathbb{N}, +, \times, = >$.

B.3 Un plus gros morceau de l'exponentielle

On peut définir avec le sucesseur et la coprimarité la restriction de la fonction $(p,q) \mapsto q^{p-1}$ à l'ensemble $\{(p,q) \backslash p$ et q sont premiers et distincts$\}$. La démonstration de ce fait repose sur des outils de théorie des nombres tels que le théorème 1, ou le théorème 4. Elle est également introduite par les résultats suivants :

Lemme 5 *On peut définir avec S et $\perp$ la relation ternaire* $\Theta_1 = \{(p,q,u) \backslash p$ *et* q *sont premiers distincts et* $u = q^{ORD(q,p)}\}$.

Lemme 6 *On peut définir avec S et $\perp$ la relation* $\Theta_2 = \{(u,x) \backslash u$ *est primaire et* $\mid SUPP(x) \mid$ *est le nombre de diviseurs de la valuation de* $u\}$.

Lemme 7 *On peut définir avec S et $\perp$ la relation* $\Theta_3 = \{(p,q) \backslash p$ *et* q *sont premiers distincts et* $ORD(q,p) = p-1\}$.

Le détail des preuves est donné dans [1].

B.4 Les extensions de $< S, \perp >$

Ces extensions représentent des langages synonymes à $< \mathbb{N}, +, times, = >$, et sont construits à partir de S et $\perp$ bien sûr, mais aussi à partir des "pistes" qui ont été pressenties lors de l'étude de la conjecture Er dös-Woods. En fait, la conjecture d'Erdös-Woods est pour chacun de ces exemples équivalent à l'expression dans $< s, \perp >$ de la relation ajoutée.

Extension par le résidu quadratique

Les relations binaires que l'on fait intervenir ici sont :
$RES = \{(x,p) \in \mathbb{N} \times P \backslash x$ est résidu quadratique modulo $p\}$,
$T = \{(x,p) \in \mathbb{N} \times P \backslash x$ est impair et l'exposant de p dans la décompo- -sition primaire de x est pair$\}$.
On commence par montrer à l'aide du théorème de Störmer et d'une extension du théorème 11 que le langage $< S, \perp, T >$ est synonyme du langage plein, puis on définit la relation T dans la langage $< S, \perp, RES >$.
On peut même obtenir un résultat plus précis en remplaçant la relation RES par sa restriction $RRES = RES \cap \mathbb{N} \times [8\mathbb{N} + 5]$.

Extension par la relation binaire " y est une puissance de x "

La relation concernée est ici :
$PUIS = \{(x,y) \backslash$ il existe $n \geq 1$ tel que $y = x^n\}$.
L'égalité s'en déduit facilement par la formule $x = y : PUIS(x,y) \wedge PUIS(y,x)$.
La synonymie s'obtient à l'aide de celle obtenue dans le cas de la résiduation quadratique, et grâce au théorème suivant :

Théorème 27 *La relation RRES est définissable dans la structure* $< \mathbb{N}, S, \perp, PUIS >$.

Extension par restrictions de l'addition, la multiplication ou la division

C'est le langage le plus proche de $< S, \perp >$ dont la synonymie avec $< +, \times, = >$ a été prouvée.
Pour $X \subseteq \mathbb{N}^2$, on note $X - ADD$ et $X - MULT$ les graphes des restrictions de l'addition et de la multiplication à X :

$$X_A DD = \{(x, y, z) \backslash (x, y) \in X \text{ et } z = x + y\}$$
$$X - MULT = \{(x, y, z) \backslash (x, y) \in X \text{ et } z = x \times y\}.$$

Le résultat se présente alors sous la forme du théorème suivant :

Théorème 28 *Il existe une fonction f, définissable dans la structure* $< \mathbb{N}, S, \perp >$*, de domaine* $\mathbb{N}$ *et à valeur dans l'ensemble des entiers premiers, pour laquelle la propriété suivante est vraie :*
Si $X \subseteq \mathbb{N}^2$ *est définissable dans la structure* $< \mathbb{N}, +, \times, = >$ *et telle que pour tout x il existe un entier primaire v tel que* $v \geq f(x)$ *et* $(x, v) \in X$*, alors les trois structures* $< \mathbb{N}, S, \perp, X - ADD >$, $< \mathbb{N}, S, \perp, X - MULT >$ *et* $< \mathbb{N}, +, \times, = >$ *définissent les mêmes relations et fonctions.*

C Résultats sur les langages synonymes de $< +, \times, =>$

C.1 $< S, |>$

On s'intéresse ici à une démonstration du lemme 2, dont on rappelle l'énoncé :
Il y a équivalence entre les propositions suivantes :
i). $z = x \times y$
ii). Pour tout nombre premier p ne divisant ni x ni y, il existe des entiers x' et y' premiers entre eux et avec x, y, et z, tels que :

$$\begin{cases} xx' \equiv -1\,[p] \\ yy' \equiv -1\,[p] \\ zx'y' \equiv 1\,[p] \end{cases}$$

<u>*Dem*</u> :

i). $\Leftarrow$ ii). : Soit p un nombre premier n'appartenant pas à l'ensemble $SUPP(x) \cup SUPP(y)$. Il existe d'après l'hypothèse des entiers x' et y' premiers entre eux et avec x, y, et z, tels que :

$$\begin{cases} xx' \equiv -1\,[p] \\ yy' \equiv -1\,[p] \\ zx'y' \equiv 1\,[p] \end{cases}$$

de ce système on déduit : $xx' + zx'y' \equiv 0\,[p] \Leftrightarrow x'(x + zy') \equiv 0\,[p]$. Or si $p \mid x'$, on a $xx' \equiv 0\,[p]$, ce qui contredit l'hypothèse, donc $p \not| x'$. D'où :
$p \mid (x + zy') \Rightarrow x + zy' \equiv 0\,[p] \Rightarrow x \equiv -zy'\,[p] \Rightarrow xy \equiv -zy'y\,[p]$.
Comme $yy' \equiv -1\,[p]$, on a $xy \equiv z\,[p]$. C'est vrai pour une infinité de nombres entiers donc on a bien $xy = z$.

i). $\Rightarrow$ ii). : Soit p un nombre premier n'appartenant pas à l'ensemble $SUPP(x) \cup SUPP(y)$. $p \geq 2$. On a :
$x \equiv u\,[p]$ et $\forall \alpha\, x \equiv u + \alpha p\,[p]$
$y \equiv v\,[p]$ et $\forall \beta\, y \equiv v + \beta p\,[p]$
D'après le théorème de Dirichlet, $p \perp u$ et $p \perp v$ entraînent l'existence de nombres a et b tels que u+ap et v+bp soient premiers.
Remarque : ces nombres premiers sont forcément différents de p, sinon u=0 ou v=0, ce qui signifierait $p \mid x$ ou $p \mid y$, donc contredirait l'hypothèse sur p. Par conséquent $p \perp u + ap$ et $p \perp v + bp$.
On considère alors les nombres de la forme :
$x_k = kp - (u + ap)^{p-2}$ et $x_{k'} = k'p - (v + bp)^{p-2}$.
D'après le théorème de Dirichlet, il existe des nombres k et k' tels que x_k et $x_{k'}$ soient positifs, différents et premiers. On pose alors $x' = x_k$ et $y' = x_{k'}$.
x' et y' étant premiers et différents, ils sont premiers entre eux et a vec x et y. En outre :

$xx' \equiv xkp - x(u+ap)^{p-2} \equiv -x(u+ap)^{p-2} \equiv -xu^{p-2}\,[p]$
or $x \equiv u\,[p]$ donc $xu^{p-2} \equiv u^{p-1}\,[p]$. D'après le petit théorème de Fermat : $u^{p-1} \equiv 1\,[p]$, d'où finalement : $xx' \equiv -1\,[p]$.
Par un raisonnement analogue on obtient $yy' \equiv -1\,[p]$.
Enfin, comme $z = xy$, on a $zx'y' \equiv xx'yy' \equiv (-1) \times (-1) \equiv 1\,[p]$, ce qui termine la preuve.

C.2 Langages du quotient, du reste et du complément au reste

On se ramène à chaque fois au langage des deux ordres, naturel et de divisibilité. On note respectivement QUOT(x,y,z), REST(x,y,t), et CR(x,y,zx) le fait que y=zx+t. (le premier argument est le diviseur, le deuxième le dividende et le troisième ce qui est annoncé à savoir le quotient, le reste et le complément au reste respectivement).

Langage du quotient

On commence par définir la constante Zero : 0 est le seul entier non divisable, donc la formule Zero(u) peut être exprimée par $\forall x \forall q \neg QUOT(x,u,q)$.
L'ordre naturel vient alors facilement : $u < v$ est $\exists z Zero(z) \wedge QUOT(u,v,z)$, que l'on peut abréger en $QUOT(u,v,0)$.
L'égalité provient de l'unicité du quotient euclidien :
$u = v$ est $\forall y \forall q (QUOT(u,y,q) \leftrightarrow QUOT(v,y,q))$.
On peut dès lors définir la fonction prédécesseur Pred avec l'ordre et l'égalité : $Pred(x,y)$ $(y = Pred(x))$ est $(x < y) \wedge \forall z((z < y) \leftrightarrow (z \leq x)))$.
La divisibilité est le point le plus délicat : u divise v si et seulement si v est nul ou le quotient de v-1 par u est le prédécesseur du quotient de v par u. D'où la formule $u \mid v$: $Zero(v) \vee \exists w \exists q \exists q'(QUOT(v,u,q) \wedge Pred(w,v) \wedge QUOT(w,u,q') \wedge Pred(q,q'))$.

Langage du reste

La constante Zero se définit de manière analogue par le fait que ce soit le seul entier indivisible : $Zero(u)$ est $\forall x \forall r \neg REST(x,u,r)$.
L'ordre naturel : u est inférieur à v si et seulement s'il est le reste de sa division par v : $u < v$ est $REST(u,v,u)$.
La divisibilité : u divise v si et seulement si les deux sont nuls ou le reste de la division de v par u est nul : $u \mid v$ est $\exists z(REST(v,u,z) \wedge Zero(z)) \vee (Zero(u) \wedge Zero(v))$.

Langage du complément au reste

Encore une fois la même chose pour la constante Zero : $Zero(u)$ est $\forall x \forall y \neg CR(x,u,z)$.

L'ordre naturel : u est inférieur à v si et seulement si le complément au reste de la division de v par u est nul : $u < v$ est $\exists z(Zero(z) \wedge CR(u, v, z))$.
La divisibilité : u divise v si et seulement si v est nul ou le complément au reste de la divisionde u par v est v : $u \mid v$ est $Zero(v) \vee CR(v, u, v)$.

C.3 Addition et coprimarité

Voici le détail des étapes permettant de définir le langage plein de l'arithmétique dans le langage de l'addition et de la coprimarité :

1. L'égalité
Deux entiers x et y sont égaux si et seulement si pour tout nombre z, x+z et y+z ont même support. (voir théorème 3) $SUPP(u) = SUPP(v)$ s'exprime à l'aide de $\perp$ par la formule : $\forall z(z \perp u) \leftrightarrow (z \perp v)$, d'o ù une formule définissant l'égalité :
$\forall z(SUPP(x+z) = SUPP(y+z)) \quad (x = y)$.
2. Les constantes, la fonction successeur et l'ordre
Un(x) : $\forall u(u \perp x)$
$x \leq y$: $\exists u(y = x + u)$
$y = S(x)$: $\exists u(Un(u) \wedge (y = x + u))$
Les constantes $Egal_n(x)$ s'obtiennent aisément à partir du successeur et de la constante 1.
3. Les premiers
Premier(x) est : $\neg Egal_0(x) \wedge \neg Egal_1(x) \wedge \forall y((\neg Egal_0(y) \wedge (y < x)) \rightarrow (y \perp x))$.
La multiplication restreinte aux premiers : si p et q sont deux premiers distincts, le produit pq est le plus petit entier qui n'est premier ni avec p ni avec q, et p^2 est le plus petit entier non premier avec p et différent de p. Cela permet de déf inir la multiplication restreinte aux nombres premiers. On notera $MULTP(p, q, z)$ la relation $z = p \times q$ quand p et q sont premiers. Cette relation s'exprime dans le langage considéré par la formule :
$Premier(p) \wedge Premier(q) \wedge (\neg(p = q) \rightarrow (\neg(z \perp p) \wedge \neg(z \perp q) \wedge \forall t((\neg(t \perp p) \wedge \neg(t \perp q)) \rightarrow (z \leq t)))) \wedge ((p = q) \rightarrow (\neg(z \perp p) \wedge \neg(z = p) \wedge \forall t((\neg(t \perp p) \wedge \neg(t = p)) \rightarrow (z \leq t))))$
4. La multiplication
Le théorème de Schnirelman-Vaughan (théorème 23) permet de décomposer les entiers en sommes de premiers que l'on sait multiplier, d'où la formule $z = x \times y$ définie dans $< +, \perp >$ par :
$((x = 0) \vee (y = 0) \rightarrow (z = 0)) \wedge ((x = 1) \rightarrow (z = y)) \wedge ((y = 1) \rightarrow (z = x)) \wedge (((x \geq 2) \wedge (y \geq 2)) \rightarrow \bigvee_{\substack{1 \leq i \leq 19 \\ 1 \leq j \leq 19}} \exists x_1 \ldots \exists x_i \exists y_1 \ldots \exists y_j \exists z_1 \ldots \exists z_{ij}((x = \sum_{n=1}^{i} x_n) \wedge (y = \sum_{m=1}^{j} y_m) \wedge (\bigwedge_{\substack{1 \leq n \leq i \\ 1 \leq m \leq j}} MULTP(x_n, y_m, z_{nm})) \wedge (z =$

$\sum_{n=1}^{i} \sum_{m=1}^{j} z_{nm})))$

C.4 Ordre et coprimarité

On présente ici la démonstration du lemme 3 :
x+y est le plus petit entier z tel que $z \equiv x + y$ [6] et pour tout entier p premier différent de 11, on a $C(x,p) + C(y,p) - C(z,p) \equiv ip$ [11] où i vaut 0 ou -1.
<u>*Dem*</u> :
x+y vérifie clairement la propriété.
On note Q(x,p) le quotient euclidien de x par p.
On rappelle le théorème de Tchebycheff, utile par la suite :

Théorème 29 (Tchebycheff) *i). Pour tout $x \geq 2$, il existe p premier tel que $x \leq p \leq \frac{7x}{5}$.*
ii). Pour tout $x \geq 8$, il existe p premier tel que $x < p < \frac{7x}{5}$.

On suppose que $t < x + y$ vérifie $t \equiv x + y$ [6] et on va montrer l'existence d'un premier p différent de 11 tel que Q(x,p)+Q(y,p)-Q(t,p) est égal à 2, 3, 4, 5, ou 6, et donc t ne vérifiera pas la propriété, puisque ces nombres ne sont pas congrus à 0 ou -1 modulo 11.
Comme $\frac{7}{5} < 2$ et $6 \mid x + y - t$, le théorème de Tchebycheff assure l'existence d'un nombre premier p tel que $\frac{x+y-y}{6} \leq p \leq \frac{x+y-t}{3}$. On peut en outre supposer que p est différent de 11 : si $a \leq 11 \leq 2a$, on constate q u'il existe un autre premier qui vérifie la même propriété : 7 pour $a = 6$ et 13 pour a =7, 8, 9, 10, 11.
Les encadrements de la forme $Q(u,p) \leq \frac{u}{p} < Q(u,p) + 1$ pour $u = x$, $u = y$ et $u = t$ entraînent l'encadrement suivant :

$$Q(x,p) + Q(y,p) - Q(t,p) - 1 \ < \ \frac{x + y - t}{p} \ < \ Q(x,p) + Q(y,p) - Q(t,p) + 2$$

d'où $\frac{x+y-t}{p} - 2 \ < \ Q(x,p) + Q(y,p) - Q(t,p) \ < \ \frac{x+y-t}{p} + 1$.
Comme $3 \leq \frac{x+y-t}{p} \leq 6$, on a finalement $2 \leq Q(x,p) + Q(y,p) - Q(t,p) \leq 6$, c'est-à-dire ce qu'on voulait.

Références

[1] S.Grigorieff - D.Richard, *Contribution à l'étude d'une conjecture de théorie des nombres par le codage ZBV, in L'Enseignement Mathématique*, 2^e série - Tome 35 - Fascicule 1-2, Janvier - Juin 1989.

[2] C.Smoryński, *Logical Number Theory 1 - An Introduction*, Springler-Verlag, 1991.

[3] R.Cori - D.Lascar, *Logique Mathématique - Cours et Exercices - T.1 et 2*, Masson, 1993.

[4] D.Richard, *Définissabilité en arithmétique et méthode de codage ZBV appliquée à des langages avec successeur et coprimarité*, Thèse de doctorat d'état, 1985.

[5] E.Mendelson, *Introduction to Mathematical Logic*, The University series in Undergraduate Mathematics, 1964.

[6] R.Smullyan, *Les théorèmes d'incomplétude de Gödel*, Masson (traduction), 1993.

[7] P.Wolper, *Introduction à la calculabilité*, InterEditions, 1991.

[8] M.Margenstern, *Langage Pascal et logique du premier ordre - T.2 : Récursivité et dérécursification, Preuves et complexité d'algorithmes*, Masson, 1990.

[9] O.Sudac, *A theorem in group theory which is not provable in Peano Arithmetic*, Second meeting of the PRC AMI on Complexity, Finite Models and Weak Arithmetics, 26/06/1997.

[10] A.W.Knapp, *Elliptic curves*, Princeton University Press, 1992.