Université d'Aix-Marseille
Faculté des sciences de Luminy

Master 2 MDFI
Année universitaire 2012-2013

Logique et théorie du calcul

Arithmétique de Peano

Sous le nom d'*arithmétique de Peano*, on désigne un système logique destiné à donner formellement une axiomatisation de l'arithmétique. L'objectif d'un tel cadre est double. D'une part, il permet l'établissement de fondements des mathématiques, au même titre que la théorie des ensembles ; dans le cas de l'arithmétique, c'est la notion de nombre entier naturel qui est primitive, le langage logique permet de construire les autres notions sur cette base. D'autre part, il donne un cadre logique dans lequel il est possible d'étudier les fonctions calculables, ce qui permet ensuite d'établir les célèbres théorèmes d'incomplétude de Gödel.

1 Axiomatique de Peano

On se place ici dans le cadre du *calcul des prédicats* du premier ordre. Il s'agit du langage dans lequel on définit précisément ce qu'est une formule logique. Intuitivement, on cherche à décrire une structure (l'ensemble des entiers naturels) et les raisonnements qui s'y appliquent au moyen de ce langage.

Définition 1 (termes)**.** Les termes sont des formules construites à partir de *variables* (notées par les lettres $x, y, z...$) en utilisant des symboles de constantes et de fonctions.

Dans l'arithmétique de Peano, on a les symboles suivants :

- la constante 0 ;
- la fonction unaire S (le successeur, c'est-à-dire intuitivement la fonction $n \mapsto n + 1$) ;
- les fonctions binaires $+$ et $\times$, notées commes des opérateurs binaires.

Les termes désignent intuitivement des éléments de la structure considérée. Par exemple, le terme $S(S(0) + S(S(x))) \times S(y)$ désignera un élément particulier un fois que seront fixées les interprétations des variables x et y et des symboles du langage.

Les énoncés désignent des propriétés logiques, qui peuvent être vraies ou fausses, démontrées ou réfutées, en fonction de la valeur des variables qu'elles contiennent.

Définition 2 (énoncés)**.** Les énoncés sont formés à partir des éléments suivants :

- les énoncés *atomiques* de la forme $R(t_1, ..., t_n)$ où R est un *symbole de relation* n-aire et les t_i sont des termes ;
- les connecteurs logiques : $A \wedge B$ (conjonction, et), $A \vee B$ (disjonction, ou), $A \to B$ (implication), $A \leftrightarrow B$ (équivalence), $\neg A$ (négation) ;
- les quantificateurs $\forall x$ (pour tout x) et $\exists x$ (il existe x).

Dans l'arithmétique de Peano, on a le symbole de relation binaire = qui sera toujours interprété comme l'égalité.

Les quantificateurs rendent *muette* la variable qu'ils contiennent, les variables muettes sont dites *liées* et les autres sont dites *libres*. Par exemple, dans l'énoncé $\forall x(S(x) = y \to x + x = y)$, la variable y est libre et la variable x est liée, on considère donc que $\forall z(S(z) = y \to z + z = y)$ est le même énoncé. On sera souvent amené à remplacer une variable par un terme dans une formule. Par convention, un écriture comme $F[x]$ désigne un énoncé ayant x pour seule variable libre ; dans ce cas $F[t]$ désigne la même formule dans laquelle toutes les occurences de x sont remplacées par t. La notation s'étend pour des énoncés à plusieurs variables libres.

On s'autorisera à ajouter de nouveaux symboles, pour étendre le vocabulaire disponible avec de nouvelles fonctions et relations. Ce qui donne leur signification à ces symboles est l'ensemble des axiomes que l'on pose. La donnée d'un langage (les symboles de fonctions et de relations) et d'un ensemble d'axiomes (c'est-à-dire des formules closes) utilisant ce langage est appelé une *théorie*.

Définition 3 (arithmétique élémentaire)**.** Le langage de base pour l'arithmétique de Peano comporte l'égalité pour seul symbole de relation, et les symboles de fonction $0, S, +, \times$. On appelle *arithmétique élémentaire* la théorie sur ce langage composée des axiomes suivants :

(s1)	$\forall x \forall y(S(x) = S(y) \to x = y)$	injectivité du successeur
(s2)	$\forall x \neg(S(x) = 0)$	0 n'est pas successeur
(s3)	$\forall x(x = 0 \vee \exists y(x = S(y)))$	tout élément est 0 ou un successeur
(a1)	$\forall x(x + 0 = x)$	addition, cas de base
(a2)	$\forall x \forall y(x + S(y) = S(x + y))$	addition, étape de récurrence
(m1)	$\forall x(x \times 0 = 0)$	multiplication, cas de base
(m2)	$\forall x \forall y(x \times S(y) = (x \times y) + x)$	multiplication, étape de récurrence

Définition 4 (arithmétique de Peano)**.** Étant donné un langage $\mathscr{L}$ contenant le langage de base, on appelle *arithmétique de Peano sur* $\mathscr{L}$ la théorie $\mathrm{PA}_{\mathscr{L}}$ contenant l'arithmétique élémentaire et, pour chaque formule $F[x]$ sur le langage $\mathscr{L}$, l'axiome

$$F[0] \to \forall x(F[x] \to F[S(x)]) \to \forall x F[x]$$

L'ensemble de ces axiomes est appelé *schéma de récurrence*.

La définition de la théorie doit dépendre du langage. En effet, quand on ajoutera des symboles au langage, le schéma de récurrence pourra faire référence à ces nouveaux symboles.

Le système formel dans lequel on se place est le calcul des prédicats du premier ordre, la logique ainsi définie est donc plus précisément appelée *arithmétique du premier ordre*, car elle ne contient que la quantification sur les individus. On peut aussi étudier les systèmes composés de ce même formalisme mais avec de la quantification plus puissante, par exemple l'arithmétique du second ordre (PA2) où il est possible de quantifier sur des ensembles d'entiers, voire l'arithmétique d'ordre supérieur ($\mathrm{PA}\omega$) où il est possible de quantifier sur des ensembles d'ensembles d'entiers et au delà.

Exercice 1 – *Entiers standard*

1. Montrer que pour tout terme clos t sur le langage de base, il existe un terme u de la forme $S(S(\dots S(0)\dots))$ tel que $t = u$ soit démontrable dans l'arithmétique élémentaire.

2. Montrer que pour tous termes clos t et u sur le langage de base, l'arithmétique élémentaire permet de démontrer $t = u$ ou $\neg(t = u)$.

Pour chaque entier naturel $n \in \mathbb{N}$, on notera «n» le terme $S(S(S(\dots S(0)\dots)))$ avec n fois le symbole S. Ce terme représente l'entier naturel n dans tout modèle de PA. On verra plus loin qu'il existe des modèles de PA qui contiennent des éléments qui ne sont pas l'interprétation d'un terme «n» ; on qualifiera ces modèles de *non-standard*, par opposition à l'ensemble $\mathbb{N}$ qui fournit le *modèle standard* de PA.

Exercice 2 – *Propriétés des opérations*
Montrer dans PA les propriétés habituelles de la somme et du produit :
- l'opération + est associative et commutative avec 0 pour neutre ;
- l'opération × est associative et commutative avec «1» pour neutre ;
- l'opération × distribue sur l'opération + et 0 est absorbant ;
- les règles de simplification s'appliquent :

$$\forall x \forall y \forall z((x + z = y + z) \to (x = y))$$
$$\forall x \forall y((x + y = 0) \to (x = 0) \wedge (y = 0))$$
$$\forall x \forall y \forall z((x \times z = y \times z) \to (z = 0) \vee (x = y))$$
$$\forall x \forall y((x \times y = 0) \to (x = 0) \vee (y = 0))$$
$$\forall x \forall y((x \times y = \text{«1»}) \to (x = \text{«1»}) \wedge (y = \text{«1»}))$$

Les deux théorèmes suivants justifient qu'il est possible d'augmenter le langage d'un théorie sans changer l'expressivité de la théorie, à condition d'ajouter des axiomes pour définir la signification des nouveaux symboles.

Théorème 1. *Soient $\mathscr{L}$ un langage et $\mathscr{T}$ une théorie sur $\mathscr{L}$. Soit $F[x_1, \dots, x_n]$ une formule sur $\mathscr{L}$ ayant $x_1, \dots, x_n$ pour seules variables libres. On définit le langage $\mathscr{L}'$ comme $\mathscr{L}$ augmenté d'un nouveau symbole de relation R d'arité n, et $\mathscr{T}'$ comme la théorie $\mathscr{T}$ augmentée de l'axiome*

$$\forall x_1 \dots \forall x_n \Big(R(x_1, \dots, x_n) \leftrightarrow F[x_1, \dots, x_n]\Big).$$

Alors tout modèle de $\mathscr{T}$ s'étend d'une façon unique en un modèle de $\mathscr{T}'$ ayant le même ensemble de base.

Théorème 2. *Soient $\mathscr{L}$ un langage et $\mathscr{T}$ une théorie sur $\mathscr{L}$. Soit $F[x_1, \dots, x_n, y]$ une formule sur $\mathscr{L}$ ayant $x_1, \dots, x_n, y$ pour seules variables libres. On définit le langage $\mathscr{L}'$ comme $\mathscr{L}$ augmenté d'un nouveau symbole de fonction f d'arité n, et $\mathscr{T}'$ comme la théorie $\mathscr{T}$ augmentée de l'axiome*

$$\forall x_1 \dots \forall x_n \Big(F[x_1, \dots, x_n, f(x_1, \dots, x_n)]\Big).$$

Si $\mathscr{T}$ permet de démontrer
- $\forall x_1 \dots \forall x_n \exists y F[x_1, \dots, x_n, y]$
- $\forall x_1 \dots \forall x_n \forall y \forall z \Big(F[x_1, \dots, x_n, y] \wedge F[x_1, \dots, x_n, z] \to y = z\Big)$

alors tout modèle de $\mathscr{T}$ s'étend d'une façon unique en un modèle de $\mathscr{T}'$ ayant le même ensemble de base.

Ces deux résultats permettent d'ajouter librement au langage des symboles de relations et de fonctions, tant qu'on ajoute aussi leur définition à la théorie. Dans le cas des fonctions, il doit être possible de démontrer que la relation définissant la fonction est bien fonctionnelle ; sans cette contrainte, deux choses peuvent arriver :
- si $\forall x_1 \dots \forall x_n \exists y F[x_1, \dots, x_n, y]$ n'est pas démontrable, alors il se peut que la théorie obtenu soit incohérente parce qu'aucune fonction ne respecte la relation voulue,

– si l'autre axiome n'est pas satrisfait, il peut y avoir plusieurs fonctions différentes répondant à la même définition.

Dans la suite, on ne précisera plus le langage, on se placera toujours dans le langage de base étendu par toutes les définitions qui auront été posées. L'exemple le plus simple consiste à définir la relation $x \neq y$ comme équivalente à $\neg(x = y)$.

Définition 5 (ordre sur les entiers)**.** On définit dans PA la relation $x \leqslant y$ comme $\exists z(x + z = y)$. On définit $x < y$ comme $(x \leqslant y) \wedge (x \neq y)$, et $x \geqslant y$ et $x > y$ comme des équivalents de $y \leqslant x$ et $y < x$ respectivement.

Exercice 3 – *Relation d'ordre*

1. Montrer dans PA que la relation $\leqslant$ est une relation d'ordre total.

2. Montrer dans PA que $x < y$ est équivalent à $S(x) \leqslant y$ et à $\neg(y \leqslant x)$.

3. Montrer que, pour tout entier naturel n, on a dans PA : $\forall x\Big(x \leqslant \text{«}n\text{»} \rightarrow \bigvee_{i=0}^{n} x = \text{«}i\text{»}\Big)$.

2 Relations et fonctions définissables

On a défini plus haut une représentation standard des entiers naturels dans le langage de l'arithmétique : l'entier n est représenté par le terme $\text{«}n\text{»} = S^n(0)$. On cherche maintenant a utiliser le langage formel de l'arithmétique pour définir des fonctions et des relations sur les entiers, d'une façon cohérente avec cette représentation des entiers.

Définition 6 (relation définissable)**.** Soit $\mathscr{T}$ une théorie sur un langage contenant 0 et S. Une relation $R \subseteq \mathbb{N}^k$ est *définissable* dans $\mathscr{T}$ s'il existe un énoncé $F[x_1, ..., x_k]$ sur le langage de $\mathscr{T}$ telle que pour tous entiers $n_1, ..., n_k \in \mathbb{N}$, l'énoncé $F[\text{«}n_1\text{»}, ..., \text{«}n_k\text{»}]$ soit démontrable dans $\mathscr{T}$ si et seulement si $(n_1, ..., n_k) \in R$.

Exercice 4

Montrer que les énoncés suivants sont définissables :

– a divise b ;

– a est premier ;

– b est le plus petit nombre premier strictement supérieur à a.

Exercice 5 – *Ensembles d'entiers*

On représente un ensemble d'entiers E par un énoncé $E[x]$, de sorte que $E[x]$ signifie intuitivement que x est élément de E. Par exemple, l'ensemble des entiers pairs est représenté par l'énoncé $\exists y(x = y + y)$. L'ensemble des entiers inférieurs à 12 est représenté par $x \leqslant \text{«}12\text{»}$, soit $\exists y(x + y = S^{12}(0))$. De même, si E et F représentent deux ensembles, l'énoncé « E est inclus dans F » s'écrit $\forall x(E(x) \rightarrow F(x))$.

1. Énoncer la propriété « x est le plus petit élément de E. »

2. Énoncer la propriété « E est infini » (en utilisant l'ordre).

3. Soit $E[x]$ un énoncé, représentant un ensemble. Écrire un énoncé $P_E[n]$ qui exprime « si E contient un élément inférieur ou égal à n, alors E a un plus petit élément et celui-ci est majoré par n. »

4. Démontrer $\forall x P_E[x]$ en utilisant le schéma de récurrence.

5. Énoncer et démontrer dans PA la propriété « si E est non vide alors il a un plus petit élément. »

Définition 7 (fonction définissable)**.** Soit $\mathscr{T}$ une théorie sur un langage contenant 0 et S. Une fonction $f : \mathbb{N}^k \to \mathbb{N}$ est *définissable* dans $\mathscr{T}$ s'il existe un énoncé $F[x_1, ..., x_k, y]$ sur le langage de $\mathscr{T}$ telle que pour tous entiers $n_1, ..., n_k \in \mathbb{N}$ on puisse démontrer dans $\mathscr{T}$

$$\forall y \left(F[\text{«}n_1\text{»}, ..., \text{«}n_k\text{»}, y] \leftrightarrow y = \text{«}f(n_1, ..., n_k)\text{»} \right).$$

En d'autres termes, une fonction est représentable s'il est possible de caractériser son graphe par une formule de l'arithmétique de Peano. Notons que toute fonction qui s'écrit par des sommes et produits de variables et d'entiers, c'est-à-dire toute fonction polynomiale à coefficients dans $\mathbb{N}$, est représentable. En effet, une telle fonction s'exprime par un terme $t[x_1, ..., x_k]$ écrit dans le langage de PA, il suffit donc de poser pour $F[x_1, ..., x_k, y]$ l'énoncé atomique $y = t[x_1, ..., x_k]$.

Il est important de noter que la définition des fonctions représentables demande simplement que l'équivalence $\forall y.F(\text{«}n_1\text{»}, ..., \text{«}n_k\text{»}, y) \leftrightarrow y = \text{«}f(n_1, ..., n_k)\text{»}$ soit démontrable pour chaque choix de $n_1, ..., n_k$ indépendamment des autres choix. Ceci implique en particulier que la démonstration d'équivalence est souvent très simple, et notamment qu'elle peut ne pas avoir besoin du schéma de récurrence. En effet, la récurrence est nécessaire pour démontrer des propriétés de tous les entiers, alors qu'ici il s'agit de démontrer une propriété d'un k-uplet d'entiers particulier ; le quantificateur $\forall y$ ne sert qu'à faire abstraction de la variable y.

Exercice 6

1. Montrer que le quotient et le reste dans la division euclidienne sont définissables.

2. Montrer que la fonction $n \mapsto \lfloor \sqrt{n} \rfloor$ est définissable.

D'après le résultat précédent sur les extensions par définition, pour chaque relation définissable on peut étendre le langage avec un nouveau symbole de relation et un axiome qui caractérise ce symbole par la formule qui définit la relation, et on obtiendra une théorie qui a les mêmes modèles que la théorie de départ.

Pour les symboles de fonction, ce n'est pas automatique : il faut aussi pouvoir démontrer l'existence et l'unicité de l'image dans la théorie considérée, sans quoi les modèles ne sont pas forcément les mêmes. Sans démonstration d'existence, certains modèles de la théorie de départ ne seront pas des modèles de la théorie enrichie ; sans démonstration d'unicité, un modèle donné de la théorie initiale aura plusieurs extensions différentes qui seront des modèles de la théorie enrichie.

Si les conditions voulues sont satisfaites, on s'autorisera donc à utiliser les fonctions définissables comme des symboles de fonctions, en sachant que tout énoncé démontrable dans le système étendu se démontre dans PA.

On va maintenant démontrer que toute fonction récursive est représentable. Le seul point délicat est la représentation du schéma de récurrence. Pour cela, la technique habituelle consiste à trouver une représentation pour les suites finies d'entiers, ce que l'on peut faire au moyen du résultat d'arithmétique connu sous le nom de *théorème des restes chinois* :

Théorème 3. *Soit k un entier non nul. Soient $n_1, ..., n_k$ non nuls et premiers entre eux deux à deux. Soit $n = n_1 \times \ldots \times n_k$. Pour toute famille d'entiers $a_1, ..., a_k$, il existe un unique entier $x < n$ tel que $x \equiv a_i \pmod{n_i}$ pour tout i.*

Démonstration. On peut procéder par récurrence sur k. Dans le cas $k = 1$, le théorème énonce que pour tout entier $n > 0$ et tout entier a il existe un unique entier $x < n$ tel que $x \equiv a \pmod{n}$; c'est une conséquence de la division euclidienne. Supposons le résultat acquis pour un k donné et considérons le cas $k+1$. On a donc des entiers $n_1, \ldots, n_{k+1}$ non nuls et premiers entre eux et des entiers $a_1, \ldots, a_{k+1}$ quelconques. Posons $n' = n_1 \times \ldots \times n_k$. Par hypothèse de récurrence il existe un unique entier $y < n'$ tel que $y \equiv a_i \pmod{n_i}$ pour tout $i \leqslant k$. Par hypothèse, n_{k+1} est premier avec n' (en effet, s'il existait un nombre premier p divisant n_{k+1} et n', alors il diviserait forcément l'un des n_i pour $i \leqslant k$). Par le théorème de Bezout il existe donc deux entiers relatifs u et v tels que $un' + vn_{k+1} = 1$. On a donc $un' \equiv 1 \pmod{n_{k+1}}$, et pour tout $i \leqslant k$ on a $un' \equiv 0 \pmod{n_i}$ puisque n_i est facteur de n'. De même, on a $vn_{k+1} \equiv 1 \pmod{n'}$, d'où $vn_{k+1} \equiv 1 \pmod{n_i}$ pour chaque $i \leqslant k$. Soit x le reste de la division euclidienne de $yvn_{k+1} + a_{k+1}un'$ par $n = n' \times n_{k+1}$, alors on a bien $0 \leqslant x < n$ et $x \equiv a_i \pmod{n_i}$ pour chaque $i \leqslant k+1$. Soit x' un autre entier vérifiant cette propriété, alors on a $x' - x \equiv 0 \pmod{n_i}$ pour tout i, donc $x' - x$ est un multiple commun de tous les n_i, or ceux-ci sont premiers entre eux donc $x' - x$ est multiple de n. Du fait que $0 \leqslant x, x' < n$ on déduit $-n < x' - x < n$ donc la seule possibilité est $x' - x = 0$, ce qui prouve l'unicité de x. □

Proposition 4. *Soit $\beta : \mathbb{N}^3 \to \mathbb{N}$ la fonction qui à (a, b, i) associe le reste de la division euclidienne de b par $a \times (i+1) + 1$. Soient $a_0, \ldots, a_k$ des entiers. Il existe deux entiers a et b tels que pour tout $i \leqslant k$ on ait $\beta(a, b, i) = a_i$.*

Démonstration. Soit s un entier supérieur à $k+1$ tel que $s!$ soit supérieur à tous les a_i. Posons $a = s!$. Pour chaque i, posons $d_i = 1 + (i+1)s!$, alors les d_i sont premiers entre eux deux à deux, et $a_i < d_i$ pour chaque i. Par le théorème 3, il existe donc un entier b tel que pour tout i, $a_i \equiv b \pmod{d_i}$. Par conséquent on a $\beta(a, b, i) = a_i$. □

Il est clair que la fonction β est définissable, il suffit de poser

$$B[a, b, i, x] = \Big(x \leqslant a \times S(i) \wedge \exists y.(b = y \times S(a \times S(i)) + x)\Big).$$

Ce résultat nous permet de traduire dans le langage de l'arithmétique de Peano des énoncés de la forme « il existe une suite finie $a_1, \ldots, a_p$ telle que P », où p est un terme du langage. En effet, un tel énoncé se traduira en « il existe deux entiers a et b tels que P', » où P' est l'énoncé P dans lequel chaque a_i est remplacé par $\beta(a, b, i)$. On peut utiliser ce genre de quantification pour définir des fonctions par récurrence, par exemple la fonction puissance peut se définir comme

> $a^b = c$ s'il existe une suite finie $a_0, \ldots, a_b$ telle que $a_0 = 1, a_{i+1} = a \times a_i$ pour tout $i < b$,
> et $c = a_b$.

On traduit ceci en une formule en posant

$$P[a, b, c] = \exists u \exists v.B[u, v, 0, 1] \wedge (\forall i \forall x.i < p \wedge B[u, v, i, x] \to B(u, v, S(i), a \times x)] \wedge B[u, v, b, c]$$

Théorème 5. *Toute fonction récursive est représentable.*

Démonstration. Les fonctions de base sont faciles à représenter. Pour la composition, soit $f : \mathbb{N}^k \to \mathbb{N}$ une fonction représentée par une formule F et $g_1, \ldots, g_k : \mathbb{N}^\ell$ des fonctions représentées par des formules $G_1, \ldots, G_k$. Posons la formule suivante :

$$H[x_1, \ldots, x_\ell, y] := \exists z_1 \ldots \exists z_k \Big(\bigwedge_{i=1}^{k} G_i[x_1, \ldots, x_\ell, z_i] \wedge F[z_1, \ldots, z_k, y] \Big)$$

Alors pour toute famille d'entiers $a_1, \ldots, a_\ell$, pour chaque i la formule $G_i(\ll a_1 \gg, \ldots, \ll a_\ell \gg, z_i)$ est équivalente à $z_i = \ll g_i(a_1, \ldots, a_\ell) \gg$ par définition, donc on a

$$H[\ll a_1 \gg, \ldots, \ll a_\ell \gg, y] \leftrightarrow \exists z_1 \ldots \exists z_k \Big(\bigwedge_{i=1}^{\ell} z_i = \ll g_i(a_1, \ldots, a_\ell) \gg \wedge F[z_1, \ldots, z_k, y] \Big)$$

d'où on peut déduire facilement $H[\ll a_1 \gg, \ldots, \ll a_\ell \gg, y] \leftrightarrow F[\ll g_1(a_1, \ldots, a_\ell) \gg, \ldots, \ll g_k(a_1, \ldots, a_\ell) \gg, y]$, puis par définition de F on a $H[\ll a_1 \gg, \ldots, \ll a_\ell \gg, y] \leftrightarrow y = \ll f(g_1(a_1, \ldots, a_\ell), \ldots, g_k(a_1, \ldots, a_\ell)) \gg$.

Le schéma de récurrence se représente en utilisant la représentation des suites finies comme dans l'exemple précédent. Pour le schéma de minimisation, prenons une fonction $f : \mathbb{N}^{k+1} \to \mathbb{N}$ représentée par une formule $F[x_1, \ldots, x_{k+1}, y]$, alors la fonction $\mu_k(f)$ est représentée par l'énoncé

$$F[x_1, \ldots, x_k, z, 0] \wedge \forall x \Big(x < y \to \exists t (F[x_1, \ldots, x_k, z, t] \wedge t \neq 0) \Big). \qquad \square$$

Ce théorème montre que toute fonction récursive est représentable en arithmétique de Peano, mais il reste une subtilité. Les fonctions récursives, en général, n'ont pas de raison d'être définies en tout point. Représenter une fonction récursive totale est une chose, mais démontrer qu'une fonction récursive est totale en est une autre : la définissabilité iplique que pour chaque valeur d'entrée, il est possible de démontrer la validité de la valeur de sortie, mais l'énoncé de totalité général est plus fort.

Définition 8 (fonction prouvablement totale)**.** Soit $f : \mathbb{N}^k \to \mathbb{N}$ une fonction définissable dans une théorie $\mathscr{T}$, et soit $F[x_1, \ldots, x_k, y]$ un énoncé qui la définit. La fonction f est *prouvablement totale dans* $\mathscr{T}$ si l'énoncé $\forall x_1 \ldots \forall x_k \exists y F[x_1, \ldots, x_k, y]$ est démontrable dans $\mathscr{T}$.

Exemple 1 (suites de Goodstein)*.* Les suites de Goodstein permettent de construire un exemple de fonction récursive totale dont la totalité n'est pas démontrable dans l'arithmétique de Peano du premier ordre. La construction de fait de la façon suivante :

Soient un entier $b \geqslant 2$ et a un entier quelconque. Considérons l'écriture de a en base b : $a = \sum_{i=0}^{p} a_i b^i$ avec $a_i < b$ pour chaque i. Dans cette écriture, les exposants i peuvent dépasser b, on les écrit donc eux aussi en base b, et ainsi de suite pour leurs exposants. Dans l'écriture obtenue, remplaçons tous les b par $b + 1$ et retranchons 1 qu résultat. On appelle $G(b, n)$ l'entier obtenu. Par exemple, on a

$$89 = 3^{3^1+1} + 2 \cdot 3^1 + 1$$
$$G(89, 3) = 4^{4^1+1} + 2 \cdot 4^1 + 1 - 1 = 1032$$

Étant donné un entier m, on définit la suite g_m par récurrence :

$$g_m(0) = m$$
$$g_m(n+1) = G(n+2, g_m(n))$$

Le théorème de Goodstein établit que, pour tout entier m, la suite g_m atteint 0, c'est-à-dire qu'il existe un entier n tel que $g_m(n) = 0$. La fonction $f(n) = \min \left\{ n \;\middle|\; g_m(n) = 0 \right\}$ est donc totale.

Il n'est pas très difficile de montrer que la fonction G est récursive primitive, et donc que la fonction $(m, n) \mapsto g_m(n)$ l'est aussi. En conséquence, f est une fonction récursive totale. En revanche, on peut montrer qu'il est impossible de démontrer la totalité de f dans l'arithmétique de Peano du premier ordre, c'est-à-dire qu'il est impossible de démontrer le théorème de Goodstein dans cette logique. On reviendra plus tard sur les raisons de cette impossibilité.