L'INFINITÉ DES NOMBRES PREMIERS : UNE ÉTUDE DE CAS DE LA PURETÉ DES MÉTHODES

Andrew Arana

P.U.F. | *Les études philosophiques*

2011/2 - n° 97
pages 193 à 213

ISSN 0014-2166

L'INFINITÉ DES NOMBRES PREMIERS : UNE ÉTUDE DE CAS DE LA PURETÉ DES MÉTHODES

Introduction

Depuis l'Antiquité toute une tradition en mathématiques privilégie les solutions à des problèmes ou les démonstrations de théorèmes qui se limitent à des considérations « proches » du problème résolu ou du théorème démontré, ou encore qui lui soient « intrinsèques ». Un exemple pouvant servir de motivation est la démonstration par Hadamard et de la Vallée Poussin, en 1896, du théorème des nombres premiers au moyen de l'analyse complexe. À propos de cette démonstration, le distingué théoricien des nombres A. E. Ingham fit la remarque qu'elle « pourrait être tenue pour insatisfaisante, parce qu'elle introduit des idées très éloignées du problème initial, et qu'il serait naturel d'attendre une démonstration du théorème des nombres premiers qui ne dépende pas de la théorie de la variable complexe » (cf. [24], p. 5-6). Une autre source classique d'exemples concerne la solution aux problèmes géométriques recourant à la géométrie analytique, par exemple à la manière de Descartes. La « convenance » de solutions analytiques à des problèmes géométriques a donné lieu à une gigantesque discussion parmi les mathématiciens, dans la mesure où ces considérations ont frappé nombre d'entre eux comme étant « plutôt éloignées » des problèmes traités. Dans le cas de ces deux exemples de départ, des questions de pureté ont été mises au centre de la discussion.

L'étude des usages de la pureté dans la pratique mathématique révèle qu'il existe plusieurs efforts différents visant à la pureté, parmi lesquels ce que j'ai appelé la « pureté syntaxique », la « pureté logique », et la « pureté topique » (cf. [1], [2], [13]). Ils diffèrent dans la façon de mesurer ce qui est « proche de » ou « intrinsèque à » ce qui est résolu ou démontré. La pureté syntaxique mesure l'intrinséquéité par les sous-termes ou sous-formules de l'énoncé qui est démontré ou du problème qui est résolu, tandis que la pureté logique mesure l'intrinséquéité par les conditions logiquement suffisantes pour démontrer ledit énoncé ou résoudre ledit problème. Dans l'article [13], écrit conjointement avec Mic Detlefsen, nous nous sommes proposés de clarifier la nature et la signification épistémique de ce qui nous

Les Études philosophiques, n° 2/2011, p. 193-213

semble être la conception de la pureté la plus importante, à savoir la pureté topique. *Grosso modo*, une solution ou une démonstration est « topiquement pure » si elle se fonde seulement sur ce qui « fait partie » du contenu de ce qui est résolu ou démontré. Nous disons d'une telle solution, ou d'une telle démonstration, qu'elle est « topiquement » pure parce que nous considérons que ce qui « fait partie » du contenu d'un problème ou d'un énoncé est ce qui fonde sa compréhension, et nous appelons « sujet » de ce problème ou de cet énoncé la famille des suppositions qui fondent cette compréhension.

Dans cet article, mon but est d'approfondir cette étude, en considérant en plus ample détail des questions de pureté soulevées à propos de l'infinité des nombres premiers. Nous avons déjà fait cette étude de cas dans [13], mais nous allons ici l'aborder de façon significativement plus détaillée. Après avoir rappelé la caractérisation proposée par [13] de la pureté topique et de sa valeur épistémique, je parlerai de deux solutions différentes au problème de savoir s'il existe une infinité de nombres premiers. Je défendrai l'idée que la démonstration classique, due à Euclide, que les nombres premiers sont en nombre infini, est topiquement pure, tandis qu'une démonstration topologique due à Furstenberg ne l'est pas[1]. En ce qui concerne la solution euclidienne, je considérerai l'objection faite à l'encontre de sa pureté selon laquelle elle fait un usage essentiel de l'addition, alors que l'addition n'est pas explicitement mentionnée dans la formulation du problème, et je montrerai quelle réponse on peut faire à cette objection. En ce qui concerne la solution impure de Furstenberg, je considérerai la conception *bourbakiste* de Colin McLarty suivant laquelle la démonstration de Furstenberg est topiquement pure, et défendrai l'idée que la notion de topicité que McLarty a en vue diffère de celle que nous avons identifiée dans [13]. La différence renvoie à des analyses rivales du type de délimitation du fait de « faire partie » du contenu qui détermine le sujet d'un problème ou d'un énoncé. Notre problème, dans [13], était de savoir quels sont les fondements d'une compréhension « élémentaire » des énoncés mathématiques, tandis que la conception bourbakiste de McLarty s'occupe davantage d'une compréhension « profonde » des mathématiques. Je voudrais ici faire valoir contre McLarty qu'une compréhension élémentaire est le type de compréhension qui est le plus pertinent lorsqu'il est question de pureté topique.

Pureté topique

L'intuition qui guide notre analyse de la pureté topique a été très bien exprimée par Hilbert dans ses cours de géométrie de l'année 1898-1899 :

Dans les mathématiques modernes, une telle critique est très souvent faite, dès que le but est de préserver *la pureté de la méthode*, *i.e.* de démontrer

1. Pour un panorama des différentes démonstrations du théorème de l'infinité des nombres premiers, voir le chapitre 1 de *Raisonnements divins : quelques démonstrations mathématiques particulièrement élégantes*, Aigner, M. & Ziegler, M., Springer, 2006.

des théorèmes si possible en n'employant que des moyens directement liés au contenu de ce théorème[1].

L'important ici pour déterminer si une démonstration est ou non pure est donc de savoir si les moyens utilisés sont ou non directement liés au contenu du théorème qu'on veut démontrer.

Ce que cela signifie précisément, pour un élément de démonstration, d'être « directement lié » au contenu de ce qui est démontré, voilà qui n'est pas particulièrement clair. Nous avons essayé, dans [13], d'éclairer un peu cette question. Appelons « sujet » d'un problème donné (pour α) l'ensemble des suppositions qui déterminent (pour une personne donnée α qui se penche sur le problème) la compréhension de ce problème. Dans ces suppositions entrent des définitions, des axiomes, des inférences, etc. Mis ensemble, tous ces éléments sont constitutifs de la compréhension qu'a α du problème, et par suite de l'identité du problème (pour α).

On pourrait dès lors déterminer plus précisément ce qui fait la pureté topique de la manière suivante. Une solution à un problème est « topiquement pure » (pour α) si elle repose sur ce qui appartient au sujet de ce problème. En d'autres termes, les solutions topiquement pures sont celles qui reposent uniquement sur ce qui est constitutif de l'identité du problème dont elles sont les solutions.

Notre analyse de la valeur *épistémique* de la pureté topique a été la suivante. Le noyau de cette analyse consiste dans ce contre-factuel : si une composante d'une solution topiquement pure à un problème était retirée par la personne qui l'examine, alors la compréhension qu'a cette personne du problème en serait changée. Ceci est dû au fait que chaque composante d'une solution topiquement pure appartient au sujet de ce problème, et par conséquent détermine en partie la compréhension qu'on en a. Tel n'est pas le cas pour une solution impure à un problème, puisque certaines de ses composantes n'appartiennent pas au sujet de ce problème.

Une solution pure à un problème demeure donc une solution à ce problème même si l'une de ses composantes est retirée, car un tel retrait « dissout » le problème, en modifiant la compréhension qu'on en a, et donc son identité. Si dissoudre un problème n'est pas généralement considéré comme une façon de le résoudre, nous soutenons que c'est pourtant bien le cas, puisque la solution à un problème vise à supprimer une ignorance rationnelle, et que nous ne pouvons être (rationnellement) ignorants de problèmes qui se trouvent dissous. Ainsi une solution topiquement pure demeure-t-elle une solution même si l'une de ses composantes est retirée. La suppression d'ignorance permise par une solution topiquement pure à un problème

1. Cf. [21], p. 315-316. Le texte original est le suivant : « In der modernen Mathematik wird solche Kritik sehr hufig gebt, wobei das Bestreben ist, *die Reinheit der Methode* zu wahren, d.h. beim Beweise eines Satzes wo möglich nur solche Hilfsmittel zu benutzen, die durch den Inhalt des Satzes nahe gelegt sind. »

s'avère donc « stable » relativement aux changements d'attitude vis-à-vis de ses composantes.

On ne peut pas dire la même chose d'une solution topiquement impure à un problème. Cela est dû au fait que certaines composantes d'une solution topiquement impure peuvent être retirées sans que le problème que celle-ci résout soit pour autant dissous, de sorte que la suppression d'ignorance qu'elle permet n'est pas aussi « stable » relativement aux changements d'attitude vis-à-vis de ses composantes que l'est celle permise par une solution topiquement pure.

Une solution topiquement pure résiste donc mieux qu'une solution topiquement impure au retrait de ses composantes. Cette résistance constitue une vertu épistémique, puisque la suppression d'ignorance est une question épistémique, et que nous avons affirmé qu'une solution topiquement pure permet une meilleure suppression d'ignorance qu'une solution topiquement impure, du fait de permettre une suppression d'ignorance plus stable ou plus résistante.

La pureté topique serait toutefois sans grand intérêt si l'on ne pouvait établir de clairs exemples de solutions topiquement pures et de solutions topiquement impures. Il est donc crucial d'identifier de tels exemples. Nous avons traité un exemple, dans [13], celui de l'infinité des nombres premiers (IP). La discussion développée dans cet article ne pouvait qu'être brève, c'est pourquoi je voudrais ici approfondir la discussion de manière significative.

Une solution pure à IP

Imaginons une personne α examinant aujourd'hui une démonstration et ayant une compréhension contemporaine typique des questions d'arithmétique. Supposons que α formule un problème comme suit : pour tout nombre naturel, existe-t-il un nombre premier qui est plus grand ? Appelons ce problème IP, pour « infinité des nombres premiers ». Une solution à IP selon α est la démonstration que pour tout entier naturel a il existe un entier naturel $b > a$ tel que b soit un nombre premier. Une solution topiquement pure à IP pour α pourra reposer sur les suppositions qui déterminent le contenu de ce problème, tel qu'il vient d'être formulé, autrement dit, sur ce qui appartient au sujet de IP.

Le sujet de IP semble inclure, entre autres suppositions, les définitions et les axiomes qui concernent la notion d'entier naturel, une relation d'ordre sur les entiers naturels, et enfin la notion de primalité. Il est possible d'être plus précis. Les entiers naturels sont typiquement compris comme commençant avec un premier nombre 1, suivi de son successeur $S(1)$, et se poursuivant à chaque fois avec le successeur de tout nombre déjà atteint. Par conséquent, les axiomes pour le successeur semblent devoir être inclus, de même que les axiomes inductifs qui expriment précisément l'idée que les entiers naturels « partent » de 1 et « continuent » ensuite à partir de là. Les définitions et les axiomes concernant une relation d'ordre sur les entiers naturels semblent également requis, et, pour respecter la pratique typique, ils devraient spécifier un ordre discret linéaire. Deuxièmement, s'agissant de la primalité, la pratique contemporaine fait d'un entier naturel a un nombre premier si et seulement si $a \neq 1$ et que les seuls entiers divisant a sont 1 et a, sachant que a divise b (ce qu'on note $a \mid b$) si et seulement si il existe x tel que $a \cdot x = b$. Les définitions de la divisibilité et de la multiplication sembleraient donc appartenir au sujet de IP pour α.

Les axiomes de Peano pour les entiers naturels, auxquels il faut ajouter les définitions de la primalité et de la divisibilité qu'on vient de donner, fournissent une formulation raisonnable de toutes ces suppositions.

À titre de première approximation d'une solution topiquement pure à IP, considérons la démonstration euclidienne bien connue tirée des *Éléments* IX, 20. Si $a = 1$, alors, puisque $2 = S(1)$ est premier, nous savons qu'il y a un nombre premier plus grand que $a = 1$. Supposons donc que $a > 1$. Soit alors $p_1, p_2, \cdots, p_n$ tous les nombres premiers plus petits ou égaux à a, et soit $Q = S(p_1 \cdot p_2 \cdot \ldots \cdot p_n)$. On peut remarquer que, par hypothèse, Q possède un diviseur premier b. Et, pour tout i, $b \neq p_i$; en effet, dans le cas contraire, $b \mid (p_1 \cdot p_2 \cdot \ldots \cdot p_n)$ et $b \mid S(p_1 \cdot p_2 \cdot \ldots \cdot p_n)$, et donc $b = 1$, ce qui contredit la primalité de b. Finalement, donc, ou bien $b > a$, ou bien $b \leq a$, mais comme $b \leq a$ contredit le fait que les p_i sont tous des nombres premiers inférieurs ou égaux à a, il faut conclure que $b > a$.

Cette démonstration comporte plusieurs étapes qui elles-mêmes appellent une démonstration. Ainsi de l'étape consistant à affirmer que si $b \mid (p_1 \cdot p_2 \cdot \ldots \cdot p_n)$ et $b \mid S(p_1 \cdot p_2 \cdot \ldots \cdot p_n)$, alors $b = 1$, ou bien de l'étape affirmant que si $a \mid b$ et $a \mid S(b)$, alors $a = 1$. Les démonstrations typiques de ces résultats (qu'on peut trouver p. ex. dans un manuel d'arithmétique élémentaire) peuvent toutes être conduites à partir des axiomes de Peano, et par suite, pour autant que les suppositions exprimées par les axiomes de Peano peuvent être conçues comme déterminant topiquement IP (pour α), la démonstration euclidienne est topiquement pure (pour α).

Remarquons que pour établir complètement ce dernier point, il faudrait vérifier en plus que les inférences faites dans le cadre de la démonstration euclidienne sont topiques relativement à IP pour α. Cela n'est pas si facile ; par exemple, il se pourrait que certains emplois de la règle de substitution soient topiques, mais non d'autres. Ce que nous avons présenté ici n'est donc qu'une ébauche.

S'il est typique en pratique aujourd'hui de traiter les problèmes de théorie des nombres dans le cadre de la logique classique, il peut être bon de regarder si la solution euclidienne à IP reste pure lorsqu'on change la logique du problème. Tout d'abord, la démonstration euclidienne serait encore topiquement pure même si la logique adoptée pour IP était intuitionniste, puisque cette démonstration fait usage du tiers exclu seulement à propos de prédicats effectivement décidables tels que « est premier », et que, si elle recourt à la réduction à l'absurde, elle ne recourt à aucune double négation.

Deuxièmement, si la logique adoptée pour IP était du second ordre, alors la solution euclidienne remplirait encore les conditions pour être topiquement pure, moyennant une modification triviale destinée à permettre l'emploi du principe d'induction au second ordre.

Troisièmement, si la logique adoptée pour sa formulation était finitiste plutôt que classique, alors il est plausible que la solution euclidienne serait à nouveau topiquement pure. Ceci parce qu'il est facile de vérifier que notre preuve ne fait usage du schéma d'induction pour aucune formule plus complexe que les formules Σ_1 – c'est-à-dire qu'elle peut être formulée dans le fragment très restreint de AP [l'arithmétique de Peano] connu sous le nom de $I\Sigma_1$. Si, avec Tait ([32]), on identifie l'arithmétique finitiste à l'arithmétique primitive récursive (APR) et, qu'on tient, avec Hájek et Pudlák ([22]), APR pour équivalente à $I\Sigma_1$, alors une solution finitiste à IP est une solution pouvant être donnée dans le cadre de $I\Sigma_1$. Dès lors (pour cette interprétation de ce qu'est l'arithmétique finitiste), la solution euclidienne s'avère finitiste, et remplirait ainsi toujours les conditions pour être topiquement pure.

Enfin, supposons que la logique adoptée pour IP soit une logique de la faisabilité plutôt que la logique classique, et qu'elle donne lieu à un problème IP_4. Si, avec Parikh ([28]), on identifie l'arithmétique faisable à $I\Delta_0$ (c'est-à-dire à AP avec un schéma d'induction restreint aux formules dont les quantificateurs sont tous bornés), alors la démonstration euclidienne n'est plus pure. La raison en est que pour déduire l'existence d'un nombre $Q = (p_1 \cdot p_2 \cdot \ldots \cdot p_n) + 1$, la multiplication dans sa totalité est requise. Cette existence peut être démontrée au moyen d'une Σ_1-induction, mais c'est une question ouverte que de savoir si elle peut être démontrée au moyen d'un principe d'induction plus faible, et en particulier si elle peut l'être dans $I\Delta_0$. On sait que l'existence de n'importe quel produit de nombre premier n'est pas démontrable dans $I\Delta_0$ (cf. [11], p. 13). Cela résulte du résultat de Parikh (*in* [28]) suivant lequel toute fonction Δ_0-définissable qui est prouvablement totale dans $I\Delta_0$ a une croissance polynomiale[1]. L'existence de Q peut être démontrée au moyen d'une induction bornée à condition d'ajouter un autre axiome garantissant que la relation exponentielle est totale, ce qui donne la théorie appelée $I\Delta_0(exp)$ (cf. [12], p. 153). $I\Delta_0(exp)$ a fait l'objet de nombreuses études (certains l'appellent AFE, pour Arithmétique des Fonctions Élémentaires). On admet souvent que chacun des résultats de la théorie élémentaire des nombres (par exemple, chacun des résultats qu'on peut trouver dans [23], un manuel élémentaire classique en théorie des nombres) peut être démontré dans AFE (cf. [12], p. 149, note 1). Grâce à un résultat de Gödel ([18]), on sait que la relation exponentielle est définissable dans $(\mathbb{N},1,S,+,\cdot)$ (pour une définition raisonnablement explicite, cf. [15], p. 276-279). Il n'est pas clair en revanche qu'un *axiome* affirmant l'existence de cette relation définissable comme relation *totale* fasse partie

1. Cf. [11-12], p. 164-167, pour plus de détail à propos de ce qui est connu du taux de croissance de la fonction donnant les produits de nombres premiers dans $I\Delta_0$.

du sujet de IP lorsque la logique en cours est celle de la faisabilité. Dans sa thèse de doctorat, A. Woods ([34]) est parvenu à résoudre IP dans $I\Delta_0$ augmenté d'une version faible du principe des tiroirs [*pigeonhole principle*]. Pour ce faire, il n'a pas proposé une version modifiée de la solution euclidienne, mais, plutôt, une version modifiée de la solution due à Sylvester. La théorie de Woods, notée $I\Delta_0 + PHP$ [PHP pour « Pigeonhole Principle »], est logiquement plus faible que $I\Delta_0(exp)$, en ceci que $I\Delta_0(exp)$ permet de démontrer $I\Delta_0 + PHP$, mais que l'inverse n'est pas vrai[1]. Par la suite, Paris, Wilkie et Woods ont remplacé la démonstration originale de Woods par une démonstration qui ne fait intervenir qu'une version faible du principe des tiroirs (cf. [34] ; voir également [12], p. 162-164). À nouveau, on peut se demander si l'un de ces axiomes du type du principe des tiroirs appartient ou non au sujet de IP. Une réponse positive impliquerait que IP admet une solution topiquement pure lorsque sa logique est comprise selon les principes de la faisabilité. En ce qui nous concerne, cette question reste ouverte.

Abordons à présent une autre question. Les axiomes de Peano incluent les axiomes de l'addition, et de fait la démonstration euclidienne, lorsqu'elle est formulée de manière complètement détaillée à partir des axiomes de Peano, fait usage de l'addition. On pourrait contester la pureté topique supposée de la démonstration euclidienne au motif que l'addition n'est pas explicitement mentionnée dans le problème tel qu'il est formulé. Une réponse à cette objection consiste à défendre l'usage de l'addition comme topiquement pure pour IP ; ou bien parce que la multiplication est comprise, comme c'est typique, comme une addition itérée, ou bien parce que les entiers naturels sont compris, comme c'est typique dans la pratique contemporaine, comme munis d'une structure d'anneau, c'est-à-dire munis à la fois d'une opération d'addition et d'une opération de multiplication.

Une seconde réponse fait appel au travail de Julia Robinson montrant comment définir l'addition pour les entiers naturels dans les termes de la fonction successeur et de la relation de divisibilité, qui toutes deux sont explicitement mentionnées dans la formulation du problème (cf. [30], p. 100-102). Robinson a montré comment définir l'addition et la multiplication pour les entiers naturels simplement dans les seuls termes de la fonction successeur et de la relation de divisibilité ([30], p. 100-102). Elle montre tout d'abord que l'addition est définissable dans les termes de la fonction successeur et de la multiplication, de la manière suivante : $a+b=c$ si et seulement si $S(a\cdot c)\cdot S(b\cdot c)=S[(c\cdot c)\cdot S(a\cdot b)]$. Elle montre ensuite qu'à la fois le fait pour deux nombres d'être premiers entre eux et le fait pour un nombre d'être le plus petit commun multiple d'autres nombres peuvent être définis dans les termes de la fonction successeur et de la relation de divisibilité, sans faire appel à l'addition. Elle montre enfin comment définir la multiplication en utilisant la fonction successeur, la primalité relative, et le plus petit commun multiple.

1. Cf. [29] ; voir également [12], p. 162-164.

Au moyen de ces définitions explicites, la solution euclidienne à IP (en tant que formulée dans AP) peut être traduite dans un langage qui ne comporte que 1, S, $|$, et $<$. En particulier, tous les axiomes, définitions et propositions employés pour démontrer la solution euclidienne pourraient être traduits dans ce langage. En évitant toute référence explicite à l'addition, cette traduction de la solution répondrait à l'objection.

On pourrait cependant opposer à cette réponse la remarque, faite par Robinson, que cette traduction « mécanique », comme Robinson la décrit, va de pair avec des axiomes qui sont « compliqués et artificiels » (cf. [30], p. 102-103). Ils sont *syntaxiquement* plus complexes que les axiomes ordinaires, ceux de AP, et en particulier *plus longs* que ces axiomes, et on ne peut les identifier « à vue d'œil » comme étant équivalents à AP. Robinson a ainsi cherché à trouver « un système d'axiomes simple et élégant » pour l'arithmétique dans ce langage restreint. Elle a identifié un candidat au titre de ce système d'axiomes, et prouvé qu'il permet de démontrer les mêmes théorèmes que AP, et par suite la solution euclidienne à IP. Cela semble répondre à l'objection. Toutefois, le système d'axiomes « simple et élégant » qu'identifie Robinson inclut l'induction au second ordre. Elle n'a pas pu démontrer que ce système d'axiomes permet de démontrer les mêmes théorèmes que AP lorsque seule l'induction au premier ordre est admise. Pour autant que nous sachions, cela reste une question ouverte que de savoir si cette démonstration peut être apportée.

Toutefois, il n'est pas évident de savoir en quoi des axiomes « compliqués et artificiels » ne conviennent pas, du point de vue de la pureté topique. Il n'est pas évident que la « simplicité » et « l'élégance » d'une définition ou d'un axiome, interprétées par exemple en termes de complexité syntaxique, soit pertinente pour savoir si une définition ou un axiome appartient au sujet d'un problème. Il se pourrait que des problèmes aient des sujets qui contiennent des éléments irréductiblement complexes. De tels problèmes ne seraient pas simples à comprendre, du moins si l'on considère toutes les suppositions requises pour fonder leur compréhension, mais il n'existe pas de raison *a priori* de penser que tout problème, et même tout problème courant, soit simple à comprendre de ce point de vue. Dans ce cas, l'approche « mécanique » de Robinson demeure une réponse valable à l'objection faite contre la pureté topique de la solution euclidienne en raison de son recours à l'addition.

Une troisième réponse à l'objection concernant le recours à l'addition dans la solution euclidienne consiste à remarquer que le seul moment où l'addition est nécessaire est pour établir des propriétés de la multiplication telles que la commutativité et l'associativité. On pourrait donc isoler ces propriétés de la multiplication et trouver une démonstration directement à partir d'elles, sans passer par l'addition[1].

1. Remarquons que Cegielski a axiomatisé l'arithmétique de la divisibilité, dans le but de parvenir à des résultats de décidabilité (cf. [6], [8]). Toutefois, l'infinité des nombres premiers est prise comme l'un des axiomes de son système. Comme nous visons à démontrer l'infinité des nombres premiers, le travail de Cegielski ne peut nous aider dans notre projet.

Les dix-sept hypothèses suivantes sont un essai en ce sens. Elles incluent des hypothèses concernant la fonction successeur et la relation d'ordre entre entiers en plus d'hypothèses concernant la multiplication, de façon à fournir un ensemble d'hypothèses suffisantes pour résoudre IP sans faire usage de l'addition.

Hypothèse 1. Pour tout x, il existe y tel que $y = S(x)$.
Hypothèse 2. Pour tous x, y, $x = y$ si et seulement si $S(x) = S(y)$.
Hypothèse 3. Pour tous x, y, il existe z tel que $z = x \cdot y$.
Hypothèse 4. Pour tout x, $x \cdot 1 = x$.
Hypothèse 5. Pour tous x, y, z, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
Hypothèse 6. Pour tous x, y, $x \cdot y = y \cdot x$.
Hypothèse 7. Pour toute suite de nombres premiers $p_1, \ldots, p_n$, il existe z tel que $z = p_1 \cdot p_2 \cdot \ldots \cdot p_n$.
Hypothèse 8. Pour tous x, y, z, si $x < y$ et que $y < z$, alors $x < z$.
Hypothèse 9. Pour tout x, $x \not< x$.
Hypothèse 10. Pour tous x, y, $x < y$ ou $x = y$ ou $y < x$.

Les trois dernières hypothèses impliquent ensemble que si $x < y$, alors $y \not< x$, et par suite que la trichotomie affirmée dans l'hypothèse 10 est exclusive, c'est-à-dire que pour tous x, y, exactement l'une des possibilités $x < y$, $x = y$ et $y < x$ est vérifiée.

Hypothèse 11. Pour tout x, $1 \leq x$.
Hypothèse 12. Pour tous x, y, $x < y$ si et seulement si $S(x) < S(y)$.
Hypothèse 13. Pour tout x, $x < S(x)$.
Hypothèse 14. Pour tous x, y, si $x < y$, alors $S(x) \leq y$.
Hypothèse 15. Pour tous x, y, z, $x < y$ si et seulement si $xz < yz$.
Hypothèse 16. Pour tout $y \neq 1$ et tout x, $S(yx) < y \cdot S(x)$.
Hypothèse 17. Pour toute formule $\varphi(x, \overline{y})$, où x est une variable libre et les $\overline{y}$ des termes, si $\varphi(1, \overline{y})$ et que pour tout a et tout $b < a$, $\varphi(b, \overline{y})$ implique que $\varphi(a, \overline{y})$, alors, pour tout a, $\varphi(a, \overline{y})$.

Ces hypothèses peuvent être regroupées de la manière suivante : les hypothèses 1 et 2 portent sur la fonction successeur, les hypothèses 3 à 7 sur la multiplication, les hypothèses 8 à 10 sur la relation d'ordre, les hypothèses 11 à 16 sur la façon dont la fonction successeur et la multiplication respectent la relation d'ordre, et l'hypothèse 17 constitue un schéma d'induction[1].

Nous allons à présent donner une solution non additive à IP en faisant usage de ces hypothèses. Pour simplifier la structure de la démonstration principale, nous allons séparer de la démonstration principale les trois lemmes suivants, et les démontrer séparément.

1. Nous ne prétendons pas que ces hypothèses sont mutuellement indépendantes les unes des autres.

Lemme 3.1. $S(1)$ *est un nombre premier.*

Lemme 3.2. *Tout entier naturel* $a \neq 1$ *admet un nombre premier* $p \leq a$ *pour diviseur.*

Lemme 3.3. *Pour tous* a, b, *si* $a \mid b$ *et que* $a \mid S(b)$, *alors* $a = 1$.

En faisant usage de ces trois lemmes, le principal résultat, à savoir que, pour tout a, il existe $b > a$ qui est un nombre premier, peut être démontré de la manière suivante, les hypothèses employées étant mentionnées au fur et à mesure après chaque étape.

1. Ou bien $a = 1$, ou bien $a > 1$. [Hypothèse 11]
2. (a) Supposons que $a = 1$.
   (b) Par le Lemme 3.1, $S(1)$ est un nombre premier. [Hypothèse 1]
   (c) $S(1) > 1$. [Hypothèse 13]
3. (a) Supposons que $a > 1$.
   (b) Soient $p_1, p_2, \dots, p_n$ tous les nombres premiers inférieurs ou égaux à a.
   (c) Soit $Q = S(p_1 \cdot p_2 \cdot \ldots \cdot p_n)$. [Hypothèses 1 et 7]
   (d) Par le Lemme 3.2, Q admet un nombre premier b pour diviseur.
   (e) i. Supposons que $b = p_i$.
   ii. Alors $b \mid (p_1 \cdot p_2 \cdot \ldots \cdot p_n)$. [Hypothèses 5 et 6]
   iii. Par le Lemme 3.3, $b = 1$, ce qui contredit la primalité de b.
   (f) Donc pour tout $i, b \neq p_i$.
   (g) Ou bien $a < b$, ou bien $b \leq a$. [Hypothèse 10]
   (h) $b \leq a$ contredit le fait que les p_i soient tous les nombres premiers inférieurs ou égaux à a.
   (i) Donc $a < b$.

Démonstration du Lemme 3.1, que $S(1)$ est un nombre premier :

1. Pour tout n, $n < S(1)$, $n = S(1)$, ou $S(1) < n$. [Hypothèses 1 et 10]
2. (a) Supposons que $n = S(1)$.
   (b) $S(1) \mid S(1)$. [Hypothèse 4]
3. (a) Supposons que $n < S(1)$.
   (b) $S(n) \leq S(1)$. [Hypothèses 1 et 14]
   (c) Si $S(n) < S(1)$, alors $n < 1$, ce qui est une contradiction. [Hypothèses 11, 12 et 8-10, qui impliquent qu'un seul des cas de la trichotomie de < est réalisé]
   (d) Si $S(n) = S(1)$, alors $n = 1$. [Hypothèse 2]
   (e) $n = 1$.
   (f) $1 \mid S(1)$. [Hypothèses 4 et 6]
4. (a) Supposons que $S(1) < n$.
   (b) i. Supposons que $n \mid S(1)$.
   ii. Il existe x tel que $nx = S(1)$.

iii. $S(1) \cdot x < nx$. [Hypothèse 15]
iv. $S(1) \cdot x < S(1) \cdot 1$. [Hypothèse 4]
v. $x < 1$, ce qui est une contradiction. [Hypothèses 11 et 15]
(c) Donc si $S(1) < n$, alors $n \nmid S(1)$.

5. Par conséquent les seuls nombres divisant $S(1)$ sont 1 et $S(1)$, et donc $S(1)$ est un nombre premier.

Démonstration du Lemme 3.2, que tout entier naturel $a \neq 1$ admet un nombre premier $p \leq a$ pour diviseur :

1. On procède par induction stricte sur a.
2. Étape de départ : $S(1)$ est un nombre premier par le Lemme 3.1.
3. Étape inductive :
   (a) Supposons que pour tout $y < a$, $y \neq 1$ admet un nombre premier $p \leq y$ pour diviseur.
   (b) a est ou bien un nombre premier, ou bien un nombre composé.
   (c) Si a est un nombre premier, alors la démonstration est terminée.
   (d) Supposons donc que a soit un nombre composé, c'est-à-dire qu'il y ait un certain b tel que $1 < b < a$ et $b \mid a$.
   (e) Par hypothèse d'induction, b admet un nombre premier $p \leq b$ pour diviseur.
   (f) Puisque $p \mid b$ et que $b \mid a$, $p \mid a$. [Hypothèse 5]
   (g) Puisque $p \leq b$ et que $b < a$, $p \leq a$. [Hypothèse 8]

4. Donc pour tout $a \neq 1$, a admet un nombre premier $p \leq a$ pour diviseur. [Hypothèse 17]

Démonstration du Lemme 3.3, que pour tous a, b, si $a \mid b$ et que $a \mid S(b)$, alors $a = 1$:

1. Supposons que $a \mid b$ et que $a \mid S(b)$.
2. Alors il existe x et y tels que $ax = b$ et $ay = S(b)$.
3. $ax = b < S(b) = ay$. [Hypothèse 13]
4. $x < y$. [Hypothèses 6 et 15]
5. (a) Supposons que $a \neq 1$.
   (b) $S(ax) < a \cdot S(x)$. [Hypothèses 1, 3 et 16]
   (c) $S(x) \leq y$. [Hypothèses 1 et 14]
   (d) $a \cdot S(x) \leq ay$. [Hypothèses 3, 6 et 15]
   (e) $S(ax) < ay$. [Hypothèse 8]
   (f) $S(b) < S(b)$, ce qui est une contradiction. [Hypothèse 9]
6. $a = 1$.

Pour justifier la conclusion que cette solution est pure (pour α), il faudrait justifier que chacune des dix-sept hypothèses appartient au sujet de IP (pour α), c'est-à-dire que chaque hypothèse détermine partiellement pour α le contenu de IP tel qu'il est formulé[1]. Si on est prêt à accorder que AP est topique, alors cela devient trivial, puisque chacune de ces hypothèses peut être dérivée de AP. Sinon, il s'agit d'une tâche délicate, car il est difficile de dire de façon absolue si une hypothèse détermine ou non le contenu de la formulation d'un problème, et ce même pour notre sujet « typique » α se penchant sur le problème. En effet, les critères à suivre pour en décider ne sont même pas clairs. Dans ce but, remarquons en particulier que l'Hypothèse 7 est démontrable par induction, c'est-à-dire à partir de l'Hypothèse 17 ; et que l'Hypothèse 16 affirme que la multiplication croît plus vite que la fonction successeur, ce qui semble essentiel à la compréhension contemporaine typique de la relation entre ces deux fonctions.

En refermant cette section, l'objection suivant laquelle la solution euclidienne fait usage de l'addition, ce qui entraîne son impureté topique, peut être contrée de plusieurs manières. Ces réponses posent d'intéressants problèmes à propos de ce qu'est la compréhension ou la supposition « implicite », que nous ne pouvons que soulever dans cet article. Par exemple, nous pouvons demander si en comprenant la « traduction » de la solution euclidienne nous supposons implicitement les propriétés ordinaires de l'addition utilisées dans la version non traduite. Nous pourrions être conduits à le penser si nous pensions qu'il y a quelque chose d'« élémentaire » à propos de ces propriétés ordinaires de l'addition, de sorte qu'il serait possible d'exprimer ces propriétés en semblant superficiellement ne pas mentionner l'addition. La démarche de Robinson en termes de définissabilité indique une façon de rendre plus précise cette idée d'« élémentarité » : si les axiomes découlant de la traduction sont trop complexes, c'est que les axiomes originels sont plus élémentaires. Cela dit, la notion de complexité invoquée ici demanderait à être clarifiée davantage. Une telle voie mériterait d'être poursuivie. Si en effet la traduction non additive de la solution euclidienne s'avère essentiellement additive en nature, alors une stratégie raisonnable pour éviter de conclure que la solution euclidienne est topiquement impure serait de faire valoir que la supposition des propriétés de l'addition est fondamentale pour toute compréhension des entiers naturels.

1. Comme on l'a remarqué plus haut, pour établir complètement la pureté de cette solution, il faudrait vérifier que les inférences qui la composent sont elles aussi topiquement pures pour α. Comme pour la précédente version additive de la démonstration euclidienne, la logique de cette solution est acceptable d'un point de vue intuitionniste.

Une solution impure à IP

Nous allons à présent considérer une solution à IP que nous pensons être impure (pour notre sujet α). Il s'agit d'une solution topologique due à Harry Furstenberg, et qui procède ainsi (cf. [16], p. 353).

1. L'ensemble $\{B_{a,b} \ : \ a,b \in \mathbb{Z},\ b > 0\}$, où $B_{a,b} = \{a + bn \ : \ n \in \mathbb{Z}\}$ est une base d'ouverts pour une topologie sur les entiers. [Ceci est démontré avec des outils de base de la topologie ensembliste et de l'arithmétique[1]]
2. Pour tous $a,b \in \mathbb{Z}$, $b > 0$, $B_{a,b}$ est à la fois ouvert et fermé. [Ceci est démontré avec des outils de base de la topologie ensembliste et de l'arithmétique[2]]
3. Dans une topologie, les unions finies d'ensembles fermés sont des fermés. [Il s'agit d'un résultat de base de la topologie ensembliste ; cf. [27] pour une démonstration]
4. Toute union finie de $B_{a,b}$ est fermée. [Par (2) et (3)]
5. Tout entier m autre que ± 1 admet un nombre premier pour facteur, c'est-à-dire que pour un certain nombre premier p et un certain entier n, $m = pn$. [Par le Théorème fondamental de l'arithmétique]
6. Tout entier autre que ± 1 est contenu dans un certain $B_{0,p}$ pour un nombre premier p. [Par (5) et la définition de $B_{0,p} = \{pn \ : \ n \in \mathbb{Z}\}$]
7. Soit $A = \bigcup_p B_{0,p}$ avec p premier. Alors $A = \mathbb{Z} - \{-1,1\}$. [Par (6)]
8. (a) Supposons qu'il existe seulement un nombre fini de nombres premiers, de sorte que A est obtenu comme l'union d'un nombre fini de $B_{0,p}$.
   (b) Alors A est un fermé de notre topologie. [Par l'étape (4)]

1. Démonstration : on démontre les deux conditions nécessaires à l'existence d'une base d'ouverts pour un espace topologique défini sur les entiers. Tout d'abord, chaque entier x est nécessairement contenu dans un élément de la base $B_{a,b}$. Pour montrer cela, on peut prendre $B_{x,b}$ pour n'importe quelle raison $b > 0$ arbitrairement fixée. Deuxièmement, si un entier x appartient à l'intersection de deux éléments de la base $B_{a,b}$ et $B_{c,d}$, alors il doit appartenir à un troisième élément de la base $B_{e,f}$ tel que $B_{e,f} \subset B_{a,b} \cap B_{c,d}$. Pour montrer cela, on peut prendre $e = x$ et $f = \text{ppcm}[b,d]$ (où $\text{ppcm}[x,y]$ désigne le plus petit commun multiple de x et y), de sorte que

$$B_{e,f} = \{x + \text{ppcm}[b,d] \cdot n : n \in \mathbb{Z}\}.$$

Clairement, $x \in B_{e,f}$. On doit à présent montrer que si $y \in B_{e,f}$, alors $y \in B_{a,b} \cap B_{c,d}$. On a que $y = x + \text{ppcm}[b,d] \cdot n$ pour quelque n. Dès lors, $y = x + bn'$ pour quelque n', et $y = x + dn''$ pour quelque n'' ; par suite, $y \in B_{x,b} \cap B_{x,d}$. Puisque par hypothèse $x \in B_{a,b} \cap B_{c,d}$, et que n'importe quel membre d'une progression arithmétique peut être pris comme son terme initial, on a également que $B_{a,b} = B_{x,b}$ et que $B_{c,d} = B_{x,d}$. Par conséquent, $y \in B_{a,b} \cap B_{c,d}$.

2. Démonstration : on remarque que

$$B_{a,b} = \mathbb{Z} - \bigcup_{1 \le i \le b-1} B_{a+i,b}$$

c'est-à-dire le complément de l'union des progressions arithmétiques autres que $B_{a,b}$ ayant la même raison b que $B_{a,b}$. Puisque l'union d'ouverts $B_{a+i,b}$ est un ouvert (par définition d'un espace topologique), $B_{a,b}$ est le complément d'un ouvert, et par conséquent un fermé.

(c) Alors $\{-1,1\}$, en tant que complément d'un ensemble fermé, est un ouvert. [Par définition d'un ensemble fermé]
(d) Les ouverts de base $B_{a,b}$ sont tous infinis. [Du fait de l'infinité de $\mathbb{Z}$]
(e) Tout ensemble ouvert contient un ouvert de base. [Par définition d'une base d'ouverts]
(f) Cela contredit la finitude de $\{-1,1\}$. [Par (8c), (8d), (8e)]

9. Par conséquent il existe un nombre infini de nombres premiers, et donc, pour tout a, il existe un nombre premier $b > a$.

Selon nous, la solution de Furstenberg à IP est topiquement impure. La première étape de sa démonstration établit que certaines progressions arithmétiques forment une base d'ouverts pour un espace topologique. Accepter ce dernier point implique plusieurs suppositions ensemblistes. Cela demande également de supposer les définitions d'un espace topologique et d'une base d'ouverts. La deuxième étape ajoute encore d'autres suppositions : celles de la définition des ensembles ouverts et des ensembles fermés relativement à une topologie. Comme nous l'avons vu, retirer n'importe laquelle de ces suppositions ne demanderait pas en soi une modification correspondante de notre compréhension de IP. Autrement dit, ces suppositions n'appartiennent pas au sujet de IP. En conséquence, eu égard à notre conception de la pureté topique, la solution de Furstenberg à IP est topiquement impure.

On pourrait objecter que certaines suppositions ensemblistes *sont* bien nécessaires pour la compréhension de IP. En rétorquant, par exemple, que la définition « correcte » d'un entier naturel est ensembliste, comme elle l'est dans le cadre des axiomes du second ordre de Dedekind-Peano, ou bien dans l'œuvre de Frege ou Russell. Cela montre clairement à quel point il est difficile de dire de façon absolue ce qui appartient au sujet d'un certain problème, car une réponse complète à cette objection devrait consister en un argument contre cette compréhension des nombres, ce qui serait en soi un exploit philosophique. Plutôt que de proposer une telle réponse, nous observerons que c'est une question ouverte que celle de savoir si ce que définissent les définitions ensemblistes des entiers naturels est la même chose que ce que définissent les définitions purement du premier ordre. Il est compatible avec ce que nous avons admis jusqu'ici qu'il existe (au moins) deux problèmes différents à discuter, l'un comportant des suppositions ensemblistes dans son sujet, et l'autre aucune[1]. Dans ce cas, la question de la pureté topique de la démonstration de Furstenberg, en ce qui concerne ses suppositions ensemblistes, revient à celle de savoir lequel de ces problèmes est le problème IP que l'on est en train d'examiner.

Une autre objection du même type serait que si les suppositions ensemblistes peuvent ne pas être nécessaires à la compréhension des entiers naturels, elles sont nécessaires à la compréhension des *fonctions* arithmétiques

1. Nous disons « au moins », car on peut imaginer que le sujet de IP puisse ne contenir aucune des suppositions requises par la démonstration de Furstenberg, tout en contenant d'autres suppositions ensemblistes.

auxquelles fait appel IP. En réponse, nous remarquerons que des fonctions arithmétiques peuvent être comprises dans une perspective algorithmique, sans faire appel à la théorie des ensembles. Il n'y a pour nous aucune raison de penser qu'une compréhension ensembliste des fonctions ait une quelconque préséance, en particulier dans le cas de IP, où les fonctions sont employées uniquement pour des calculs.

Dans une correspondance, Neil Tennant a soulevé une autre objection encore du même type. On peut remarquer que la topologie employée dans la démonstration de Furstenberg, lorsqu'elle est formulée en théorie des ensembles, est assez faible, c'est-à-dire qu'elle peut être formulée dans un fragment de la théorie des ensembles qui utilise seulement des opérations booléennes sur des ensembles « simples » d'entiers naturels. Sur ce point, D. Cass and G. Wildenberg ont montré que la démonstration de Furstenberg peut être reformulée en termes de fonctions périodiques sur les entiers, « en évitant le langage de la topologie » (cf. [10], p. 203). En réponse, nous observerons que le problème, à nouveau, est de savoir si des suppositions ensemblistes, *quelles qu'elles soient*, sont suscitées par la compréhension de problèmes arithmétiques. Or que ces suppositions soient ou non « faibles » n'est pertinent que dans la mesure où cela concerne la question de savoir si ces suppositions appartiennent au sujet de IP, et pour nous il n'y a aucune raison de le penser.

Une autre objection du même type serait que pour avoir une pleine compréhension de IP, il faudrait faire intervenir non seulement des suppositions ensemblistes mais également des suppositions topologiques du type de celles auxquelles fait appel la démonstration de Furstenberg. Ainsi, la démonstration de Furstenberg ne serait donc pas à considérer comme impure simplement parce qu'elle fait appel à des principes topologiques. Dans une correspondance, Colin McLarty a clairement exprimé cette position.

En défendant cette position, McLarty s'aligne sur la tradition bourbakiste de recherche en arithmétique, tradition dans laquelle s'inscrit également le travail de Furstenberg. McLarty identifie la solution de Furstenberg comme bourbakiste en ce qu'elle commence par introduire une topologie sur les entiers avec pour base d'ouverts $B_{a,b} = \{a + bn \ : \ n \in \mathbb{Z}\}$, pour $a, b \in \mathbb{Z}, b > 0$. Conformément à cette tradition, remarque McLarty, le choix par Furstenberg de cette base d'ouverts n'est sans doute pas un hasard. En effet, prendre les progressions arithmétiques pour ouverts de base engendre la topologie connue sous le nom de « topologie profinie » sur les entiers, ce qui correspond à un type bien connu d'espace topologique présentant un grand intérêt dans toutes les mathématiques[1].

McLarty pense deviner que Furstenberg a développé sa démonstration à partir des travaux alors en cours de Claude Chevalley en théorie du corps de

1. Pour une définition précise de la topologie profinie, ainsi qu'une discussion de ses origines dans les œuvres de Kronecker, Dedekind et Hensel, cf. [31], p. 162-164 ; voir également [17].

classes, travaux alors tenus pour une recherche de pointe en *arithmétique* en dépit du rôle central qu'y joue la topologie. Dans [7], Chevalley considère lui-même avoir progressé en réalisant un idéal puriste ; comme il le remarque dans les premières lignes de son article, « La théorie du corps de classes se présente un peu plus simplement aujourd'hui qu'il y a quelques années, notamment du fait de l'élimination des "moyens transcendants" (cf. [7], p. 394). » Les « moyens transcendants » en question sont les fonctions ζ ; comme Olga Taussky-Todd le remarque dans sa recension de l'article, l'un des tours de force de l'article fut « d'exclure les méthodes analytiques [...] ; la théorie des fonctions ζ, qui depuis si longtemps semblait indispensable, se trouve ici laissée de côté[1]. » Ainsi, Chevalley chercha et parvint à éliminer l'analyse complexe de ce qu'il considérait être l'arithmétique, même s'il avait une conception large de ce qui tombe sous l'arithmétique ; comme le dit Taussky-Todd, « les méthodes topologiques jouent un rôle important dans sa présentation nouvelle de la théorie du corps de classes. »

De ce point de vue, la démonstration de Furstenberg est une façon d'illustrer, à l'attention des non-spécialistes, ces méthodes sophistiquées, et, en fournissant une solution à un problème arithmétique classique, de faire la preuve qu'elles sont de nature arithmétique. Elles sont topologiques, mais seulement en un sens axiomatique, qui relève de la théorie des treillis, plutôt que typiquement topologiques au sens de la topologie de Poincaré-Lefschetz, conformément à laquelle des continus tels que la ligne réelle ou complexe sont d'un usage essentiel. Chevalley considérait d'ailleurs cette dernière topologie comme non arithmétique.

Une telle approche apporta de nouveaux résultats de pointe en arithmétique, mais la solution de Furstenberg à IP montre que cette approche apporta également de nouvelles solutions à des problèmes arithmétiques élémentaires. Chevalley et les Bourbakistes reconnurent dans cet apport un changement important dans la pratique arithmétique ; tel que Bourbaki décrivait ce travail en 1948, c'est un exemple de cette « chose plus étonnante encore, la topologie envahit ce qui était jusqu'alors le règne du *discret*, du discontinu par excellence, l'ensemble des nombres entiers » (cf. [3], p. 43). Néanmoins, leur position mûrement réfléchie semble avoir été que la fusion

1. Cf. *Math. Reviews* MR0002357 (2, 38c). La fonction zeta de Riemann $\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}$ est une fonction ζ bien connue, employée intensivement en théorie analytique des nombres (cf. [20]). La notion générale des fonctions ζ, connues aussi sous le nom de *L*-fonctions, provient des travaux d'Euler et de Dirichlet, et a été employée intensivement en théorie analytique et algébrique des nombres (cf. [26], [5]). H. Weber a employé des fonctions ζ dans la théorie du corps de classes (cf. [33]) ; c'est cet emploi de l'analyse que les travaux de Chevalley ont essayé de purifier. Pour une discussion historique des fonctions ζ dans le contexte de l'œuvre de Chevalley, cf. [9] ; pour une discussion technique des fonctions ζ dans ce même contexte, cf. [25], Chapter 11.

de la topologie et de l'arithmétique permet une compréhension plus profonde des problèmes arithmétiques. Comme le dit Bourbaki :

> Là où l'observateur superficiel ne voit que deux ou plusieurs théories en apparence très distinctes, se prêtant, par l'entremise d'un mathématicien de génie, un « secours inattendu » [[4], p. 446], la méthode axiomatique enseigne à rechercher les raisons profondes de cette découverte, à trouver les idées communes enfouies sous l'appareil extérieur des détails propres à chacune des théories considérées, à dégager ces idées et à les mettre en lumière. (cf. [3], § 2)

Il ajoute :

> [L]a méthode axiomatique a montré que les « vérités » dont on voulait faire le pivot des mathématiques n'étaient que des aspects très spéciaux de conceptions générales qui n'y limitaient nullement leur portée. Si bien qu'en fin de compte, cette intime fusion dont on nous faisait admirer l'harmonieuse nécessité, n'apparaît plus que comme un contact fortuit de deux disciplines dont les liens sont beaucoup plus cachés qu'on ne pouvait le supposer *a priori*. (cf. [3], § 7)

Dans le cas particulier de IP et de la fusion de la topologie et de l'arithmétique, la conception de Bourbaki semble être que les travaux de Furstenberg révèlent des éléments du contenu de IP jusque-là inconnus, et en particulier des éléments ensemblistes et topologiques. Au fond du fond, dans la conception de Bourbaki, IP porte sur des ensembles, et ainsi, plus particulièrement, sur des entités topologiques.

Telle est donc la conception que McLarty propose comme objection à notre détermination de la solution de Furstenberg à IP comme topiquement impure. Il défend l'idée que les éléments topologiques de la solution de Furstenberg appartiennent au sujet de IP, et par suite que la solution de Furstenberg ne devrait pas être tenue pour topiquement impure du fait de son utilisation de tels éléments.

Nous rejetons pour notre part cette idée, comme nous l'avons déjà exprimé. Si IP concernait réellement les éléments topologiques sur lesquels est fondée la solution de Furstenberg, alors il n'y aurait aucune raison de penser que ce problème pourrait survivre au retrait de ces parties de la démonstration de Furstenberg qui se fondent sur ces éléments. Pourtant, il existe bien de telles raisons : les ressources conceptuelles qui sous-tendent notre intelligence de IP n'incluent pas ces éléments topologiques. Lorsque nous retirons la supposition par exemple de la définition d'un espace topologique, notre compréhension de IP demeure intacte. Nous nions par conséquent que ces éléments topologiques appartiennent au sujet de IP, et nions ainsi que la solution de Furstenberg soit topiquement pure.

Néanmoins, l'argument bourbakiste de McLarty est important. Les travaux comme ceux de Chevalley ou de Furstenberg montrent que IP n'est pas un problème d'importance simplement pour l'arithmétique, mais tout autant pour la topologie. Ils montrent qu'il existe des liens « profonds » entre l'arithmétique et la topologie, des liens qui étaient inconnus des chercheurs précédents. Ils mettent en lumière la fusion de ce qui était autrefois pensé comme formant deux domaines séparés. Une discussion plus complète de ce type de registre approfondi dépasserait les limites de cet article. Mais il semble clair que la profondeur d'une solution est différente de la stabilité d'une solution. Une solution profonde à un problème peut en effet inclure des suppositions dont le retrait ne changerait pas notre intelligence du problème, tandis que c'est impossible dans le cas d'une solution stable. Une solution peut se fonder sur des ressources conceptuelles qui relient notre compréhension d'un problème avec un autre domaine, sans que ce lien soit déterminant quant à l'identité du problème. L'argument de McLarty est que les solutions à des problèmes qui se fondent sur des suppositions relatives à des domaines reliés « en profondeur » au sujet de l'un de ces problèmes sont d'une importance épistémique particulière, même si ces suppositions ne déterminent pas l'identité du problème. Leur importance semble double : premièrement, elles améliorent notre connaissance des liens existant entre des domaines en montrant comment l'un d'eux peut être employé pour résoudre des problèmes dans un autre ; et, deuxièmement, par cette connaissance accrue de tels liens, elles gratifient le chercheur d'une « économie de pensée considérable » en lui fournissant des résultats applicables à de multiples domaines de recherche plutôt qu'à un seul uniquement (cf. [3], § 5). De telles solutions aident à combattre la scission des mathématiques en disciplines autonomes n'ayant ni les mêmes méthodes ni les mêmes buts (cf. [3], § 1). Ainsi McLarty, dans le sillage de Bourbaki, tente-t-il d'expliquer les vertus épistémiques d'une solution *topiquement impure*.

Si ces dernières sont bien les vertus d'une démonstration topiquement impure, cela donne alors une idée de la raison théorique pour laquelle les mathématiciens recherchent des solutions multiples à un même problème, comme l'histoire en a souvent donné des exemples[1]. Il existe bien de multiples et diverses vertus épistémiques à trouver dans la résolution d'un problème, et certaines d'entre elles ne peuvent être satisfaites par une seule solution (car une solution à un problème ne peut être à la fois topiquement pure et topiquement impure). C'est pourquoi, pour que la recherche à propos d'un problème donne lieu à une connaissance ayant chacune de ces différentes vertus, il convient de rechercher de multiples solutions au même problème.

Dernières remarques

Le cas de l'infinité des nombres premiers est intéressant en ce qu'il permet de souligner plusieurs enjeux cruciaux pour parvenir à une conception

1. Voir [14] pour une longue discussion de la question de savoir pourquoi les mathématiciens redémontrent des théorèmes.

plus claire de la pureté topique. Il reste à étudier plus systématiquement la façon dont les sujets de problèmes se trouvent déterminés. Des études de cas telles que celle présentée ici sont des préalables nécessaires et importants à ce type de recherche. Ce cas particulier permet de souligner la difficulté qu'il y a à déterminer exactement ce qui appartient au sujet d'un problème même assez élémentaire. Tandis que l'addition n'apparaît pas explicitement dans la formulation du problème, il est très naturel de penser que l'addition appartient au sujet de tout problème arithmétique, du fait de la structure additive attachée à ce que sont les entiers naturels. La discussion de la solution euclidienne qui a été menée ici a cherché à montrer comment soutenir sa pureté topique sans simplement admettre cette idée d'une nature additive intrinsèque des entiers naturels. La discussion de la solution topologique de Furstenberg illustre deux notions rivales de ce que c'est que comprendre un problème et pouvoir déterminer par là un sujet, qui correspondent à ce qu'on peut appeler une compréhension « élémentaire » et une compréhension « profonde ». Selon la seconde, notion bourbakiste suggérée par McLarty, la solution de Furstenberg remplit les conditions pour être topiquement pure. Même si cette notion de compréhension profonde est importante et mérite une analyse plus détaillée, la position défendue ici est que cette notion ne doit pas se substituer au sens « élémentaire » de ce qu'est la compréhension dans la détermination d'un sujet. C'est pourquoi McLarty et Bourbaki indiquent clairement qu'ils considèrent la compréhension profonde comme l'expression de liens entre le domaine dont relève le problème étudié et d'autres domaines, plutôt que comme l'expression du simple contenu du problème étudié. Or des suppositions relevant de ce second type sont celles qui sont pertinentes lorsqu'on vise à la pureté topique, puisqu'il vaut mieux penser à une solution topiquement pure à un problème comme étant une solution à précisément ce problème, et non à un autre – et ce même s'il existe de bonnes raisons de rechercher la solution de cet autre problème, comme la conception de McLarty/Bourbaki le défend. Ainsi cette étude de cas faitelle apparaître un éventail de problèmes qui sont cruciaux pour progresser davantage dans notre compréhension philosophique de ce qu'est la pureté.

Andrew Arana

aarana@ksu.edu

(Traduction Brice Halimi)

Références

[1] Andrew Arana. Logical and semantic purity. *Protosociology*, 25:36-48, 2008. Repris dans *Philosophy of Mathematics: Set Theory, Measuring Theories, and Nominalism*, Gerhard Preyer et Georg Peter (dir.), Ontos, 2008.

[2] Andrew Arana. On formally measuring and eliminating extraneous notions in proofs. *Philosophia Mathematica*, 17:208-219, 2009.
[3] Nicholas Bourbaki. L'architecture des mathématiques. *In* François Le Lionnais, dir., *Les grands courants de la pensée mathématique*. Éditions des Cahiers du Sud, 1948.
[4] Léon Brunschvicg. *Les étapes de la philosophie mathématique*. Alcan, Paris, 1912.
[5] Kevin Buzzard. L-functions. *In* [17]. 2008.
[6] Patrick Cegielski. La théorie élémentaire de la divisibilité est finiment axiomatisable. *C. R. Acad. Sci. Paris Sér. I Math.*, 299(9):367-369, 1984.
[7] Claude Chevalley. La théorie du corps de classes. *Annals of Mathematics (2)*, 41:394-418, 1940.
[8] Patrick Cegielski, Yuri Matijasevich et Denis Richard. Definability and decidability issues in extensions of the integers with the divisibility predicate. *Journal of Symbolic Logic*, 61(2):515-540, juin 1996.
[9] J.W. Cogdell. On Artin L-functions. http://www.math.ohio-state.edu/~cogdell/artin-www.pdf, 2007.
[10] Daniel Cass et Gerald Wildenberg. A novel proof of the infinitude of primes, revisited. *Mathematics Magazine*, 76(3):203, juin 2003.
[11] Paola D'Aquino. Local behaviour of the Chebyshev theorem in models of $I\Delta_0$. *Journal of Symbolic Logic*, 57(1):12-27, 1992.
[12] Paola D'Aquino. Weak fragments of Peano arithmetic. *In The Notre Dame Lectures*, volume 18 de *Lecture Notes In Logic*, p. 149-185. Association for Symbolic Logic, Urbana, IL, 2005.
[13] Michael Detlefsen et Andrew Arana. Purity of methods. Preprint, 2010.
[14] John W. Dawson, Jr. Why do mathematicians re-prove theorems? *Philosophia Mathematica*, 14(3):269-286, 2006.
[15] Herbert B. Enderton. *A mathematical introduction to logic*. Harcourt/Academic Press, Burlington, MA, seconde édition, 2001.
[16] Harry Furstenberg. On the infinitude of primes. *American Mathematical Monthly*, 62(5):353, mai 1955.
[17] Timothy Gowers, June Barrow-Green et Imre Leader, dir. *The Princeton companion to mathematics*. Princeton University Press, Princeton, NJ, 2008.
[18] Kurt Gödel. Über formal unentscheidhare Sätze der *Principia Mathematica* und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173-198, 1931. Repris et traduit dans *Collected Works* Volume 1, Solomon Feferman *et al.* (dir.), Oxford University Press, 1986.
[19] Fernando Q. Gouvêa. Local and Global in Number Theory. *In* [17]. 2008.
[20] Andrew Granville. Analytic Number Theory. *In* [17]. 2008.
[21] Michael Hallett et Ulrich Majer, dir. *David Hilbert's lectures on the foundations of geometry, 1891-1902*. Springer-Verlag, Berlin, 2004.
[22] Petr Hájek et Pavel Pudlák. *Metamathematics of first-order arithmetic*. Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1998. Deuxième impression.
[23] G. H. Hardy et E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, New York, 5e édition, 1979.
[24] A. E. Ingham. *The distribution of prime numbers*. Cambridge University Press, 1932.

[25] Kenneth Ireland et Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, deuxième édition, 1990.
[26] Barry Mazur. Algebraic Numbers. *In* [17]. 2008.
[27] James R. Munkres. *Topology: a first course*. Prentice-Hall Inc., Englewood Cliffs, N.J., 1975.
[28] Rohit Parikh. Existence and feasibility in arithmetic. *Journal of Symbolic Logic*, 36:494-508, 1971.
[29] J. B. Paris, A. J. Wilkie et A. R. Woods. Probability of the pigeonhole principle and the existence of infinitely many primes. *Journal of Symbolic Logic*, 53(4):1235-1244, 1988.
[30] Julia Robinson. Definability and decision problems in arithmetic. *Journal of Symbolic Logic*, 14:98-114, 1949.
[31] Joachim Schwermer. Minkowski, Hensel et Hasse: On the Beginnings of the Local-Global Principle. *In* Jeremy Gray and Karen Parshall, dir., *Episodes in the History of Modern Algebra (1800-1950)*. American Mathematical Society, Providence, 2007.
[32] William W. Tait. Finitism. *The Journal of Philosophy*, 78(9):524-546, 1981.
[33] Heinrich Weber. *Lehrbuch der Algebra*, volume III. F. Vieweg und Sohn, Braunschweig, deuxième édition, 1908.
[34] Alan Woods. *Some problems in logic and number theory and their connections*. Thèse de doctorat, University of Manchester, 1981.