Thierry DELORT

9 rue MALTE BRUN

75020 PARIS

France 2/6

21 Avril 2024

Titre :LE PROBLEME P=NP (version 4)

RESUME :

Dans cet article, nous allons résoudre le problème P=NP pour un cas particulier de problèmes appelés *problèmes de détermination numérique basiques*. Nous allons proposer 3 Axiomes fondamentaux permettant de résoudre le problème considéré pour les problèmes de détermination numérique basiques, ces Axiomes pouvant aussi être considérés comme des assertions de logique pure évidentes intuitivement et jamais contredites permettant de comprendre la solution du problème considéré. On verra que ces Axiomes entraînent l'indécidabilité du problème P=NP pour les problèmes de détermination numérique basiques. On montrera cependant qu'on peut donner une justification théorique (qui n'est pas une démonstration classique) de P≠NP. Nous étudierons ensuite un 2nd problème, appelé problème « $P_N$=$DP_N$ », analogue au problème P=NP mais ayant une importance fondamentale en mathématique.

## I)INTRODUCTION

Dans cet article nous allons donner une solution au problème P=NP. Pour commencer nous allons définir une classe de problèmes appelés *problèmes de détermination numérique basique*. Cette définition est importante car c'est une définition très générale de problèmes potentiellement de classe P ou NP, et aussi car elle donne une base concrète pour justifier intuitivement les Axiomes que nous allons introduire, et aussi pour tester leur validité. On sait que la conjecture P=NP (tout problème de classe P est de classe NP et réciproquement) n'a jamais été démontrée ni sa négation. Dans cet article nous allons proposer 3 assertions de logique pure intuitivement évidentes et jamais contredites, appelées pour cette raison « Axiomes », permettant de donner une solution au problème P=NP. On sait en effet que dans une théorie mathématique on peut introduire des Axiomes, ceux-ci devant être évidents ou avoir une justification intuitive évidente et jamais contredits. De plus, le fait qu'on n'ait jamais obtenu de résultats fondamentaux sur le problème P=NP en utilisant les théories mathématiques classiques conduit à penser que la solution du problème P=NP nécessite l'introduction de nouveaux Axiomes, et qu'elle ne peut pas être obtenue en utilisant seulement les théories mathématiques classiques.

La théorie présentée dans cet article n'est pas purement mathématique. C'est une théorie de logique mathématique. Il est cependant quasi-certain que la conclusion de cette théorie ne pourra pas être obtenue par une théorie purement mathématique. On peut aussi considérer cette théorie comme purement logique car elle n'introduit pas d'équations nouvelles. Elle est cependant en accord avec toutes les équations relatives au problème P=NP connues à ce jour, de plus ses implications concernent les équations du problème P=NP et enfin seules des équations relatives au problème P=NP pourraient éventuellement la contredire, elle et ses Axiomes.

Dans cet article, l'approche du problème P=NP est complètement nouvelle et n'utilise pas d'autres articles publiés sur le sujet. Néanmoins, sa conclusion est en accord avec tous les articles scientifiques sur ce sujet. Nous allons justifier qu'on ne peut démontrer ni P=NP ni P≠NP pour les problèmes de détermination numérique basiques.

Cependant on montrera qu'il existe une justification théorique (Qui n'est pas une démonstration classique) de P≠NP.

Nous étudierons enfin un $2^{nd}$ problème, appelé problème « $P_N=DP_N$ », analogue au problème P=NP et avec une résolution analogue, mais ayant une importance fondamentale en mathématique.

## II)SOLUTION DU PROBLEME P=NP

### A)PROBLEMES DE DETERMINATION NUMERIQUE BASIQUES (DEFINITION).

Par définition, *un problème de détermination numérique basique* contient les données suivantes :

Pour tout naturel n différent de 0:

-Un ensemble fini A(n) défini en fonction de n.

-Une fonction k(n) appartenant à $F(\mathbf{N},\mathbf{N})$ croissante, pouvant être constante avec un polynôme $P_k$ de $F(\mathbf{N},\mathbf{N})$ tel que pour tout naturel n $k(n)<P_k(n)$.

-Dans certains cas, r ensembles finis $B_1(n),..,B_r(n)$ (r naturel donné), avec pour i dans {1,..,r} $B_i(n)$ défini par une proposition du type $P_{Bi}(B_i(n),A(n),n)$. (Certains $B_i(n)$ peuvent être définis simultanément par une proposition du type $P_{Bi,..Bis}(B_{i1}(n),\ldots,B_{is}(n),A(n),n)$. Pour chaque n il peut y avoir plusieurs $B_i(n)$, mais en nombre fini.)

-Une proposition $P(a_1,\ldots,a_{k(n)},A(n),n,k(n),B_1(n)..,B_r(n))$ définie pour toute séquence $(a_1,..,a_{k(n)})$ d'éléments de A(n).

On définit une *fonction numérique explicite* comme une fonction de $F(A^p,B)$, avec p naturel >0, A,B=**N** ou **Z**, (On pourra remplacer $A^p$ par l'ensemble $S_{FA}$ dont les éléments sont les éléments de A et toutes les séquences finies d'éléments de A) définie explicitement par les opérations dans **N** ou **Z** (addition, multiplication, puissance..) ou utilisant Int(f(n)), f fonction réelle croissante tendant vers l'infini avec n, définie explicitement en fonction des fonctions réelles classiques (Log,exp..)  et des opérations classiques dans **R** (Et des symboles représentant des réels « 1/3 », « 3/7 »…) ou $r_{DE}$, $r_{DE}$ définie pour tout couples d'entiers (p,q) avec $q\neq0$ par $r_{DE}(p,q)$ est le reste de la division Euclidienne de p par q, ou un produit ou une somme des éléments d'une séquence finie d'entiers (Notées « Π » et « Σ »), ou la fonction « valeur absolue » (D'entiers), ou des symboles représentant des entiers « 0 »,« 1 », « 2 »… et les termes $a_1,\ldots,a_p$ d' un élément de l'ensemble de départ.

Par exemple avec l'ensemble de départ $S_{FA}$ :

$f(a_1,\ldots,a_p)=\Pi(a_1,\ldots,a_p)$, représenté par $f(a_1,\ldots,a_p)=\Pi_{i=1,..,p}a_i$.

Ensemble de départ **N** :

$f(n)=\Pi(1,..,n)$ représenté par $f(n)=\Pi_{i=1,..,n}i$ pour n>0 et f(0)=0.

$f(n)=n^3+n^2+1$.

Ensemble de départ $\mathbf{N}^2$ :

$f(a_1,p)=a_1^p$ sauf si $(a_1,p)=(0,0)$ où $f(0,0)=0$.

On pourra donc identifier une fonction numérique explicite avec un sous-ensemble infini de $A^p\times B$. Dans le cas où $A^p=\mathbf{N}$, f étant une fonction numérique explicite appartenant à $F(\mathbf{N},\mathbf{N})$, f sera identifiée à la séquence infinie (Qui est aussi un ensemble) $((i,f(i)))_{\mathbf{N}}$.

On admettra qu'on pourra toujours trouver un problème équivalent où les éléments de A(n) et des $B_i(n)$ sont des entiers ou des familles ou des séquences finies définies à l'aide d'entiers et de familles ou séquences finies. On supposera que dans ce problème, $P(a_1,\ldots,a_{k(n)},A(n),n,k(n),B_1(n)..,B_r(n))$ de même que les propositions définissant A(n), k(n) et les $B_i(n)$ ne définissent et n'utilisent que des ensembles et des séquences dont les éléments ou les termes sont définis à partir d'entiers et de familles ou de séquences finies et que tous les ensembles infinis qu'elle utilise sont ou bien du type $A^p$ ou $S_{FA}$ (A=**N** ou **Z**) ou bien des fonctions numériques explicites. On dira que les éléments des ensembles ou les termes des séquences utilisés sont des *éléments numériques*, qui peuvent être définis par les 2 règles suivantes :

a)Tout entier est un élément numérique.

b)Toute famille ou séquence finie dont les éléments ou les termes sont des éléments numériques est un élément numérique.

(Ces propositions seront analogues à des propositions, appelées *propositions numériques*, définies dans la section E. On pourra ajouter des conditions pour qu'elles soient des propositions numériques.)

Il y aura une exception pour définir des fonctions numériques explicites car dans ce cas elles pourront utiliser des symboles du type $F(\mathbf{N}^p,\mathbf{N})$. On peut cependant éviter cette exception remplaçant « f est élément de $F(\mathbf{N}^p,\mathbf{N})$ » par « f est une application de $\mathbf{N}^p$ dans $\mathbf{N}$ ».

On dira alors que le problème est un problème de détermination basique *numérique*.

Un problème de détermination numérique mathématique ne devra utiliser ni algorithme, ni système formel ni concept mathématique logique équivalent. On prend cette condition pour éviter les singularités logiques et parce que la quasi-totalité des problèmes classiques intéressants concernés par le problème P=NP vérifient cette condition.

$P_B$ étant un problème de détermination numérique basique, on définira $P_B(n)$ comme la partie de $P_B$ relative à n (Avec A(n), $B_i(n)$, k(n)…). On dira que $P_B(n)$ est l'*ordre* n de $P_B$.

Par définition résoudre ce problème signifie que pour chaque n on détermine si elle existe une séquence de k(n) éléments de A(n) $(a_1,..,a_{k(n)})$ vérifiant $P(a_1,\ldots,a_{k(n)},A(n),n,k(n),B_1(n),..,B_r(n))$ (On dira alors $(a_1,\ldots,a_{k(n)})$ est une solution de $P_B(n)$).

Nous étendrons la définition précédente au cas où k(n) doit être déterminé avec $a_1,..,a_{k(n)},$ avec la condition $k(n)<P_k(n)$, $P_k$ polynôme donné de $F(\mathbf{N},\mathbf{N})$. Ce qui suit demeure valide si on remplace la classe de problèmes considérés par une classe beaucoup plus large.

D'après la définition de la classe P, $P_B$ étant un problème de détermination numérique basique on dira que $P_B$ est de la classe P s'il existe une séquence d'algorithmes $(Alg_{DPB}(n))$, *polynomiale* (C'est-à-dire qu'il existe un Polynôme $Pol_{DPB}$ tel que pour tout n le temps d'exécution de $Alg_{DPB}(n)$ est inférieure à $Pol_{DPB}(n)$) et *déterministe* c'est-à-dire que pour tout n $Alg_{DPB}(n)$ détermine si elle existe une séquence $(a_1,.,a_{k(n)})$ solution de $P_B(n)$. $Alg_{DPB}(n)$ peut naturellement utiliser les données du problème $P_B$, A(n), $B_i(n)$..On dira que $(Alg_{DPB}(n))$ est *une séquence polynomiale déterministe d'algorithmes résolvant* $P_B$.

D'après la définition de la classe NP, $P_B$ étant un problème de détermination numérique basique, on dira que $P_B$ est de classe NP s'il est de classe P ou s'il existe une séquence polynomiale d'algorithme $((Alg_{NDPB}(n))$ non déterministe c'est-à-dire que pour toute séquence $(a_1,..,a_{k(n)})$ de A(n), $Alg_{NDPB}(n)$ permet de vérifier si $(a_1,..,a_{k(n)})$ (et éventuellement k(n)) sont solution du problème $P_B(n)$. On dira que $(Alg_{NDPB}(n))$ est une *séquence polynomiale non-déterministe d'algorithmes vérifiant* $P_B$.

Ce qui suit demeure valide si dans les définitions précédentes on n'a pas P inclus dans NP ou que $Alg_{DPB}(n)$ permet d'obtenir toutes les solutions de $P_B(n)$.

Il existe des problèmes de classe P ou de classe NP qui ne sont pas des problèmes de détermination numérique basiques mais ces derniers constituent l'essentiel des problèmes classiques intéressants de type P ou NP. De plus ce qui suit demeure généralisable pour des classes beaucoup plus larges que la classe des problèmes de détermination numérique basiques.

Par exemple on peut considérer le problème de détermination numérique classique consistant à chercher 2 diviseurs distincts $a_1,a_2$ d'un naturel n, s'ils existent.

On a alors $A(n)=\{1,..,n\}$, $k(n)=2$, et $P(a_1,a_2,n)$ : « $a_1$ et $a_2$ sont 2 naturels distincts et différents de n et $a_1\times a_2=n$ ».

Concernant l'exemple de l'Institut de mathématiques Clay [(1)], on considère 400 étudiants ,on a 100 chambres et une liste $L_P$ de 100 paires d'étudiants et on cherche une liste $L_{RN}$ de 100 étudiants avec la condition que cette liste ne contient aucune paire d'étudiants appartenant à $L_P$. Ce problème est équivalent au problème de détermination numérique basique suivant, avec n=400 :

-A(n) est un ensemble contenant les noms de n étudiants (Représentés par $e_1,..,e_n$). Dans l'exemple n=400.

-k(n)=Int(n/4) (k(400)=100 dans l'exemple).

-$B_1(n)$ est défini par $P_{B1}(B_1(n),A(n),n)$ : « $Card(B_1(n))=Int(n/4)$ et les éléments de $B_1(n)$ sont des paires d'éléments de A(n) ». ($B_1(400)$ est la liste $L_P$ dans l'exemple)

- $P(a_1,..,a_{k(n)},k(n),B_1(n))$ : « Pour tous i,j distincts éléments de $\{1,..,k(n)\}$, $\{a_i,a_j\}$ n'est pas élément de $B_1(n)$ et $a_i\neq a_j$». ($a_1,..,a_{k(400)}$ sont les éléments de $L_{RN}$ dans l'exemple).

( On peut se ramener à un problème numérique en remplaçant $e_i$ par le couple (1,i).

On rappelle que les 2 exemples de problème précédents sont de classe NP.

P=NP, pour les problèmes de détermination numérique basiques, signifie que tout problème de détermination numérique basique de classe P est de classe NP et réciproquement. Nous allons montrer que ce problème est *indécidable*, c'est-à-dire :

-Si P=NP, il est impossible de le démontrer.

-Si P≠NP, il est impossible de le démontrer.

## B)IMPOSSIBILITE DE DEMONTRER P≠NP POUR LES PROBLEMES DE DETERMINATION NUMERIQUE BASIQUES.

Dans cette section on considèrera seulement des problèmes de détermination numérique basique. Pour prouver P≠NP, on doit montrer ou bien que P n'est pas inclus dans NP ou bien que NP n'est pas inclus dans P. D'après la définition de NP, P est inclus dans NP, on doit donc démontrer NP n'est pas inclus dans P, et donc on doit déterminer un problème de détermination numérique basique qui est de classe NP mais pas de classe P.

Or on admet l'Axiome suivant :

Axiome 1 :

Il est impossible de prouver qu'un problème de détermination numérique basique n'admet pas de séquence polynomiale déterministe d'algorithmes le résolvant. (C'est-à-dire qu'il n'est pas de classe P).

Cet Axiome 1, non démontrable formellement comme tout axiome, admet la justification intuitive suivante :

Par hypothèse, $P_B$ étant un problème de détermination numérique basique, Card(A(n)) et Card($B_i$(n)) seront définis par des fonctions numériques explicites et on a vu que $P(a_1,..,a_{k(n)},A(n), n, k(n),B_1(n),..,B_{r(n)})$ pourra aussi en employer. $P_B$ exprimera donc des propriétés de naturels (Incluant celles de Card(A(n)), si on a défini pour tout naturel n A(n) ou(et) de fonctions numériques explicites). A cause de cela une séquence d'algorithmes solution de $P_B$ pourra être définie de façon très complexe, utilisant notamment des fonctions numériques très complexes. Intuitivement on comprend que les Axiomes basiques (Axiomes de la Théorie des ensembles, Axiomes de Peano (Définissant **N**), Axiome du choix), pourraient être insuffisants pour démontrer classiquement qu'il n'existe aucune séquence d'algorithmes solution de $P_B$, $P_B$ problème de détermination basique donné quelconque.

De plus cet Axiome 1 n'a jamais été contredit, on n'a jamais prouvé qu'un problème de détermination numérique basique n'admettait pas de solution, ce qui serait nécessaire pour montrer l'invalidité de cet Axiome 1. On rappelle que comme tout Axiome, même s'il est vrai et se comprend intuitivement, il n'admet pas de démonstration classique.

A cause de cet Axiome 1, il est impossible de prouver qu'un problème de détermination numérique est de classe NP mais n'est pas de classe P et donc de prouver P≠NP pour les problèmes de détermination numérique basiques.

C)IMPOSSIBILITE DE PROUVER P=NP POUR LES PROBLEMES DE DETERMINATION NUMERIQUE BASIQUES.

Dans cette section on considère seulement les problèmes de détermination numérique basiques.Pour prouver P=NP, on doit prouver que tout problème de détermination numérique basique de classe NP est de classe P.

Or on admet l'Axiome 2 suivant :

Axiome 2 :

Pour montrer qu'un problème de détermination numérique basique est de classe P, on doit nécessairement déterminer une séquence polynomiale déterministe d'algorithmes le résolvant.

Cet Axiome 2 a la justification intuitive suivante : Il n'existe pas d'Axiomes généraux permettant de justifier qu'il existe une séquence polynomiale d'algorithmes résolvant un problème de détermination numérique basique $P_B$ sans déterminer explicitement une séquence polynomiale déterministe particulière le résolvant ou une façon de l'obtenir. Ainsi, on n'a jamais prouvé qu'un problème de détermination numérique était de classe P autrement qu'en explicitant une séquence polynomiale déterministe d'algorithmes le résolvant ou en donnant une façon de l'obtenir. Et donc, tout comme l'Axiome 1, il n'a jamais été contredit. Pour le contredire, il faudrait prouver qu'un problème de détermination basique est de classe P sans déterminer une séquence polynomiale déterministe d'algorithmes le résolvant (ou une façon de l'obtenir).

Une conséquence de cet Axiome 2 est l'assertion suivante, pouvant être aussi considérée comme sa seconde partie :

ASSERTION 1 :

Pour prouver NP est inclus dans P pour les problèmes de détermination numérique basique il est nécessaire de trouver un algorithme permettant de déterminer, pour tout problème de détermination numérique basique $P_B$ de classe NP une séquence polynomiale déterministe d' algorithmes ($Alg_{DPB}(n)$) résolvant $P_B$.

Or il est évident qu'il sera toujours impossible de trouver un tel algorithme comme on l'admet dans l'Axiome 3 suivant :

Axiome 3 :

Il n'existe pas d'algorithme général permettant de déterminer pour tout problème de détermination numérique basique $P_B$ de classe NP un algorithme polynomial déterministe ($Alg_{DPB}(n)$) résolvant $P_B$.

Pour démontrer l'invalidité de cet Axiome 3, il faudrait trouver un tel algorithme général, ce qui est certainement impossible. Il est en effet évident qu'on n'a pas assez d'éléments permettant de construire un algorithme général permettant d'obtenir une séquence polynomiale déterministe pour chaque problème de détermination numérique basique, même en supposant que P=NP. On n'a pas la première ligne d'un tel algorithme général. Et donc on a justifié qu'il était impossible de démontrer P=NP pour les problèmes de détermination numérique basiques (même si c'est vrai), puisque pour démontrer P=NP on doit démontrer que NP est inclus dans P.

On a donc comme conséquence des Axiomes 1,2,3 le Théorème :

THEOREME 1 :

Considérant la classe des problèmes de détermination numérique basique, la proposition P=NP est indécidable.

On a donc justifié en admettant les Axiomes précédents que même si on l'on a P=NP est vrai ou P≠NP pour les problèmes de détermination numérique basiques, il est dans les 2 cas impossible de le démontrer. Utilisant l'Axiome 1 et généralisant immédiatement les Axiomes 2 et 3, avec les mêmes justifications intuitives, on obtient que le problème P=NP est aussi indécidable pour tous les problèmes de détermination basique avec la condition sur k(n),

$k(n)<n^3+1000$. (On peut évidemment remplacer « $n^3+1000$ par tout Polynôme non-constant de $F(\mathbf{N},\mathbf{N})$, ou prendre pour k(n) une fonction croissante de $F(\mathbf{N},\mathbf{N})$ avec k(n) tend vers l'infini pour n tend vers l'infini par exemple k(n)=Int(n/4) comme dans l'exemple).

On a donc comme conséquence de l'Axiome 1 et des généralisations d'Axiomes 2,3 le Corolaire 1 :

COROLAIRE 1 :

Si on considère la classe des problèmes de détermination numérique basique $P_B$ avec la condition sur $k_{PB}(n)$, $k_{PB}(n)<Pol(n)$, Pol polynôme non-constant donné de $F(\mathbf{N},\mathbf{N})$, ou $k_{PB}(n)=f(n)$, f fonction croissante de $F(\mathbf{N},\mathbf{N})$ tendant vers l'infini n tendant vers l'infini, alors pour cette classe on a aussi P=NP est indécidable.

Notons qu'on peut aussi considérer les Axiomes 1,2,3 comme des assertions de logique pures qu'on peut admettre et qui peuvent permettre de résoudre le problème P=NP pour les problèmes de détermination numérique basiques. Le fait qu'on n'a considéré qu'une classe de problème, les problèmes de détermination numérique basiques, permet de comprendre et de tester plus facilement les Axiomes 1,2,3. Comme des Axiomes ordinaires, il est quasi-certain que même s'ils sont vrais ils ne peuvent pas être démontrés formellement.

D)JUSTIIFICATION THEORIQUE DE P≠NP PAR LA THEORIE ALEATOIRE DES NOMBRES.

On a démontré que pour les problèmes de détermination numérique basiques il était impossible de prouver classiquement P=NP ou P≠NP. Cependant, il existe une théorie, la Théorie Aléatoire des Nombres [(2)], qui peut être utilisée pour donner une justification théorique (Qui n'est pas une démonstration classique) de P≠NP. On a montré [(2)] que cette théorie donnait une justification théorique aux Conjectures faible et forte de Goldbach ainsi qu'à celles des nombres premiers jumeaux, et qu'il est tout à fait possible qu'il n'existe aucune démonstration classique de ces conjectures ou de leurs négations. Cette théorie montre en effet que des lois du hasard dans les nombres peuvent avoir comme conséquences certaines propositions pour lesquelles il est tout à fait possible qu'il n'existe aucune démonstration classique de même que pour leur négation. Ces justifications théoriques utilisant des lois du hasard dans les nombres, permettent cependant de comprendre l'origine de la validité des propositions obtenues, de la même façon qu'une démonstration classique.

A l'aide de certains éléments de la Théorie Aléatoire des Nombres (que nous allons rappeler) nous allons exposer une justification théorique basée sur le hasard dans les nombres de P≠NP.

La Théorie Aléatoire des Nombres est basée sur des propositions, appelées *pseudo-Axiomes aléatoires*, qui sont analogues à des Axiomes classiques mais expriment des lois du hasard en théorie des nombres. Ces pseudo-Axiomes aléatoires induisent des modèles statistiques qui peuvent être valides avec une bonne approximation mais aussi complètement faux. Malgré ce problème les pseudo-Axiomes aléatoires apparaissent comme étant la seule solution pour utiliser les lois du hasard dans les nombres, celles-ci pouvant donner des justifications théoriques à des propositions qui n'ont pas de démonstration classique de même que leur négation. On utilisera ici le pseudo-axiome aléatoire suivant :

Pseudo-Axiome 1 :

Si A est un ensemble fini et B un sous-ensemble de A, si x est un élément de A, la proposition « x est élément de B» sera modélisé par l'évènement de l'espace probabilisé équiprobable $(A,\mathcal{P}(A),p_{eqA})$ « x est élément de B ».

Dans la Théorie Aléatoire des Nombres, d'après la définition de la relation « est modélisée par », qui peut exister entre une proposition et un évènement d'un espace probabilisé, si P est une proposition modélisée par un évènement Ev, alors Non(P) sera modélisée par l'évènement Non(Ev).

On admet aussi dans la Théorie Aléatoire des Nombres le résultat fondamental et intuitivement évident le processus de déduction consistant, si une proposition P est modélisée par un évènement Ev de probabilité égale ou très proche de 1 (On dira alors que P a une *pseudo-preuve aléatoire*, qui est l'obtention de « P est modélisée par Ev » par des Axiomes classiques et au moins un pseudo-axiome aléatoire), à déduire que P pourra être vraie comme conséquence de la modélisation de P par un évènement de probabilité très proche de 1. Plus généralement si une proposition Q s'obtient en utilisant des Axiomes classiques et des propositions ayant une pseudo-preuve aléatoire, on dira que Q a une pseudo-preuve aléatoire qui est son obtention utilisant des Axiomes classiques et les propositions ayant une pseudo-preuve aléatoire. On considèrera donc que la pseudo-preuve aléatoire de P est une justification théorique basée sur les lois du hasard dans les nombres de la validité de P. Cependant contrairement au cas où elle a une preuve classique, P ne sera pas nécessairement vraie si elle a une pseudo-preuve aléatoire. C'est donc seulement si il n'existe de preuve classique ni de P ni de Non(P) (Et donc qu'on n'en n'a jamais trouvé) qu'une pseudo-preuve aléatoire de P sera intéressante. Et c'est le cas pour la proposition « P=NP ». Mod(P,Ev) : « P est modélisé par Ev », avec $p(Ev)\approx 1$, signifiera intuitivement : « Si les lois du hasard utilisées pour obtenir Mod(P,Ev) sont valides avec une suffisamment bonne approximation, alors P se comporte comme si elle avait une probabilité très proche de 1 d'être vraie ».

On illustre les concepts de « pseudo-preuve aléatoire » ou « justification théorique basée sur le hasard de la façon suivante :

On considère une boîte contenant 1000 boules, 999 boules rouges et une boule blanche. John tire une boule de la boîte sans la regarder.

Les lois du hasard dans les boîtes de boules sont exprimées par le pseudo-Axiome aléatoire 2 suivant :

Pseudo-Axiome 2 :

Si A est un ensemble fini (ou « boîte », « jeu »…) d'objets (ex. boules, cartes..) et B est un sous-ensemble de A, alors si N. (ex. John) tire un objet x de A sans le regarder, on aura : La proposition « x est élément de B » est modélisé par l'évènement de l'espace probabilisé équiprobable $(A,\mathcal{P}(A),p_{eq})$ « x est élément de B » (Donc de probabilité égale à Card(B)/Card(A)). (La proposition « x est élément de B » sera équivalente à « N. tire un objet appartenant à B ».)

D'après les lois sur le hasard des boîtes de boules, si P est la proposition P : « John tire une boule rouge » P est modélisée par un évènement Ev, avec p(Ev)=0,999. Cela signifie que P se comporte comme si elle avait la probabilité 0,999 d'être vraie. L'obtention de Mod(P,Ev) en utilisant les lois du hasard des boîtes de boules (Pseudo-Axiome 2) sera appelée *pseudo-preuve aléatoire* de P. Si P est vraie, elle sera considérée comme une *justification théorique basée sur le hasard* de P.

Dans ce cet exemple cependant, on est sûr de la validité du modèle probabiliste obtenu permettant d'obtenir Mod(P,Ev), on dira que ce modèle probabiliste est *exact*. Cela ne sera pas le cas en général si P est une proposition en Théorie des Nombres, ou le modèle probabiliste permettant d'obtenir Mod(P,Ev) pourra être approximativement valide, voire complètement faux.

Soit H l'ensemble des problèmes de détermination numérique basiques de classe NP écrits avec un nombre de caractères inférieur à $10^5$ (Et donc H fini, mais avec Card(H) très élevé. On admettra Card(H)>10000). Soit A l'ensemble $A=\mathcal{P}(H)$. Soit x le sous-ensemble de H contenant tous les problèmes de détermination numérique basiques de classe P. On a donc x est élément de A. Soit B l'ensemble B={H}. On a donc B est inclus dans A. D'après le pseudo-Axiome aléatoire 1, on a :

La proposition « x est élément de B » est modélisée par l'évènement Ev de $(A, \mathcal{P}(A), p_{eqA})$ : « x est élément de B », avec $p_{eqA}(B)=1/\mathrm{Card}(A)=1/2^{\mathrm{Card}(H)}\approx 0$ car Card(B)=1 et Card(H)>10000.

Or la proposition « x est élément de B » est équivalente à la proposition « P=NP pour les problèmes de détermination numériques basiques écrits avec moins de $10^5$ caractères ».

Et donc Non( « P=NP pour les problèmes considérés ») est modélisée par l'évènement Non(Ev) de probabilité très proche de 1, et donc la proposition « P≠NP pour les problèmes considérés » a une pseudo-preuve aléatoire. Comme « P≠NP pour les problèmes considérés » entraîne « P≠NP dans le cas général », « P≠NP dans le cas général » a une pseudo-preuve aléatoire. Et donc les lois du hasard dans les nombres peuvent être à l'origine de la validité de la proposition « P≠NP dans le cas général ».

Il est très probable que l'exemple précédent de l'Institut Clay soit un problème de détermination numérique basique de classe NP mais non de classe P, en accord avec la justification théorique basée sur le hasard de P≠NP. Cependant, il sera impossible de le démontrer si l'Axiome 1 est valide.

On pourra remplacer H par H/X, X l'ensemble des problèmes de détermination numérique basiques pour lesquels on a montré l'appartenance à la classe P.

E)LE PROBLEME $P_N$=$DP_N$.

Nous allons maintenant étudier un 2nd problème, nommé problème $P_N$=$DP_N$, totalement analogue au problème P=NP dans sa résolution, mais qui a une importance fondamentale en mathématique.

On définit le problème $P_N$=$DP_N$ de la façon suivante : On dira qu'une proposition P appartient à la classe $P_N$ (On dira alors que P est une *proposition numérique*), si P est une proposition mathématique utilisant exclusivement, en plus des symboles définis :

(i)Des concepts primitifs relationnels entre propositions (« Non », « et », « ou », « est équivalent à »…).

(ii)Des concepts typiques de la Théorie des nombres (« est premier », « est premier avec », « divise », « est pair », « 0 »,« 1 », « 2 »….,$\mathbf{N}^p$ , $\mathbf{Z}^p$, « fini », « infini », « est congru modulo p avec » (Défini par « a est congru modulo p avec b » est équivalent à « Il existe un entier k tel que a-b=kp) des fonctions numériques explicites, « Card », « > », « < » (Entre entiers), « = » (Entre entiers ou ensembles), ou « $N_S$ » donnant le nombre de termes d'une séquence ou $d_S$(i, ), i naturel non nul, donnant le ième terme d'une séquence finie ayant au moins i termes.

(iii) Des fonctions numériques explicites et des définitions de fonctions numériques explicites.

(On rappelle que f est une *fonction numérique explicite* si f est une fonction de $F(A^p,B)$, avec p naturel >0, A,B=**N** ou **Z**, (On pourra remplacer $A^p$ par l'ensemble $S_{FA}$ dont les éléments sont les éléments de A et toutes les séquences finies d'éléments de A) définie explicitement par les opérations dans **N** ou **Z** (addition, multiplication, puissance..), ou utilisant des expressions E(f(n)), f fonction réelle croissante et tendant vers l'infini, définie explicitement en fonction des fonctions réelles classiques (Log,exp..) et des opérations classiques dans **R**,(Et de symboles représentant des réels « 1/3 », « 3/7 »…) ou $r_{DE}$ (fonction donnant le reste de la division Euclidienne d'un entier p par un entier q), ou des produits ou sommes d'éléments de séquence finies d'entiers (Notées « Π » et « Σ »), ou « valeur absolue » (D'un entier), ou des symboles représentant des entiers « 0 », « 1 », « 2 »....On pourra donc identifier une fonction numérique explicite avec un ensemble infini, et avec une séquence infinie si $A^p$=**N**.

(iv) Les concepts classiques de la Théorie des ensembles, « est élément de », « est inclus dans », « est un ensemble (fini, infini) », « est une séquence (finie ou sur un sous-ensemble infini de **N**)».

(v) Les quantificateurs « Il existe», « Pour tout», de même que « (est) défini par ».

(vi)Des sous-ensembles finis ou infinis B de $A^p$, A=**N** ou **Z**, p naturel, définis par une expression du type :« B est défini par $P(B,A^p, B_1,.., B_k,a_1,…,a_t)$, $B_1,..,B_k$ définis comme B ou égaux à $A^q$ (A=**N** ou **Z**), des éléments numériques (C'est-à-dire définis à partir d'entiers et de familles ou séquences finies) définis par B, $A^p$, $B_1$,.,$B_k$, les éléments numériques pré-definis $a_1,\ldots,a_t$, et comme ensembles infinis seulement parmi B,$A^p$, $B_1$,..,$B_k$ et des fonctions numériques explicites. La définition de B pourra ne pas utiliser de $B_i$ ou ne pas utiliser $A^p$ ou ne pas utiliser d'$a_j$. On pourrait supprimer la condition que B est un sous-ensemble de $A^p$, mais on aura toujours la condition exprimée par le point (ix).

(vii) Des ensembles finis C(n), définis pour n élément de B, B sous-ensemble infini de **N** (ou **Z**) défini comme en (vi), avec C(n) défini par « C(n) est défini par P(C(n), n, $C_1(n)$,..,$C_l(n)$, $B_1$,..,$B_k$,$a_1$,..,$a_t$), P(C(n), n, $C_1(n)$,..,$B_k$,$a_1$,..,$a_t$) proposition mathématiques utilisant les termes définis de (i) à (v), des éléments numériques définis par C(n), les $C_i(n)$ et les $B_j$, les éléments numériques pré-définis $a_1$,..,$a_t$, les ensembles $B_j$ définis comme en (vi) et les ensembles finis $C_i(n)$ définis comme C(n) et comme ensembles infinis seulement les $B_j$ et des fonctions numériques explicites. Cette proposition pourra ne pas utiliser de $B_j$ ou ne pas utiliser d'$a_j$ ou ne pas utiliser de $C_i(n)$ ou ne pas utiliser n si elle utilise au moins un $C_i(n)$.

Si C(n) est défini sans utiliser aucun $C_i(n)$, la proposition numérique pourra utiliser les séquences $(C(n))_B$ ou $(\mathrm{Card}(C(n))_B$.

(viii)Des expressions du type « $\lim_{n\to\infty}(\mathrm{Card}(C(n))/f(n))=1$, avec $(C(n))_B$ séquence définie comme en (vii) et f(n), f fonction numérique explicite.

(ix)Tout ensemble utilisé dans une propositions numérique a des éléments définis à partir d'entiers et de familles ou séquences finies (Et donc ces éléments seront en particulier ou bien des entiers ou bien des familles ou séquences finies d'entiers. On dira que les éléments des ensembles considérés sont des *éléments numériques*, qui peuvent être définis par les 2 règles suivantes :

a)Tout entier est un élément numérique.

b)Toute famille ou séquence finie dont les éléments ou les termes sont des éléments numériques est un élément numérique.

Il y aura une exception pour des ensembles de type $F(\mathbf{N}^p,\mathbf{N})$ qui pourront être utilisés dans une proposition numérique s'ils sont utilisés pour définir une fonction numérique explicite (On peut cependant éviter cette exception remplaçant « f est élément de $F(\mathbf{N}^p,\mathbf{N})$ » par « f est une application de $\mathbf{N}^p$ dans **N** »).

Une proposition numérique pourra utiliser des éléments numériques définis à partir d'ensembles $A^p$, (A=**N** ou **Z**) ou d'ensembles B comme définis au (vi) ou d'ensembles C(n) ou $(C(n))_B$ définis au point (vii).

(x)Une proposition numérique P pourra seulement utiliser (excepté pour la proposition du point (viii)) comme ensemble infinis (appelés *ensembles numériques*) $A^p$ ,$S_{FA}$ (A=**N** ou **Z**),les ensembles B définis au point (vi), des fonctions numériques explicites et les séquences définies au point (vii). On pourra généraliser le point (viii) pour un ensemble numérique qui est une séquence d'entiers indexée sur un sous-ensemble infini de **N**. On peut obtenir $S_{FA}$ comme un ensemble B défini en (vi) sans la condition « B est inclus dans $A^p$ »..

En conséquence une proposition numérique ne pourra pas utiliser des concepts logiques comme « une proposition », « une preuve classique» car ces concepts ne sont pas définis comme pouvant être utilisés dans une proposition numérique dans les points (i) à (x).

Par exemple le Théorème de BEZOUT, le Théorème de FERMAT, les Conjectures de GOLDBACH faibles et fortes seront des propositions numériques. Mais non le Théorème de CAILEY-HAMILTON, le Théorème de CANTOR-BERNSTEIN, l'Hypothèse du Continu », les problèmes « P=NP » ou « $P_N$=$DP_N$ ».

Cependant si on considère seulement les matrices à coefficients entiers, on peut montrer que le Théorème de CAILEY-HAMILTON est équivalent à (au sens « a la même signification, est interchangeable avec ») une proposition numérique. On rappelle que le Théorème de CAILEY-HAMILTON est exprimé par la proposition : « Pour tout naturel non nul n, pour toute matrice réelle n×n A, $X_A(A)=0_{n\times n}$, avec $X_A(x)$ est le polynôme $\det(A-xId_{n\times n})$.

On définit alors la proposition numérique suivante :

n étant un naturel non nul, on définit classiquement la matrice n×n à coefficients entiers :

$A(n)=\{((1,1),a_{11}), \ldots..,((n,n),a_{nn})\}$, $a_{11},\ldots,a_{nn}$ étant des entiers.

On définit alors la fonction numérique explicite $f_{XA(A)}$, de $S_{FZ}$ dans **Z** par :

Pour toute séquence $(n,i,j,a_{11},\ldots,a_{nn})$, avec n naturel non nul, i,j naturels non nuls inférieurs ou égaux à n, $a_{11},..,a_{nn}$ étant des entiers, alors $f_{XA(A)}((n,i,j,a_{11},..,a_{nn}))$ définit le terme (i,j) de la matrice $X_A(A)$, en fonction de $n,i,j,a_{11},..,a_{nn}$. (On admettra comme évident que $f_{XA(A)}$ existe, puisque $x_{i,j}$ est défini en utilisant $a_{11},\ldots,a_{nn}$ et les opérations dans **Z** « + », « × », « -»).

Pour définir $f_{XA(A)}$, on commence par définir le fonction numérique explicite $g_{XA}$ telle que si i est un naturel inférieur ou égal à n, $g_{XA}(n,i,a_{11},\ldots.,a_{nn})$ est le coefficient du terme de degrés i dans $X_A(x)$.

Puis on définit la fonction numérique explicite $h_{Ap}$ telle que si k est un naturel et i,j des naturels différents de 0 inférieurs ou égaux à n, $h_{Ap}(k,n,i,j,a_{11},..,a_{nn})$ est le terme (i,j) de $A(n)^k$. ($h_{Ap}$ pourra être définie par récurrence sur k).

Utilisant alors $g_{XA}$ et $h_{Ap}$, on pourra définir $f_{XA(A)}$.

Pour un élément s de $S_{FZ}$ qui n'est pas une séquence du type précédent, on prendra $f_{XA(A)}(s)=1$.

Alors le Théorème de CAILEY-HAMILTON pour les matrices à coefficients entiers est équivalent à :

Pour tout n naturel non nul, pour tous i,j naturels non nuls inférieurs ou égaux à n, pour tous entiers $a_{11},..,a_{nn}$, $f_{XA(A)}((n,i,j,a_{11},\ldots,a_{nn}))=0$.

Il est clair qu'on pourrait élargir la définition de proposition numérique donnée par les points (i) à (viii).Par exemple en permettant à une proposition numérique d'utiliser des suites $(d(i,r))_{\mathbf{N}^*}$ (ensemble numérique) tel que r est un réel et d(i,r) est la ième décimale de r. Le point (ix) est nécessaire pour obtenir que tous les ensembles considérés sont dénombrables. On montre facilement le résultat fondamental que si on a une séquence sur un sous-ensemble infini B de **N** $(u(n))_B$ qui est un ensemble numérique, et si de plus on a une fonction numérique explicite f telle que pour tout n élément de B u(n) appartient à l'ensemble de départ de f, alors la séquence $(f(u(n))_B$ est un ensemble numérique qui est une séquence sur B dont tous les termes sont des entiers. Concernant les ensembles numériques définis au point (x), an a vu qu'on avait une exception si on utilise le point (viii) car dans ce cas on utilisera des fonctions qui ne sont pas des ensembles numériques (Par exemple la division dans **R** ou **Q**).

Cependant le point (viii) n'est pas nécessaire. En effet on appelle *proposition strictement numérique* une proposition définie comme une proposition numérique mais en supprimant le point (viii). Il apparaît que la proposition du point (viii) est équivalente (au sens « a la même signification, est interchangeable dans son utilisation avec ») à une proposition strictement mathématique, c'est-à-dire que le point (viii) est la conséquence des autres points de la définition d'une fonction numérique.

Pour montrer cela, on définit la suite sur **N*** $(\varepsilon_p)_{\mathbf{N}^*}$ avec $\varepsilon_p=1/10^p$. On rappelle que la proposition (viii) signifie P1: « Pour tout ε élément de $\mathbf{R}^{*+}$, il existe N élément de **N** tel que pour tout n naturel élément de B et supérieur à N, $|Card(C(n))/f(n)-1|<\varepsilon$.

Pour obtenir une proposition numérique équivalente à P1, on remplace « Pour tout ε réel >0 » par « Pour tout p élément de **N*** » et « <ε » par « $<\varepsilon_p=1/10^p$ ». On obtient alors immédiatement une proposition strictement numérique équivalente à P1, multipliant les 2 termes de l'inégalité stricte par $f(n)10^p$.

On peut généraliser ce qui précède, remplaçant $(Card(C(n))_B$ par une séquence d'entiers $(u(n))_B$ qui est un ensemble numérique. En effet u(n) est alors un élément numérique défini par $(u(n))_B$, qui peut donc être utilisé dans une proposition strictement numérique.

En fait il est très probable qu'on puisse admettre **Q** comme ensemble numérique, et qu'une fonction numérique explicite puisse être de $\mathbf{Q}^p$ (Ou $S_{FQ}$) dans **Q**. Une telle fonction sera appelée *fonction numérique explicite de rationnels* et celles dont l'ensemble de départ est $A^p$ (Ou $S_{FA}$) avec A=**N** ou **Z** seront appelées *fonction numérique explicite d'entiers*. La définition d'une fonction numérique explicite de rationnels sera complètement analogue à celle des fonctions numériques explicites d'entiers, sauf pour la fonction « puissance » car une fonction numérique explicite de rationnels pourra utiliser une expression $a^p$ seulement si p est un entier. Ceci est nécessaire pour qu'une expression qui est une égalité (ou une inégalité) entre 2 rationnels définis en utilisant des rationnels et des fonctions numériques explicites de rationnels soit toujours équivalente à une expression qui est une égalité (Ou une inégalité) entre 2 entiers définis en utilisant des entiers et des fonctions numériques explicites d'entiers.

Il semble cependant que toute proposition numérique utilisant **Q** comme ensemble numérique ou des fonctions numériques explicites de rationnels est équivalente à une proposition strictement numérique, de la même façon que pour la proposition du point (viii).

P étant une proposition numérique, on dira qu'elle appartient à la classe $DP_N$ si P ou Non(P) peut être démontrée par une démonstration classique, celle-ci pouvant cependant utiliser tous les théorèmes mathématiques démontrés, sans se restreindre aux propositions numériques. Par exemple le Théorème de Fermat est une proposition numérique appartenant à la classe $DP_N$ alors que sa démonstration utilise de nombreuses propositions qui ne sont pas des propositions numériques. La classe $DP_N$ est donc incluse dans la classe $P_N$, et le problème $P_N=DP_N$ consiste à rechercher si la classe $DP_N$ est égale à la classe $P_N$, en toute analogie avec le problème P=NP qui consistait à rechercher si la classe P était égale à la classe NP.

Le problème $P_N=DP_N$ se résout de façon totalement analogue au problème P=NP : On commence par montrer qu'il est impossible de montrer classiquement $P_N=DP_N$ et $P_N \neq DP_N$.

On considère l'Axiome 1B, analogue à l'Axiome 1 :

AXIOME 1B :

P étant une proposition numérique il est impossible de montrer classiquement que ni P ni Non(P) ne sont démontrables classiquement (C'est-à-dire P n'appartient pas à $DP_N$).

Cet Axiome 1B se justifie intuitivement de la même façon que l'Axiome 1 : P étant une proposition numérique, elle exprime des propriétés de naturels (Incluant des propriétés de Card(A(n)) si on a une séquence d'ensembles finis A(n) ou de fonctions numériques explicites). A cause de cela, P pourra admettre une démonstration classique très complexe, utilisant des fonctions numériques complexes. Et on comprend intuitivement que les Axiomes basiques (Axiomes de la Théorie des Ensembles, Axiomes de Peano (Définissant **N**), Axiome du choix) sont insuffisants pour montrer que ni P ni Non(P) n'admet aucune démonstration classique, même parmi les plus complexes. Et on n'a jamais montré, pour aucune proposition numérique telle qu'on l'a définie, que ni elle ni sa négation n'étaient démontrables classiquement. On rappelle cependant que cet Axiome, comme tout Axiome, ne peut pas être démontré formellement même s'il est vrai.

On remarque que l'Axiome 1B ne se généralise pas à toute proposition mathématique ni même à toute *proposition strictement mathématique*. (On définit une *proposition strictement mathématique* comme une proposition mathématique n'utilisant pas directement ou indirectement les concepts logiques paramathématiques comme par exemple « une proposition » , « est démontrable », « un problème »..)

En effet l'Axiome 1B ne s'applique pas à l'hypothèse du continu qui est une proposition strictement mathématique : $H_C$ :« Il n'existe pas d'ensemble de cardinal strictement compris entre **N** et **R** ». En effet cette proposition n'est clairement pas une proposition numérique, elle utilise **R** (ou *F*(**N**,**N**)) qui ne correspondent pas aux points (vi) et (vii) de la définition des propositions numériques et de plus les éléments de ces ensembles sont constituées de séquences infinies ce qui n'est pas possible pour des ensembles utilisés dans une proposition numérique, excepté pour définir une fonction numérique explicite ce qui n'est pas le cas. Le fait qu'on ne peut pas lui appliquer l'Axiome 1B s'explique aussi intuitivement car $H_C$ utilise des concepts obtenus par des Axiomes basiques (remplaçant **R** par *F*(**N**,**N**)), ce qui conduit à justifier intuitivement qu'il est plus facile de justifier que ce type de proposition est indécidable. De plus il semble évident intuitivement qu'une démonstration de $H_C$ ou de Non($H_C$) ne nécessite pas l'introduction de fonctions explicites ce qui justifie qu'on n'a pas besoin de considérer les démonstrations contenant des fonctions numériques explicites pour montrer l'indécidabilité de $H_C$ (Ce qui n'est évidemment pas le cas pour une proposition numérique). On rappelle que l'indécidabilité de $H_C$ relativement aux Axiomes basiques a été établie (3).

Comme conséquence de l'Axiome 1B, on a l'impossibilité de prouver $P_N \neq DP_N$.

Pour prouver l'impossibilité de prouver $P_N = DP_N$, on admet l'Axiome 2B, analogue à l'Axiome 2 :

AXIOME 2B :

Pour montrer qu'une proposition numérique P est démontrable classiquement on doit donner explicitement une démonstration classique de P ou un algorithme permettant d'en obtenir.

Cet Axiome 2B se justifie intuitivement exactement comme l'Axiome 2.

A l'aide de l'Axiome 2B, de la même façon que dans la solution du problème P=NP, on montre que pour montrer $P_N = DP_N$ il serait nécessaire de donner un algorithme permettant d'obtenir une démonstration classique de toute proposition numérique ce qui est impossible d'où l'impossibilité de prouver $P_N = DP_N$.

On a donc montré utilisant nos Axiomes l'impossibilité de prouver classiquement $P_N = DP_N$ ou sa négation.

Cependant procédant exactement comme pour le problème P=NP, on montre que les lois du hasard justifient théoriquement $P_N \neq DP_N$.

On remarque que contrairement au cas P=NP, il existe des propositions numériques pour lesquelles on peut penser intuitivement qu'elles ne sont pas de classe $DP_N$, c'est-à-dire qu'elles n'ont pas de démonstration classique de même que leur négation. C'est le cas par exemple des Conjectures faibles et fortes de GOLDBACH ou des Nombres Premiers Jumeaux. En accord avec l'Axiome 1B, cela devrait être impossible à prouver classiquement mais il est remarquable que ces propositions ont des justifications théoriques basées sur le hasard qu'on peut obtenir dans la Théorie Aléatoire des Nombres (2). C'est précisément l'existence de telles justifications théoriques basées sur le hasard et le fait qu'on n'a jamais trouvé de preuve classique de ces Conjectures ni de leurs négations qui nous amènent à penser intuitivement que ces propositions n'ont probablement pas de démonstration classique de même que leurs négations.

On remarque que le problème $P_N$=$DP_N$ est équivalent à un problème fondamental en mathématique : « La Théorie des Nombres (Restreinte aux propositions numériques sauf pour les démonstrations) est-elle complète ? ».

Les problèmes numériques sont intéressants car ils sont simples (N'utilisant que des propositions élémentaires de la Théorie des Nombres) et de plus c'est dans ces problèmes qu'on trouve le plus facilement des propositions qui sont indécidables, parmi toutes les propositions strictement mathématiques, définissant des propositions à l'aide de fonctions numériques explicites complexes (Définies par exemple avec E(Log(n)) On en trouve aisément une infinité. L'existence de ces propositions est en accord avec la justification basée sur le hasard de l'incomplétude de la Théorie des Nombres. C'est aussi pour ce type de problème que la Théorie Aléatoire des Nombres peut être appliquée, pour donner des justifications théoriques basées sur le hasard de propositions qui semblent vraies mais ne peuvent pas être démontrées classiquement à cause de l'Axiome 1B. Elles permettent aussi de comprendre la solution du problème P=NP et en particulier l'Axiome 1, qui est très proche de l'Axiome 1B. L'utilisation du concept de proposition numérique permet aussi de donner une classe de propositions strictement mathématique pour laquelle l'Axiome 1B s'applique, on rappelle qu'il ne s'applique pas à toutes les propositions strictement mathématiques.

Si on a un problème basique de détermination numérique $P_B$ de classe NP mais pas de classe P, par définition il ne sera pas possible de trouver une séquence d'algorithmes le résolvant. De plus d'après l'Axiome 1, il ne sera pas possible par une preuve classique (C'est-à-dire utilisant les Axiomes basiques mathématiques), de prouver qu'il n'admet pas de solution.

De même, si une proposition P est de classe $P_N$ mais pas de classe $DP_N$, par définition il ne sera pas possible de prouver classiquement P ou Non(P). De plus d'après l'Axiome 1B, il sera impossible de prouver classiquement que ni P ni Non(P) n'ont de démonstration classique.

Tout amène à penser que de tels problèmes basiques de détermination numérique ou de telles propositions existent considérant la pseudo-preuve aléatoiredes Axiomes 1 et 1B, mais aussi les multiples propositions numériques qui ont des justifications théoriques basées sur le hasard.

On pourra appeler les Axiomes 1 et 1B *Axiomes d'indéterminisme* de la Théorie des Nombres. Comme tout Axiome, ils n'ont pas de démonstration classique, mais ils ont une justification intuitive, ils ont une expression très simple et n'ont jamais été contredit alors qu'ils concernent une infinité de propositions. De plus, ils sont fondamentaux.

Il est possible que la définition d'un concept équivalent à celui d'un Système formel classique puisse être obtenue par une proposition numérique. (Même si cela reste à prouver).

Soit $Sys_F$ un tel système, supposé défini par une proposition numérique.

Considérons la proposition classique appartenant à $Sys_F$ :« P :P est non démontrable dans $Sys_F$ ».

Supposons que la proposition Q : « P est vraie dans $Sys_F$ » soit équivalente (C'est à dire avec la même signification) elle aussi à une proposition numérique (On peut s'attendre à ce que cela soit le cas si le Système formel $Sys_F$ peut être défini par une proposition numérique).

On sait qu'on peut prouver classiquement que Q est vraie. Et donc on n'a pas « Ni Q ni Non(Q) n'ont de démonstration classique », et donc on n'a pas une contradiction de l'Axiome 1B.

Considérons maintenant la proposition R : « P est démontrable dans $Sys_F$ ».

On sait qu'on peut montrer classiquement que R n'est pas vraie. Et donc comme pour Q il n'y a pas de contradiction avec l'Axiome 1B.

Supposons aussi que R soit équivalent à une proposition numérique. On rappelle que les démonstrations classiques de Q et de Non(R) constituent la démonstration du Théorème d'incomplétude de GODEL. On a donc montré que même si on montrait qu'un système formel pouvait être défini par une proposition numérique, le Théorème de GODEL n'invaliderait pas l'Axiome 1B. On remarque que l'Axiome 1B concerne aussi les démonstrations des systèmes formels puisque ces derniers sont définis pour que ces démonstrations puissent être identifiées avec des preuves classiques.

Ainsi, si une proposition numérique P est telle que ni P ni Non(P) n'admettent de preuve classique, (Comme il semble que cela le soit pour les Conjectures faibles et fortes de GOLDBACH et pour une infinité de propositions numériques ayant une justification numérique aléatoire, qui semblent vraies mais n'ont jamais été prouvées classiquement), il ne sera pas possible à un système formel classique, c'est-à-dire un système formel dont les règles modélisent les Axiomes basiques des mathématiques, de donner une preuve à P ou à Non(P). De plus, si l'Axiome 1B est valide, il ne sera pas possible à un tel système formel de donner une démonstration que ni P ni Non(P) n'admettent de démonstration classique, ou si l'Axiome 1 est valide de donner une démonstration qu'un problème basique de détermination numérique n'admet pas de solution.

## III)CONCLUSION

On n'a pas montré que l'on a ni P=NP est vrai ni P $\neq$NP est vrai, mais on a justifié qu'il est impossible de le démontrer dans les 2 cas pour une classe de problèmes appelés *problèmes de détermination numérique basiques*. On remarque cependant que le fait qu'on ne puisse prouver P=NP pour les problèmes de détermination numérique basique entraîne qu'on ne peut aussi pas le prouver dans le cas général.

La théorie qu'on a présentée n'est pas purement mathématique. C'est une théorie de logique mathématique. Il semble certain qu'on ne pourra pas obtenir le résultat de cette théorie par une théorie mathématique pure. On peut considérer les Axiomes 1,2,3 non comme des Axiomes mais comme des assertions de logique pures évidentes et jamais contredites permettant de comprendre pourquoi le problème considéré P=NP est indécidable. Ces Axiomes s'appliquent naturellement à des classes beaucoup plus larges que les problèmes de détermination numérique basiques, la conclusion des Axiomes 2,3 (P=NP ne peut être prouvé) s'applique à l'ensemble des problèmes concernés par le problème P=NP et il semble très difficile de trouver un problème pour lequel l'Axiome 1 ne s'applique pas (Utilisé pour prouver que P≠NP ne peut être prouvé). De plus, le fait qu'on n'ait jamais obtenu de résultats fondamentaux sur le problème P=NP en utilisant les théories mathématiques classiques conduit à penser que la solution du problème P=NP nécessite l'introduction de nouveaux Axiomes, et qu'elle ne peut pas être obtenue en utilisant seulement les théories mathématiques de logique classiques. On rappelle que comme des Axiomes ordinaires, il est quasi-certain que même s'ils sont vrais les Axiomes 1,2,3 ne peuvent pas être démontrés formellement. La théorie est cependant en accord avec toutes les équations relatives au problème P=NP, de plus ses implications concernent ces équations et pour la contredire elle ou ses Axiomes on devrait utiliser de telles équations. On rappelle qu'on peut considérer cet article ou bien comme une preuve mathématique ou bien comme une justification logique, si on considère les Axiomes comme des assertions logiques. Dans les 2 cas la conclusion est un résultat mathématique fondamental qui à priori ne peut être obtenu qu'en utilisant des assertions logiques analogues à celles introduites dans cet article.

On rappelle que la définition d'*un problème de détermination numérique basique* est importante car c'est une définition très générale de problèmes potentiellement de classe P ou NP, et aussi car elle donne une base concrète pour justifier intuitivement les Axiomes que nous avons introduits, et aussi pour tester leur validité.

En ce qui concerne les problèmes de détermination numérique basiques, on n'a donc démontré ni P=NP ni P≠NP , mais on a néanmoins résolu le problème P=NP, de la même façon que la preuve qu'il n'existait pas d'algorithme permettant d'obtenir avec un compas la trisection d'un angle ou la quadrature du cercle résolvaient ces problèmes. La conclusion de cet article est bien en accord avec tous les articles scientifiques publiés dont le sujet est la problème P=NP. Pour prouver P=NP ou sa négation pour les problèmes de détermination numérique basiques, on devra donc en premier lieu prouver l'invalidité de la théorie présentée dans cet article c'est-à-dire d'un de ses Axiomes, ce qui est clairement beaucoup plus facile (si c'est possible) que de prouver P=NP ou sa négation pour le cas général.

Cependant nous avons montré que les lois du hasard dans les nombres pouvaient être à l'origine de la validité de la proposition « P≠NP », la justification théorique basée sur le hasard de « P≠NP » étant fondamentale puisqu'on ne l'a jamais prouvé classiquement ,ni sa négation (Et que cela semble impossible comme on l'a montré).

On a enfin proposé une solution analogue à la solution du problème P=NP du problème $P_N=DP_N$, ce dernier problème étant fondamental en mathématique, puisqu'équivalent au problème de la complétude de la Théorie de Nombres.

Références :


1)P=NP (archive), Web Clay Mathematics Institute (Archive)

2)Théories d'or 11e edition, Thierry DELORT, ed BOOKS ON DEMAND, PARIS (2024) (In French).

3)The independence of continuum hypothesis", Paul COHEN, PNAS Vol 51, p105-110 (1964)