Théorie des nombres et informatique

Patrick CÉGIELSKI* François HEROULT† Denis RICHARD‡

April 2, 2001

Abstract

An interval $[a, a+d]$ of natural numbers verifies the property of no coprimeness if and only if every element $a+1$, $a+2$, ... , $a+d-1$ is not coprime with a or with $a+d$. We show the set of such a and the set of such d are recursive.

Résumé

Un intervalle $[a, a+d]$ d'entiers naturels vérifie la propriété de n'avoir aucun élément premier avec simultanément ses deux bornes, si aucun de ses éléments, à savoir $a+1$, $a+2$, ... , $a+d-1$, n'est premier avec les deux extrémités a et $a+d$. Nous montrons que l'ensemble des tels a et l'ensemble des tels d sont récursifs.

Notre but, dans cet article, est de montrer comment l'utilisation d'ordinateurs peut contribuer à l'avancée d'une discipline mathématique aussi ancienne que la théorie des nombres. Nous choisissons un exemple pour cela, correspondant à un problème élémentaire, sur lequel on ne peut pas dire grand chose sans recours à des ordinateurs (relativement puissants).

1 Énoncés des problèmes

Introduction.- Dans sa thèse ([WOO, 81]), le mathématicien australien Alan Woods a énoncé quelques problèmes nouveaux intéressants de théorie des nombres. Le plus célèbre d'entre eux (connu sous le nom de *conjecture d'Erdös-Woods* après sa publication dans le livre de Richard Guy ([GUY,81])) est le suivant.

Conjecture d'Erdös-Woods : *Il existe un entier naturel k tel que les entiers naturels x et y sont égaux si, et seulement si, pour $i = 0 \ldots k$, les entiers $x+i$ et $y+i$ ont les mêmes diviseurs premiers.*

Ce problème est la source d'un domaine actif de recherches en théorie des nombres, comme à chaque fois qu'il est attaché au nom de Paul Erdös.

*L.A.C.L., IUT de Fontainebleau, Université Paris XII
†LLAIC1, IUT de Clermond-Ferrand, Université d'Auvergne
‡LLAIC1, IUT de Clermont-Ferrand, Université d'Auvergne

Alan Woods a aussi conjecturé ([WOO, 81], p. 88) que pour tout couple $\langle a,\ d\rangle$ d'entiers naturels, avec $d \geq 3$, il existe un entier c tel que $a < c < a + d$ et tel que c est premier avec a et $a + d$. En d'autres termes :

$$\forall a, \forall d > 2, \exists c\ [\ a < c < a + d\ \wedge\ a \perp c\ \wedge\ c \perp a + d\ ].$$

Alan Woods s'est très rapidement rendu compte que sa conjecture était fausse, en trouvant le contre-exemple (2184, 16) ([DOW, 89]). En 1987, David Dowe a prouvé qu'il existe une infinité de d pour lesquels on a un contre-exemple ([DOW, 89]). Il utilise un ordinateur pour trouver de tels couples, avec a et d inférieurs à 2000, mais n'en trouve pas.

Notation.- Notons $NoCoprimeness(a, d)$ la propriété :

$$\forall c\ [\ a < c < a + d \rightarrow \neg(a \perp c) \vee \neg(c \perp a + d)\ ].$$

Remarques.- 1°) La relation $NoCoprimeness(a, d)$ est vérifiable sur ordinateur. Il est facile d'écrire un programme pour voir si un couple (a, d) la vérifie ou non.

2°) L'ensemble $\{< a, d > / NoCoprimeness(a, d)\}$ est infini.

Nous connaissons un élément (2184, 16) de cet ensemble. Il est alors facile de montrer que $(2184 + k.30030, 16)$ en est aussi un élément, où $30030 = \prod_{p \in \mathcal{P}, p \leq 16} p$ est le produit des nombres premiers inférieurs à 16.

3°) Les deux propriétés, projections de $NoCoprimeness(a, d)$, définies par :

$$ExtremNoCoprime(a) \quad iff \quad \exists d\, NoCoprimeness(a, d)\},$$

$$AmplitudeNoCoprime(d) \quad iff \quad \exists a\, NoCoprimess(a, d)\}$$

sont ce qu'on appelle *récursivement énumérables*, c'est-à-dire qu'il est facile d'écrire un programme d'ordinateur qui liste les éléments des ensembles vérifiant ces propriétés (mais pas dans l'ordre naturel, malheureusement).

Notre but, dans cet article, est de démontrer que ces deux ensembles sont récursifs, c'est-à-dire qu'il existe, pour chacun d'eux, un programme d'ordinateur permettant de nous dire si un entier appartient ou non à cet ensemble.

Avant de démontrer la récursivité de ces ensembles, prouvons deux propriétés intéressantes.

PROPOSITION 1.- *Si $d \in AmplitudeNoCoprime$, alors il existe deux nombres premiers divisant $d - 1$.*

Démonstration.- Soit d un élément de $AmplitudeNoCoprime$. Soit a un entier tel que $NoCoprimeness(a,\ d)$. Nous avons $a \perp a + 1$, donc $\neg(a + 1 \perp a + d)$. Il existe un nombre premier p tel que $p \mid a + 1$ et $p \mid a + d$, et p divise la différence $d - 1$.

De même, il existe un nombre premier q divisant a, $a + d - 1$, et donc $d - 1$. Les nombres premiers p et q sont nécessairement différents. □

Corollaire 1.- *Si $d \in AmplitudeNoCoprime$, alors $d \geq 7$.*

Corollaire 2.- $\mathbb{N} \setminus AmplitudeNoCoprime$ *est infini.*

Démonstration.- Puisque $2^n + 1$ appartient à cet ensemble pour tout entier naturel n. Plus généralement, ceci est également vrai de $p^n + 1$ pour tout nombre premier p. □

2 Récursivité de ExtremNoCoprime

PROPOSITION 2.- *Pour tous les entiers naturels a et d tels que :*

$$NoCoprimeness(a,\ d),$$

nous avons :

$$d < a.$$

Démonstration.- Si $a \leq d$, il existe un nombre premier p_0 tel que :

$$a \leq \frac{d+a}{2} < p_0 < a + d,$$

d'après le théorème de Bertrand-Tchebychev. D'où :

$$a < p_0 = a + (p_0 - a) < a + d.$$

Il existe un nombre premier q tel que :

(i) $q \mid p_0 \, and \, q \mid a$; ou
(ii) $q \mid p_0 \, and \, q \mid a + d$.

Dans les deux cas on a $q \mid p_0$, d'où $q = p_0$.

Dans le cas (i), on a $p_0 = q \mid a$, mais $a < p_0$, ce qui est absurde.

Dans le cas (ii), on a $q \mid d - (p_0 - a)$, mais :

$$p_0 - a > \frac{a+d}{2} - a = \frac{d-a}{2},$$

donc :

$$p_0 = q < d - \frac{d-a}{2} = \frac{a+d}{2},$$

ce qui est absurde. □

Corollaire.- *L'ensemble $ExtremNoCoprime$ est récursif.*

Démonstration.- Le corollaire résulte du fait que, étant donné un entier a, il nous suffit de tester si nous avons la propriété $NoCoprimeness(a, d)$ pour un nombre fini de d, à savoir pour les d tels que $d < a$. □

3 Récursivité de AmplitudeNoCoprime

Quelques essais pour trouver de tels nombres d à la main nous conduisent à la caractérisation combinatoire suivante de *AmplitudeNoCoprime*.

THÉORÈME 1.- *Un entier d appartient à AmplitudeNoCoprime si, et seulement si, il existe une partition de l'ensemble $P_{<d}$ des nombres premiers strictement plus petits que d en deux ensembles A et$B$, ainsi qu'une application P de $[1, d-1]$ dans $P_{<d}$ telles que :*

(i) pour tous les entiers i tels que $1 \leq i < d$, si $P(i) \in A$ alors $P(i) \mid i$ et $P(i) \mid a$, et si $P(i) \in B$ alors $P(i) \mid d-1$ et $P(i) \mid a+d$;

(ii) pour i tel que $1 \leq i < i + P(i) < d$, on a $P(i) \in B$ si, et seulement si, $p(i + P(i)) \in B$.

Démonstration.-

Condition nécessaire Soit d un élément de *AmplitudeNoCoprime*.

Soit a un entier naturel tel que $NoCoprimeness(a, d)$.

Soit A_0 l'ensemble des nombres premiers divisant à la fois a et d.

Soit C l'ensemble des entiers i, avec $1 \leq i < d$, tels qu'aucun nombre premier de A_0 ne divise i et tel qu'il existe un nombre premier p tel que $p \mid a+d$ et $p \mid a+i$.

Soit B l'ensemble des nombres premiers p de $P_{<d}$ qui n'appartiennent pas à A_0 et tels qu'il existe un $i \in C$ vérifiant $p \mid a+i$ et $p \mid a+d$ (ainsi $p \mid d-i$).

Soit A l'ensemble des nombres premiers inférieurs à $d-1$ qui n'appartiennent pas à B.

C est non vide car $1 \in C$. Ainsi B est non vide.

(i) Pour tout entier $i < d$, il existe un nombre premier p tel que p/a et $p/a+i$, ou $p/a+d$ et $p/a+i$; par différence, p divise i ou $d-i$, et donc $p \leq d-1$.

Si $i \in C$, soit $P(i)$ le plus petit nombre premier p tel que $p \mid a+d$ et $p \mid a+i$. Si $P(i) \mid i$, alors $P(i) \mid a$ et $P(i) \mid d$, et donc $P(i) \in A_0$, ce qui est absurde. Ainsi $P(i) \in B$.

Si $i \notin C$, alors :

(a) $\exists a \in A_0\ q \mid i$; ou

(b) $(a+i, a+d) = 1$.

Dans le cas (a), soit $P(i)$ le plus petit $p \in A_0$ tel que $p \mid i$. Ainsi $P(i) \in A$.

Dans le cas (b), nous avons $(a, a+i) = 1$, par définition de $NoCoprimeness$. Ainsi il existe un nombre premier p tel que $p \mid a$ et $p \mid a+i$. Si $p \in B$, il existe $i_0 \in C$ tel que $p \mid a+i_0$ et $p \mid a+d$, ainsi $p \mid d$ et $p \mid a$; nous avons $p \in A_0$, contraire à la définition de B. Ainsi $p \in A$.

Soit $P(i)$ le plus petit tel nombre premier.

(ii) Si $P(i) \in B$ alors $P(i) \notin A_0$, $P(i) \mid a+i$ et $P(i) \mid a+d$. Donc $P(i) \mid a+i+P(i)$ et $P(i) \mid a+d$, d'où $i+P(i) \in C$. Nous avons $P(i+P(i)) = P(i)$ puisque nous avons choisi le plus petit nombre premier vérifiant une certaine condition.

Les ensembles A et B sont non vides pour les raisons expliquées dans la proposition 1.

Condition suffisante Considérons l'ensemble de conditions :

$a \equiv 0\ [p]$ pour $p \in A$,

$a + i \equiv 0\ [p]$ pour $p \in B$ et un entier i correspondant (celui qui est choisi n'est pas important d'après la condition (ii)).

On utilise le théorème des restes chinois pour trouver un entier a qui convient. □

Corollaire 1.- *AmplitudeNoCoprime est récursif.*

Notation.- Pour un entier naturel n, notons $\pi\pi(n)$ le produit des nombres premiers inférieurs à n. Nous avons, par exemple : $\pi\pi(1) = 1$, $\pi\pi(2) = 2$, $\pi\pi(3) = 6$, $\pi\pi(5) = 30$.

Corollaire 2.- *Si $d \in AmplitudeNoCoprime$ alors le plus petit a tel que :*

$$NoCoprimeness(a, d)$$

vérifie $a \leq \pi\pi(d-1)$.

Le deuxième corollaire nous donne une autre méthode pour trouver de tels d.

4 Calculs et problèmes ouverts

Application.- Un programme en langage C donne le début de l'ensemble *AmplitudeNoCoprime*:

{16, 22, 34, 36, 46, 56, 64, 66, 70, 76, 78, 86, 88, 92, 94, 96, 100, 106, 112, 116, 118, 120, 124, 130, 134, 142, 144, 146, 154, 160, 162, 186, 190, 196, 204, 210, 216, 218, 220, 222, 232, 238, 248, 250, 256, 260, 262, 268, 276, 280, 286, 288, 292, 296, 298, 300, 302, 306, 310, 316, 320, 324, 326, 328, 330, 336, 340, 342, 346, 356, 366, 372, 378, 382, 294, 396, 400, 404, 406, 408, 414, 416, 424, 426, 428, 430, 438, 446, 454, 456, 466, 470, 472, 474, 476, 484, 486, 490, 494, 498, 512, 516, 518, 520, ... }.

Sur les éléments impairs de AmplitudeNoCoprime.- Comme nous l'avons déjà dit, Dowe ([DOW,89]) a trouvé un sous-ensemble infini de *AmplitudeNoCoprime*, chaque élément de celui-ci étant pair. Il conjectura alors que tout élément de *AmplitudeNoCoprime* est pair, ce que semble confirmer le résultat ci-dessus. Marcin Bienkowski, Mirek Korzeniowski et Krysztof Lorys, de l'université de Wroclaw (Pologne), ont trouvé les contre-exemples d = 903 et d = 2545 par calcul ([B-K,01]), par une méthode différente ce celle donnée ci-dessus, puis une méthode générale pour engendrer d'autres exemples ([LOR,01]) : 4533, 5067, 8759, 9071, 9269, 10353, 11035, 11625, 11865, 13629, 15395, ... Nik Lygeros, de l'université Lyon 1, a trouvé indépendamment le contre-exemple d = 903, en précisant a = 9522262 6669542934 3821381424 8428848908 8652426153 5943535745 4655023337 6559616611 8590972022 0963272377 1706584855 8346 243755 6704487000 8254825237 2177729811 3684783645 9948140782 2255756088 3686154164 4378245545 4341250989 5747350810 8457570482 4410159674 0520 09775 3981676715 6709443841 8310762640 9084843313 5776815310 93717028660

1167977288 9225337579 8305738503 033846246 769704747 450128124 100053 617 ; il en a trouvé d'autres (d = 907 et 909), ce qui montre que la condition suffisante de [LOR,01] n'est pas nécessaire. Lors de recherches bibliographiques, Nik Lygeros a découvert que la solution d = 903 avait déjà été trouvée par Erdös et Seldfridge trente ans avant ([E-S,71]).

Sur les carrés pairs de AmplitudeNoCoprime.- L'examen de la liste donnée ci-dessus montre que chaque carré pair (hormis 4) apparaît au début de `AmplitudeNoCoprime`. Cependant $676 = 26 \times 26$, $1156 = 34 \times 34$ ([LYG,01a] et $1024 = 32 \times 32$ ([VSE,01]) ne sont pas des éléments de `AmplitudeNoCoprime`.

Sur les nombres premiers éléments de AmplitudeNoCoprime.- Un nombre premier peut être élément de `AmplitudeNoCoprime`, comme le montrent 15 493 et 18 637 ([LYG,01b]).

La liste ci-dessus suggère un grand nombre de problèmes ouverts, semblables à ceux qui concernent l'ensemble des nombres premiers.

Dans la caractérisation combinatoire de *AmplitudeNoCoprime*, une variante du programme montre que l'on a toujours $P(2) = 2$ pour d pair, et donc que 2 divise a. The solution $< a, 2545 >$, avec le a de Nik Lygeros, montre que ceci n'est pas le cas pour d pair. Est-ce une propriété générale ?

PROBLÈME OUVERT 1 *Pour un d pair, est-ce que tout élément a tel que NoCoprimeness(a,d) est pair ?*

Nous pouvons remarquer un grand nombre de *nombres jumeaux* dans l'ensemble *AmplitudeNoCoprime* : 34 et 36, 64 et 66, 76 et 78, 86 et 88, 92 et 94, ...

PROBLÈME OUVERT 2 *Existe-t-il une infinité d'entiers d tel que d et $d+2$ appartenant à AmplitudeNoCoprime ?*

Nous avons en fait aussi des suites de trois entiers pairs consécutifs (telle que 92, 94, 96), quatre entiers pairs consécutifs (telle que 216, 218, 220, 222).

PROBLÈME OUVERT 3 *Existe-t-il, pour tout entier k, un entier (pair) d tel que d, $d+2$, $d+4$, ... , $d+2.k$ appartiennent à AmplitudeNoCoprime ?*

Laissons là la recherche des motifs dans *AmplitudeNoCoprime* (il y a bien d'autres questions à se poser à ce propos) et passons à des questions de complexité. Remarquons tout d'abord que notre algorithme pour décider si un entier appartient à *AmplitudeNoCoprime* est pire qu'exponentiel.

PROBLÈME OUVERT 4 *À quelle classe de complexité AmplitudeNoCoprime appartient-il ?*

PROBLÈME OUVERT 5 *Trouver une borne inférieure pour AmplitudeNoCoprime.*

Notons $d(n)$ le n-ième élément de *AmplitudeNoCoprime* : $d(0) = 16$, $d(1) = 22$, $d(2) = 34$, ...

PROBLÈME OUVERT 6 *Quelle est la complexité (de Kolmogorov) de la suite* $d \mapsto d(n)$ *?*

Nous pouvons aussi poser des questions *à la* Vallée-Poussin–Hadmard.

PROBLÈME OUVERT 7 *Trouver une fonction (simple)* f *telle que :*

$$d(n) \sim f(n).$$

Passons maintenant à la densité de l'ensemble *AmplitudeNoCoprime*. Notons $\rho(n)$ le cardinal de l'ensemble $\{ d \leq n \mid AmplitudeNoCoprime(d) \}$.

PROBLÈME OUVERT 8 *La densité de AmplitudeNoCoprime est-elle linéaire ? Plus précisément :*

$$\rho(n) = O(n) \ ?$$

Peut-être :

$$\frac{\rho(n)}{n} \to \frac{1}{4}$$

La plupart des problèmes énoncés ci-dessus peuvent être résolus en répondant positivement aux problèmes suivants d'arithmétique faible.

PROBLÈME OUVERT 9 *La théorie* $Th(\mathbb{N}, NoCoprimeness, R)$ *est-elle décidable ?*

où R est une certaine relation ou fonction à spécifier (l'addition $+$ étant un candidat intéressant). À l'opposé, nous pouvons aussi chercher des théories indécidables.

PROBLÈME OUVERT 10 *La théorie* $Th(\mathbb{N}, +, AmplitudeNoCoprime)$ *est-elle déf-complète (i.e. la multiplication est-elle définissable dans la structure sous-jacente) ?*

RÉFÉRENCES

[B-K,01] Bienkowski, Marcin & Korzeniowki, Mirek, communication personnelle du 14 janvier 2001.

[DOW,89] Dowe, David L., *On the existence of sequences of co-prime pairs of integers*, **J. Austral. Math. Soc.**, Series A, vol. 47, 1989, pp. 84–89.

[E-S,71] P. Erds, J.L. Selfridge, *Complete prime subsets of consecutive integers*, **Proceedings of the Manitobe Conference on Numerical Mathematics**, pp. 1-14, 1971.

[GUY,81] Guy, Richard K., **Unolved Problems in Number Theory**, Springer, 1981, XVIII+161 p.

[LOR,01] Lorys, Krzysztof, communication personnelle du 20 janvier 2001.

[LYG,01] Lygeros, Nik, communication personnelle du 19 janvier 2001.

[LYG,01a] Lygeros, Nik, communication personnelle du 2 février 2001.

[LYG,01b] Lygeros, Nik, communication personnelle du 8 février 2001.

[VSE,01] Vsemirnov, Maxim, communication personnelle du 8 février 2001.

[WOO,81] Woods, Alan R., **Some problems in logic and number theory, and their connections**, Ph.D. thesis, University of Manchester, 1981.