Available at
www.ComputerScienceWeb.com
POWERED BY SCIENCE DIRECT®

Theoretical Computer Science 303 (2003) 53–62

Theoretical Computer Science

www.elsevier.com/locate/tcs

On the amplitude of intervals of natural numbers whose every element has a common prime divisor with at least an extremity

Patrick Cégielski[a,*], François Heroult[b], Denis Richard[b]

[a]Laboratoire d'Algorthmique, Complexité et Logique (LACL) Université Paris 12 (IUT), Route forestière Hurtault, F-77300 Fontainebleau, France

[b]Laboratoire de Logique, Algorithmique et Informatique de Clermont I (LLAIC1) I.U.T. Informatique, Université d'Auvergne, B.P. 86, F-63172 Aubière Cedex, France

Abstract

An interval $[a, a+d]$ of natural numbers verifies the property of no coprimeness if and only if every element $a+1, a+2, \ldots, a+d-1$ has a common prime divisor with extremity a or $a+d$. We show the set of such a and the set of such d are recursive. The computation of the first d leads to rise a lot of open problems.

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 $a+1, a+2, \ldots, a+d-1$, n'est premier avec les deux extrémités a et $a+d$ à la fois. Nous montrons que l'ensemble des tels a et l'ensemble des tels d sont récursifs. Le calcul des premiers d conduit à poser de nombreux problèmes ouverts.

© 2002 Elsevier Science B.V. All rights reserved.

Keywords: Number theory; Recursivity; Erdős-woods; Complexity; Weak arithmetics

1. Enunciation of problems

Introduction. Many interesting problems in number theory emerge from the thesis of Alan Woods [10]. The most famous of them is now known as *Erdős-Woods conjecture*, after its publication in the book of Guy [4]. It is

* Corresponding author.
E-mail addresses: cegielski@univ-paris12.fr (P. Cégielski), richard@llaic.univ-bpclermont.fr (D. Richard).
URL: http://www.univ-paris12.fr/lacl/cegielski

0304-3975/03/$ - see front matter © 2002 Elsevier Science B.V. All rights reserved.
PII: S0304-3975(02)00444-9

Erdős-Woods conjecture. *There exists an integer k such that integers x and y are equal if and only if for $i = 0 \dots k$, integers $x + i$ and $y + i$ have same prime divisors.*

This problem is a source of an active domain of research.

In relation with this problem, Alan Woods had conjectured [10, p. 88] that for any ordered pair $\langle a, d\rangle$ of natural numbers, with $d \geqslant 3$, there exists a natural number c such that $a < c < a + d$ and c is coprime with a and with $a + d$. In other words:

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

where we denote by $\perp$ the coprimality predicate, notation introduced by Julia Robinson. Also, sometimes, we shall use the most traditional notation $(a, c) = 1$.

Very quickly, he realized the conjecture is false, finding the counterexample $\langle 2184, 16\rangle$ (published in [2]). In 1987, David Dowe proved in [2] that there exist infinitely many such numbers d. We call **Erdős-Woods numbers** such numbers d.

The main aim of this paper is to prove that the set of Erdős-Woods numbers is recursive. A second aim is to give the first values of Erdős-Woods numbers and to show there is a lot of natural open problems concerning these numbers.

Notation. Let us denote by $NoCoprimeness(a, d)$ the property:

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

Let begin by some remarks.

Remarks. (1) *The relation $NoCoprimeness(a, d)$ is recursive*: it is easy to write a program to see whether an ordered pair belongs to it.

(2) *The set $\{\langle a, d\rangle / NoCoprimeness(a, d)\}$ is infinite.*

We know an element $\langle 2184, 16\rangle$ of this set. It is easy to show that for every $k \geqslant 0$, the ordered pair

$$\left\langle 2184 + k \prod_{\substack{p \in \mathbb{P} \\ p \leqslant 16}} p, 16 \right\rangle$$

is also an element of this set, where $\mathbb{P}$ denotes the set of primes.

(3) *The two unary relations, projections of $NoCoprimeness(a, d)$, defined by*

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

$$AmplitudeNoCoprime(d) \quad \textit{iff} \quad \exists a NoCoprimeness(a, d)$$

are recursively enumerable: it is easy to write a program to list elements of these sets (but not in natural order, unfortunately).

Our main aim is to prove these relations are recursive. Before this, let us prove two properties.

Proposition 1. *If $d \in AmplitudeNoCoprime$, there exist two primes dividing $d-1$.*

Proof. Let d be an element of $AmplitudeNoCoprime$. Let a be an integer such that $NoCoprimeness(a,d)$. We have $a \perp a+1$ hence $\neg(a+1 \perp a+d)$. There exists a prime p such that $p \mid a+1$ and $p \mid a+d$, and p divides the difference $d-1$.

Symmetrically, there exists a prime q dividing a, $a+d-1$, and $d-1$. The primes p and q are different because p does not divide a. □

Corollary 1. *If $d \in AmplitudeNoCoprime$, then $d \geqslant 7$.*

Corollary 2. *$\mathbb{N} \setminus AmplitudeNoCoprime$ is infinite.*

Proof. The claim holds because 2^n+1 belongs to this set for any natural number n. More generally, this is true for p^n+1 for any prime p. □

2. Recursivity of ExtremNoCoprime

Recursivity of *ExtremNoCoprime* is a consequence of the following result.

Proposition 2. *For any integers a and d such that $NoCoprimeness(a,d)$, we have*

$$d < a.$$

Proof. If $a \leqslant d$, there exists a prime number p_0 such that

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

using the Bertrand–Chebychev Theorem. Then

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

There exists a prime number q such that
(i) $q \mid p_0$ *and* $q \mid a$; or
(ii) $q \mid p_0$ *and* $q \mid a+d$.

In both cases, $q \mid p_0$ hence $q = p_0$.

In case (i), we have $p_0 = q \mid a$, but $a < p_0$, which is a contradiction.

In case (ii), we have $q \mid d - (p_0 - a)$, but

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

then

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

which is a contradiction. □

Corollary. *The set ExtremNoCoprime is recursive.*

Proof. Corollary results of the fact that, for a given number a, it is sufficient to test whether we have property $NoCoprimeness(a,d)$ for the finite number of d such that $d<a$. □

We will see later (Section 5.2) that the first values of *ExtremNoCoprime* are big integers. Since it is difficult for a human being to guess properties of a set of big integers, we cannot formulate natural questions about the set *ExtremNoCoprime*. We will see that the situation is different for *AmplitudeNoCoprime*.

3. Recursivity of AmplitudeNoCoprime

Notation. For a positive integer n, let denote by $\pi\pi(n)$ the product of primes less than n. For instance, we have: $\pi\pi(1)=1$, $\pi\pi(2)=2$, $\pi\pi(3)=6$, $\pi\pi(5)=30$.

Proposition 3. *If $d \in AmplitudeNoCoprime$ then the smallest a such that*

$$NoCoprimeness(a,d)$$

verifies $a \leqslant \pi\pi(d-1)$.

Proof. Let a be a natural number such that $NoCoprimeness(a,d)$.

Let a' be the remainder of a modulo $\pi\pi(d-1)$:

$$a = q.\pi\pi(d-1) + a',$$

and $0 \leqslant a' < \pi\pi(d-1)$.

For a natural number c such that:

$$a < c < a+d,$$

let us write $c = a+i$, with $0<i<d$.

Let us prove that:

$$(a, a+i) \neq 1 \text{ iff } (a', a'+i) \neq 1.$$

If a prime p divides a and $a+i$ then p divides i, hence $p<d-1$. We deduce that p divides simultaneously a and $a+i$ iff p divides simultaneously a' and $a'+i$.

We have also:

$$(a+i, a+d) \neq 1 \text{ iff } (a'+i, a'+d) \neq 1.$$

Hence $NoCoprimeness(a,d)$ holds iff $NoCoprimeness(a',d)$ holds.

This proves the proposition. □

Corollary. *AmplitudeNoCoprime is recursive.*

4. A better algorithm to decide AmplitudeNoCoprime

In the last section we have proved that *AmplitudeNoCoprime* is recursive. Unfortunately, the algorithm associated to this proposition is not efficient for two reasons: the function $d \mapsto \pi\pi(d-1)$ is too rapidly growing hence complexity (in time) is not good and a program has to use very long integers. Indeed an approximation of $\pi\pi(n)$ is $n!$, hence we have to test on $n!$ integers of size $n\log(n)$.

In this section we give another algorithm: there is no dramatic improvement of the complexity but we may implement it with the usual integers of a standard programming language (we may use the language C, for instance, without having to implement arbitrary precision integers).

Some attempts for searching Erdős-Woods numbers led to the following combinatorial characterization of *AmplitudeNoCoprime*. Let $\langle a, d\rangle$ such that *NoCoprimeness* (a,d). For every c such that $a<c<a+d$, we have $(a,c)\neq 1$ or $(c,a+d)\neq 1$. Hence there exists a prime p such that $p\mid a$ and $p\mid c$, or $p\mid c$ and $p\mid a+d$. Let us write c as $a+i$, with $1\leqslant i<d$. Let P be a mapping from $[1,d-1]$ into $\mathbb{P}$ such that $P(i)$ is a witnessing prime. An integer d is an Erdős-Woods number iff such a mapping exists, with some extra conditions.

Proposition 4. *An integer d belongs to AmplitudeNoCoprime if and only if there exist a partition of the set $\mathbb{P}_{<d}$ of primes* (*strictly*) *less than d in two sets A and B, and a function P from* $[1,d-1]$ *on $\mathbb{P}_{<d}$ such that*:
(i) *for any integer i, $1\leqslant i<d$, if $P(i)\in A$ then $P(i)\mid i$, if $P(i)\in B$ then $P(i)\mid d-i$;*
(ii) *for $1\leqslant i<i+P(i)<d$, we have $P(i)\in B$ iff $P(i+P(i))\in B$.*

Proof. *Necessity of condition* (i), (ii): Let
- d be an element of *AmplitudeNoCoprime*;
- a be a natural number such that *NoCoprimeness*(a,d);
- A_0 denote the set of primes dividing a and d;
- C denote the set of integer i, $1\leqslant i<d$, such that no prime of A_0 divides i and there exists a prime p such that $p\mid a+d$ and $p\mid a+i$;
- B denote the set of primes p of $\mathbb{P}_{<d}$ not in A_0 such that there exists an $i\in C$ verifying $p\mid a+i$ and $p\mid a+d$ (hence $p\mid d-i$);
- A be the set of primes less than $d-1$ who do not belong to B.

C is not empty because $1\in C$. Hence B is not empty.
(i) For any integer $i<d$, there exists a prime p such that $p\mid a$ and $p\mid a+i$, or $p\mid a+d$ and $p\mid a+i$; by difference, p divides i or $d-i$, hence $p\leqslant d-1$.

If $i\in C$, let $P(i)$ be the smallest prime p such that $p\mid a+d$ and $p\mid a+i$. If $P(i)\mid i$ then $P(i)\mid a$ and $P(i)\mid d$, hence $P(i)\in A_0$, absurd. Hence $P(i)\in B$.

If $i\notin C$, then:
(a) $\exists q\in A_0$ such that $q\mid i$; or
(b) $(a+i,a+d)=1$.

In case (a), let $P(i)$ the smallest $p \in A_0$ such that $p \mid i$. Hence $P(i) \in A$.

In case (b), we have $(a, a+i) \neq 1$, by definition of *NoCoprimeness*. Hence there exists a prime p such that $p \mid a$ and $p \mid a+i$. If $p \in B$, there exists $i_0 \in C$ such that $p \mid a+i_0$ and $p \mid a+d$, hence $p \mid d$ and $p \mid a$; we have $p \in A_0$, contrary to definition of B. Hence $p \in A$.

Let $P(i)$ the smallest such prime.

(ii) If $P(i) \in B$ then $P(i) \notin A_0$, $P(i) \mid a+i$, and $P(i) \mid a+d$. Hence $P(i) \mid a+i+P(i)$ and $P(i) \mid a+d$, hence $i+P(i) \in C$. We have $P(i+P(i)) = P(i)$ because we have chosen the smaller prime verifying a certain condition.

The sets A and B are nonempty by Proposition 1.

Sufficiency of condition (i), (ii): Consider the set of conditions:

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

$a+i \equiv 0\ [p]$ for $p \in B$ and every corresponding integer i.

We use the theorem of Chinese remainders to find an integer a which is suitable: for a given p, we have many integers i such that $a+i \equiv 0\ [p]$ but the condition of compatibility (ii) shows it is not important. □

5. Computations, applications, and open problems

The main part of our paper (Sections 2 and 3) consists of proofs that the sets *ExtremNoCoprime* and *AmplitudeNoCoprime* are recursive. In this section we report on the computation of the first elements of *AmplitudeNoCoprime*, which leads to interesting remarks.

The cited results (with *personal communication* label) are not published. Dates given here are important for priority reasons. The reference to the Erdős-Woods sequence in *The On-Line Encyclopedia of Integer Sequences*:

`http://www.research.att.com/ njas/sequences/`

is a good location to follow works in progress.

5.1. First elements of AmplitudeNoCoprime

Proposition 4 allows to implement an algorithm (in language C) to compute first elements of *AmplitudeNoCoprime*. The algorithm is not very efficient, but it allows to test quickly the first six hundred integers. We obtain the beginning of the set *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, 246, 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, 394, 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, 526, 528, 532, 534, 536, 538, 540, 546, 550, 552, 554,
556, 560, 574, 576, 580, 582, 584, 590, 604, 606, 612, 616...}.

5.2. About some patterns in AmplitudeNoCoprime

Immediately we remark some patterns in *AmplitudeNoCoprime*, more exactly in the beginning of this set. We ask about the appearance of these patterns in the full set. Here we report on the state of art at our knowledge, without proofs: counterexamples are not found by a simple application of the above algorithm, its complexity does not allow it.

On odd elements of AmplitudeNoCoprime: Dowe [2] has found an infinite subset of *AmplitudeNoCoprime*, every element being even. He conjectures every element of *AmplitudeNoCoprime* is even. Marcin Bienkowski, Mirek Korzeniowski, and Krysztof Lorys, from Wroclaw University (Poland), have found the counterexamples $d=903$ and 2545 by computation [1], then a general method to generate many other examples [5]: 4533, 5067, 8759, 9071, 9269, 10353, 11035, 11625, 11865, 13629, 15395, ... Nik Lygeros, from Lyon 1 University (France), independently has found the counterexample $d=903$, making precise [6] the related extremity:

$$\begin{aligned}a = 9\ 522\ 262\ 666\ 954\ 293\ 438\ 213\ 814\ 248\ 428\ 848\ 908\ 865\ 242\ 615\ 359\\ 435\ 357\ 454\ 655\ 023\ 337\ 655\ 961\ 661\ 185\ 909\ 720\ 220\ 963\ 272\ 377\ 170\\ 658\ 485\ 583\ 462\ 437\ 556\ 704\ 487\ 000\ 825\ 482\ 523\ 721\ 777\ 298\ 113\ 684\\ 783\ 645\ 994\ 814\ 078\ 222\ 557\ 560\ 883\ 686\ 154\ 164\ 437\ 824\ 554\ 543\ 412\\ 509\ 895\ 747\ 350\ 810\ 845\ 757\ 048\ 244\ 101\ 596\ 740\ 520\ 097\ 753\ 981\ 676\\ 715\ 670\ 944\ 384\ 183\ 107\ 626\ 409\ 084\ 843\ 313\ 577\ 681\ 531\ 093\ 717\ 028\\ 660\ 116\ 797\ 728\ 892\ 253\ 375\ 798\ 305\ 738\ 503\ 033\ 846\ 246\ 769\ 704\ 747\\ 450\ 128\ 124\ 100\ 053\ 617.\end{aligned}$$

He found other ones ($d=907$ and 909), proving that the sufficient condition of [5] is not necessary. Also he discovers that the solution $d=903$ is an old result from Erdős and Seldfridge [3].

On even squares of AmplitudeNoCoprime: We see, in scanning the above list, that every even square but 4 appears at the beginning. However $676=26\times 26$, $1156=34 \times 34$ [7] and $1024=32\times 32$ [9] are not Erdős-Woods numbers.

On prime elements of AmplitudeNoCoprime: An Erdős-Woods number may be a prime number as 15 493 and 18 637 show it [8].

5.3. Open problems

The above list of first elements of *AmplitudeNoCoprime* suggests a great number of open problems, curiously similar to problems for the set of primes.

We may implement a program to compute, for an Erdős-Woods number d, the smallest associated extremity a. Numerical experiments suggest that $2 \mid a+1$ whenever the amplitude d is even, hence 2 divides a. Is it a general property?

The solution $\langle a, 903\rangle$, with the a found by Nik Lygeros, shows it is not the case for d odd.

Open problem 1 (Even extremity for even amplitude). *For an even d, is every element a such that*

$$NoCoprimeness(a, d)$$

even?

We may note we have a great number of *twin Erdős-Woods numbers* among the first elements of *AmplitudeNoCoprime*: 34 and 36, 64 and 66, 76 and 78, 86 and 88, 92 and 94,...

Open problem 2 (Infinity of twin Erdős-Woods numbers). *There exists an infinity of integers d such that d, $d+2$ belongs to AmplitudeNoCoprime.*

Indeed we also have a sequence of three consecutive even Erdős-Woods numbers (as 92, 94, 96), even four consecutive ones (as 216, 218, 220, 222).

Open problem 3 (Polignac's conjecture for Erdős-Woods numbers). *For any integer k, there exists an even integer d such that $d, d+2, d+4, \ldots, d+2.k$ belong to AmplitudeNoCoprime.*

Nik Lygeros is searching segments of consecutive natural numbers which are not Erdős-Woods numbers. He has found long such segments.

Open problem 4. *There exists segments of any length without elements of AmplitudeNoCoprime*:

$$\forall k,\ \exists e[e, e+1, \ldots, e+k \notin AmpitudeNoCoprime].$$

Passing from patterns in *AmplitudeNoCoprime* to complexity, we may remark the algorithm we have given to decide whether an integer belongs to *AmplitudeNoCoprime* is worst than exponential. It is interesting to improve it if it is possible.

Open problem 5 (Complexity of AmplitudeNoCoprime). *To which complexity classes does AmplitudeNoCoprime belong*?

Open problem 6. *Find a lower bound for AmplitudeNoCoprime.*

Let denote by $d(n)$ the nth number of *AmplitudeNoCoprime*: $d(0)=16$, $d(1)=22$, $d(2)=34,\ldots$

Open problem 7. *What is the* (*Kolmogorov*) *complexity of the sequence* $n \mapsto d(n)$?

Also we may ask for questions *à la* Vallée-Poussin–Hadamard.

Open problem 8. *Find a* (*simple*) *function* f *such that*

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

Passing from the complexity to the density of the set *AmplitudeNoCoprime*, let denote by $\rho(n)$ the cardinality of the set $\{d \leqslant n \mid AmplitudeNoCoprime(d)\}$.

Open problem 9. *Is the density of AmplitudeNoCoprime linear*? *More precisely*

$$\rho(n) = \mathrm{O}(n)?$$

The last open problems we propose concern Logic, more precisely Weak Arithmetics. Problems of definability and decidability are important: Presburger's proof of decidability for the elementary theory of $\langle \mathbb{N}, + \rangle$ implies that a set $X \subset \mathbb{N}$ is definable in $\langle \mathbb{N}, + \rangle$ iff X is ultimately periodic; the negative solution given by Matiyasevich to Hilbert's Tenth Problem relies on the fact that exponentiation function is existentially definable in $\langle \mathbb{N}, +, \bullet \rangle$. In the same way, the following problems deserve consideration.

Open problem 10. *Is the theory* $Th(\mathbb{N}, NoCoprimeness, R)$ *decidable*? *where R is some relation or function to specify* (*the addition* $+$ *is an interesting candidate*).

At the opposite, we may search for undecidability.

Open problem 11. *Is the theory* $Th(\mathbb{N}, +, AmplitudeNoCoprime)$ *def-complete* (*i.e. is multiplication definable in the underlying structure*)?

Acknowledgements

Authors thank referees for suggestions to improve this paper.

References

[1] M. Bienkowski, M. Korzeniowki, personal communication, January 14, 2001.
[2] D.L. Dowe, On the existence of sequences of co-prime pairs of integers, J. Austral. Math. Soc. Series A 47 (1989) 84–89.
[3] P. Erdős, J.L. Selfridge, Complete prime subsets of consecutive integers, Proc. Manitobe Conf. on Numerical Mathematics, 1971, pp. 1–14.
[4] R.K. Guy, Unsolved Problems in Number Theory, Springer, Berlin, 1981, XVIII+161pp.

[5] K. Lorys, personal communication, January 20, 2001.
[6] N. Lygeros, personal communication, January 18, 2001.
[7] N. Lygeros, personal communication, February 2, 2001.
[8] N. Lygeros, personal communication, February 8, 2001.
[9] M. Vsemirnov, personal communication, February 8, 2001.
[10] A.R. Woods, Some problems in logic and number theory, and their connections, Ph.D. Thesis, University of Manchester, 1981.