Tatra Mt. Math. Publ. **32** (2005), 15–32

TATRA MOUNTAINS
Mathematical Publications

ON A PROBLEM OF H. J. A. DUPARC

Andrzej Paszkiewicz — Andrzej Rotkiewicz

ABSTRACT. In this paper we restrict the number of possible exceptions for which the problem of Duparc may not have positive answer.

We support our considerations by results of numerical computations.

1. Formulation of the problem and its solution

During the International Congress of Mathematicians in Stockholm in 1962 H. J. A. Duparc put forward the following problem:

Let p be a prime number and a and b positive integers not divisible by p. Do there exist infinitely many composite integers n divisible by p such that $n \mid a^{n-1} - b^{n-1}$?

A composite number n is called a *pseudoprime* if $n \mid 2^n - 2$. The smallest pseudoprime number is $341 = 11 \cdot 31$. In the paper [6] it was proved that for every prime p there exist infinitely many composites n such that $n \mid 2^n - 2$ and $p \mid n$ and that for every $s \geqslant 3$ and every prime p there exists a pseudoprime divisible by p which is a product of s different prime factors.

In the paper [3] the following theorem was proved

Given natural numbers a, b and s such that $a > b$ and $(a, b) = 1$, there exist infinitely many composite integers n each the product of exactly s distinct primes, such that $n \mid a^{n-1} - b^{n-1}$.

The numbers n such that $n \mid a^{n-1} - b^{n-1}$ are called *pseudoprimes to bases a and b* [8]. In the paper [7] the second author solved Duparc's problem for $p > 3$ by proving:

Theorem 1. *For every prime $p > 3$ and all a, b, not divisible by p there are infinitely many n such that*

$$p \mid n \quad \text{and} \quad n \mid a^{n-1} - b^{n-1} . \tag{1}$$

2000 Mathematics Subject Classification: Primary: 11A07; Secondary: 11-04.
Keywords: pseudoprime, pseudoprimes to bases a and b, primitive prime factors, Carmichael numbers.

Here we shall prove the following

Theorem 2. *For $p = 2$ and $p = 3$ the problem of Duparc has a positive answer with the following possible exceptions (with $a > b$):*

a) $p = 2$, $b = a - 2$, *a is a positive integer greater than* 512,

b) $p = 3$, $a = 3 \cdot 2^{\alpha} + 1$, $b = 3 \cdot 2^{\alpha} - 1$, $\alpha \equiv 2 \pmod 5$, $\alpha > 2556$.

For simplicity of our further consideration we substitute $a := a + 2$ and $b := a$. In the paper [5] it was proved that for every $a < 13$, $a \neq 4, 8$ and every $s \geqslant 3$ there exists an even number n, which is a product of s different prime factors and $n \mid (a+2)^{n-1} - a^{n-1}$. Let a and b be natural numbers such that $2 \mid a - b$ and $a - b \geqslant 4$ then there exist infinitely many even numbers n such that $n \mid a^{n-1} - b^{n-1}$ (see [4]). Before giving a proof for Theorem 2, we shall state the following

Theorem 3. *For every natural $a \leqslant 512$ and every natural number $s \geqslant 4$, there exists an even natural number n which is a product of s different prime factors and*

$$n \mid (a+2)^{n-1} - a^{n-1}. \tag{2}$$

P r o o f. As we can see from Tables 1, 2, and 3 our theorem is true for $s = 3$ or $s = 4$ and all $a \leqslant 512$. (Factors of the numbers n are not given explicitly in the Table 4 but for each number n in the Table 4, we checked the number of its factors). In these tables we consider $2n$ instead of n because n in the Theorem 3 is even. Suppose that Theorem 3 is true for all $a \leqslant 512$ and n's which are products of exactly $s \geqslant 4$ factors. Let a and n be natural numbers for which the relation (2) holds, and $1 \leqslant a \leqslant 512$, n consists of exactly s factors. We shall construct a new natural number consisting of exactly $s+1$ factors for which the relation (2) holds.

By theorem of Z s i g m o n d y [9] there exists a primitive prime factor p of the number

$$a_1^{n-1} - b_1^{n-1},$$

where $a_1 = \frac{a+2}{(a+2,a)}$, $b_1 = \frac{a}{(a+2,a)}$, such that $n - 1 \mid p - 1$.

We have $np - 1 = (p-1)n + n - 1$ and $p \mid a_1^{n-1} - b_1^{n-1} \mid a_1^{np-1} - b_1^{np-1} \mid (a+2)^{np-1} - a^{np-1}$. From $n-1 \mid p-1$ it follows $n \leqslant p$, hence $n < p$, since n is a product of $s \geqslant 3$ prime factors. Thus $n \mid (a+2)^{n-1} - a^{n-1} \mid (a+2)^{np-1} - a^{np-1}$, $p \mid (a+2)^{np-1} - a^{np-1}$, hence $np \mid (a+2)^{np-1} - a^{np-1}$. For the number np the relation (2) holds and np consists of exactly $s+1$ prime factors, so the proof by induction is completed. □

Now we are ready to give a proof of the Theorem 2.

P r o o f o f t h e T h e o r e m 2. The first case $p = 2$ follows from the Theorem 3. Now we shall consider the special case of Duparc's problem for $p = 3$ in which

$$3n \mid a^{3n-1} - b^{3n-1} \text{ and } 3 \nmid ab, \text{ and } 2 \nmid n, \qquad (a, b) = 1 . \tag{3}$$

Since $(3, ab) = 1$ we have $3 \mid a^2 - b^2$. If $9 \mid a^2 - b^2$ then (3) holds for $n = 3$ and we denote by q a primitive prime factor of $a^8 - b^8$. Such a q exists by theorem of Z s i g m o n d y [9] and we have $q = 8l + 1 > 9$ and $9q - 1 = 9(8l + 1) - 1$, hence $8 \mid 9q - 1$, $9q \mid a^8 - b^8 \mid a^{9q-1} - b^{9q-1}$. If $a^2 - b^2 = 3A$, $(A, 3) = 1$ let $q > 3$ denote a prime factor of A. We have $q \mid a^2 - b^2$, $(q, 3) = 1$, hence $3q \mid a^{3q-1} - b^{3q-1}$.

Let now $a^2 - b^2 = 2^\alpha \cdot 3$. If $\alpha = 0$, $a^2 - b^2 = 3$, then $a = 2$, $b = 1$ and $n \mid 2^{n-1} - 1$, for $n = 3 \cdot 11 \cdot 19$. If $\alpha = 1$ then $a^2 - b^2 = 6$, which is impossible. If $\alpha > 1$ then

a) $a - b \equiv 0 \pmod 3 \Rightarrow a - b \equiv 0 \pmod 6 \Rightarrow 6 \mid a^5 - b^5$.

b) $a - b \not\equiv 0 \pmod 3 \Rightarrow a - b = 2$ or $a - b = 2^{\alpha-1}$.

If $a - b = 2$, $a^2 - b^2 = 2^\alpha \cdot 3$, then $a - b = 2$, $a + b = 2^{\alpha-1} \cdot 3$. If $\alpha = 2$ then $a - b = 2$, $a + b = 6$, $a = 4$, $b = 2$, which is impossible since $(a, b) = 1$. If $\alpha > 2$, $a - b = 2$, $a + b = 2^{\alpha-1} \cdot 3$, then $a = 3 \cdot 2^{\alpha-2} + 1$, $b = 2^{\alpha-2} - 1$. If $\alpha = 3$ then $a = 5$, $b = 1$ and we can take $n = 3 \cdot 11 \cdot 17$. We have $a = 3 \cdot 2^\alpha + 1$, $b = 3 \cdot 2^\alpha - 1$. If $\alpha \not\equiv 2 \pmod 5$ we can take $n = 3 \cdot 11 \cdot 17$ since for $\alpha \not\equiv 2 \pmod 5$ we have $11 \nmid 3 \cdot 2^\alpha \pm 1$, $17 \nmid 3 \cdot 2^\alpha \pm 1$ and $3 \nmid 3 \cdot 2^\alpha \pm 1$.

Thus Theorem 2 is completely proved for $\alpha \not\equiv 2 \pmod 5$. Observing Table 4 we see that

$$3n \mid (3 \cdot 2^\alpha + 1)^{3n-1} - (3 \cdot 2^\alpha - 1)^{3n-1} \tag{4}$$

holds 63 times on 104 cases for the number $n = 1457 = 31 \cdot 47$, for which $3n - 1 = 2 \cdot 5 \cdot 19 \cdot 23$. It is easy to see that the difference $(3 \cdot 2^\alpha + 1)^{2 \cdot 5 \cdot 19 \cdot 23} - (3 \cdot 2^\alpha - 1)^{2 \cdot 5 \cdot 19 \cdot 23}$ is divisible by 3 and 31. Divisibility by 3 is obvious because we have difference between squares of two numbers, both not divisible by 3. Divisibility by 31 should be explained. We have $3 \cdot 2^{5k+2} + 1 \equiv 13 \pmod{31}$, $3 \cdot 2^{5k+2} - 1 \equiv 11 \pmod{31}$, $13^5 - 11^5 \equiv 0 \pmod{31}$ hence $(3 \cdot 2^\alpha + 1)^{2 \cdot 5 \cdot 19 \cdot 23} - (3 \cdot 2^\alpha - 1)^{2 \cdot 5 \cdot 19 \cdot 23} \equiv 0 \pmod{31}$. We show now restrictions for the divisibility by 47. It is easy to see that the exponent $3n - 1 = 2 \cdot 5 \cdot 19 \cdot 23$ is divisible by $\varphi(47) = 46$, where φ is Euler's totient function. By Fermat's Little Theorem if both numbers $3 \cdot 2^{5k+2} + 1$ and $3 \cdot 2^{5k+2} - 1$ are not divisible by 47, then their 46th powers are equal to 1 (mod 47) and the difference $(3 \cdot 2^{5k+2} + 1)^{46} - (3 \cdot 2^6 - 1)^{46}$ is divisible by 47. It is easy to see that $3 \cdot 2^{5k+2} + 1$ is not divisible by 47. We have $3 \cdot 2^{5k+2} + 1 \equiv 2^{5k-2} + 1 \pmod{47}$ and if $47 \mid 3 \cdot 2^{5k+2} + 1$ then also $47 \mid 2^{5k-2} + 1$, hence $2^{5k-2} \equiv -1 \pmod{47}$ which is impossible because 2 is a quadratic residue mod 47. Hence only the second number $3 \cdot 2^{5k+2} - 1$ can be divisible by 47, and as a consequence

$47 \mid 2^{5k-2} - 1$. The multiplicative order of 2 mod 47 is 23, hence $5k - 2$ is a multiple of 23. Taking this into account we conclude that k has the form $k = 23t + 5$ and $5k + 2 = 115t + 27$, where t is integer. For the sequence $\alpha = 115t + 27$, $t = 0, 1, 2, \ldots$ the number $n = 1457$ does not fulfil a condition of the problem of Duparc. In this case the number $n = 737707 = 31 \cdot 53 \cdot 449$ for which $3n - 1 = 2213120 = 2^8 \cdot 5 \cdot 7 \cdot 13 \cdot 19$ is a solution of Duparc problem for most numbers in the sequence $\alpha = 115t + 27$. The least t for which (4) does not hold is equal to 22, hence the problem of Duparc has a positive solution for all $\alpha < 115 \cdot 22 + 27 = 2557$, what finishes our proof. $\square$

Examples. For $\alpha = 1$ we have $a = 7$, $b = 5$ and we can take $n = 3 \cdot 11 \cdot 17 = 561$.

For $\alpha = 2$, $a = 13$, $b = 11$ we can take $n = C_{14}^2 = 62745 = 3 \cdot 47 \cdot 89$ (14th Carmichael number and the second divisible by 3).

For $\alpha = 7$, $3 \cdot 2^\alpha + 1 = 385 = 5 \cdot 7 \cdot 11$, $3 \cdot 2^\alpha - 1 = 383$—a prime number, we can take $n = C_{114}^4 = 11921001 = 3 \cdot 29 \cdot 263 \cdot 521$. C_{114}^4 is the 114th Carmichael number and the 4th divisible by 3.

For $\alpha = 12$ we have $a = 12289$ which is a prime number, $b = 12287 = 11 \cdot 1117$ and we can take $n = C_{14}^2 = 3 \cdot 5 \cdot 47 \cdot 89$.

Theorem 4. *For every $\alpha \equiv 2 \pmod{5}$, $\alpha \leqslant 2556$, there exist infinitely many natural numbers n such that $3n \mid (3 \cdot 2^\alpha + 1)^{3n-1} - (3 \cdot 2^\alpha - 1)^{3n-1}$.*

The proof of the Theorem 4 runs in the same way as the proof of the Theorem 3.

Remark 1. An odd composite number n such that $n \mid a^n - a$ for every natural number a is called *Carmichael number*. There are infinitely many Carmichael numbers [1].

Conjecture 1. *For every natural number a not divisible by 3 there exist infinitely many Carmichael numbers n divisible by 3 and coprime with a.*

From Conjecture 1 it follows that the problem of Duparc has positive answer for $p = 3$.

Conjecture 2. *For every natural number a not divisible by odd prime p there exist infinitely many Carmichael numbers n divisible by p and coprime with a.*

From Conjecture 2 it follows that for every prime $p > 2$ and all a, b not divisible by p there are infinitely many Carmichael numbers n divisible by p such that

$$n \mid a^{n-1} - b^{n-1}.$$

2. Computational results

All computations were performed on a PC Pentium 4 computer with the clock 1.5 GHz. The whole software we developed in C++ high level programming language and compiled under Microsoft C++ compiler v. 6.0. There is extremely helpful the existence in C++ language an embedded 64 bit integer type. The computation took about 17–18 hours of non interrupted work of that computer and the results are listed in tables 1–4.

For all $a < 116$ and $p = 2$ we found all solutions n of the Duparc's problem for $n < 10^8$. For $116 \leqslant a \leqslant 512$ and $p = 2$ we determined only the least solution n of the problem. Graphs of the least solution of the Duparc's problem for $p = 2$ are illustrated on Fig. 1 and 2, respectively, in the linear and logarithmic scale. It can be seen that the least solution of the Duparc's problem is in general a small natural number, but in some cases of a it grow large. As an example it can be showed the least solution of the Duparc's problem for $a = 299$ and $p = 2$. The solution $n = 41536541$ in this case. Graphs of solutions of the Duparc's problem for $n < 10^8$ and consecutive $a = 1, 2$ are shown on Fig. 3, 4. These graphs are representative because for other a's the graphs look very similar. All computational results we collected in Tables 1–4. An interesting observation is that the number of solutions of Duparc's Problem below a given positive x grows slightly faster than logarithmically dependent on x.

Remark 2. Theorem 4 holds for all $\alpha \leqslant 2556$. All possible exceptions for which (4) may not hold are contained in the progression $115k + 27$, $k = 0, 1, 2, \ldots$

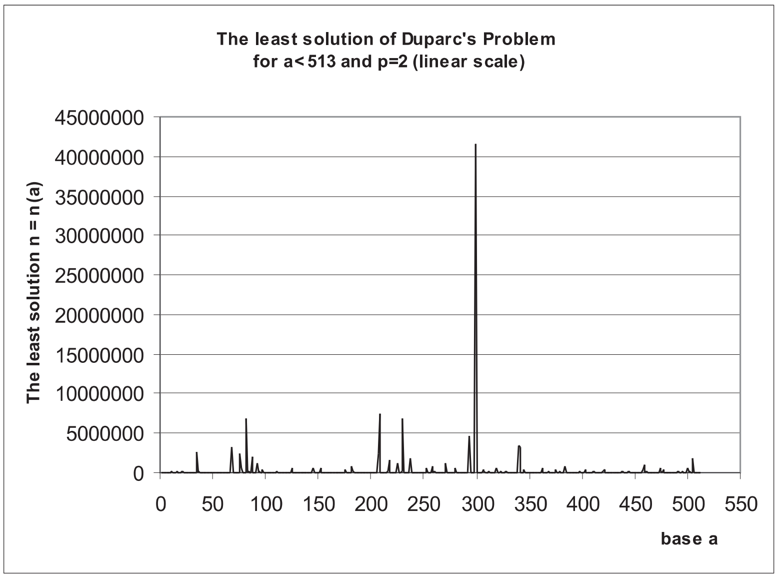

FIGURE 1. The least solution of Duparc's problem for $a < 513$ and $p = 2$.

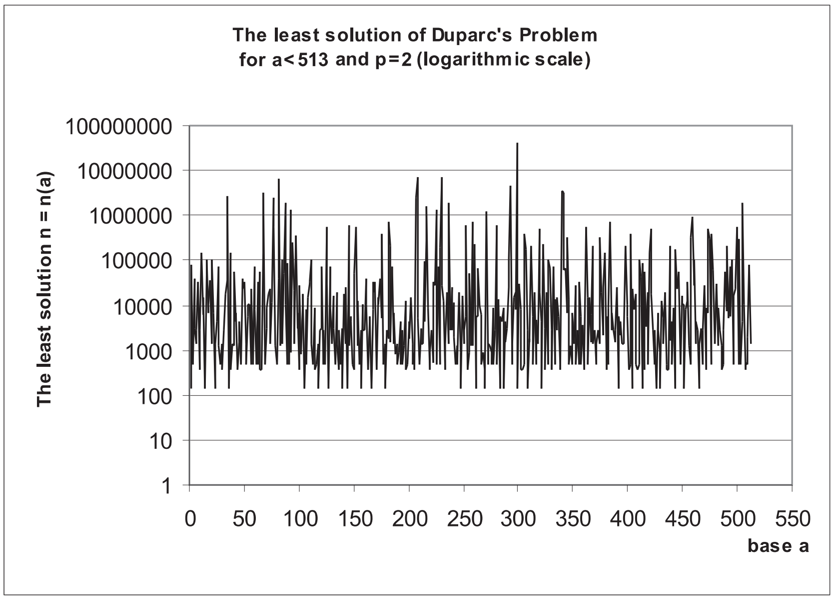

Figure 2. The least solution of Duparc's problem for $a < 513$ and $p = 2$.

Table 1. Consecutive solutions of Duparc's problem for $p = 2$ and $n < 10^8$.

Solutions of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for odd integer n below 10^8		
$a = 1$	n	Factorization of n
	143	$11 \cdot 13$ see [5]
	12023	$11 \cdot 1093$
	116363	$13 \cdot 8951$
	652223	$11 \cdot 13 \cdot 4561$
	853633	$11 \cdot 71 \cdot 1093$
	1116013	$191 \cdot 5843$
	1598903	$683 \cdot 2341$
	1961063	$13 \cdot 251 \cdot 601$
	2223491	$109 \cdot 20399$
	2801663	$313 \cdot 8951$
	2943083	$11^2 \cdot 131871$
	5061683	$11 \cdot 421 \cdot 1093$
	5084963	$13 \cdot 391151$
	6152387	$839 \cdot 7333$
	6829043	$13 \cdot 541 \cdot 971$

(Continuation) Solutions of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for an odd integer n below 10^8		
	22566863	$11^2 \cdot 421 \cdot 443$
	23883143	$1093 \cdot 21851$
	26124827	$757 \cdot 34511$
	31328063	$13 \cdot 251 \cdot 9601$
	37710563	$11 \cdot 383 \cdot 8951$
	38127023	$11 \cdot 421 \cdot 8233$
	45729563	$11 \cdot 433 \cdot 9601$
	45806123	$11^2 \cdot 83 \cdot 4561$
	48478463	$11 \cdot 601 \cdot 7333$
	54285803	$112 \cdot 13 \cdot 34511$
	69934163	$13 \cdot 601 \cdot 8951$
	75756923	$11 \cdot 1093 \cdot 6301$
$a = 2$	n	Factorization of n
	80519	$73 \cdot 1103$ see [5] and [2]
	107663	$23 \cdot 31 \cdot 151$
	1284113	$23 \cdot 31 \cdot 1801$
	1510313	$7 \cdot 359 \cdot 601$
	3933023	$23 \cdot 271 \cdot 631$
	4557713	$31 \cdot 233 \cdot 631$
	24849833	$311 \cdot 79903$
	71871113	$23 \cdot 31 \cdot 100801$
	80646143	$127 \cdot 199 \cdot 3191$
	98058097	$127 \cdot 599 \cdot 1289$
$a = 3$	n	Factorization of n
	473	$11 \cdot 43$ see [5]
	8393	$7 \cdot 11 \cdot 109$
	9713	$11 \cdot 883$
	33583	$11 \cdot 43 \cdot 71$
	68513	$131 \cdot 523$
	232243	$11 \cdot 43 \cdot 491$
	249293	$11 \cdot 131 \cdot 173$
	343613	$43 \cdot 61 \cdot 131$
	430073	$7^2 \cdot 67 \cdot 131$
	689623	$11 \cdot 71 \cdot 883$
	1037513	$293 \cdot 3541$
	1519133	$7 \cdot 11 \cdot 109 \cdot 181$
	1800293	$11 \cdot 61 \cdot 2683$
	2814053	$11 \cdot 109 \cdot 2347$
	4436873	$7 \cdot 179 \cdot 3541$
	4769083	$11 \cdot 491 \cdot 883$
	6796913	$109 \cdot 127 \cdot 491$
	7056053	$61 \cdot 131 \cdot 883$
	7152233	$11 \cdot 43 \cdot 15121$
	11545253	$311 \cdot 37123$

(Continuation) Solutions of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for an odd integer n below 10^8		
	13637579	$43 \cdot 239 \cdot 1327$
	15854333	$11 \cdot 181 \cdot 7963$
	16489253	$11 \cdot 43 \cdot 71 \cdot 491$
	20336033	$43 \cdot 71 \cdot 6661$
	25166383	$11 \cdot 883 \cdot 2591$
	37745873	$11 \cdot 43 \cdot 79801$
	47778713	$103 \cdot 131 \cdot 3541$
	53042693	$11 \cdot 43 \cdot 127 \cdot 883$
	58358273	$61 \cdot 67 \cdot 109 \cdot 131$
	58719833	$131 \cdot 173 \cdot 2591$
	83120513	$7^2 \cdot 971 \cdot 17471$
	93916193	$7^2 \cdot 431 \cdot 4447$
	94707113	$43 \cdot 67 \cdot 71 \cdot 463$
$a=4$	n	Factorization of n
	38399	$19 \cdot 43 \cdot 47$
	204551	$43 \cdot 67 \cdot 71$
	322823	$53 \cdot 6091$
	763439	$19 \cdot 23 \cdot 1747$
	1213853	$19 \cdot 29 \cdot 2203$
	1615037	$23^2 \cdot 43 \cdot 71$
	2637863	$53 \cdot 71 \cdot 701$
	2760383	$773 \cdot 3571$
	3782741	$23 \cdot 163 \cdot 1009$
	4692461	$29 \cdot 43 \cdot 53 \cdot 71$
	5068991	$19 \cdot 431 \cdot 619$
	7373279	$29 \cdot 71 \cdot 3581$
	7399123	$23^2 \cdot 71 \cdot 197$
	8001263	$23 \cdot 331 \cdot 1051$
	17302613	$101 \cdot 163 \cdot 1051$
	22332239	$19 \cdot 53 \cdot 67 \cdot 331$
	23387711	$23 \cdot 379 \cdot 2683$
	44511149	$43 \cdot 53 \cdot 19531$
	66870143	$29 \cdot 47 \cdot 71 \cdot 691$
$a=5$	n	Factorization of n
	2921	$23 \cdot 127$
	4307	$59 \cdot 73$ see [5]
	7729	$59 \cdot 131$
	53213	$127 \cdot 419$
	74447	$109 \cdot 683$
	128651	$127 \cdot 1013$
	256913	$109 \cdot 2357$
	581279	$23 \cdot 127 \cdot 199$
	763439	$19 \cdot 23 \cdot 1747$
	1159637	$23 \cdot 127 \cdot 397$

(Continuation) Solutions of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for an odd integer n below 10^8		
	1757183	$73 \cdot 24071$
	2346713	$23 \cdot 102031$
	4051427	$19 \cdot 23 \cdot 73 \cdot 127$
	4659503	$19 \cdot 127 \cdot 1931$
	5284043	$23 \cdot 31 \cdot 7411$
	10589387	$127 \cdot 199 \cdot 419$
	12726797	$23 \cdot 127 \cdot 4357$
	21125561	$127 \cdot 397 \cdot 419$
	59506043	$19 \cdot 59 \cdot 109 \cdot 487$
	61196207	$19 \cdot 419 \cdot 7687$
	73806431	$19 \cdot 73 \cdot 127 \cdot 419$
	79848203	$19 \cdot 23 \cdot 73 \cdot 2503$
	80973041	$19 \cdot 23 \cdot 127 \cdot 1459$
$a = 6$	n	Factorization of n
	1403	$23 \cdot 61$ see [5]
	7729	$59 \cdot 131$
	14617	$47 \cdot 311$
	120203	$71 \cdot 1693$
	927383	$23 \cdot 61 \cdot 661$
	1747103	$23 \cdot 37 \cdot 2053$
	3438143	$61 \cdot 157 \cdot 359$
	4397063	$11 \cdot 61 \cdot 6553$
	6562727	$37 \cdot 83 \cdot 2137$
	12081647	$23 \cdot 37 \cdot 14197$
	20858459	$47 \cdot 311 \cdot 1427$
	43321883	$11 \cdot 601 \cdot 6553$
	53401619	$37 \cdot 83 \cdot 17389$
$a = 7$	n	Factorization of n
	2831	$19 \cdot 149$ see [5]
	117683	$137 \cdot 859$
	395789	$19 \cdot 37 \cdot 563$
	513959	$193 \cdot 2663$
	1858301	$197 \cdot 9433$
	5971613	$193 \cdot 30941$
	7430693	$193 \cdot 38501$
	19443293	$31 \cdot 367 \cdot 1709$
	36640013	$53 \cdot 271 \cdot 2551$
	39926543	$19 \cdot 31 \cdot 53 \cdot 1279$
	41253557	$37 \cdot 53 \cdot 109 \cdot 193$
	54332009	$193 \cdot 197 \cdot 1429$
$a = 8$	n	Factorization of n
	33611	$19 \cdot 29 \cdot 61$
	387899	$61 \cdot 6359$
	428159	$61 \cdot 7019$

(Continuation) Solutions of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for an odd integer n below 10^8		
	2109839	$991 \cdot 2129$
	21208541	$19 \cdot 29 \cdot 61 \cdot 631$
	37721729	$61 \cdot 479 \cdot 1291$
	68078399	$29 \cdot 1459 \cdot 1609$
	73932431	$2381 \cdot 31051$
	89922619	$79 \cdot 179 \cdot 6359$
$a = 9$	n	Factorization of n
	371	$7 \cdot 53$
	5891	$43 \cdot 137$ see [5]
	29309	$7 \cdot 53 \cdot 79$
	58247	$7 \cdot 53 \cdot 157$
	72443	$7 \cdot 79 \cdot 131$ see [5]
	102383	$43 \cdot 2381$
	288113	$7 \cdot 79 \cdot 521$
	310289	$7 \cdot 19 \cdot 2333$
	321683	$43 \cdot 7481$
	372863	$571 \cdot 653$
	470807	$43 \cdot 10949$
	1808537	$43 \cdot 137 \cdot 307$
	2203793	$43 \cdot 53 \cdot 967$
	2749481	$7 \cdot 53 \cdot 7411$
	3188063	$43 \cdot 151 \cdot 491$
	4601513	$7 \cdot 53 \cdot 79 \cdot 157$
	6126683	$19 \cdot 43 \cdot 7499$
	13637579	$43 \cdot 239 \cdot 1327$
	17110373	$7 \cdot 79 \cdot 30941$
	34148303	$7 \cdot 79 \cdot 61751$
	39664103	$43 \cdot 137 \cdot 6733$
	50911613	$43 \cdot 151 \cdot 7841$
$a = 10$	n	Factorization of n
	2831	$19 \cdot 149$ see [5]
	17683	$137 \cdot 859$
	263627	$7 \cdot 13 \cdot 2897$
	355163	$29 \cdot 37 \cdot 331$
	395789	$19 \cdot 37 \cdot 563$
	554513	$311 \cdot 1783$
	1436747	$13 \cdot 29 \cdot 37 \cdot 103$
	3188633	$7 \cdot 389 \cdot 1171$
	3485417	$13 \cdot 19 \cdot 103 \cdot 137$
	4292873	$13 \cdot 71 \cdot 4651$
	9373469	$7 \cdot 37 \cdot 36191$
	9430061	$19 \cdot 149 \cdot 3331$
	10664123	$1783 \cdot 5981$
	11270363	$13 \cdot 19 \cdot 103 \cdot 443$
	13840151	$13 \cdot 19 \cdot 137 \cdot 409$

(Continuation) Solutions of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for an odd integer n below 10^8		
	15015083	$127 \cdot 191 \cdot 619$
	23910341	$7 \cdot 13 \cdot 19 \cdot 13829$
	25445963	$29 \cdot 827 \cdot 1061$
	30653753	$13 \cdot 71 \cdot 33211$
	41550593	$13 \cdot 71 \cdot 33211$
	42384563	$13 \cdot 701 \cdot 4651$
	44070593	$7 \cdot 83 \cdot 75853$
	44753189	$13 \cdot 19 \cdot 409 \cdot 443$
	49794269	$7 \cdot 19 \cdot 107 \cdot 3499$
	73778999	$7 \cdot 37 \cdot 127 \cdot 2243$
	82406363	$13 \cdot 19 \cdot 37 \cdot 71 \cdot 127$
	85226873	$37 \cdot 331 \cdot 6959$
	96160577	$19 \cdot 149 \cdot 33967$

TABLE 2. The least odd solutions n of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$

The least odd solutions n of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for $10 < a < 31$ with n having exactly two and three prime factors		
a	n_2	n_3
11	$150251 = 347 \cdot 433$	$953033 = 31 \cdot 71 \cdot 433$
12	$5969 = 47 \cdot 127$	$264947 = 53 \cdot 4999$
13	$14617 = 47 \cdot 311$	$38399 = 19 \cdot 43 \cdot 47$
14	$143 = 11 \cdot 13$	$4433 = 11 \cdot 13 \cdot 31$
15	$45371 = 59 \cdot 769$	$6364859 = 23 \cdot 127 \cdot 2179$
16	$2697833 = 743 \cdot 3631$	$107663 = 23 \cdot 31 \cdot 151$
17	$6683 = 41 \cdot 163$	$10703 = 7 \cdot 11 \cdot 139$
18	$10841 = 37 \cdot 293$	$461003 = 43 \cdot 71 \cdot 151$
19	$34829 = 29 \cdot 1201$	$5690003 = 11 \cdot 29 \cdot 17837$
20	$1043 = 23 \cdot 61$	$226493 = 47 \cdot 61 \cdot 79$
21	$103163 = 71 \cdot 1453$	$2637863 = 53 \cdot 71 \cdot 701$
22	$6683 = 41 \cdot 163$	$588473 = 31 \cdot 41 \cdot 463$
23	$143 = 11 \cdot 13$	$1463 = 7 \cdot 11 \cdot 19$
24	$1403 = 23 \cdot 61$	$107663 = 23 \cdot 31 \cdot 151$
25	$4307 = 59 \cdot 73$	$62123 = 23 \cdot 37 \cdot 73$
26	$69913 = 151 \cdot 463$	$3188063 = 43 \cdot 151 \cdot 491$
27	$1313 = 13 \cdot 101$	$28613 = 13 \cdot 31 \cdot 71$
28	$473 = 11 \cdot 43$	$298463 = 11 \cdot 43 \cdot 631$
29	$1403 = 23 \cdot 61$	$62123 = 23 \cdot 37 \cdot 73$
30	$371 = 7 \cdot 53$	$69113 = 11 \cdot 61 \cdot 103$

(Continuation) The least odd solutions n of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for $30 < a < 74$ with n having exactly two and three prime factors		
31	$2831 = 19 \cdot 149$	$906857 = 7 \cdot 353 \cdot 367$
32	$2831 = 19 \cdot 149$	$38399 = 19 \cdot 43 \cdot 47$
33	$17063 = 113 \cdot 151$	$358763 = 31 \cdot 71 \cdot 163$
34	$35179 = 127 \cdot 277$	$239063 = 11 \cdot 103 \cdot 211$
35	$2625823 = 331 \cdot 7933$	$20318603 = 127 \cdot 139 \cdot 1151$
36	$143 = 11 \cdot 13$	$4433 = 11 \cdot 13 \cdot 31$
37	$142643 = 67 \cdot 2129$	$244979 = 7 \cdot 79 \cdot 443$
38	$371 = 7 \cdot 53$	$29309 = 7 \cdot 53 \cdot 79$
39	$1403 = 23 \cdot 61$	$62843 = 11 \cdot 29 \cdot 197$
40	$1313 = 13 \cdot 101$	$198263 = 13 \cdot 101 \cdot 151$
41	$124109 = 79 \cdot 1571$	$58223 = 11 \cdot 67 \cdot 79$
42	$4307 = 59 \cdot 73$	$71231 = 19 \cdot 23 \cdot 163$
43	$6463 = 23 \cdot 281$	$395789 = 19 \cdot 37 \cdot 563$
44	$371 = 7 \cdot 53$	$29309 = 7 \cdot 53 \cdot 79$
45	$2831 = 19 \cdot 149$	$1463 = 7 \cdot 11 \cdot 19$
46	$4307 = 59 \cdot 73$	$316103 = 19 \cdot 127 \cdot 131$
47	$473 = 11 \cdot 43$	$76043 = 11 \cdot 31 \cdot 223$
48	$13970357 = 1801 \cdot 7757$	$38399 = 19 \cdot 43 \cdot 47$
49	$22723 = 31 \cdot 733$	$1576133 = 13 \cdot 31 \cdot 3911$
50	$33899 = 109 \cdot 311$	$763439 = 19 \cdot 23 \cdot 1747$
51	$1403 = 23 \cdot 61$	$77063 = 7 \cdot 101 \cdot 109$
52	$473 = 11 \cdot 43$	$14663 = 11 \cdot 31 \cdot 43$
53	$5603 = 13 \cdot 431$	$28613 = 13 \cdot 31 \cdot 71$
54	$10841 = 37 \cdot 293$	$25004363 = 131 \cdot 163 \cdot 1171$
55	$10841 = 37 \cdot 293$	$27225743 = 83 \cdot 331 \cdot 991$
56	$473 = 11 \cdot 43$	$99803 = 11 \cdot 43 \cdot 211$
57	$23797 = 53 \cdot 449$	$4497413 = 41 \cdot 43 \cdot 2551$
58	$473 = 11 \cdot 43$	$33583 = 11 \cdot 43 \cdot 71$
59	$5283779 = 599 \cdot 8821$	$72443 = 7 \cdot 79 \cdot 131$
60	$7729 = 59 \cdot 131$	$14931263 = 89 \cdot 127 \cdot 1321$
61	$473 = 11 \cdot 43$	$38399 = 19 \cdot 43 \cdot 47$
62	$33443 = 53 \cdot 631$	$84767 = 29 \cdot 37 \cdot 79$
63	$473 = 11 \cdot 43$	$298463 = 11 \cdot 43 \cdot 631$
64	$16450697 = 1597 \cdot 10301$	$54653 = 31 \cdot 41 \cdot 43$
65	$371 = 7 \cdot 53$	$29309 = 7 \cdot 53 \cdot 79$
66	$371 = 7 \cdot 53$	$5957 = 7 \cdot 23 \cdot 37$
67	$152603 = 11 \cdot 13873$	$4730693 = 11 \cdot 31 \cdot 13873$
68	$3225713 = 271 \cdot 11903$	$25004363 = 131 \cdot 163 \cdot 1171$
69	$473 = 11 \cdot 43$	$48983 = 11 \cdot 61 \cdot 73$
70	$2921 = 23 \cdot 127$	$504773 = 19 \cdot 31 \cdot 857$
71	$8549 = 83 \cdot 103$	$653711 = 23 \cdot 67 \cdot 2371$
72	$17843 = 7 \cdot 2549$	$29183 = 7 \cdot 11 \cdot 379$
73	$22723 = 31 \cdot 733$	$107663 = 23 \cdot 31 \cdot 151$

(Continuation) The least odd solutions n of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for $73 < a < 116$ with n having exactly two and three prime factors		
74	$1403 = 23 \cdot 61$	$137863 = 11 \cdot 83 \cdot 151$
75	$53743 = 223 \cdot 241$	$11687 = 13 \cdot 29 \cdot 31$
76	$3842543 = 31 \cdot 123953$	$2435453 = 31 \cdot 251 \cdot 313$
77	$529337 = 29 \cdot 18253$	$19375403 = 31 \cdot 71 \cdot 8803$
78	$1243 = 11 \cdot 113$	$121253 = 11 \cdot 73 \cdot 151$
79	$1313 = 13 \cdot 101$	$1379963 = 13 \cdot 101 \cdot 1051$
80	$473 = 11 \cdot 43$	$1463 = 7 \cdot 11 \cdot 19$
81	$78271 = 29 \cdot 2699$	$38399 = 19 \cdot 43 \cdot 47$
82	Not known for n below 10^{10}	$6796913 = 109 \cdot 127 \cdot 491$
83	$1243 = 11 \cdot 113$	$249293 = 11 \cdot 131 \cdot 173$
84	$1289693 = 31 \cdot 41603$	$107663 = 23 \cdot 31 \cdot 151$
85	$1403 = 23 \cdot 61$	$363743 = 61 \cdot 67 \cdot 89$
86	$49781 = 67 \cdot 743$	$107663 = 23 \cdot 31 \cdot 151$
87	$11436079 = 347 \cdot 32957$	$1950683 = 7 \cdot 191 \cdot 1459$
88	$10511 = 23 \cdot 457$	$408101 = 19 \cdot 47 \cdot 457$
89	$473 = 11 \cdot 43$	$33583 = 11 \cdot 43 \cdot 71$
90	$88633 = 61 \cdot 1453$	$226493 = 47 \cdot 61 \cdot 79$
91	$473 = 11 \cdot 43$	$40513 = 11 \cdot 29 \cdot 127$
92	$12160363 = 313 \cdot 38851$	$1310873 = 37 \cdot 71 \cdot 499$
93	$917 = 7 \cdot 131$	$287021 = 7 \cdot 131 \cdot 313$
94	$396653 = 103 \cdot 3851$	$244979 = 7 \cdot 79 \cdot 443$
95	$21353 = 131 \cdot 163$	$174623 = 31 \cdot 43 \cdot 131$
96	$1403 = 23 \cdot 61$	$927383 = 23 \cdot 61 \cdot 661$
97	$364163 = 53 \cdot 6871$	$2375753 = 59 \cdot 67 \cdot 601$
98	$2993 = 41 \cdot 73$	$107663 = 23 \cdot 31 \cdot 151$
99	$6683 = 41 \cdot 163$	$28823 = 19 \cdot 37 \cdot 41$
100	$371 = 7 \cdot 53$	$1463 = 7 \cdot 11 \cdot 19$
101	$252137 = 89 \cdot 2833$	$28613 = 13 \cdot 31 \cdot 71$
102	$803 = 11 \cdot 73$	$217613 = 11 \cdot 73 \cdot 271$
103	$10841 = 37 \cdot 293$	Not known for n below 10^7
104	$17753 = 41 \cdot 433$	$54653 = 31 \cdot 41 \cdot 43$
105	$143 = 11 \cdot 131$	$57551 = 13 \cdot 19 \cdot 233$
106	$8033 = 29 \cdot 277$	$110639 = 31 \cdot 43 \cdot 83$
107	$473 = 11 \cdot 43$	$1463 = 7 \cdot 11 \cdot 19$
108	$150461 = 19 \cdot 7919$	$14231 = 7 \cdot 19 \cdot 107$
109	$30287 = 31 \cdot 977$	$107663 = 23 \cdot 31 \cdot 151$
110	$33443 = 53 \cdot 631$	$1226033 = 29 \cdot 67 \cdot 631$
111	$372863 = 571 \cdot 653$	$107663 = 23 \cdot 31 \cdot 151$
112	$1403 = 23 \cdot 61$	$825269 = 61 \cdot 83 \cdot 163$
113	$473 = 11 \cdot 43$	$204551 = 43 \cdot 67 \cdot 71$
114	$9113 = 13 \cdot 701$	$28613 = 13 \cdot 31 \cdot 71$
115	$371 = 7 \cdot 53$	$29309 = 7 \cdot 53 \cdot 79$

Table 3. The least odd solutions n of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for $115 < a < 513$.

The least odd solutions n of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for $115 < a < 296$							
a	n	a	n	a	n	a	n
116	473	161	38399	206	371	251	2831
117	1403	162	10483	207	2513963	252	5429
118	143	163	371	208	7399123	253	609733
119	2831	164	4193	209	5213	254	371
120	2921	165	5891	210	473	255	917
121	72443	166	143	211	3161	256	51811
122	473	167	7729	212	1403	257	1313
123	2831	168	33443	213	1403	258	717403
124	473	169	19667	214	92093	259	1243
125	545563	170	33131	215	4307	260	220183
126	30523	171	371	216	273983	261	143
127	143	172	14617	217	1568303	262	5891
128	72443	173	10841	218	8509	263	5891
129	8509	174	39917	219	371	264	68987
130	1403	175	5183	220	917	265	9563
131	16913	176	395789	221	2831	266	5969
132	2921	177	473	222	533	267	473
133	473	178	1403	223	31763	268	917
134	20093	179	143	224	27821	269	371
135	1403	180	2831	225	1294313	270	143
136	371	181	1763	226	473	271	1226033
137	2831	182	741647	227	72443	272	473
138	473	183	204089	228	473	273	1403
139	2921	184	1463	229	190103	274	1313
140	143	185	72443	230	6945383	275	917
141	17063	186	1403	231	28613	276	473
142	1403	187	6683	232	12793	277	8549
143	25403	188	803	233	371	278	473
144	143	189	1403	234	1403	279	2831
145	588473	190	473	235	18863	280	609733
146	1243	191	917	236	1403	281	473
147	5891	192	4307	237	1869263	282	14021
148	4307	193	473	238	2831	283	143
149	473	194	2831	239	26123	284	5891
150	371	195	473	240	2831	285	4307
151	48983	196	1313	241	11267	286	8639
152	554513	197	12773	242	1943	287	143
153	1313	198	371	243	473	288	4307
154	12029	199	473	244	1313	289	1463
155	473	200	4439	245	473	290	3053
156	2831	201	1793	246	20093	291	25691
157	143	202	14617	247	917	292	107663
158	10841	203	1403	248	143	293	4557713
159	2831	204	473	249	16559	294	473
160	2831	205	923	250	1403	295	1403

(Continuation) The least odd solutions n of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for $295 < a < 476$

a	n	a	n	a	n	a	n
296	14617	341	3161363	386	6683	431	12029
297	19061	342	62843	387	2831	432	5093
298	7729	343	68987	388	1463	433	1403
299	41536541	344	6683	389	2831	434	18827
300	143	345	335237	390	26123	435	473
301	30619	346	13433	391	143	436	371
302	7729	347	473	392	5891	437	371
303	371	348	1313	393	2123	438	201527
304	371	349	473	394	4193	439	1703
305	473	350	6683	395	1403	440	4307
306	382013	351	1403	396	1403	441	473
307	178133	352	28613	397	2453	442	8549
308	2831	353	473	398	205277	443	143
309	143	354	2831	399	10841	444	178829
310	1763	355	473	400	5891	445	22723
311	1463	356	33443	401	371	446	57893
312	211823	357	5891	402	473	447	52421
313	5429	358	473	403	402533	448	473
314	473	359	3647	404	143	449	16463
315	18827	360	371	405	22723	450	10841
316	473	361	923	406	7729	451	10841
317	4739	362	550793	407	17009	452	143
318	1403	363	14617	408	473	453	7729
319	516497	364	473	409	371	454	12773
320	20093	365	14573	410	473	455	31613
321	4307	366	1463	411	107663	456	1313
322	143	367	5969	412	41663	457	473
323	233657	368	212063	413	143	458	335237
324	2921	369	1403	414	84767	459	952571
325	371	370	2831	415	371	460	27563
326	18941	371	473	416	55129	461	107663
327	473	372	1403	417	3263	462	1403
328	107663	373	2831	418	20093	463	4307
329	68987	374	1403	419	473	464	2831
330	2831	375	322823	420	148661	465	143
331	371	376	18533	421	498581	466	1403
332	72443	377	2123	422	17063	467	2993
333	473	378	26051	423	2831	468	473
334	13943	379	142643	424	473	469	2831
335	2831	380	371	425	2831	470	26653
336	14617	381	5891	426	143	471	371
337	5891	382	473	427	6683	472	8509
338	473	383	8509	428	2831	473	6683
339	371	384	732089	429	917	474	506473
340	3485413	385	2831	430	143	475	300533

(Continuation) The least odd solutions n of the congruence $(a+2)^{2n-1} \equiv a^{2n-1} \pmod{2n}$ for $475 < a < 513$							
a	n	a	n	a	n	a	n
476	473	485	1243	494	5891	504	4307
477	405017	486	371	495	105053	505	1869941
478	61763	487	473	496	473	506	10841
479	1463	488	2831	497	16559	507	371
480	1403	489	54113	498	22723	508	533
481	30287	490	7403	499	544163	509	473
482	1313	491	204551	501	473	510	1943
483	8549	492	5093	502	302473	511	76073
484	2831	493	72443	503	473	512	1403

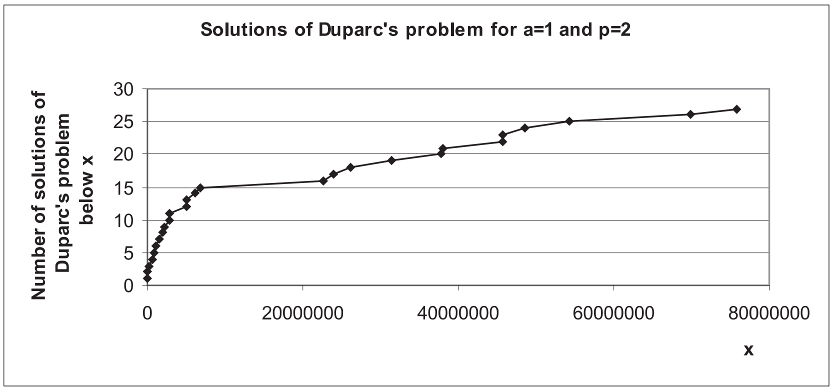

FIGURE 3

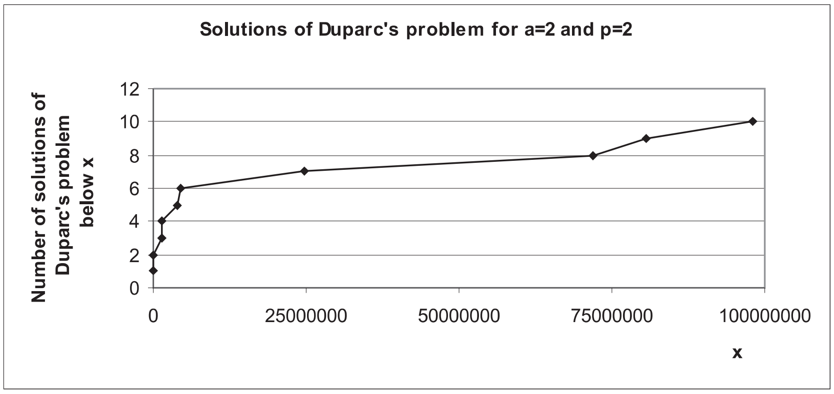

FIGURE 4

TABLE 4. The least odd solutions of Duparc's problem for the case $p = 3$.

The least odd solutions of Duparc's problem for the case $p = 3$							
α	n	α	n	α	n	α	n
2	1457	132	355	262	1457	392	215
7	1457	137	1457	267	1457	397	851
12	355	142	4267	272	355	402	1457
17	1457	147	1457	277	1457	407	1457
22	1055	152	355	282	1457	412	355
27	5627	157	1457	287	1457	417	1457
32	1457	162	1055	292	355	422	1457
37	851	167	1457	297	355	427	1457
42	215	172	1055	302	1457	432	355
47	1457	177	1457	307	851	437	1457
52	1457	182	215	312	1055	442	1055
57	1457	187	1457	317	1457	447	1457
62	355	192	1457	322	215	452	1457
67	1457	197	1457	327	1457	457	1457
72	1457	202	355	332	1457	462	215
77	1457	207	1457	337	1457	467	1457
82	355	212	1457	342	355	472	1457
87	1457	217	851	347	1457	477	1457
92	1457	222	355	352	1457	482	355
97	1457	227	1457	357	1457	487	1147
102	1055	232	1055	362	355	492	1457
107	1457	237	1457	367	1457	497	1457
112	215	242	1457	372	1055	502	355
117	1457	247	1457	377	1457	507	1457
122	1457	252	215	382	1055	512	1457
127	851	257	3007	387	1457	517	1457

REFERENCES

[1] ALFORD, W. R.—GRANVILLE, A.—POMERANCE, C.: *There are infinitely many Carmichael numbers*, Ann. Math. **140** (1994), 703–722.

[2] BEEGER, N. G. W. H.: *On even numbers m dividing* $2^m - 2$, Amer. Math. Monthly **58** (1951), 553–555.

[3] ROTKIEWICZ, A.: *Sur les nombres composés n qui divisent* $a^{n-1} - b^{n-1}$, Rend. Circ. Mat. Palermo **8** (1959), 115–116.

[4] ROTKIEWICZ, A.: *Sur les nombres pairs n pour lesquels les nombres* $a^n b - ab^n$*, respectivement* $a^{n-1} - b^{n-1}$*, sont divisibles par* n, Rend. Circ. Mat. Palermo **8** (1960), 341–342.

[5] ROTKIEWICZ, A.: *Sur les nombres n qui divisent* $(a+2)^{n-1} - a^{n-1}$, Rend. Circ. Mat. Palermo **9** (1960), 78–80.

[6] ROTKIEWICZ, A.: *Sur les nombres premiers p et q tels que* $pq \mid 2^{pq} - 2$, Rend. Circ. Mat. Palermo **11** (1962), 280–282.

[7] ROTKIEWICZ, A.: *Un problème sur les nombres pseudo-premiers*, Indag. Math. **34** (1972), 86–91.

[8] ROTKIEWICZ, A.: *Pseudoprime Numbers and Their Generalizations*, Student Associatio of the Faculty of Sciences, University of Novi Sad, Novi Sad, Yugoslavia, 1972.

[9] ZSIGMONDY, K.: *Zur Theorie der Potenzreste*, Monatsh. Math. **3** (1892), 264–284.

Received October 28, 2004

Andrzej Paszkiewicz
Warsaw University of Technology
Institute of Telecommunications
Division of Telecommunications Fundamental
ul. Nowowiejska 15/19
PL–00-661 Warsaw
POLAND

E-mail: anpa@tele.pw.edu.pl

Andrzej Rotkiewicz
Institute of Mathematics
Polish Academy of Sciences
ul. Śniadeckich 8
Skr. Poczt. 21
PL–00-956 Warsaw
POLAND

E-mail: rotkiewi@impan.gov.pl