Acta Mathematica et Informatica Universitatis Ostraviensis

Andrzej Rotkiewicz

Arithmetic progressions formed by pseudoprimes

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 8 (2000), No. 1, 61--74

Persistent URL: http://dml.cz/dmlcz/120560

Acta Mathematica et Informatica Universitatis Ostraviensis 8 (2000) 61–74

Arithmetic progressions formed by pseudoprimes

Andrzej Rotkiewicz

Abstract: A composite number n is called a pseudoprime if $2^{n-1} \equiv 1 \mod n$. This paper presents all that is known about arithmetic progressions formed by pseudoprimes or their generalizations. We include the proof of a new result on the existence of arithmetic progressions formed by Lehmer pseudoprimes.

Key Words: Pseudoprime, Super pseudoprime, Prime pretender, Carmichael number, Fibonacci pseudoprime, Lucas pseudoprime, Lehmer pseudoprime, Fibonacci sequence, Lucas number, Lehmer number

Mathematics Subject Classification: primary 11A07; secondary 11B39.

1. Historical remarks

A composite number n is called a pseudoprime if $2^{n-1} \equiv 1 \mod n$. Leibniz in September 1680 and December 1681 gave incorrect proof that the number $2^n - 2$ is not divisible by n unless n is a prime [9], Vol. I, p. 23.

I was informed by Prof. A. Schinzel that the first proof that there exist infinitely many pseudoprimes was given by J.H. Jeans in 1898 (see [16]).

In his paper Jeans wrote:

"The problem is to find n, not a prime, so that

$$2^{n-1} - 1 \equiv 0 \mod n.$$

Writing $f(p)$ for $2^{2^p} + 1$, $n = f(p)$ is clearly a solution if p is any integer such that $f(p)$ is not prime; and

$$n = f(p) \cdot f(q)$$

is another solution if $f(p)$, $f(q)$ are both prime, and $p < q < 2^p$: For $2^{f(p)-1} - 1 \equiv 0 \mod f(q)$ and $2^{f(q)-1} - 1 \equiv 0 \mod f(p)$."

In the same paper Jeans wrote that Chinese mathematicians claimed 25 centuries ago that composite numbers such that $2^{n-1} - 1 \equiv 0 \mod n$ do not exist.

This information is wrong (see Ribenboim [26] and Sierpiński [46] Addendum and corrigendum insert in July, 1987).

Needham (see [24]) wrote that this arose from misunderstanding by Jeans what was only a statement of the fact that even numbers can be divided by 2 and that odd ones cannot.

Let u_n denote the n-th term of the Fibonacci sequence

$$1, 1, 2, 3, 5, 8, 13, \ldots$$

Let u_k $(k > 0)$ be the first term of the Fibonacci sequence divisible by p. Then p is called a primitive prime factor of u_k and $k = \vartheta(p)$ is called the rank of apparition of p. By Carmichael theorem [4] every u_n, $n \neq 1, 2, 6, 12$, has at least one primitive prime factor p.

A composite n is called a Fibonacci pseudoprime if $u_{n-(\frac{5}{n})} \equiv 0 \mod n$, where $(\frac{5}{n})$ is the Jacobi symbol.

The theorem that if p is any prime greater than 5, then the number u_{2p} is Fibonacci pseudoprime is usually attributed to Duparc (1955) [10] or E. Lehmer (1964) [20].

We note here that in 1911 Niewiadomski [25] claimed that Fibonacci pseudoprimes do not exist.

In 1921 Kernbaum [17] proved that this is not true since $17 \cdot 19$, $13 \cdot 29$, $89 \cdot 199$, $233 \cdot 521$, $53 \cdot 109$, $139 \cdot 461$ are Fibonacci pseudoprimes.

He proved also that the number $N = \prod_i n_i$, where n_i are different primes and rank of apparition $\vartheta(n_i)$ is k or $2k$, where k is odd, is a Fibonacci pseudoprime.

¿From the above it follows that u_{2p}, where p is a prime > 5, is a Fibonacci pseudoprime.

Indeed, if $N = u_{2p} = \prod_i n_i$ then for every i, $\vartheta(n_i) = p$ or $2p$ and by the theorem of Kernbaum u_{2p} is a Fibonacci pseudoprime.

Also if $n = (2k + 1)10$, where $k > 1$, then by a theorem of A. Schinzel [43], u_n has at least two primitive prime factors n_1 and n_2. Then $\vartheta(n_1) = \vartheta(n_2) = n = 2k$, where $k = (2k + 1)5$ is odd and by the theorem of Kernbaum $n_1 n_2$ is a Fibonacci pseudoprime.

In 1904, M. Cipolla [6] proved the following theorem:

The number $F_m \cdot F_n \cdots F_s$, where $F_i = 2^{2^i} + 1$, $m < n < \ldots < s$ is a pseudoprime if and only if $2^m > s$. It follows at once from this theorem that every number $F_m \cdot \cdot F_{m+1}$, $m = 2, 3, \ldots$ is a pseudoprime. Cipolla's results remained long unnoticed by later writers on the subject.

A composite n is called a pseudoprime to base a if $a^{n-1} \equiv 1 \mod n$.

In 1965 K. Szymiczek [48] generalized Cipolla's theorem and proved the following theorem:

Let $a > 1$, $2^\alpha \| a$, $\alpha > 0$, $n_1 < n_2 < \ldots < n_s$ then $(a^{2^{n_1}} + 1)(a^{2^{n_2}} + 1) \cdots (a^{2^{n_s}} + 1)$ is a pseudoprime to base a if and only if $\alpha 2^{n_1} > n_s$.

A composite n is called a pseudoprime to the pair $\langle a, b \rangle$ if $a^{n-1} - b^{n-1} \equiv 0 \mod n$. The above definition was proposed by A. Mąkowski.

K. Szymiczek [48] proved also the following theorem.

Let $2^\alpha \| a$, $\alpha \geq 0$, $2^{\lambda+1} \| b^2 - 1$, $n_1 < n_2 < \ldots < n_s$, $\lambda + n_1 \neq \alpha \cdot 2^{n_s}$.

The number $(a^{2^{n_1}}+b^{2^{n_1}})\dots(a^{2^{n_1}}+b^{2^{n_s}})$ is pseudoprime to pair the $\langle a,b\rangle$ if and only if

$$n_s < \min(\lambda + n_1, \alpha \cdot 2^{n_1}).$$

If $b=1$, we have $\lambda=\infty$ and the condition is

$$\alpha \cdot 2^{n_1} > n_s.$$

In 1964 I proved [27] the following theorem.

If $n_1 < n_2 < \dots, n_s$, $2^{n_1} > n_s$ then the number $(2^{F_{n_1}}-1)(2^{F_{n_2}}-1)\cdots(2^{F_{n_s}}-1)$ is a pseudoprime.

In 1947 W. Sierpiński [45] proved that there exist infinitely many pseudoprimes which are at the same time Mersenne numbers. The same result was published later by R. Steuerwald [47].

Any composite number q such that $b^q \equiv b \mod q$ is called a prime pretender to base b [7], [40].

Every pseudoprime to base b is a prime pretender to base b but not conversely.

In the paper [40] I proved that for every $b>1$ these exist infinitely many prime pretenders to base b which are not pseudoprimes to base b.

Until 1950 only odd prime pretenders to base 2 were known.

D.H. Lehmer (see Erdős [13]) found the first even prime pretender: $161038 = 2 \cdot 73 \cdot 1103$ to base 2. In 1951 Beeger [3] showed the existence of infinitely many even prime pretenders to base 2.

In my book [30] I put forward the following problems:

Does there exist a prime pretender to base 2 of the form 2^n-2? (problem #22) and: Do there exist infinitely many even prime pretenders which are the products of three primes? (problem #51).

In 1989 McDaniel [22] gave an example of an even prime pretender which is itself of the form $2^n-2 = 2(2^{pq}-1)$ by showing that 2^n-2 is a prime pretender to base 2 if $n = 465794 = 2 \cdot 7^4 \cdot 97$, $p=37$, and $q=12589$. He believed, but has not shown, that $n=465794$ is the smallest integer such that 2^n-2 is an even prime pretender to base 2.

In the paper [37] we found 24 even prime pretenders to base 2 with $3,4,5,6,7$ and 8 prime factors.

The problem: Do there exist infinitely many, or at least one, arithmetic progressions formed by three even prime pretenders to base 2?
is still open.

It is easy to see that if $[1,2,\dots,k] \mid a-1$ where $[1,2,\dots,k]$ denotes the least common multiple of the integers $1,2,\dots,k$ then the numbers $2\cdot a, 3\cdot a, \dots, k\cdot a$ form an arithmetic progression formed by $(k-1)$ prime pretenders to base a but we do not know whether there exist infinitely many such progressions.

In 1963 W. Sierpiński raised the question whether there exist infinitely many arithmetic progressions consisting of three pseudoprimes.

It is known that there exist infinitely many arithmetic progressions consisting of three prime numbers. This was proved by Van der Corput in 1939 [50] and again by Chowla [5] in 1944. The proof of this fact however, is difficult and we do not know whether there exist infinitely many arithmetic progressions consisting of four

prime numbers. To date the best result was obtained by Heath-Brown [15], who showed in 1981 that there exist infinitely many arithmetic progressions consisting of four numbers, of which three are primes and the other is a prime, or the product of two, not necessarily distinct, prime factors.

In 1964 [28] I proved that there exist infinitely many arithmetic progressions formed of three pseudoprimes. One of such progressions is the progression

$$\frac{2^{37}+1}{3},\ \frac{2^{38}-1}{3},\ 2^{37}-1.$$

Another is given by

$$\frac{2^{26}+1}{5},\ \frac{2^{28}-1}{15},\ \frac{2^{26}-1}{3}.$$

There exist 690 arithmetic progressions below 10^8 consisting of three different odd pseudoprimes.

The arithmetic progression which is formed from the least three odd pseudoprimes is the progression

$$561 = 3 \cdot 11 \cdot 17,\ 2645 = 5 \cdot 17 \cdot 29,\ 4369 = 17 \cdot 257.$$

Later [30], [32] I proved that there exist infinitely many arithmetic progressions formed of four pseudoprimes.

One of such progression is given by

$$2^{109}-1,\ (2^{109}-1)\frac{2^{73}+1}{3},\ (2^{109}-1)\left(\frac{2^{74}-1}{3}\right) \text{ and } (2^{109}-1)(2^{73}-1).$$

Below 10^8 there exist 23 arithmetic progressions consisting of four pseudoprimes [22]. The arithmetic progression which is formed from the least four pseudoprimes is the progression:

$$1729,\ 63973,\ 126217,\ 188461.$$

In [32] the third number was given with a misprint, as noticed by A. Mąkowski.

There exist only two arithmetic progressions below 10^8 consisting of five odd pseudoprimes. These are

1) 172081, 285541, 399001, 512461, 625921,

2) 172081, 512461, 852841, 1193221, 1533601.

The problem #28 of my book [30]:

Does there exist an infinity of arithmetic progressions consisting of five pseudoprimes?

is still open.

A composite number n is called super pseudoprime if each divisor d of n satisfies the congruence $2^{d-1} \equiv 1 \mod d$. An example for super pseudoprime n is 2047. Szymiczek proved that the number F_nF_{n+1}, where $F_n = 2^{2^n}+1$, $n > 1$ is super-pseudoprime (Szymiczek [49]). It is not known if there exist infinitely many super pseudoprimes of the form $F_nF_{n+1}F_{n+2}$ (Szymiczek [49]). It is easy to prove that

If $p > 3$ and $2p - 1$ are primes and the numbers

$$\frac{2^{2p-1}+1}{3}, \quad \frac{2^{2p}-1}{3}, \quad 2^{2p-1}-1$$

are composite then these numbers form an arithmetic progression of three super pseudoprimes.

The problem of K. Szymiczek (problem 31 [30]):

Do there exist infinitely many arithmetic progressions formed by three super pseudoprime numbers?
is still open.

2. Arithmetic progressions formed by three pseudoprimes to base a

There exist infinitely many arithmetic progressions consisting of three diffrent pseudoprimes to base 3 [30].

A prime factor of $a^n - b^n$ is called primitive if $p \mid a^n - b^n$ and $p \nmid a^x - b^x$ for $0 < x < n$. If $a > b \geq 1$, $(a, b) = 1$, $n > 6$ then every number $a^n - b^n$ by theorem of Zsigmondy [52] has a primitive prime factor. I proved [30] pp. 118–121 that if $M_p = 2^p - 1 \nmid a^2 - 1$, $2 \mid a$, M_p is a prime number, $2^n \geq n + p$, q is a primitive prime factor of the number $a^{M_p 2^{n+p}} - 1$ then the numbers

$$\frac{a^{M_p 2^n}+1}{a^{2^n}+1}q, \quad \frac{a^{2^{n+p}}-1}{a^{2^{n+1}}-1}q, \quad \frac{a^{M_p 2^n}-1}{a^{2^n}-1}q$$

are pseudoprimes for base a and form an arithmetic progression.

¿From this theorem it follows that for every even $a < 2^{6972593} - 1$ there exist infinitely many arithmetic progressions consisting of three different pseudoprimes for the base a. The number $2^{6972593} - 1$ is the 38^{th} Mersenne prime and has more than two million digits.

An odd composite n is called Euler pseudoprime to base a [2], [19], [21], if

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \mod n$$

where $\left(\frac{a}{n}\right)$ is the Jacobi symbol.

In 1980 [33] I proved the following theorem

For every odd $a \geq 3$ the numbers

$$\frac{a^{a^{2(2a)^n}}+1}{a^{a^{(2a)^n}}+1}, \quad \frac{a^{a^{2(2a)^n}+a^{(2a)^n}}-1}{a^{2a^{(2a)^n}}-1}, \quad \frac{a^{a^{2(2a)^n}}-1}{a^{a^{(2a)^n}}-1}$$

for $n = 1, 2, \ldots$ are Euler pseudoprimes to the base a and form an arithmetic progression.

Problem: Does there exist for every even a an infinity of arithmetic progressions consisting of three pseudoprimes to the base a?
is still open.

3. Arithmetic progressions formed by Carmichael numbers

A composite n is called a Carmichael number if $a^n \equiv a \mod n$ for every integer $a \geq 1$. The smallest Carmichael number is $561 = 3 \cdot 11 \cdot 17$. By Korselt's criterion [18], n is a Carmichael number if and only if n is squarefree and $p-1$ divides $n-1$ for all primes dividing n.

In 1994 Alford, Granville and Pomerance [1] proved that there exist infinitely many Carmichael numbers and that there are more than $x^{2/7}$ Carmichael numbers up to x, for sufficiently large x.

It is easy to see [30] that if $n \equiv 1 \mod 12$ and the numbers $6n+1$, $12n+1$, $18n+1$, $36n+1$, $72n+1$, $108n+1$, $144n+1$ are prime then the numbers $a_1 = N = (6n+1)(12n+1)(18n+1)$, $a_2 = N(36n+1)$, $a_3 = N(72n+1)$, $a_4 = N(108n+1)$, $a_5 = N(144n+1)$ form an arithmetic progression consisting of 5 Carmichael numbers.

For $n \equiv 1 \mod 6$ the first four numbers form an arithmetic progression consisting of four Carmichael numbers.

For $n = 1$ we get the following arithmetic progression $a_1 = 7 \cdot 13 \cdot 19 = 1729$, $a_2 = 7 \cdot 13 \cdot 19 \cdot 37 = 63973$, $a_3 = 7 \cdot 13 \cdot 19 \cdot 73 = 126217$, $a_4 = 7 \cdot 13 \cdot 19 \cdot 109 = 188461$.

Below 10^8 there exist only 17 arithmetic progressions consisting of three Carmichael numbers.

4. Arithmetic progressions formed by Fibonacci pseudoprimes

Let $u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$, where $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$, denote the n^{th} Fibonacci number.

A composite n is called a Fibonacci pseudoprime if

$$u_{n-\left(\frac{5}{n}\right)} \equiv 0 \mod n,$$

where $\left(\frac{5}{n}\right)$ is the Jacobi symbol.

The smallest Fibonacci pseudoprimes are $323 = 17 \cdot 19$ and $377 = 13 \cdot 29$; indeed $\left(\frac{5}{323}\right) = \left(\frac{5}{377}\right) = -1$ and it may be calculated that $u_{324} \equiv 0 \mod 323$ and $u_{378} \equiv 0 \mod 377$.

In 1994 [36] I found the following three Fibonacci pseudoprimes which form an arithmetic progression

$$u_{73} = \frac{\alpha^{73} - \beta^{73}}{\sqrt{5}} = 9375829 \cdot 86020717,$$

$$u_{74} = \frac{\alpha^{74} - \beta^{74}}{\sqrt{5}} = 73 \cdot 149 \cdot 2221 \cdot 54018521,$$

$$v_{73} = \alpha^{73} + \beta^{73} = 151549 \cdot 11899937029.$$

The difference of the above progression is the Fibonacci number u_{72}.

In the paper [38] I proved that there exist infinitely many arithmetic progressions formed by three distinct Fibonacci pseudoprimes.

5. Arithmetic progressions formed by Lucas pseudoprimes

Let D, P, Q be integers such that $D = P^2 - 4Q \neq 0$, $z^2 - Pz + Q = (z - \alpha)(z - \beta)$, $U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$.

A composite number n is a Lucas pseudoprime with parameters P and Q if

$$U_{n-(\frac{D}{n})} \equiv 0 \mod n$$

where $(\frac{D}{n})$ denotes the Jacobi symbol.

Let $\overline{k}$ denote the square-free kernel of k, that is k divided by its greatest square factor.

The following theorem holds [39]:

If $D = P^2 - 4Q > 0$, $\overline{D} \equiv 1 \mod 4$, $(P, Q) = 1$, $p > 3$ and $2p - 1$ are primes of the form $\overline{D}\varphi(\overline{D})x + 1$, $(p(2p-1), PQD) = 1$, φ is the Euler function, then there exist infinitely many arithmetic progressions formed by three different Lucas pseudoprimes with parametrs P and Q which are given by the formula

$$\frac{\alpha^{(2p-1)p^m} + \beta^{(2p-1)p^m}}{\alpha^{p^m} + \beta^{p^m}}, \quad \frac{\alpha^{2p^{m+1}} - \beta^{2p^{m+1}}}{\alpha^{2p^m} - \beta^{2p^m}}, \quad \frac{\alpha^{(2p-1)p^m} - \beta^{(2p-1)p^m}}{\alpha^{p^m} - \beta^{p^m}}$$

for $m = 1, 2, \ldots,$.

¿From the above theorem we get the following corollary:

Let a and b be natural numbers, $(a, b) = 1$, $a > b$. If $p > 3$ and $(2p - 1)$ are primes $(p(2p-1), (a^2 - b^2)ab) = 1$ then the numbers

$$\frac{a^{(2p-1)p^m} + b^{(2p-1)p^m}}{a^{p^m} + b^{p^m}}, \quad \frac{a^{2p^{m+1}} - b^{2p^{m+1}}}{a^{2p^m} - b^{2p^m}}, \quad \frac{a^{(2p-1)p^m} - b^{(2p-1)p^m}}{a^{p^m} - b^{p^m}}$$

are pseudoprimes for the pair $\langle a, b \rangle$ and form an arithmetic progression.

For $b = 1$ I proved the above Corollary in my book [30].

6. Arithmetic progressions formed by Lehmer pseudoprimes

The Lehmer numbers are defined as follows

$$P(\alpha, \beta; n) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & if n is odd, \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & if n is even \end{cases}$$

where α and β are distinct roots of trinomial $f(z) = z^2 - \sqrt{L}z + M$, its discriminant is $K = L - 4M$, $L > 0$ and M are rational integers.

We can assume without any essential loss of generality that $(L, M) = 1$ and $M \neq 0$.

A composite number n is called Lehmer pseudoprime with parameters L and M if

$$P\Big(\alpha, \beta; \big(n - (KL/n)\big)\Big) \equiv 0 \mod n,$$

where (KL/n) is the Jacobi symbol [31], [31], [35].

By theorem T of my paper [35] the following theorem holds

If α/β is not a root of unity (i.e. $\langle L, M\rangle \neq \langle 1,1\rangle, \langle 2,1\rangle, \langle 3,1\rangle$) then every arithmetic progression $ax + b$, where $(a,b) = 1$ contains an infinite number of Lehmer pseudoprimes with parameters L and M.

For each positive n we denote by $\phi(\alpha,\beta;n)$ the nth homogeneous cyclotomic polynomial

$$\phi(\alpha,\beta;n) = \prod(\alpha - \zeta_n^m\beta) = \prod(\alpha^d - \beta^d)^{\mu(n/\alpha)},$$

where ζ_n is a primitive nth root of unity and the product is over the $\varphi(n)$ integers n with $1 \leq m \leq n$ and $(m,n) = 1$, μ is the Möbius function.

A prime factor p of $P(\alpha,\beta;n)$ is called a primitive prime factor of $P(\alpha,\beta;n)$ if $p \mid P(\alpha,\beta;n)$ but $p \nmid KLP(\alpha,\beta;3)\dots P(\alpha,\beta;n-1)$.

The following results are well known.

Lemma 1 (Lehmer [21]). *Let $n \neq 2^g$, $3\cdot 2^g$. Denote by $r = r(n)$ the largest prime factor of n. If $r \nmid \phi(\alpha,\beta;n)$ then every prime p dividing $\phi(\alpha,\beta;n)$ is a primitive prime divisor of $P(\alpha,\beta;n)$.*

Every primitive divisor p of $P(\alpha,\beta;n)$ is $\equiv (KL/n) \mod n$. If $r|\phi(\alpha,\beta;n)$, $n \neq r^l$, $n \neq 2r^l$, $r^\varepsilon \| n$, $\varepsilon > 0$, then $r\|\phi(\alpha,\beta;n^\varepsilon)$ and r is a primitive prime divisor of $P(\alpha,\beta;n/r^\varepsilon)$. If $n = r^l$ or $n = 2r^l$ then $r|\phi(\alpha,\beta;n)$ if and only if $r|K$ or $r|L$ respectively. If $r \mid \phi(\alpha,\beta;n)$ then $r\|\phi(\alpha,\beta;n)$.

For $n > 12$ and $K > 0$ the number $P(\alpha,\beta;n)$ has a primitive prime divisor (Durst [12], Ward [51]).

If $K < 0$ and β/α is not a root of unity, then $P(\alpha,\beta;n)$ has a primitive prime divisor for $n > n_0(\alpha,\beta)$. Here $n_0(\alpha,\beta)$ can be effectively computed (Schinzel [42]). *We have $|\phi(\alpha,\beta;n)| > 1$ for $n > n_0$.*

Lemma 2 (Rotkiewicz [31], Lemma 5). *Let $\psi(a) = 2a^2 \prod_{p|a}(p^2-1)$, where p runs over the prime factor of the positive integer a. If q is a prime such that $q^2\|n$ and a is a natural number with $\psi(a) \mid q-1$, then*

$$\phi(\alpha,\beta;n) \equiv 1 \mod a.$$

In 1958 A. Schinzel [44] formulated the following Hypothesis H. Let k be a natural number and let $f_1(x),\dots,f_k(x)$ be irreducible polynomial with integral coefficients and positive leading coefficient.

Then if there is no natural number > 1 which is a divisor of the product $f_1(x)\dots f_k(x)$ for every integer x, then there exist infinitely many natural values of x for which each of the numbers $f_1(x), f_2(x),\dots,f_k(x)$ is prime.

In 1904 Dickson [8] formulated the above conjecture for linear polynomials and this conjecture is called Dickson's conjecture D.

¿From Dickson's conjecture it follows the following corollary. Let $n > 1$, let d be a multiple of all primes $p \leq n$. Then there exist infinitely many arithmetic progressions, with difference d, each consisting of n consecutive primes (Schinzel and Sierpiński [44]).

In 1969 I proved [29] that from Dickson's conjecture it follows that there exist infinitely many arbitrarily long arithmetic progressions whose terms are pseudoprime numbers and in 1964 I proved that the same is true for Lehmer's pseudoprimes.

In 1972 I proposed [30] (problem #29) whether it follows from Hypothesis H of A. Schinzel that there exist arbitrarily long arithmetic progressions of Carmichael numbers.

Granville [14] proved the following theorem: Dickson conjecture D implies that there are arbitrarily long arithmetic progressions of Carmichael numbers.

In the joint paper [41] with A. Schinzel we proved the following theorem

Given integers P, Q with $D = P^2 - 4Q \neq 0, -2Q, -3Q$ and $\varepsilon = \pm 1$, every arithmetic progression $ax+b$, where $(a,b) = 1$ which contains an odd integer n_0 with $(D/n_0) = \varepsilon$ contains infinitely many strong Lucas pseudoprimes n with parameters P and Q such that $(D/n) = \varepsilon$. The number $N(x)$ of such strong pseudoprimes not exceeding x satisfies

$$N(x) > c(P,Q,a,b,\varepsilon)\frac{\log x}{\log\log x},$$

where $c(P,Q,a,b,\varepsilon)$ is a positive constant depending on P,Q,a,b,ε. This theorem gives an affirmative answer to a question of C. Pomerance: Given integers P, Q with $D = P^2 - 4Q$ not a square, do there exist infinitely many, or at least one, Lucas pseudoprimes n with parameters P and Q satisfying $(D/n) = -1$?

Here we shall prove the following

Theorem. *If α, β defined above are different from zero and α/β is not a root of unity (i.e. $\langle L, M\rangle \neq \langle 1,1\rangle, \langle 2,1\rangle, \langle 3,1\rangle$), $\varepsilon = \pm 1$, then from Dickson's conjecture D it follows that every arithmetic progression $ax + b$, where $(a,b) = 1$, which contains an odd integer n_0 with $(KL/n_0) = \varepsilon$, contains infinitely many arithmetic progressions formed by k different Lehmer pseudoprimes n_i with parameters L, M such that $(KL/n_i) = \varepsilon$.*

Proof. Let $a \geq 2$ and let $b, b+a, \ldots, b+(k-1)a$ be k prime numbers in arithmetic progression, then by theorem of M. Cantor (1861) quoted in [8], Vol. I, p. 425 either the difference a is divisible by every prime $\leq k$, or $b = k$ and the difference a is divisible by every prime $< k$. So we can assume without any essential loss of generality that a is divisible by every prime $\leq k$.

We may suppose without loss of generality that b is odd and $4KL \mid a$.

Since arithmetic progression $ax + b$, where $(a,b) = 1$ contains an odd integer n_0 with $(KL/n_0) = \varepsilon$, we can assume that

$$b \equiv n_0 \mod 4KL \text{ and } (KL/n_0) = \varepsilon.$$

Let $c = \prod_{i=1}^{k}((i-1)a+1)$ and $p_1, p_2, \ldots, p_{k+5}$ be odd primes such that

$$(p_1 p_2 \ldots p_{k+5}, 4acKL) = 1$$

and q be a prime number such that

$$\psi(ac^2 p_1 p_2 \ldots p_{k+5}) \mid q - 1.$$

By the Chinese Remainder Theorem exists a natural number m such that

$$m \equiv \varepsilon + cq \mod c^2 p_1^2 p_2^2 \dots p_{k+5}^2 q^3,$$
$$m \equiv b \mod a.$$

Since $(ac^2 p_1^2 p_2^2 \dots p_{k+5}^2 q^3, m) = 1$ by Dirichlet's theorem there exist infinitely many primes p of the form $ac^2 p_1^2 p_2^2 \dots p_{k+5}^2 q^3 x + m$.

Let $A_i = ((i-1)a+1)(p-\varepsilon)+\varepsilon$. We have $A_i(x) \equiv b \mod a$.

Suppose that there exists a natural number $d > 1$ such that

$$1 < d \mid N(x) = \prod_{i=1}^{k} A_i(x) = \prod_{i=1}^{k} \Big[\big((i-1)a+1\big)(p-\varepsilon)+\varepsilon\Big].$$

We have $N(x) = \prod\limits_{i=1}^{k} \Big[\big((i-1)a+1\big)(ac^2 p_1^2 p_2^2 \dots p_{k+5}^2 q^3 x + m - \varepsilon) + \varepsilon\Big] = \prod\limits_{i=1}^{k} \Big[\big((i-1)a+1\big)ac^2 p_1^2 p_2^2 \dots p_{k+5}^2 q^3 x + \big((i-1)a+1\big)(m-\varepsilon)+\varepsilon\Big]$.

We have $\Big(\big((i-1)a+1\big)ac^2 p_1^2 p_2^2 \dots p_{k+5}^2 q^3, \big((i-1)a+1\big)(m-\varepsilon)+\varepsilon\Big) = 1$. Then there exists also $\overline{p} > 2$ such that $N(x) \equiv o \mod \overline{p}$. Since $\prod\limits_{p \le k} p \mid a$, $(p_i, a) = 1$, $(p_i, c) = 1$, $(p_i, q) = 1$ we have $\overline{p} > k$.

Thus $N(x)$ is a polynomial of degree k with the leading coefficient not divisible by $\overline{p}$.

By Lagrange's theorem the congruence

$$N(x) \equiv 0 \mod \overline{p}$$

has at most k roots. Since $\overline{p} > k$ there exists a natural number x such that $N(x) \not\equiv 0 \mod \overline{p}$. Thus the polynomials $A_i(x)$ satisfy the conditions of Dickson's conjecture D and there exist infinitely many integers x for which each of the number $A_i(x)$ is a prime number. Let x be one of these numbers and put $A_i(x) = A_i$ for $i = 1, 2, \dots, k$. We have $A_1(x) = p$.

Now our considerations rest on the fact that by Lemma 1 at most one of the numbers $m_i = \phi\left(\alpha, \beta; \frac{p-\varepsilon}{p_i}\right)$ $(i = 1, 2, \dots, k+5)$ is divisible by p and at most one of them is divisible by the highest prime factor of $p - \varepsilon$ (for the proof see [34], [35]).

Also by Lemma 1 at most one of the numbers m_i is divisible by A_j. Thus without loss of generality one can assume that neither $m_1 = \phi\left(\alpha, \beta; \frac{p-\varepsilon}{p_1}\right)$ nor $m_2 = \phi\left(\alpha, \beta; \frac{p-\varepsilon}{p_2}\right)$ nor $m_3 = \phi\left(\alpha, \beta; \frac{p-\varepsilon}{p_3}\right)$ is divisible by p or r or $A_i (i = 1, 2, \dots, k)$.

Thus without loss of generality one can assume that the numbers m_1 and m_2 have the same sign, hence $m_1 m_2 > 0$. By Lemma 1 we can assume that

$$\left|\phi\left(\alpha, \beta; \frac{p-\varepsilon}{p_i}\right)\right| > 1 \text{ for } i = 1, 2.$$

Now we shall prove that the numbers

$$n_1 = A_1\phi\left(\alpha,\beta;\frac{p-\varepsilon}{p_1}\right)\phi\left(\alpha,\beta;\frac{p-\varepsilon}{p_2}\right)$$
$$n_2 = A_2\phi\left(\alpha,\beta;\frac{p-\varepsilon}{p_1}\right)\phi\left(\alpha,\beta;\frac{p-\varepsilon}{p_2}\right)$$
$$\vdots$$
$$n_k = A_k\phi\left(\alpha,\beta;\frac{p-\varepsilon}{p_1}\right)\phi\left(\alpha,\beta;\frac{p-\varepsilon}{p_2}\right)$$

form an arithmetic progression of Lehmer pseudoprimes with parameters L and M, when each of the numbers $n_i = A_i\phi\left(\alpha,\beta;\frac{p-\varepsilon}{p_1}\right)\phi\left(\alpha,\beta;\frac{p-\varepsilon}{p_2}\right)$ $(i = 1,2,\ldots,k)$ is $\equiv b \mod a$ with $(KL/n_i) = \varepsilon$.

Since $m_1m_2 > 0$ we have

$$m_1m_2 \equiv (KL/m_1m_2) \mod (p-\varepsilon)/p_1p_2.$$

Certainly $q^2\|(p-\varepsilon)/p_1p_2$ and $\psi(a) \mid q-1$. By Lemma 2 we have $m_i \equiv 1 \mod a$ for $i = 1,2$, hence

$$m_1m_2 \equiv 1 \mod a.$$

Since $4KL \mid a$, we obtain $m_1m_2 \equiv 1 \mod 4KL$, hence $(KL/m_1m_2) = 1$ and

$$m_1m_2 \equiv 1 \mod (p-\varepsilon)/p_1p_2.$$

Since $\psi(p_1p_2) \mid q-1$, $q^2\|(p-\varepsilon)/p_1p_2$, by Lemma 2 we have $m_i \equiv 1 \mod p_1p_2$. But $p_1p_2\|p-\varepsilon$, hence

$$m_1m_2 \equiv 1 \mod (p-\varepsilon).$$

The requirement on q that $\psi(c^2) \mid q-1$ by Lemma 2 implies $m_1m_2 \equiv 1 \mod c^2$. Since $p-\varepsilon \equiv cq \mod c^2$ we have $\frac{p-\varepsilon}{c} \equiv q \mod c$. Thus $m_1m_2 \equiv 1 \mod (p-\varepsilon)c$, hence

$$m_1m_2 \equiv 1 \mod \big((i-1)a+1\big)(p-\varepsilon).$$

But $A_i \equiv \varepsilon \mod \big((i-1)a+1\big)(p-\varepsilon)$. Since $\left(A_i, \phi\left(\frac{p-\varepsilon}{p_1}\right)\phi\left(\frac{p-\varepsilon}{p_2}\right)\right) = 1$ we have

$$n_i = A_im_1m_2 \mid P\left(\alpha,\beta;(p-\varepsilon)\big((i-1)a+1\big)\middle|P\big(\alpha,\beta;n_i-(KL/n_i)\big)\right),$$

where $(KL/n_i) = (KL/A_im_1m_2) = (KL/A_i)(KL/m_1m_2) = \varepsilon\cdot 1 = \varepsilon$.

Since $A_i \equiv b \mod a$, $m_1m_2 \equiv 1 \mod a$ we have $n_i \equiv b \mod a$. So each number $A_im_1m_2$ is a Lehmer pseudoprime with parameters L, M and the numbers $A_im_1m_2$ form an arithmetic progression with the common difference $(A_{i+1}-A_i)m_1m_2 = a(p-\varepsilon)m_1m_2$.

This completes the proof of our Theorem.

References

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

[2] BAILLIE R. & WAGSTAFF S. JR., *Lucas pseudoprimes*, Math. Comp. 35 (1980), 1391–1417.

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

[4] CARMICHAEL R.D., *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2) 15 (1913), 30–70.

[5] CHOWLA S., *There exists an infinity of 3-combinations of primes in A.P.*, Proc. Lahore Philos. Ser. 6, no 2 (1944), 15–16.

[6] CIPOLLA M., *Sui numeri composti P che verificiano la congruenza di Fermat* $a^{P-1} \equiv 1 \pmod{P}$, Annali di Matematica (3) 9 (1904), 139–160.

[7] CONWAY J.H., GUY R.K., SCHNEEBERGER W.A., SLOANE N.J.A., *The primary pretenders*, Acta Arith. 78 (1997), 307–313.

[8] DICKSON L.E., *A new extension of Dirichlet's theorem on prime numbers*, Messenger Math. 33 (1904), 155-161.

[9] DICKSON L.E., *History of the Theory of Numbers*, 3 vols., Washington 1919–1923, reprint New York 1966.

[10] DUPARC H.J.A., *On almost primes of the second order*, Math. Centrum Amsterdam. Rap. ZW 1955-013, (1955), 1–13 .

[11] DUPARC H.J.A., *A remark to report Z.W.-013*, Math. Centrum Amsterdam, Rap. Z.W. 1956-008.

[12] DURST L.K., *Exceptional real Lehmer sequences*, Pacific J. Math. 9 (1959), 437–441.

[13] ERDŐS P., *On almost primes*, Amer. Math. Monthly 57 (1950), 404–407.

[14] GRANVILLE A.J., *The prime k-tuplets conjecture implies that there are arbitrarily long arithmetic progressions of Carmichael numbers* (written communication of December 1995).

[15] HEATH-BROWN D.R., *Three primes and an almost prime in arithmetic progression*, J. London Math. Soc., (2) 23 (1981), 396–414.

[16] JEANS J.A., *The converse of Fermat's theorem*, Messenger of Mathematics 27 (1898), p. 174.

[17] KERNBAUM S., *O szeregu Fibonacciego i jego uogólnieniach*, Wiadom. Mat. 24 (1920), 203–217, II ibid. 25 (1921), 49–68.

[18] KORSELT A., *Probléme chinois*, L'intermédiare des mathematiciens 6 (1899), 142–143.

[19] LEHMER D.H., *An extended theory of Lucas functions*, Ann. of Math. 31 (1930), 419–448.

[20] LEHMER E., *On the infinitude of Fibonacci pseudoprimes*, Fibonacci Quart. 2 (1964), 229–230.

[21] LEHMER D.H., *Strong Carmichael numbers*, J. Austral. Math. Soc. Ser. A 21 (1978), 508–510.

[22] MCDANIEL W.L., *Some pseudoprimes and related numbers having special forms*, Math. Comp. 53 (1989), 407–409.

[23] MAHNKE D., *Leibniz and der Suche nach einer allgemeinem Primzahlgleichung*, Bibliotheca Math. Vol. 13 (1913), 29–61.

[24] NEEDHAM J., *Science and Civilization in China*, vol. 3: Mathematics and Sciences of the Heavens and the Earth, Cambridge 1959, p. 54, footnote A.

[25] NIEWIADOMSKI R., *Spostrze.zenia nad liczbami szeregu Fibonacciego*, Wiadom. Mat. 15 (1911), 225–233.

[26] RIBENBOIM P., *The New Book of Prime Number Records*, Springer–Verlag, New York – Heidelberg – Berlin, 1996.

[27] ROTKIEWICZ A., *Sur les formules donnant des nombres pseudopremiers*, Colloq. Math. 12 (1964), 69–72.

[28] ROTKIEWICZ A., *Sur les progressions arithmétiques et géométriques formées de trois nombres pseudopremiers distincts*, Acta Arith. 10 (1964), 325–328.

[29] ROTKIEWICZ A., *On arithmetical progressions formed by k different pseudoprimes*, J. Math. Sci. 4 (1969), 5–10.

[30] ROTKIEWICZ A., *Pseudoprime numbers and their generalizations*, Student Association of the Faculty of Sciences, University of Novi Sad, Novi Sad 1972, pp. i+169.

[31] ROTKIEWICZ A., *On the pseudoprimes of the form $ax + b$ with respect to the sequence of Lehmer*, Bull. Acad. Polon. Sci. Sér. Math. Astronom. Phys. 20 (1972), 349–354.

[32] ROTKIEWICZ A., *The solution of W. Sierpiński's problem*, Rend. Circ. Mat. Palermo (2) 28 (1979), 62–64.

[33] ROTKIEWICZ A., *Arithmetical progression formed from three different Euler pseudoprimes for the odd base a*, Rend. Circ. Mat. Palermo (2) 29 (1980), 420–426.

[34] ROTKIEWICZ A., *On Euler Lehmer pseudoprimes and strong Lehmer pseudoprimes with parameters L, Q in arithmetic progression*, Math. Comp. 39 (1982), 239–247.

[35] ROTKIEWICZ A., *On strong Lehmer pseudoprimes in the case of negative discriminant in arithmetic progressions*, Acta Arith. 68 (1994), 145–151.

[36] ROTKIEWICZ A., *Arithmetical progressions formed by k different pseudoprimes*, Rend. Circ. Mat. Palermo (2) 43 (1994), 391–402.

[37] ROTKIEWICZ A. AND ZIEMAK K., *On even pseudoprimes*, The Fibonacci Quarterly, 33 (1995), 123–125.

[38] ROTKIEWICZ A., *There are infinitely many arithmetical progressions formed by three different Fibonacci pseudoprimes*, Applications of Fibonacci Numbers, Volume 7, Edited by G.E. Bergum, A.N. Philippou and A.F. Horadam, Kluwer Academic Publishers, Dordrecht, the Netherlands 1998, 327–332.

[39] ROTKIEWICZ A., *Arithmetical progression formed by Lucas pseudoprimes*, Number Theory, Diophantine, Computational and Algebraic Aspects, Editors: Kálmán Győry, Attila Pethő and Vera T. Sós, Walter de Gruyter GmbH & Co., Berlin, New York 1998, 465–472.

[40] ROTKIEWICZ A., *Periodic sequences of pseudoprimes connected with Carmichael numbers and the least period of the function* l_x^C, Acta Arith. 91 (1999), 75–83.

[41] ROTKIEWICZ A., Schinzel A., *Lucas pseudoprimes with a prescribed value of the Jacobi symbol*, Bull. Polish Acad. Sci. Math. 48 (2000), 77–80.

[42] SCHINZEL A., *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Mat. 4 (1962), 413–416.

[43] SCHINZEL A., *On primitive prime factors of Lehmer numbers I*, Acta Arith. 8 (1963), 213–223.

[44] SCHINZEL A., SIERPIŃSKI W., *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), 185–208, and corrigendum, ibidem 5 (1960), 259.

[45] SIERPIŃSKI W., *Remarque sur une hypothèse des Chinois concernant les nombres* $(2^n - 2)/n$, Colloq. Math. 1 (1947), 9.

[46] SIERPIŃSKI, W., *Elementary Theory of Numbers*, Monografie Matematyczne 42, PWN, Warsaw 1964 (second edition: North-Holland, Amsterdam, New York, Oxford 1987).

[47] STEUERWALD R., *Über die Kongruenz* $2^{n-1} \equiv 1 (\mod n)$, Sitz.-Ber. math. naturw. Kl. Bayer. Akad. Wiss. München 1947, 177.

[48] SZYMICZEK K., *Kilka twierdzeń o liczbach pseudopierwszych*, Zeszyty naukowe Wy.zszej Szkoły Pedagogicznej w Katowicach, Sekcja Matematyki, Zeszyt Nr 5 (1966), 39–46.

[49] SZYMICZEK K., *Note on Fermat numbers*, Elem. Math. 21 (1966), 59.

[50] VAN DER CORPUT J.G., *Über Summen von Primzahlen und Primzahlquadraten*, Math. Ann. 116 (1939), 1–50.

[51] WARD M., *The intrinsic divisor of Lehmer numbers*, Ann. of Math. (2) 62 (1955), 230–236.

[52] ZSIGMONDY K., *Zur Theorie der Potenzreste*, Monatsh. Math. 3 (1892), 265–284.

Author's address: Institute of Mathematics, Polish Academy of Sciences, ul. Śniadeckich 8, skr. poczt. 137, 00-950 Warszawa, Poland

E-mail: rotkiewi@impan.gov.pl

Received: May 20, 2000