Annales Mathematicae Silesianae **21** (2007), 49–60
Prace Naukowe Uniwersytetu Śląskiego nr 2617, Katowice

ON LUCAS NUMBERS, LUCAS PSEUDOPRIMES AND A NUMBERTHEORETICAL SERIES INVOLVING LUCAS PSEUDOPRIMES AND CARMICHAEL NUMBERS

Andrzej Rotkiewicz

Abstract. The following theorems are proved:

(1) If α and $\beta \neq \alpha$ are roots of the polynomial $x^2 - Px + Q$, where $\gcd(P, Q) = 1$, $P = \alpha + \beta$ is an odd positive integer, then $(\alpha+\beta)^{n+1} | \alpha^x + \beta^x$ if and only if $x = (2l+1)(\alpha+\beta)^n$, where $l = 0, 1, 2, \ldots$ and then

$$\gcd\left(\frac{\alpha^{(\alpha+\beta)^n} + \beta^{(\alpha+\beta)^n}}{(\alpha+\beta)^{n+1}},\ \alpha+\beta\right) = 1.$$

(2) Given integers P, Q with $D = P^2 - 4Q \neq 0, -Q, -2Q, -3Q$ and $\varepsilon = \pm 1$, every arithmetic progression $ax + b$, where $\gcd(a, b) = 1$ contains an odd integer n_0 such that $(D|n_0) = \varepsilon$. The series $\sum_{n=1}^{\infty} 1/\log P_n^{(a)}$, where $P_n^{(a)}$ is the n-th strong Lucas pseudoprime with parameters P and Q of the form $ax + b$, where $\gcd(a, b) = 1$ such that $(D|P_n^{(a)}) = \varepsilon$, is divergent.

(3) Let C_n denote the n-th Carmichael number. From the conjecture of P. Erdős that $C(x) > x^{1-\varepsilon}$ for every $\varepsilon > 0$ and $x \geq x_0(\varepsilon)$, where $C(x)$ denotes the number of Carmichael numbers not exceeding x it follows that the series $\sum_{n=1}^{\infty} 1/C_n^{1-\varepsilon}$ is divergent for every $\varepsilon > 0$.

Let P, Q be non-zero integers. Then the polynomial $x^2 - Px + Q$, has the roots $\alpha, \beta = \frac{P \pm \sqrt{D}}{2}$, where $D = P^2 - 4Q$.

Received: 1.12.2006. Revised: 27.02.2007.
(2000) Mathematics Subject Classification: 11A07, 11B39.
Key words and phrases: Carmichael number, Lucas number, Lucas pseudoprime.

For each $n \geq 0$, define $u_n = u_n(P,Q)$ and $v_n = v_n(P,Q)$ by:

$$u_0 = 0,\ u_1 = 1,\ u_n = Pu_{n-1} - Qu_{n-2} \text{ (for } n \geq 2),$$
$$v_0 = 2,\ v_1 = P,\ v_n = Pv_{n-1} - Qv_{n-2} \text{ (for } n \geq 2).$$

The sequences $u_n(P,Q)$ and $v_n(P,Q)$ are called the first and second Lucas sequences with parameters P and Q. If $\eta = \alpha/\beta$ is a root of unity then the sequences $u_n(P,Q)$, $v_n(P,Q)$ are said to be *degenerate*.

If $\gcd(P,Q) = 1$, then for degenerate sequence we have $(P,Q) = (1,1)$, $(-1,1), (2,1)$ or $(-2,1)$. If the sequence is degenerate, then $D = 0$ or $D = -3$. For $D \neq 0$ by Binet's formulas:

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},\ v_n = \alpha^n + \beta^n,$$
$$u_n(-P,Q) = (-1)^{n-1}u_n(P,Q),\ v_n(-P,Q) = (-1)^n v_n(P,Q).$$

1. Historical remarks

In the book [2], which contains every extant work by E. Galois (1811–1832) on page 301 it is written:

$$8,\ 27,\ 64,\ 125,\ 343,\ 512,\ 729,\ 1000$$
$$\frac{3^3+5^3}{2^3},\ \frac{4^3+5^3}{3^3},\ \frac{2^3+7^3}{3^3},\ \frac{5^3+7^3}{3^3}$$

(in the denominator of last number, instead 3^3 should be $3^2 \cdot 2^2$).

The above passage of Galois manuscript suggests that $m(a+b)|a^m + b^m$ if $2 \nmid m$ and every prime factor of m divides $a+b$.

We note here that E.E. Kummer [11] (see L.E. Dickson [5], p. 737) showed that if an n is odd prime we have

$$\frac{a^n \pm b^n}{a \pm b} = (a \pm b)^{n-1} \mp (a \pm b)^{n-3}ab + \frac{n(n-3)}{2}(a \pm b)^{n-5}a^2b^2 \mp \dots$$

and if the above number and $a \pm b$ have a common factor, it divides the last term $\pm n(ab)^{(n-1)/2}$, and is equal n if a and b are relatively prime with n.

Since the coefficients n, $n(n-3)/2, \dots$ are divisible by n, the exponent of the highest power of n dividing $a^n \pm b^n$ exceeds by unity that in $a \pm b$. T. Boncler (see W. Sierpiński [24], p. 67) proved that for every odd n and coprime integers a and b we have $(a+b)^2|a^n + b^n$ if and only if $(a+b)|n$.

The author proved [17] that if $(a,b)=1$ and $a+b$ is a positive odd integer then $(a+b)^{n+1}|a^x+b^x$ if and only if $x=(2l+1)(a+b)^n$, where $l=0,1,2,\dots$ and

$$\gcd\left(\frac{a^{(a+b)^n}+b^{(a+b)^n}}{(a+b)^{n+1}},\ a+b\right)=1.$$

Here we shall prove the following generalization of the above theorem.

Theorem 1. *If α and $\beta\neq\alpha$ are roots of the polynomial x^2-Px+Q, where $\gcd(P,Q)=1$, $P=\alpha+\beta$ is an odd positive integer, then $(\alpha+\beta)^{n+1}|\alpha^x+\beta^x$ if and only if $x=(2l+1)(\alpha+\beta)^n$, where $l=0,1,2,\dots$ and then*

$$\gcd\left(\frac{\alpha^{(\alpha+\beta)^n}+\beta^{(\alpha+\beta)^n}}{(\alpha+\beta)^{n+1}},\ \alpha+\beta\right)=1.$$

Proof. By the so-called law of repetition [26, p. 87] we have:

Let p^e (with $e\geq 1$) be the exact power of p dividing u_n. We shall write $p^e\|u_n$ when $p^e|u_n$, $p^{e+1}\nmid u_n$. Let $f\geq 1$, $p\nmid k$. Then, p^{e+f} divides u_{nkp^f}. Moreover, if $p\nmid Q$, $p^e\neq 2$ then p^{e+f} is the exact power of p dividing u_{nkp^f}.

For the sequence v_n we have:

If p is an odd prime, $\lambda>0$ and $p^\lambda\|v_m$, then $p^{\alpha+\mu}\|v_{mnp^\mu}$, where $p\nmid n$, n is odd, and $\mu\geq 0$.

Let $v_1=\alpha+\beta=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, where $p_1,p_2,\dots,p_k$ are odd primes. We have $(\alpha+\beta)^{n+1}=p_1^{\alpha_1+n\alpha_1}p_2^{\alpha_2+n\alpha_2}\dots p_k^{\alpha_k+n\alpha_k}$ and by law of repetition for v_n we have
$(\alpha+\beta)^{n+1}|\alpha^x+\beta^x$ if and only if $x=(2l+1)p_1^{n\alpha_1}p_2^{n\alpha_2}\dots p_k^{n\alpha_k}=(2l+1)(\alpha+\beta)^n$, where $l=0,1,2,\dots$ and since by law of repetition: $p_1^{\alpha_i+n\alpha_i}\|v_{p_i^{n\alpha_i}}$ for $i=1,2,\dots,k$ thus

$$\gcd\left(\frac{\alpha^{p_1^{n\alpha_1}p_2^{n\alpha_2}\dots p_k^{n\alpha_k}}+\beta^{p_1^{n\alpha_1}p_2^{n\alpha_2}\dots p_k^{n\alpha_k}}}{p_1^{\alpha_1+n\alpha_1}p_2^{\alpha_2+n\alpha_2}\dots p_k^{\alpha_k+n\alpha_k}},\ p_1p_2\dots p_k\right)=1$$

and

$$\gcd\left(\frac{\alpha^{(\alpha+\beta)^n}+\beta^{(\alpha+\beta)^n}}{(\alpha+\beta)^{n+1}},\ \alpha+\beta\right)=1. \qquad \square$$

Examples

1) $P=\alpha+\beta=3$, $Q=\alpha\cdot\beta=-1$, $D=P^2-4Q=13$; the characteristic polynomial is x^2-3x-1; $v_0=2$, $v_1=3$, $v_n=3v_{n-1}+v_{n-2}$ $(n\geq 2)$,
$v_0=2$, $v_1=3$; $v_2=11$, $v_3=36=2^2\cdot 3^2$, $v_4=119=7\cdot 17$, $v_5=393=3\cdot 131$,

$v_6 = 1298 = 2 \cdot 11 \cdot 59$, $v_7 = 4287 = 3 \cdot 1429$, $v_8 = 14159$, $v_9 = 46764 = 2^2 \cdot 3^3 \cdot 433$, $(\alpha+\beta)^3 = 3^3 | \alpha^{(\alpha+\beta)^2} + \beta^{(\alpha+\beta)^2}$ and

$$\gcd\left(\frac{\alpha^{(\alpha+\beta)^2} + \beta^{(\alpha+\beta)^2}}{(\alpha+\beta)^3},\ \alpha+\beta\right) = \gcd\left(\frac{2^2 \cdot 3^3 \cdot 443}{3^3},\ 3\right) = 1.$$

2) $P = 3$, $Q = 1$ we have $\alpha, \beta = \frac{3 \pm \sqrt{5}}{2}$, $v_0 = 2$, $v_1 = 3$, $\alpha, \beta = \frac{3 \pm \sqrt{5}}{2}$, $v_n = 3v_{n-1} - v_{n-2}$ $(n \geq 2)$
$v_0 = 2$, $v_1 = 3$, $v_2 = 7$, $v_3 = 18$, $v_4 = 47$, $v_5 = 123 = 3 \cdot 41$, $v_6 = 322 = 2 \cdot 7 \cdot 23$, $v_7 = 843 = 3 \cdot 281$, $v_8 = 2207$, $v_9 = 5778 = 2 \cdot 3^3 \cdot 107$

$$3^3 \| v_9,\ \gcd\left(\frac{\alpha^{(\alpha+\beta)^2} + \beta^{(\alpha+\beta)^2}}{(\alpha+\beta)^3},\ \alpha+\beta\right) = \gcd\left(\frac{2 \cdot 3^3 \cdot 107}{3^3},\ 3\right) = 1.$$

2. Landau's and Jarden's results

Let $P = 1$, $Q = -1$, so $D = 5$.

The Lambert series is $L(x) = \sum_{n=1}^{\infty} \frac{x^n}{1-x^n} = x + 2x^2 + 2x^3 + \ldots$ in which the coefficient of x^n is $d(n)$ – the number of the divisors of n. The Lambert series is convergent for $0 < x < 1$. Let F_n denote the n-th Fibonacci number.

E. Landau [12] had evaluated $\sum_{n=0}^{\infty} 1/F_n$ in terms of the sum of Lambert's series and $\sum_{n=0}^{\infty} 1/F_{2n+1}$ in relation to theta Jacobi series which are defined as follows, for $0 < |q| < 1$ and $z \in C$:

$$\theta_1(z,q) = i \sum_{n=-\infty}^{\infty} (-1)^n q^{(n-\frac{1}{2})^2} e^{(2n-1)\pi i z},$$

$$\theta_2(z,q) = \sum_{n=-\infty}^{\infty} q^{(n+\frac{1}{2})^2} e^{(2n-1)\pi i z},$$

$$\theta_3(z,q) = \sum_{n=-\infty}^{\infty} q^{n^2} e^{2n\pi i z},$$

$$\theta_4(z,q) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} e^{2n\pi i z}.$$

In particular, we have

$$\begin{aligned}
\theta_1(0,q) &= 0,\\
\theta_2(0,q) &= 2q^{1/4} + 2q^{9/4} + 2q^{25/4} + \ldots,\\
\theta_3(0,q) &= 1 + 2q + 2q^4 + 2q^9 + \ldots,\\
\theta_4(0,q) &= 1 - 2q + 2q^4 - 2q^9 + \ldots.
\end{aligned}$$

Landau's result (see E. Landau [12] and P. Ribenboim [16, pp. 51–61]) are

Theorem L_1:
$\sum\limits_{n=1}^{\infty} 1/F_{2n} = \sqrt{5}\left[L\left(\frac{3-\sqrt{5}}{2}\right) - L\left(\frac{7-3\sqrt{5}}{2}\right)\right] = \sqrt{5}\left[L\left(\beta^2\right) - L\left(\beta^4\right)\right],\ \beta = \frac{1-\sqrt{5}}{2}.$

Theorem L_2:
$\sum\limits_{n=0}^{\infty} 1/F_{2n+1} = -\sqrt{5}\left(1 + 2\beta^4 + 2\beta^{16} + 2\beta^{36} + \ldots\right)$
$\left(\beta + \beta^9 + \beta^{25} + \ldots\right) = -\frac{\sqrt{5}}{2}\left[\theta_3(0,\beta) - \theta_2(0,\beta^4)\right]\theta_2(0,\beta^4).$

In 1948 D.R. Jarden [10] gave the following generalization of Landau's theorem.

Let $u_0 = 0$, $u_1 = 1$, $u_n = Pu_{n-1} + u_{n-2}$ ($n = 2, 3, 4, \ldots$; P, an arbitrary positive real number) and $D = P^2 + 4$. Let $a = \frac{P-\sqrt{D}}{2}$ ans $b = \frac{P+\sqrt{D}}{2} = -\frac{1}{a}$ be the roots of the equation $x^2 - Px - 1 = 0$.

Jarden's results are the following:

Theorem J_1: *The series* $\sum\limits_{n=1}^{\infty} \frac{1}{u_{2n}}$ *converges and*

$$\sum_{n=1}^{\infty} 1/u_{2n} = \sqrt{D}\left(L\left(a^2\right) - L\left(a^4\right)\right).$$

Theorem J_2: *The series* $\sum 1/u_{2n+1}$ *converges and*

$$\sum_{n=0}^{\infty} 1/u_{2n+1} = -\sqrt{D}\left(1 + 2a^4 + 2a^{16} + 2a^{36} + \ldots\right)\left(a + a^9 + a^{25} + \ldots\right).$$

3. Lucas pseudoprimes

Let a, b be relatively prime integers with $|a| > |b| > 0$. For any $n > 0$, let $\phi_n(a, b)$ denote the n-th homogeneous cyclotomic polynomial, defined by

$$\phi_n(a,b) = \prod_{d|n} \left(a^d - b^d\right)^{\mu(n/d)},$$

where μ is the Möbius function.

Definition 1. A composite n is called a *pseudoprime* if $n|2^n - 2$.

Definition 2. If $1 \leq d_1 < d_2 < \ldots < d_k$ are integers, we shall call the number $n = \prod_{i=1}^{n} \phi_{d_i}(2,1)$ a cyclotomic number and if n is a pseudoprime we shall call it a cyclotomic pseudoprime.

The above definition was introduced in 1982 by C. Pomerance (see [15]). In the paper [22] it was proved the following:

Theorem P$_1$: *If $n > 3$ is a prime or an odd pseudoprime then the number $(2^n - 1)\phi_{2^n-2}(2)$ is a cyclotomic pseudoprime.*

Examples

The least cyclotomic pseudoprime of the form $(2^n - 1)\phi_{2^n-2}(2)$ is $(2^5 - 1)\phi_{30}(2) = 31 \cdot 331 = 10261$. For pseudoprime 341 we get the cyclotomic pseudoprime $(2^{341} - 1)\phi_{2^{341}-2}(2)$.

Definition 3. A composite number n is called a Lucas pseudoprime with parameters P and Q if $(n, 2DQ) = 1$ and

$$U_{n-(D|n)} \equiv 0 \pmod{n}, \tag{1}$$

where $(D|n)$ is the Jacobi symbol.

Instead of $\phi_n(\alpha, \beta)$, where α and β are roots of the polynomial $x^2 - Px + Q$ we shall write ϕ_n.

Definition 4. If $1 \leq d_1 < d_2 < \ldots < d_k$ are integers, we shall call the number $n = \prod_{i=1}^{k} \phi_{d_i}$ a cyclotomic Lucas number and if n is a pseudoprime we shall call it Lucas cyclotomic pseudoprime.

In the paper [22] the author proved the following:

Theorem P_2: *If $p > 5$, $P = \alpha + \beta \geq 1$, $Q = \alpha\beta = -1$, $p \nmid P^2 + 4 = D$, then the number $u_p \phi_{u_p - (D|u_p)}$ is a cyclotomic Lucas pseudoprime.*

Examples

1) For $P = 1$, $Q = -1$ we get Fibonacci sequence $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \dots$ and companion Fibonacci sequence

$$v_n(1, -1) : 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, \dots .$$

The least Fibonacci cyclotomic pseudoprime (that is cyclotomic Lucas pseudoprime for $P = 1$, $Q = -1$) we get for $p = 7$. For $p = 7$ we have $u_p \phi_{u_p - (5|u_p)} = u_7 \cdot \phi_{14} = u_7 \cdot v_7 = 13 \cdot 29 = 377$.

2) For $P = 2$, $Q = -1$ the numbers $u_n = u_n(2, -1)$ and $v_n = v_n(2, -1)$ are the *Pell numbers* and the *companion Pell numbers*. We have

$$u_n(2, -1) : 0, 1, 2, 5, 12, 29, 70, 169, \dots ,$$
$$v_n(2, -1) : 2, 2, 6, 14, 34, 82, 198, 478, \dots .$$

The smallest Pell cyclotomic pseudoprime of the form $u_p \phi_{u_p - (8|u_p)}$ we get for $p = 3$. We have $u_3 \phi_{u_3 - (8|u_3)} = 5\phi_{5-(8|5)} = 5\phi_{5+1} = 5\phi_6 = 5 \cdot 7 = 35$.

Problem 1. Let P, Q be non-zero rational integers $P \geq 1$, $Q \neq -1$. Does there exist a natural number n_0 such that for every prime number $p > n_0$ the number $u_p \Phi_{u_p - (D|u_p)}$ is a cyclotomic Lucas pseudoprime with parameters P and Q?

3.1. Number theoretical series involving Lucas pseudoprimes and Carmichael numbers

Let $P(x)$ denote the number of pseudoprimes $\leq x$. In 1949 P. Erdős stated that

$$C_1 \log x < P(x) < c_2 x / (\log x)^k, \quad \text{for every } k \text{ and } x > x_0(k). \tag{2}$$

K. Szymiczek [25] proved, using the following result of P. Erdős [6]

$$P(x) < 2x \exp\left\{-\frac{1}{3}(\log x)^{1/4}\right\} \text{ if } x > x_0 \tag{3}$$

that $1/P_n < 2/n(\log n)^{4/3}$. Therefore $\sum\limits_{n=1}^{\infty} 1/P_n < \sum\limits_{n=1}^{\infty} 2/(\log n)^{4/3}$ and since the last series is convergent $\sum\limits_{n=1}^{\infty} 1/P_n$ is also convergent.

The author asked [18, Problem 47] whether the series $\sum 1/\log P_n$ is convergent. A. Mąkowski [13] proved that the series $\sum 1/\log P_n$ is divergent, where P_n denotes the n-th pseudoprime with respect to c (n is a pseudoprime to the base c if n is composite and $n|c^n - c$). He used the fact established by M. Cipolla [3] that the number $(c^{2p}-1)/(c^2-1)$ is a pseudoprime to the base c such that $p \nmid c^2 - 1$ and that the series $\sum 1/p$, where p runs over the primes, is divergent.

First we note that the divergence of $\sum\limits_{n=1}^{\infty} 1/\log P_n$ follows from the estimation $P(x) > c \log x$ (see A. Rotkiewicz, R. Wasén [19]). Indeed, if we put $x = P_n$ in the last inequality we get

$$P(P_n) > c \log P_n \tag{4}$$

and the divergence follows at once from the well-known divergence of the harmonic series.

Definition 5. A composite number n is called a strong Lucas pseudoprime with parameters P and Q if $(n, 2QD) = 1$, $n-(D|n) = 2^3 \cdot r$ are odd and

(5) either $\quad u_r \equiv 0 \pmod{n} \quad$ or $\quad v_{2^t r} \equiv 0 \pmod{n} \quad$ for some $t,\ 0 \le t < 9$.

C. Pomerance put forward (see [21, p. 78]) the following question.

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 $(D|n) = -1$.

An affirmative answer to this question in the strong sense (infinitely many n) is contained, except in the trivial cases $P^2 = Q, 2Q, 3Q$ in the following theorem, which follows from the results of [21].

Theorem T (see [21]): *Given integers P, Q with $D = P^2 - 4Q \neq 0, -Q, -2Q, -3Q$ 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.

Now we shall prove the following

Theorem 2. *Given integers* P, Q *with* $D = P^2 - 4Q \neq 0, -Q, -2Q, -3Q$ *and* $\varepsilon = \pm 1$, *every arithmetic progression* $ax + b$, *where* $(a, b) = 1$ *contains an odd integer* n_0 *such that* $(D|n) = \varepsilon$. *The series* $\sum_{n=1}^{\infty} 1/\log P_n^{(a)}$, *where* $P_n^{(a)}$ *is the* n*-th strong Lucas pseudoprime with parameters* P *and* Q *of the form* $ax + b$, *where* $(a, b) = 1$ *such that* $(D|P_n^{(a)}) = \varepsilon$ *is divergent.*

Proof. Let $P^{(a)}$ the n-th strong pseudoprime of the form $ax + b$, where $(a, b) = 1$ with $(D|P_n^{(a)}) = \varepsilon$.

By Theorem T

$$\mathcal{N}^{(a)}(X) \gg \frac{\log X}{\log\log X}.$$

Put $X = P_n^{(a)}$, hence

$$\mathcal{N}^{(a)}\left(P_n^{(a)}\right) \gg \frac{\log P_n^{(a)}}{\log\log P_n^{(a)}},$$

hence

$$n \gg \frac{\log P_n^{(a)}}{\log\log P_n^{(a)}}. \tag{6}$$

Thus by (6) we have

$$\log n \gg \log\log P_n^{(a)}. \tag{7}$$

By (6) and (7) we have

$$\log P_n^{(a)} \ll n\left(\log\log P_n^{(a)}\right) \ll n \log n. \tag{8}$$

Hence, it follows that

$$\sum 1/\log P_n^{(a)} \gg \sum 1/n \log n \tag{9}$$

and the divergence of the series $\sum 1/\log P_n^{(a)}$ follows from well known divergence of $\sum 1/n \log n$. $\square$

3.2. Carmichael numbers

Definition 6. A composite number n is Carmichael number if

$$n|\,(a^n - a) \quad \text{for all } a \in \mathcal{N}.$$

In 1994 W.R. Alford, A. Granville and C. Pomerance proved [1] the following

Theorem A. G. P. *There are infinitely many Carmichael numbers. In particular, for x sufficiently large, the number $C(x)$ of Carmichael numbers not exceeding x satisfies $C(x) > x^{2/7}$.*

The best result belongs to Glyn Harman. In 2005 he proved [9] the following theorem.

Theorem G. H. [9] *There exists $\beta > 0.33$ such that, for all sufficiently large x, we have*

$$C(x) > x^{\beta}. \tag{10}$$

Though P. Erdős [7] (see also A. Granville and C. Pomerance [8]), has conjectured that $C(x) > x^{1-\varepsilon}$ for every $\varepsilon > 0$ and $x \geq x_0(\varepsilon)$, we known no numerical value of x with $C(x) > x^{1/2}$ (see R. Crandall and C. Pomerance [4, p. 123]).

The following theorem holds

Theorem 3. *Let C_n denote the n-th Carmichael number. From the conjecture of P. Erdős that $C(x) > x^{1-\varepsilon}$ for every $\varepsilon > 0$ and $x > x_0(\varepsilon)$ it follows that the series $\sum\limits_{n=1}^{\infty} 1/C_n^{1-\varepsilon}$ is divergent for every $\varepsilon > 0$.*

Proof. Suppose that $\varepsilon > 0$ then by the conjecture of P. Erdős:

$$C(x) > x^{1-\varepsilon} \quad \text{for every } \varepsilon > 0 \text{ and } x > x_0(\varepsilon).$$

Put $x = C_n$. Then

$$C\left(C_n\right) > C_n^{1-\varepsilon} \quad \text{for } n > n_0(\varepsilon),$$

hence

$$n > C_n^{1-\varepsilon} \quad \text{for } n > n_0(\varepsilon), \tag{11}$$

and hence

$$\sum 1/C_n^{1-\varepsilon} \geq \sum 1/n, \tag{12}$$

and it follows that the series $\sum 1/C_n^{1-\varepsilon}$ is divergent. □

By conjecture of P. Erdős and C. Pomerance [7] the number $C(x)$ of Carmichael numbers not exceeding x satisfies

$$C(x) = x^{1-(1+0(1))\ln\ln\ln x/\ln\ln x}$$

as $x \to \infty$.

Denoting by $P_2(x)$ the number of base – 2 pseudoprimes up to x, C. Pomerance [14] proved that

$$C(x) < x^{1-\ln\ln\ln x/\ln\ln x},$$
$$P_2(x) < x^{1-\ln\ln\ln x/(2\ln\ln x)}$$

for all sufficiently large values of x.

References

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

[2] Bourgne R., Azra J.-P., *Ecrits mathematiques d'Évariste Galois*, Gauthier–Villars & Cle, Paris 1962.

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

[4] Crandall R., Pomerance C., *Prime numbers. A computational perspective*, Springer--Verlag, New York 200l.

[5] Dickson L.E., *History of the theory of numbers*, Vol. 2, New York 1952.

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

[7] Erdős P., *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1955), 201–206.

[8] Granville A., Pomerance C., *Two contradictory conjectures concerning Carmichael numbers*, Math. Comp. **71** (2001), 883–908.

[9] Harman G., *On the number of Carmichael numbers up to x*, Bull. London Math. Soc. **37** (2005), 641–650.

[10] Jarden D.R., *The series of inverses of a second order recurring sequence*, 3rd edition, Riveon Lematematika, Jerusalem 1973.

[11] Kummer E.E., *De aequatione $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ per numeros integros*, J. Reine Angew. Math. **17** (1897), 203–209.

[12] Landau E., *Sur la serie des inverses de nombres de Fibonacci*, Bull. Soc. Math. France **27** (1899), 298–300.

[13] Mąkowski A., *On a problem of Rotkiewicz on pseudoprimes*, Elem. Math. **29** (1974), 13.
[14] Pomerance C., *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593.
[15] Pomerance C., *A new lower bound for the pseudoprimes counting function*, Illinois J. Math. **26** (1982), 4–9.
[16] Ribenboim P., *My numbers, my friends*, Springer–Verlag, New York–Berlin–Heidelberg 2000.
[17] Rotkiewicz A., *On the properties of the expression* $a^n \pm b^n$, Prace Mat. **6** (1961), 1–20 (in Polish).
[18] Rotkiewicz A., *Pseudoprime numbers and their generalizations*, Student Association of the Faculty of Sciences, Univ. of Novi Sad, Novi Sad 1972.
[19] Rotkiewicz A., Wasen R., *On a numbertheoretical series*, Publ. Math. Debrecen **26** (1979), 1–4.
[20] Rotkiewicz A., *On strong Lehmer pseudoprimes in the case of negative discriminant in arithmetic progressions*, Acta Arith. **68** (1994), 145–151.
[21] Rotkiewicz A., Schinzel A., *Lucas pseudoprimes with a prescribed value of the Jacobi symbol*, Bull. Polish Acad. Sci. Math. **48** (2000), 77–80.
[22] Rotkiewicz A., *On pseudoprimes having special forms and a solution of K. Szymiczek's problem*, to appear in Acta Math. Univ. Ostraviensis (2007).
[23] Rotkiewicz A., *On Lucas cyclotomic pseudoprimes having special forms*, to appear in the Proceedings of the Twelfth International Conference on "Fibonacci Numbers and Their Applications", July 17 – July 21, 2006, San Francisco.
[24] Sierpiński W., *Teoria liczb*, Warszawa–Wrocław 1950.
[25] Szymiczek K., *On pseudoprimes which are products of distinct primes*, Amer. Math. Monthly **74** (1967), 95–97.
[26] Williams H.C., *Edouard Lucas and primality testing*, In: Canadian Mathematical Society Series of Monographs and Advanced Texts, Vol. 22, John Wiley & Sons Inc., New York 1998.

Institute of Mathematics
Polish Academy of Sciences
ul. Śniadeckich 8
00-956 Warszawa 10
skrytka pocztowa 21
Poland
e-mail: rotkiewi@impan.gov.pl