Periodic sequences of pseudoprimes connected with Carmichael numbers and the least period of the function $I^C_x$

by

A. Rotkiewicz (Warszawa)

The starting point of the present paper are the papers of Schinzel [10] and of Conway, Guy, Schneeberger and Sloane [4]. Following recent papers ([1], [4], [6], [7]) a composite $n$ is called a pseudoprime to base $b$ if $b^{n-1} \equiv 1 \mod n$. This definition does not coincide with the definition given in my book [9], where I defined

(i) a pseudoprime as a composite number dividing $2^n - 2$,
(ii) a pseudoprime with respect to $b$ as a composite number $n$ dividing $b^n - b$,
(iii) an absolute pseudoprime as a composite number $n$ that divides $b^n - b$ for every integer $b$ (see also Sierpiński [12]).

It is also worth pointing out that this terminology differs slightly from that of literature of tests for primality (Brillhart, Lehmer, Selfridge, et al.), where usual primes are included among the pseudoprimes.

Following recent papers a composite number $n$ is called a Carmichael number if $a^n \equiv a \mod n$ for every integer $a \geq 1$. The smallest Carmichael number is $561 = 3 \cdot 11 \cdot 17$.

The set of Carmichael numbers coincides with the set of composite $n$ for which $a^{n-1} \equiv 1 \mod n$ for every $a$ prime to $n$ (see Ribenboim [8], pp. 118, 119, and Sierpiński [12], p. 217). By Korselt’s criterion [5], $n$ 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 $x$. Recently, Conway, Guy, Schneeberger and Sloane [4] introduced the following

1991 Mathematics Subject Classification: Primary 11A07; Secondary 11B39.
A. Rotkiewicz

**Definition 1.** Any composite number $q$ such that $b^q \equiv b \pmod{q}$ is called a prime pretender to base $b$.

**Definition 2.** By $q_b$ we denote the least prime pretender $q$ to base $b$ and call such $q$ the primary pretender.

First we shall prove the following

**Theorem 1.** For every $b > 1$ there exist infinitely many prime pretenders to base $b$ which are not pseudoprimes to base $b$. That is, there exist infinitely many composite integers $n$ with $(b, n) > 1$ and $b^n \equiv b \pmod{n}$.

**Proof.** We begin with a definition. A prime $p$ which divides $b^n - 1$ and does not divide $b^k - 1$ for $0 < k < n$ is called a primitive prime factor of $b^n - 1$. By a theorem of Zsigmondy [13] such a prime factor $p \equiv 1 \pmod{n}$ exists for any $n > 2$ with the only exception $2^6 - 1 = 63$.

Now we note that to prove Theorem 1 it is enough to find one prime pretender $q$ with the required property. For, suppose $b^q \equiv b \pmod{q}$, $b^q - 1 \not\equiv 1 \pmod{q}$ and let $p$ be a primitive prime factor of $b^q - 1$.

We have $p = (q - 1)k + 1$, where $k$ is a positive integer. If $k = 1$ then $p = q$, which is impossible, since $q$ is composite, hence $p > q$ and $(p, q) = 1$.

From $b^{q-1} \equiv 1 \pmod{p}$ it follows that $b^q \equiv b \pmod{p}$ and from $b^q \equiv b \pmod{q}$ we get $b^q \equiv b \pmod{pq}$, hence $b^p \equiv b^p \pmod{pq}$. But since $q - 1 \mid p - 1$ we have

$$pq \mid b(b^{p-1} - 1) \mid b(b^{p-1} - 1) = b^p - b,$$

hence

$$b^p \equiv b \pmod{pq} \quad \text{and} \quad b^{pq} \equiv b \pmod{pq}.$$

From $b^{q-1} \not\equiv 1 \pmod{q}$, $b^q \equiv b \pmod{q}$ it follows that $(b, q) > 1$, hence $(b, pq) > 1$ and $b^{pq-1} \not\equiv 1 \pmod{pq}$.

It remains to find one prime pretender $q$ with the required property. For $b = 2$ such a $q = 2 \cdot 73 \cdot 1103$ was found by Lehmer in 1950, and Beeger [2] showed the existence of infinitely many even prime pretenders to base 2.

If $b > 2$ is composite, such a $q$ is equal to $b$, since $b^b \equiv b \pmod{b}$, but $b^{b-1} \not\equiv 1 \pmod{b}$, and if $b$ is prime $> 2$, such a $q$ is equal to $2b$, since $b^{2b} \equiv b \pmod{2b}$, $b^{2b-1} \not\equiv 1 \pmod{2b}$ (see Sierpiński [11]). Thus Theorem 1 is proved.

Already in 1958 Schinzel [10] proved that in the infinite sequence $q_1, q_2, \ldots$, there exist infinitely many terms equal to $q_b$ and that every term of this sequence belongs to the sequence $q_1, q_2, \ldots, q_{561!}$, so we can find all possible values of $q_b$. We have of course $q_b \leq 561$ for every $b$. Schinzel [10] also proved that there exists $b$ such that $q_b = 561$. He proved that $q_b \neq 4, 6$ if and only if $b \equiv 2, 11 \pmod{12}$ and put forward the following problem: Find all distinct primary pretenders [11].

In 1997 Conway, Guy, Schneeberger and Sloane [4] proved that there are only 132 distinct primary pretenders, and that $q_b$ is a periodic function of $b$. 
whose least period is the 122-digit number
1956858433460072587245340037736278982017213829337604336734362-
294738647777395483196097971852999259921329236506842360439300.

Let \( l_b \) denote the least pseudoprime to base \( b \). By a theorem of Cipolla [3] the number \( \left( \left( n! \right)^2 - 1 \right) / \left( \left( n! \right)^2 - 1 \right) \), where \( p \) is any odd prime such that \( p \) does not divide \( \left( n! \right)^2 - 1 \), is a pseudoprime to base \( n! \). If \( k \) is a pseudoprime to base \( n! \), then \( \left( n! \right)^k - 1 \equiv 1 \mod k \), hence \( (k, n!) = 1 \) and \( k \geq n! > n \). Thus the number of distinct values of \( l_b \) is unbounded, since \( l_{n!} > n \) and \( l_b \) is not a periodic function of \( b \).

We introduce the following definition.

**Definition 3.** Let \( C \) be a given Carmichael number. Then

\[
l^C_x = \begin{cases} 
  l_x & \text{if } (x, C) = 1, \\
  1 & \text{if } (x, C) > 1.
\end{cases}
\]

We have:

\[
\begin{align*}
l^{561}_1 &= l_1 = 4, & l^{561}_2 &= l_2 = 341, & l^{561}_3 &= 1, & l^{561}_4 &= l_4 = 15, & l^{561}_5 &= l_5 = 4, \\
l^{561}_6 &= 1, & l^{561}_7 &= l_7 = 6, & l^{561}_8 &= l_8 = 9, & l^{561}_9 &= 1, & l^{561}_{10} &= l_{10} = 9.
\end{align*}
\]

We have \( a^{C-1} \equiv 1 \mod C \) for every \( a \) coprime to \( C \). Let \( b \equiv a \mod C! \). Then \( b^{h-1} - 1 \equiv a^{h-1} - 1 \mod C! \), hence, for every \( h \leq C \), \( a^{h-1} \equiv 1 \mod h \) if and only if \( b^{h-1} \equiv 1 \mod h \), hence \( l^C_h = l^C_b \) for \( (a, C) = 1 \) and \( b \equiv a \mod C! \). Thus in the sequence \( \{l^C_a\}_{a=1}^\infty \), the numbers greater than 1 appear with period \( C! \), while the ones appear with period \( C \). Since \( \text{lcm}(C!, C) = C! \), the sequence \( \{l^C_x\}_{x=1}^\infty \) is periodic with period \( C! \) and the function \( l^C_x \) has period \( C! \). The following problems arise.

**Problem 1.** Find the least period of the function \( l^C_x \).

**Problem 2.** Find all composite numbers \( n \) which are values of the function \( l^C_x \).

Now we introduce the following

**Definition 4.** The Carmichael number \( C \) has property D if there exists a natural base \( a \) coprime to \( C \) such that \( l^C_a = C \).

**Definition 5.** The Carmichael number \( C \) has property A if there exists a Carmichael number \( C_1 < C \) such that \( C_1 | C \).

**Definition 6.** The Carmichael number \( C \) has property B if there does not exist a Carmichael number \( C_1 < C \) such that \( C_1 | C \).

Denote by \( C_n \) the \( n \)th Carmichael number. Among first 55 Carmichael numbers 7 have property A. These are: \( C_{15} = 7 \cdot 13 \cdot 19 \cdot 37, \ C_{19} = 7 \cdot 13 \cdot 19 \cdot 73, \ C_{21} = 7 \cdot 13 \cdot 31 \cdot 61, \ C_{22} = 7 \cdot 13 \cdot 19 \cdot 109, \ C_{24} = 5 \cdot 17 \cdot 29 \cdot 113, \ C_{39} = 7 \cdot 13 \cdot 19 \cdot 433, \)
$C_{43} = 7 \cdot 13 \cdot 19 \cdot 577$. Five numbers: $C_{15}, C_{19}, C_{22}, C_{39}, C_{43}$ are divisible by $C_3 = 7 \cdot 13 \cdot 19$ and $5 \cdot 17 \cdot 29 = C_4 \mid C_{24}, \; 7 \cdot 13 \cdot 31 = C_5 \mid C_{24}, \; 7 \cdot 13 \cdot 31 = C_5 \mid C_{21}$. The other 48 Carmichael numbers have property B.

**Theorem 2.** A Carmichael number $C$ has property D if and only if it has property B.

**Proof.** First, we prove that if a Carmichael number $C$ has property B then it has property D.

Let $C = p_1 \ldots p_k$. For each $p_i$ let $e_i$ be such that $p_i^{e_i} < C < p_i^{e_i+1}$, and let $g_i$ be a primitive root modulo $p_i^{e_i}$. By the Chinese remainder theorem, let $a$ be such that

1. $a \equiv 0 \mod p$ for all $p < C$, $p \neq p_1, \ldots, p_k$,
2. $a \equiv g_i \mod p_i^{e_i}$ ($1 \leq i \leq k$).

Suppose that $a^{n-1} \equiv 1 \mod n$ for $n$ composite. Then $(a, n) = 1$. From (1) it follows that $n > C$ or

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}, \quad \text{where } \alpha_i \geq 0.$$  

From $p_1^{e_1} \ldots p_k^{e_k} = n \leq C < p_i^{e_i+1}$, $p_i^{e_i} < C < p_i^{e_i+1}$ we get $\alpha_i \leq e_i$ for $i = 1, \ldots, k$.

Since $a$ is a primitive root modulo $p_i^{e_i}$ and $\alpha_i \leq e_i$, it follows that $a$ is also a primitive root modulo $p_i^{\alpha_i}$, hence

$$n \equiv 1 \mod \varphi(p_i^{\alpha_i}).$$

If $\alpha_i > 1$ then $n \equiv 1 \mod p_i(p_i - 1)$ and $0 \equiv 1 \mod p_i$, which is impossible. Thus $\alpha_i \leq 1$ ($1 \leq i \leq k$), and by (4), $n$ is a Carmichael number. But since we assumed that $C$ has property B we have $n = C$ and $C$ has property D.

Now we shall prove that if $C$ has property D then it has property B. It is enough to prove that if $C$ does not have property B, then $C$ does not have property D. But this is obvious, since then there exists $C_1 < C$, where $C_1$ is a Carmichael number such that $C_1 \mid C$, hence $a^{C_1 - 1} \equiv 1 \mod C_1$, where $C_1 < C, \; C_1 \mid C$ and $C$ does not have property D. $\blacksquare$

I raised the question: Do there exist infinitely many Carmichael numbers with property D?

A. Schinzel proved that the answer to this question is in the affirmative and the following theorem holds:

**Theorem 3.** There exist infinitely many Carmichael numbers with property D. There exist infinitely many Carmichael numbers with property A.
**Theorem of Alford, Granville and Pomerance** (see [1], p. 708). There are arbitrarily large sets of Carmichael numbers such that the product of any subset is itself a Carmichael number.

**Proof of Theorem 3** (due to A. Schinzel). Let \( \{C_1, \ldots, C_n\} \) be a set from the Theorem of Alford, Granville and Pomerance. Then each of the numbers \( C_1C_n, C_2C_n, \ldots, C_{n-1}C_n \) has property A.

It is easy to see that \( (C_i, C_j) = 1 \) for \( i \neq j \). Indeed, if \( (C_i, C_j) = d > 1 \) then a Carmichael number \( C_i \cdot C_j \) would be divisible by \( d^2 > 1 \), which is impossible.

Let \( c \) be the least divisor of a Carmichael number \( C \), which is itself a Carmichael number. Then \( c \) is a Carmichael number with property D. Indeed, if \( c = C \) then this is true. If \( c < C \) then \( c \) has property B and by Theorem 2 also property D.

Thus if in an arbitrarily large set \( \{C_1, \ldots, C_n\} \) we denote by \( c_i \) the least divisor of \( C_i \), which is itself a Carmichael number, then in the sequence \( c_1, \ldots, c_n \) we have \( (c_i, c_j) = 1 \), where each Carmichael number \( c_i \) has property B and by Theorem 2 also property D. Since \( n \) can be arbitrarily large, there exist infinitely many Carmichael numbers with property D and Theorem 3 is proved.

Now we solve Problem 1.

Let \( p!_k = p_1 \ldots p_k \) denote the product of the first \( k \) primes.

Let \( \varrho \) denote the least period of the function \( \ell^C_x \) \( (x = 1, 2, \ldots) \) and \([a_1, \ldots, a_n]\) denote the least common multiple of the integers \( a_1, \ldots, a_n \).

The following theorem holds:

**Theorem 4.** If a Carmichael number \( C \) has property D then the function \( \ell^C_x \) \( (x = 1, 2, \ldots) \) has period \( C! \) and the least period of \( \ell^C_x \) is \( \varrho = p!_mp!_r \), where \( p_m \) is the largest prime such that \( 2p_m < C \) and \( p_r \) is the largest prime such that \( p_r < C \).

If a Carmichael number \( C \) does not have property D, let \( C_1 \) denote the least Carmichael number such that \( C_1 \mid C \). Then the function \( \ell^C_x \) \( (x = 1, 2, \ldots) \) has period \( [C_1!, C] \) and the least period of \( \ell^C_x \) is equal to \([p!_mp!_r, C]\), where \( p_m \) denotes the largest prime such that \( 2p_m < C_1 \), and \( p_r \) is the largest prime number such that \( p_r^2 < C_1 \).

First we prove the following

**Lemma 1.** Let \( C = p_1 \ldots p_k \), \( g \) be a primitive root mod \( p^2 \), where \( p^2 < C \), and \( g_i \) be a primitive root mod \( p_i^2 \). Let \( x \) be such that (it exists, in view of the Chinese remainder theorem)
Then \( L^C_x = p^2 \).

Let \( p \) be a given prime such that \( 2p < C \), where \( p \) is odd. Let \( x \) be such that
\[
\begin{align*}
  x &\equiv 3 \mod 4, \\
  x &\equiv 1 \mod p, \\
  x &\equiv 0 \mod q \quad \text{for all } q < p, \ (q, C) = 1, \\
  x &\equiv g_i \mod p^2_i \quad \text{for } p_i \neq p, \ 1 \leq i \leq k.
\end{align*}
\]

Then \( L^C_x = 2p \).

**Proof.** If \( x \equiv g^p \mod p^2 \) then \( x^{p-1} \equiv g^{(p-1)p} \equiv 1 \mod p^2 \), hence \( x^{p-1} \equiv 1 \mod p^2 \), \( x^{p^2-1} \equiv 1 \mod p^2 \) and \( p^2 \) is a pseudoprime to base \( x \).

Now we prove that there does not exist a composite \( n \) such that \( x^{n-1} \equiv 1 \mod n \), where \( n < p^2 \). If such an \( n \) existed then it would be divisible by a prime \( q < p \). If \( (q, C) = 1 \) this is impossible, since by congruence (5) we have \( x \equiv 0 \mod q \).

Now we consider the case \( q, C \). If \( n \equiv g^p \equiv g \mod p \), where \( g \) is a primitive root mod \( p \).

Then \( n \equiv g^p \equiv 1 \mod p \), \( x \equiv 0 \mod q \), \( p \equiv g \equiv 1 \mod q \), \( p \equiv g \equiv 1 \mod q \).

Both cases are impossible.

In the first case we have \( x^{p^2} \equiv 1 \mod n \), where \( x \equiv g^{p^2} \equiv g \mod p \), \( g \equiv 1 \mod q \).

If \( n \equiv g^p \equiv 1 \mod p \), then from \( x \equiv g \mod p \), \( x^{p^2} \equiv 1 \mod p \) it follows that \( n - 1 \equiv 0 \mod p_i (p_i - 1) \), hence \( p_i \mid n \). Thus \( \beta_i \leq 1 \) and \( n - 1 \equiv 0 \mod (p_i - 1) \) and \( n \) is a Carmichael number, but this is impossible since \( n < p^2 < C \), \( x^{n-1} \equiv 1 \mod n \) and \( C \) has property D.

Now we prove the second part of the lemma. From \( x \equiv 3 \mod 4, x \equiv 1 \mod p \) we get \( x \equiv 1 \mod 2p \), hence \( x^{2p-1} \equiv 1 \mod 2p \) and \( 2p \) is a pseudoprime to base \( x \).

Now we show that there does not exist a composite number \( n < 2p \) such that \( x^{n-1} \equiv 1 \mod n \). We have \( n \neq 4 \). Indeed, if \( n = 4 \) then \( x^3 = 1 \mod 4 \), hence \( x \equiv 1 \mod 4 \), which is impossible, since by (6), \( x \equiv 3 \mod 4 \).

If there exists a composite \( n \) such that \( x^{n-1} \equiv 1 \mod n \), then \( n < 2p \), then \( n \) is divisible by a prime \( q < p \). If \( (q, C) = 1 \) and \( q \) is odd then this is impossible since by (6), \( x \equiv 0 \mod q \) for all \( 2 < q < p, (q, C) = 1 \). Now we consider the case when \( q \mid C \).
Then
\[ n = 2p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad \text{where } \alpha_i \geq 0, n < 2p, \text{ or} \]
\[ n = p_1^{\beta_1} \cdots p_k^{\beta_k}, \quad \text{where } \beta_i \geq 0, n < 2p. \]
Both cases are impossible. In the first case \( x^{2m-1} \equiv 1 \mod 2m \), where \( \beta_i \geq 2, \) hence \( p_i \mid 1 \), which is impossible.

If \( \alpha_i \leq 1 \) then \( 2m - 1 \equiv 0 \mod (p_i - 1) \), which is impossible since \( p_i - 1 \) is even.

In the second case we have \( x^{n-1} \equiv 1 \mod n \), where \( n = p_1^{\beta_1} \cdots p_k^{\beta_k} \), \( \beta_i \geq 0, n \mid C \). From \( x \equiv g_i \mod p_i^2 \) we have \( n - 1 \equiv 0 \mod p_i(p_i - 1) \). If \( \beta_i \geq 2 \) then \( p_i \mid 1 \), which is impossible. Thus \( \beta_i \leq 1 \), \( n - 1 \equiv 0 \mod (p_i - 1) \), \( n \) is a Carmichael number and in view of \( n < 2p < C \) this is impossible, since \( C \) has property D.

**Proof of Theorem 4.** First we note that the number \( n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \), where \( \alpha_i \geq 2 \) for some \( i, l > 1 \), is not a value of the function \( \iota_x^C \). Indeed, if \( x^{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} \equiv 1 \mod \iota_x^C \) then \( x^{\alpha_i} \equiv 1 \mod p_i^2 \), and since \( (p_i, n - 1) = 1 \), from the congruence \( x^{n-1} \equiv 1 \mod n \) it follows that \( x^{p_i^{\alpha_i}} \equiv 1 \mod p_i^2 \), and from \( \alpha_i \geq 2 \) we see that \( p_i^2 \) is a pseudoprime to base \( x \). From \( l > 1 \), \( p_i^2 < n \) it follows that \( n \) is not a value of \( \iota_x^C \). Let \( C \) be a Carmichael number with property D. By Lemma 1 there exist \( x_1, \ldots, x_m \) such that \( \iota_{x_1}^C = 2p_1, \ldots, \iota_{x_m}^C = 2p_m \) and \( y_1, \ldots, y_r \), such that \( \iota_{y_1}^C = p_1^2, \ldots, \iota_{y_r}^C = p_r^2 \), where \( p_m \) is the largest prime such that \( 2p_m < C \) and \( p_r \) is the largest prime such that \( p_r^2 < C \). There exist some other squarefree numbers \( m \) such that \( \iota_{x}^C = m \), where \( m \leq C \), for example \( m = C \). Thus every value of \( \iota_x^C \) divides \( q = [2p_1, \ldots, 2p_m, p_1^2, \ldots, p_r^2] = p_1^m p_r^r \).

We have \( a^{C-1} \equiv 1 \mod C \) for every \( a \) coprime to \( C \).

Let \( b \equiv a \mod \varrho \), where \( \varrho = p_1^m p_r^r \). Then \( b^{h-1} - 1 \equiv a^{h-1} - 1 \mod \varrho \) for every \( h \leq C \). Since every value of \( \iota_x^C \) divides \( \varrho \), for every \( h \leq C \) we have \( a^{h-1} \equiv 1 \mod h \) if and only if \( b^{h-1} \equiv 1 \mod h \), hence \( \iota_y^C = \iota_x^C \) for \((a, C) = 1 \) and \( b \equiv a \mod \varrho \). Thus in the sequence \( \{\iota_x^C\}_{x=1}^{\infty} \), the numbers greater than 1 appear with period \( \varrho \). On the other hand, the ones appear with period \( C \).

Since \( [\varrho, C] = \varrho \), the sequence \( \{\iota_x^C\}_{x=1}^{\infty} \) is periodic with period \( \varrho \). Now we prove that \( \varrho \) is the least period of \( \iota_x^C \). It is enough to show that no proper divisor \( \varrho' \) of \( \varrho \) is a period of \( \iota_x^C \). If \( \varrho' \mid \varrho \), \( \varrho' < \varrho \) then for some \( 1 \leq i \leq m \) we have \( p_i \nmid \varrho' \) or for some \( j \) with \( 1 \leq j \leq r \leq m \) we have \( p_j \nmid \varrho' \).

Let \( \iota_x^C = 2p_i \) and suppose that \( p_i \nmid \varrho' \).

We have \( a^{2p_i - 1} \equiv 1 \mod 2p_i \), hence \( a \equiv 1 \mod 2p_i \).

Since \( \varrho' \) is a period of \( \iota_x^C \) we have \( a^{2p_i - 1} \equiv (a + \varrho')^{2p_i - 1} \mod 2p_i \) and from \( a^{2p_i - 1} \equiv 1 \mod 2p_i \) we get \( (a + \varrho')^{2p_i - 1} \equiv 1 \mod 2p_i \), hence \( a + \varrho' \equiv 1 \mod 2p_i \) and since \( a \equiv 1 \mod 2p_i \) we have \( \varrho' \equiv 0 \mod 2p_i \), which is impossible, since \( p_i \nmid \varrho' \).
Suppose that \( p_j^2 \nmid q \) \((1 \leq j \leq r)\). We can assume that \( p_j \mid q' \) since \( m \geq r \).

Let \( t_x^C = p_j^2 \). We have

\[
  b^{p_j^2 - 1} \equiv 1 \mod p_j^2, \quad \text{hence} \quad b^{p_j - 1} \equiv 1 \mod p_j^2.
\]

Thus if \( q' \) is a period of \( t_x^C \) then \( b^{p_j^2 - 1} \equiv (b + q')^{p_j - 1} \equiv 1 \mod p_j^2 \).

Thus

\[
  (b + q')^{p_j} \equiv b + q' \mod p_j^2,
\]

hence

\[
  b^{p_j} + \left( \frac{p_j}{1} \right) b^{p_j - 1} q' + \left( \frac{p_j}{2} \right) b^{p_j - 2} q'^2 + \ldots \equiv b + q' \mod p_j^2.
\]

Since \( b^{p_j} \equiv b \mod p_j^2 \), \( p_j \mid q' \), \( p_j^2 \nmid q' \), we get \( p_j b^{p_j - 1} q' \equiv q' \mod p_j^2 \), and since \( p_j \mid q' \), \( p_j^2 \nmid q' \) we have \( p_j b^{p_j - 1} \equiv 1 \mod p_j \), which is impossible.

If \( C \) does not have property D then let \( C_1 < C \) denote the least divisor of \( C \) which is a Carmichael number. Then \( C_1 \) has property D. Since in the sequence \( \{t_x^C\}_{x=1}^{\infty} \) the number 1 appears with period \( C \), the function \( t_x^C \) has period \( [C_1!, C] \).

Analogously to the case when \( C \) has property D we prove that the least period of \( t_x^C \) is \( q_1 = [p_1! p_2! C] \), where \( p_m \) denotes the largest prime such that \( 2p_m < C_1 \), and \( p_r \) is the largest prime number such that \( p_r^2 < C_1 \).

References

[3] M. Cipolla, Sui numeri composti \( P \), che verificano la congruenza di Fermat \( a^{P-1} \equiv 1 \mod P \), Ann. di Mat. (3) 9 (1904), 139–160.
[9] A. Rotkiewicz, Pseudoprime Numbers and Their Generalizations, Student Association of Faculty of Sciences, Univ. of Novi Sad, 1972.
[11] W. Sierpiński, A remark on composite numbers \( m \) which are factors of \( a^m - a \), Wiadom. Mat. 4 (1961), 183–184 (in Polish; MR 23#A87).
Periodic sequences of pseudoprimes


Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
00-950 Warszawa, Poland
E-mail: rotkiew@impan.gov.pl

Received on 26.5.1998
and in revised form on 24.5.1999