Andrzej Rotkiewicz
On pseudoprimes having special forms and a solution of K. Szymiczek’s problem


Persistent URL: [http://dml.cz/dmlcz/137472](http://dml.cz/dmlcz/137472)

Terms of use:

© University of Ostrava, 2005

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* [http://project.dml.cz](http://project.dml.cz)
On pseudoprimes having special forms and a solution of K. Szymiczek’s problem

A. Rotkiewicz

Abstract. Several new constructions of different kinds of pseudoprimes are given. We introduce the first and second kind of Aurifeuillian pseudoprimes. It is shown that there are exactly six prime numbers $p$ below $10^{10}$ such that $p - 1$ is pseudoprime which solves a problem of K. Szymiczek.

Historic remarks

Leibniz (1646–1716) left a manuscript giving a proof of Fermat’s little theorem that if $p$ is a prime, then $a^p \equiv a \pmod{p}$ for all integers $a$ (see L. E. Dickson [4], p. 59).

Definition 1. Composite number $n$ for which

$$a^n \equiv a \pmod{n}$$

is called pseudoprime to the base $a$.

A pseudoprime to base 2 we shall call briefly pseudoprime and similarly for different kinds of pseudoprimes to base $a$.

According to Mahnke [21] Leibniz in September 1680 and December 1681 stated incorrectly that pseudoprimes do not exist (see Dickson [4], pp. 91, 92).

Fermat in 1640 expressed his belief that every number $F_n = 2^{2^n} + 1$ is prime. Euler (1707–1784) was the first who found that $F_5 = 2^{32} + 1 = 641 \cdot 6700417$ (see L. E. Dickson [4], p. 375).

János Bolyai (1802–1860), one of the founders of non-Euclidean geometry, was the first who showed that $F_5$ is a pseudoprime (see Kiss [12], p. 72).

The information that Chinese mathematicians claimed 25 centuries ago that pseudoprime numbers do not exist is wrong and Needham (see [22]) wrote that this arose from misunderstanding by Jeans a trivial statement of the fact that even
number can be divided by 2 and that odd ones cannot (see also Ribenboim [26], pp. 104, 105 and Williams [44], p. 398).

If we treat \( F_5 \) as the earliest known example of a pseudoprime, then the second one \( 341 = 11 \cdot 31 \) has been found by Sarrus [36] in 1819.

J. H. Jeans [9] in 1898 was the first who proved that there exist infinitely many pseudoprimes by showing that \( F_p \cdot F_q \) is a pseudoprime if \( p < q < 2^p \).

Ph. Jolivald (see Dickson [4], p. 93) asked whether \( 2^{N-1} \equiv 1 \pmod{N} \) if \( N = 2^p - 1 \), \( N \) composite and \( p \) is a prime, noting that this is true if \( p = 11 \), whence \( N = 2047 = 23 \cdot 89 \), not a prime.

In 1948 Sierpiński [38] and later Steuerwald [41] proved that if \( n \) is a pseudoprime then \( 2^n - 1 \) is also a pseudoprime.

Sierpiński’s Theorem was proved in 1903 by Malo [20] for the case in which \( N \) is a prime and \( 2^N - 1 \) is composite (see also [17]).

In 1904 Cipolla [3] proved: If \( a > b > \cdots > s > 1 \) and \( N = F_a F_b \cdots F_s \), then \( N \) is a pseudoprime if and only if \( 2^s > a \).

In 1964 I proved [32] the following theorem:

If \( n_1 > n_2 > \cdots > n_s > 1 \), \( s > 1 \), and \( N = (2^{F_{n_1}} - 1)(2^{F_{n_2}} - 1) \cdots (2^{F_{n_s}} - 1) \), then \( N \) is a pseudoprime.

From the above theorem it follows that for any positive integer \( M \), there exist infinitely many pseudoprimes with at least \( M \) distinct prime divisors.

In a joint note with Sierpiński [30] we proved that the equation \( 2^x - xy = 2 \) has one solution with both \( x \) and \( y \) prime, infinitely many with both \( x \) and \( y \) composite and none with \( x \) composite and \( y \) prime. The last case offers the principal difficulty.

The following theorems hold.

1. Every arithmetic progression \( ax + b \ (x = 1, 2, \ldots) \), where \((a, b) = 1\) contains an infinite number of pseudoprimes (Rotkiewicz [29]).

2. Let \( a, b \) be fixed coprime positive integers. If \( D > 0 \) is given and \( x > x_0(a, D) \), there exists at least one pseudoprime \( P \) satisfying:

\[
P \equiv b(\text{mod } a), \ x < P < \exp \left\{ \frac{\log x}{(\log \log)D} \right\}
\]

(Halberstam and Rotkiewicz [8]).

3. Let \( ax^2 + bxy + cy^2 \) be a primitive quadratic form (positive or indefinite) with fundamental discriminant \( d = b^2 - 4ac \) and belonging to the principal genus.

Then, there are infinitely many pseudoprimes of the form \( ax^2 + bxy + cy^2 \) (Rotkiewicz and Schinzel [31]).

4. There exist infinitely many square-free pseudoprimes divisible by an arbitrary given prime (Rotkiewicz [28]).

5. There exist infinitely many arithmetic progressions formed by four pseudoprimes (Rotkiewicz [34]).

The smallest even pseudoprime was found by Lehmer in 1950 (see Erdős [6]), namely \( 161038 = 2 \cdot 73 \cdot 1103 \).

The last results given by G. E. Pinch [23] in 2000 are as follows: There are 38975 odd pseudoprimes up to \( 10^{11} \), 101629 up to \( 10^{12} \) and 264239 up to \( 10^{12} \), the 40 even pseudoprimes less than \( 10^{10} \).
Problems of K. Szymiczek

It is easy to prove that there is no pseudoprime of the form \( p + 1 \), where \( p \) is an odd prime. Indeed, if \( p + 1 \) is an even pseudoprime then \( p + 1 \mid 2^{p+1} - 2 \) and \( 2 \cdot \frac{p+1}{2} \mid 2(2^p - 1) \), hence \( \frac{p+1}{2} \mid 2^p - 1 \), which is impossible, since every divisor of \( 2^p - 1 \) is of the form \( 2pk + 1 \) which is greater than \( \frac{p+1}{2} \).

In 1972 K. Szymiczek put forward the following problem:

Do there exist pseudoprimes of the form \( p - 1 \), where \( p \) is prime? (see problem 42 of my book [33]).

I found that there are exactly 6 such even pseudoprimes below \( 10^{10} \). These are:

1) \( 161038 = 2 \cdot 73 \cdot 1103 \), \( 161039 \) is prime
2) \( 9115426 = 2 \cdot 31 \cdot 233 \cdot 631 \), \( 9115427 \) is prime
3) \( 14374226 = 2 \cdot 23 \cdot 10801 \), \( 14373227 \) is prime
4) \( 665387746 = 2 \cdot 23 \cdot 3463 \cdot 4177 \), \( 665987747 \) is prime
5) \( 1105826338 = 2 \cdot 23 \cdot 10801 \cdot 2593 \), \( 1105826339 \) is prime
6) \( 3434672242 = 2 \cdot 727 \cdot 911 \cdot 2593 \), \( 3434672243 \) is prime

In 1972 K. Szymiczek put forward the following problem:

Do there exist infinitely many pseudoprime numbers of the form \( p + 2 \) or \( p - 2 \), where \( p \) is prime? (see my book [33], problem 43).

K. Szymiczek found that \( p - 2 \) is a pseudoprime for \( p = 563, 647, 1907 \) and \( p + 2 \) is a pseudoprime for \( p = 1103, 2699 \).

Definition 2. A composite integer \( n \) is called Carmichael number if \( a^n \equiv a \pmod{n} \) for all integers \( a \).

The first ten Carmichael numbers are as follows:

561 = 3 \cdot 11 \cdot 17, 1105 = 5 \cdot 13 \cdot 17, 1729 = 7 \cdot 13 \cdot 19, 2465 = 5 \cdot 17 \cdot 29, 2821 = 7 \cdot 13 \cdot 31,
6601 = 7 \cdot 23 \cdot 41, 8911 = 7 \cdot 19 \cdot 67, 10585 = 5 \cdot 29 \cdot 73, 15841 = 7 \cdot 31 \cdot 73,
29341 = 13 \cdot 37 \cdot 61.

The largest known Carmichael number which is a product of three primes was found by H. Dubner in 1994; it has 8060 digits. Dubner expressed the following conjecture.

For each \( k \geq 3 \), there exist infinitely many Carmichael numbers which are the products of \( k \) Carmichael numbers (see Ribenboim [26], p. 125).

The first six Carmichael numbers of the form \( p - 2 \) are: 561, 2465, 2821, 46657, 656601, 1909001.

The first nine Carmichael numbers of the form \( p + 2 \) are: 1105, 6601, 29341, 41041, 62745, 172081, 188461, 278545, 340561.

With the second problem of K. Szymiczek the following conjecture arises:

Conjecture 1. There exist infinitely many Carmichael numbers of the form \( p + 2 \) or \( p - 2 \), where \( p \) is a prime.

In 1899 Korselt [14] gave the following criterion:
A composite integer $n$ is a Carmichael number if and only if $n$ is positive, square-free and for each prime $p$ dividing $n$ we have $p - 1 \mid n - 1$.

In 1910 Carmichael showed that a Carmichael number has at least three prime divisors.

In 1994 W. R. Alford, A. Granville and C. Pomerance proved the following theorem (see [1]):

There are infinitely many Carmichael numbers and, for $x$ sufficiently large, the number $C(x)$ of Carmichael numbers not exceeding $x$ satisfies $C(x) > x^{2/7}$.

In 1995 Granville [7] proved that the prime $k$-tuplets conjecture implies that there are arbitrarily long arithmetic progressions of Carmichael numbers.

**Definition 3.** An odd composite $n$ is an Euler pseudoprime to base $a$ if $(a, n) = 1$ and

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

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

**Definition 4.** An odd composite number $n$ with $n - 1 = d \cdot 2^s$, $d$ odd, is strong pseudoprime to base $a$ if

$$a^d \equiv 1 \pmod{n}, \quad \text{or}$$

$$a^{d-2^r} \equiv -1 \pmod{n}, \quad \text{for some } r, 0 \leq r < s.$$

In 1980 in joint paper with A. J. van der Poorten [35] we proved that every arithmetic progression $ax + b$ ($x = 0, 1, 2, \ldots$), where $a, b$ are relatively prime integers, contains an infinite number of odd strong pseudoprimes for each base $c \geq 2$.

The least pseudoprime, Euler pseudoprime and strong pseudoprime are: $341 = 11 \cdot 31, 1905 = 3 \cdot 5 \cdot 127, 2047 = 23 \cdot 89$, respectively.

**Definition 5.** A superpseudoprime $n$ to base $a$ and coprime with $a$ is a pseudoprime to base $a$ all of whose divisors greater than 1 are either primes or pseudoprimes to base $a$; that is if $d \mid n$ then $a^{d-1} \equiv 1 \pmod{d}$.

The number $F_n F_{n+1}$, where $F_n = 2^{2^n} + 1, n > 1$ is superpseudoprime and it is not known if there exist infinitely many superpseudoprimes of the form $F_n F_{n+1} F_{n+2}$ (see Szymiczek [43] and Duparc [5]).

Today we know complete factorizations for

$F_5, F_6, F_7, F_8, F_9, F_{10}$ and $F_{11}$

and incomplete factorizations for

$F_{12}, F_{13}, F_{15}, F_{16}, F_{17}, F_{18}, F_{19}, F_{21}, F_{23}$,

251 prime factors are known and 218 Fermat numbers are known to be composite (see Keller [10], [11]).

Let $(a, b) = 1, |a| > |b| > 0$. For any integer $n > 0$, let $\Phi_n(a, b)$ denote the $n$-th homogeneous cyclotomic polynomial, defined by

$$\Phi_n(a, b) = \prod_{r=1}^{n} (a - \zeta_n^r b) = \prod_{d \mid n} (a^d - b^d)^{\mu(n/d)},$$
where $\zeta_n$ is a primitive $n$-th root of unity and $\mu$ is the Möbius function.

A prime is called a primitive prime factor of $a^n - b^n$ if it divides this number but does not divide $a^d - b^d$ for $0 < d < n$.

In 1892 Zsigmondy (see [45]) proved the following theorem:

Z.: The primitive prime factors of $a^n - b^n$ coincide with the prime factors of $\Phi_n(a, b)$, except for a possible prime $q_1$ which may divide $\Phi_n(a, b)$ (to the first power only) and also divide $n$, and may be a primitive prime factor of $a^\sigma - b^\sigma$, where $\sigma = \frac{n}{q_1}$ and $(q_1, \sigma) = 1$. If there is such a prime $q_1$, then $q_1 = P(n)$, the greatest prime factor of $n$, since $\sigma | q_1 - 1$, whence $\sigma < q_1$.

For $n > 6$ the number $a^n - b^n$ has a primitive prime divisor. Every primitive prime divisor of the number $a^n - b^n$ is of the form $nk + 1$. For $n \leq 6$ we have the following exceptions:

- $n = 1$, $a - b = 1$;
- $n = 2, a + b = \pm 2^\mu$ ($\mu \geq 1$);
- $n = 3$, $a = \pm 2$, $b = \mp 1$; $n = 6$, $a = \pm 2$, $b = \pm 1$.

Let $k(n)$ denote the square-free kernel of $n$, that is, $n$ divided by its greatest square factor.

In 1962 A. Schinzel (see [37]) proved the following theorem.

**Theorem S2.** Let

$$\eta = \begin{cases} 
1 & \text{if } k(ab) \equiv 1 \pmod{4} \\
2 & \text{if } k(ab) \equiv 2 \text{ or } 3 \pmod{4}.
\end{cases}$$

If $n/\eta k(ab)$ is an odd integer, then $a^n - b^n$ has at least two primitive prime factor except the following cases:

- $n = 1; a = \pm (2^\alpha + 1)^2, b = \pm (2^\alpha - 1)^2, \text{ or } 4a = \pm (p^\alpha + 1)^2, 4b = \pm (p^\alpha - 1)^2$,
- $n = 2; \text{ same but with } \pm \text{ for } b \text{ instead of } \pm$;
- $n = 3; a = \pm 3, b = \mp 1 \text{ or } a = \pm 4, b = \mp 1 \text{ or } a = \pm 4, b = \pm 3$;
- $n = 4; |a| = 2, |b| = 1$;
- $n = 6; a = \pm 3, b = \mp 1 \text{ or } a = \pm 4, b = \mp 1 \text{ or } a = \pm 4, b = \mp 3$;
- $n = 12; |a| = 2, |b| = 1 \text{ or } |a| = 3, |b| = 2$;
- $n = 20; |a| = 2, |b| = 1$.

The proof of Theorem S2 is based on the following properties of the cyclotomic polynomials. We write $\Phi_n(x)$ for $\Phi_n(x, n)$. 
Theorem S1. Let $n > 1$ be square-free and let $m$ be a divisor of $n$ such that $\frac{n}{m}$ is odd. Then there exist polynomials $P_{n,m}(x)$, $Q_{n,m}(x)$ with integral coefficients such that

$$\Phi_n(x) = P_{n,m}^2(x) - \left\{ \left( \frac{1}{m} \right) m \right\} \frac{1}{2} x Q_{n,m}(x) \quad (m \text{ odd}),$$

(5)

$$\Phi_{2n}(x) = P_{n,m}^2(-x) + \left\{ \left( \frac{1}{m} \right) m \right\} \frac{1}{2} x Q_{n,m}(-x) \quad (m \text{ odd}),$$

(6)

$$\Phi_{2n}(x) = P_{n,m}^2(x) - m x Q_{n,m}^2(x) \quad (m \text{ even}).$$

(7)

Further, these polynomials can be found from the following formulae (where $\sqrt{c} \geq 0$ if $c \geq 0$ and $\sqrt{c} = i\sqrt{|c|}$ if $c < 0$):

$$P_{n,m}(x^2) - \left\{ \left( \frac{1}{m} \right) m \right\} \frac{1}{2} x Q_{n,m}(x^2) = \prod_s (x - \zeta_s^m) \prod_t (x - \zeta_t^n) = \Psi_{n,m}(x) \quad (m \text{ odd}).$$

(8)

If $m = 1$, the product over $t$ is empty, and in (8) we get $\Psi_{n,1}(x) = \Phi_n(x)$

$$P_{n,m}(-x^2) - i \left\{ \left( \frac{1}{m} \right) m \right\} \frac{1}{2} x Q_{n,m}(-x^2) = \prod_s (x + i\zeta_s^m) \prod_t (x - i\zeta_t^n) = \Psi_{2n,m}(x) \quad (m \text{ odd}),$$

(9)

where the products are over

$$0 < s < n, \ 0 < t < n, \ (st, n) = 1, \ \left( \frac{s}{m} \right) = 1, \ \left( \frac{m}{s} \right) = -1;$$

(10)

and

$$P_{n,m}(x^2) - m \frac{1}{2} x Q_{n,m}(x^2) = \prod_s (x - \zeta_{4m}^s) = \Psi_{2n,m}(x) \quad (m \text{ even})$$

(11)

where the product is over

$$0 < s < 4n, \ (s, 4n) = 1, \ \left( \frac{m}{s} \right) = 1.$$  

(12)

Definition 6. If $1 \leq d_1 < d_2 < \ldots < d_k$ are integers, we shall call the number $n = \prod_{i=1}^{k} \Phi_d(2)$ a cyclotomic number and if $n$ is a pseudoprime we shall call it cyclotomic pseudoprime.

The above definition was introduced in 1982 by Pomerance (see [24]). In the paper [25] the authors proved the following

Theorem. Let $\Phi_n(x)$ denote the $n$-th cyclotomic polynomial $(n > 2)$, $S_a(x)$ denote the number of pseudoprimes to base $a$ not exceeding $x$; and let

$$f_n(a) = \frac{\Phi_n(a)}{(\Phi_n(a), n)} \text{ for each integer } a > 1.$$

If $f_n(a)$ is composite, then $f_n(a)$ is a strong pseudoprime to base $a$. For all $s > 1$ and $x \geq a^{15s} + 1$, we have

$$S_a(x) > \frac{\log x}{4a \log a}.$$
It is easy to see that if \( n \) is a pseudoprime, then \( 2^n - 1 \) is a strong pseudoprime. Indeed \( 2^n - 1 - 1 = (2^{n-1} - 1) \cdot 2 = d \cdot 2 \), where \( d = 2^{n-1} - 1 \) and \( 2^d \equiv 1 \text{ (mod } 2^n - 1 \text{) and by the Definition 4, } 2^n - 1 \text{ is a strong pseudoprime.}

At the present, 42 Mersenne primes have been discovered (see [17]). The number \( M_p \) is prime if

\[
p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466317, 20996011, 24036583, 25964513.
\]

A forty third Mersenne prime found Dec. 2005: \( 2^{30402457} - 1 \).

On February 18, 2005, Dr Martin Novak from Germany found the new largest prime number: \( 2^{30402457} - 1 \). The prime number has 7,152,223 digits. It took more than 50 days of calculations on Dr Novak’s 2.4 GHz Pentium 4 computer. The new prime was independently verified in 5 days by Tony Reix of Grenoble, France. A second verification was completed by Jeff Gilchrist of Elytra Enterprises Inc. in Ottawa, Canada.

All Mersenne numbers \( 2^p - 1 \), where \( p \) is a prime and which are composite are at the same time strong pseudoprimes and cyclotomic pseudoprimes.

The same is true for all 218 Fermat numbers known to be composite and may be for all Fermat numbers after \( F_4 \), the point where Fermat stopped his calculations.

Now we shall prove the following

**Theorem 1.** The numbers \( \Phi_{Fm}(2) \) and \( \Phi_{2^{p-1}}(2) \), where \( p \) is a prime, are prime or are simultaneously cyclotomic pseudoprimes, superpseudoprimes and strong pseudoprimes.

**Proof.** Let \( f_k = f_k(2) \). Then \( f_{Fm}(2) = \frac{\Phi_{Fm}(2)}{(\Phi_{Fm}(2), F_m)}, f_{2^{p-1}} = \frac{\Phi_{2^{p-1}}(2)}{(\Phi_{2^{p-1}}(2), 2^{p-1})} \). From our previous considerations it follows that if \( (\Phi_{Fm}(2), F_m) = 1 \) and \( (\Phi_{M_p}(2), M_p) = 1 \) then every prime factor of \( f_{Fm}(2) \) and \( f_{2^{p-1}}(2) \) is a primitive prime divisor of \( 2^{Fm} - 1 \) and \( 2^{M_p} - 1 \), respectively and by the definitions of cyclotomic pseudoprimes, superpseudoprimes and strong pseudoprimes Theorem 1 is proved. First we shall prove that \( (\Phi_{Fm}(2), F_m) = 1 \). Indeed, if \( d \mid \Phi_{Fm}(2) \) and \( d \mid F_m \) then \( d \mid 2^{Fm} - 1 \) and \( d \mid 2^{m+1} - 1 \), hence \( d \mid 2(F_m, 2^{m+1}) - 1 = 2^1 - 1, d = 1 \).

Similarly, if \( d \mid \Phi_{2^{p-1}}(2) \) and \( d \mid 2^{p-1} \) then \( d \mid 2^{2^{p-1}} - 1 \) and \( d \mid 2^p - 1 \), hence \( d \mid (2^{(2^{p-1})p} - 1) - 1 = 2^1 - 1 = 1 \), since \( (2^p - 1, p) = (2^{(2^{p-1}) + 1, p}) = (2kp + 1, p) = 1 \).

A. Makowski has proved the following

**Lemma.** If \( n \) is an odd integer \( > 3 \) and \( P \) is the greatest prime factor of \( 2^n - 2 \), then \( \frac{2^n - 2}{p-2} \mid P - 1 \).

Indeed, suppose that \( \frac{2^n - 2}{p-2} \mid P - 1 \). Then

\[
2^n - 2 = 2\left(\frac{2^{n+1}}{p} - 1\right)\left(\frac{2^{n+1}}{p} + 1\right) \mid P(P - 1).
\]

\(^1\text{For details see}\)

http://www.mersenne.org/30402457.htm
But the greatest prime factor of the product \(a \cdot b \cdot c\) does not exceed \(\max(a, b, c)\).

Hence

\[
P \leq 2^{\frac{n-1}{2}} + 1. \tag{13}
\]

On the other hand

\[
2^n - 2 \leq P(P - 1),
\]

as a divisor of number does not exceed the number itself.

The last inequality implies that

\[
P^2 - P - (2^n - 2) \geq 0
\]
or

\[
P \geq \frac{1}{2} \left(1 + \sqrt{1 + 4(2^n - 2)} \right). \tag{14}
\]

Inequalities (13) and (14) imply

\[
\frac{1}{2} \left(1 + \sqrt{1 + 4(2^n - 2)} \right) \leq 2^{\frac{n-1}{2}} + 1,
\]

which leads to

\[
\sqrt{2^{n+2} - 7} \leq 2^{\frac{n+1}{2}} + 1, \quad 2^{n+2} - 7 \leq 2^{n+1} + 2 \cdot 2^{\frac{n+1}{2}} + 1, \quad 2^{n+1} - 2 \cdot 2^{\frac{n+1}{2}} + 1 \leq 9, \quad \left(2^{\frac{n+1}{2}} - 1 \right)^2 \leq 3^2, \quad 2^{\frac{n+1}{2}} - 1 \leq 3, \quad 2^{\frac{n+1}{2}} \leq 2^2, \quad \frac{n+1}{2} \leq 2, \quad n \leq 3,
\]
a contradiction.

Now, we shall prove the following

**Theorem 2.** If \(n > 3\) is a prime or odd pseudoprime then the number \((2^n - 1) \Phi_{2^n - 2}(2)\) is a cyclotomic pseudoprime.

*Proof.* By Lemma applied for \(n\) prime \(>3\) or odd pseudoprime, we have \(\frac{2^n - 2}{P} \nmid P - 1\), where \(P\) is the largest prime divisor of \(2^n - 2\) and by Theorem of Zsigmondy we have

\[
\Phi_{2^n - 2}(2) \equiv 1 \pmod{2^n - 2}
\]

and

\[
(2^n - 1) \Phi_{2^n - 2}(2) = (2^n - 1)((2^n - 2)l + 1), \quad l > 1 \quad \text{(since} \ n > 3\text{)}.
\]

Since every prime factor of \(\Phi_{2^n - 2}(2)\) is a primitive prime factor of \(2^{2^n - 2} - 1\) we have \((2^n - 1, \Phi_{2^n - 2}(2)) = 1\) and

\[
(2^n - 1) \Phi_{2^n - 2}(2) - 1 = (2^n - 1)((2^n - 2)l + 1) - 1 = (2^n - 1)(2^n - 2)l + 2^n - 2,
\]

\(n \mid 2^n - 2\), hence

\[
(2^n - 1) \Phi_{2^n - 2}(2) \mid 2^{(2^n - 1)\Phi_{2^n - 2}(2)} - 1 - 1
\]

and the number \((2^n - 1) \Phi_{2^n - 2}(2)\) is a cyclotomic pseudoprime.

**Example.** 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 \(n = 341\) we get cyclotomic pseudoprime \((2^{341} - 1) \Phi_{2^{341} - 2}(2)\).
Aurifeuillian factorizations and Aurifeuillian pseudoprimes

Lucas (see [18] and Dickson [4], p. 383) gave tables due to LeLasseur and Aurifeuille of functions \(\frac{x^2 + y^n}{x + y}(n \text{ odd}), \frac{x^{2m} + y^{2n}}{x^{m} + y^{n}}(m \text{ odd})\) expressed in the form \(Y^2 \pm pxYZ^2\), which is factorable if \(xy = pv^2\). Aurifeuille (see [19]) discovered special polynomial identities which show how to write cyclotomic polynomial \(\Phi_n(x)\) as a difference of squares when \(x\) has certain values.

Tables of Aurifeuillian polynomials can be found also in the books of Kraitchik [15], paper [16] and Riesel’s book [27]. A fast way to compute the Aurifeuillian squares when \(n\) which is factorable if \(n\) identities which show how to write cyclotomic polynomial \(\Phi_n(x)\) we can find in Stevnhagen’s paper [41].

Tabels of Aurifeuillian polynomials can be found also in the books of Kraitchik [15], paper [16] and Riesel’s book [27]. A fast way to compute the Aurifeuillian squares when \(n\) which is factorable if \(n\) identities which show how to write cyclotomic polynomial \(\Phi_n(x)\) we can find in Stevnhagen’s paper [41].

Let \(\Phi_n(x) = X_n^2 - nxY_n^2\).

Here is the table of coefficients of Aurifeuillian polynomials \(X_n\) and \(Y_n\) for \(n = 2, 3, 5, 6, 7, 10, 11, 13, 14, 17, 19\) and \(21\) (see [16]).

<table>
<thead>
<tr>
<th>(n)</th>
<th>(X_n)</th>
<th>(Y_n)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1 1</td>
<td>5 7 5 1</td>
<td>10 2 2 1</td>
</tr>
<tr>
<td>1 1</td>
<td>5 -1 -1</td>
<td>11 1 1 1</td>
</tr>
<tr>
<td>1 7 5 1</td>
<td>13 1 3 5 5 3 1</td>
<td></td>
</tr>
<tr>
<td>1 3 3 1</td>
<td>14 1 2 -1 -1 2 1</td>
<td></td>
</tr>
<tr>
<td>1 8 13 8 1</td>
<td>15 1 3 3 1</td>
<td></td>
</tr>
<tr>
<td>1 1 11 -5 -15 -5 11 9 1</td>
<td>17 1 3 1 -3 -3 1 3 1</td>
<td></td>
</tr>
<tr>
<td>1 1 9 17 27 31 31 27 17 9 1</td>
<td>19 1 3 5 7 7 7 5 3 1</td>
<td></td>
</tr>
<tr>
<td>1 1 10 19 7 13 10 1</td>
<td>21 1 3 2 2 3 1</td>
<td></td>
</tr>
</tbody>
</table>

We have

\[
x^2 + 1 = \Phi_2(x^2) = (x + 1)^2 - 2x, \text{ hence substituting } x = 2^{2k-1} \text{ we get } 2^{4k-2} + 1 = (2^{2k-1} - 2^k + 1)(2^{2k-1} + 2^k + 1),
\]

\[
\Phi_3(-x) = x^2 - x + 1 = (x + 1)^2 - 3x, \text{ hence substituting } x = 3^{2k-1} \text{ we get } \Phi_3(3^{2k-1}) = (-3^{2k-1} - 3k + 1)(3^{2k-1} + 3k + 1).
\]

\[
2^{2k} + 1 = L_{2k} \cdot M_{2k}; L_{2k}, M_{2k} = 2^k + 1 \pm \frac{\sqrt{k+1}}{2},
\]

\[
3^{3k} + 1 = (3^k + 1)L_{3k} \cdot M_{3k}; L_{3k}, M_{3k} = 3^k + 1 \pm \frac{3k+1}{2}.
\]

\[
\Phi_5(x) = (x^2 + 3x + 1)^2 - 5x(x + 1)^2; L_{5k}, M_{5k} = 5^{2k} + 3 \cdot 5^k + 1 \pm \frac{5^{k+1}}{2}(5^k + 1).
\]

\[
\Phi_6(x^2) = (x^2 + 3x + 1)^2 - 6x(x + 1)^2; L_{6k}, M_{6k} = 6^{2k} + 3 \cdot 6^k + 1 \pm \frac{6^{k+1}}{2}(6^k + 1).
\]

\[
\Phi_7(-x) = (x^3 + 3x^2 + 3x + 1)^2 - 7x(x^2 + x + 1)^2;
\]

\[
L_{7k}, M_{7k} = (7^k + 1)^2 \pm \frac{7^{k+1}}{2}(7^{2k} + 7^k + 1)10^{10k} + 1 = (10^{2k} + 1)L_{10k}M_{10k};
\]
\[ L_{10k}, M_{10k} = 10^{4k} + 5 \cdot 10^{3k} + 7 \cdot 10^{2k} + 5 \cdot 10^k + 1 + 10^{\frac{k+1}{4}} (10^{3k} + 2 \cdot 10^{2k} + 2 \cdot 10^k + 1) \]
\[ \Phi_{11}(-x) = \left(x^5 + 5x^4 - x^3 - x^2 + 5x + 1\right)^2 - 11x \left(x^4 + x^3 - x^2 + x + 1\right)^2 \]
\[ 11^{11k} + 1 = (11^k + 1)L_{11k}M_{11k}, \text{ where } L_{11k}, M_{11k} = 11^{5k} + 5 \cdot 11^{4k} - 11^{3k} - 11^{2k} + 5 \cdot 11^k + 1 \pm 11^{\frac{k+1}{2}} (11^{4k} + 11^{3k} - 11^{2k} + 11^k + 1). \]

An algebraic prime factor of \( \Phi_n(b) \) is called intrinsic and is indicated by an asterisk. For example \( \Phi_{3,7}(2) = 7 \cdot 337, 7 \) is a primitive prime factor of \( 2^3 - 1 \).

Denote primitive parts of \( L \) and \( M \) by \( L_n^* \) and \( M_n^* \), respectively.

For base \( b \), let \( \varepsilon_d = \varepsilon_d(b) = \left[1 + \left(\frac{b}{d}\right)\right]/2 \), where \( d \) is odd, \( (b, d) = 1 \). \( \left(\frac{b}{d}\right) \) is the Jacobi symbol.

Let \( n = 2^s m, m \) odd, \( s \geq 0 \).

We have the formulas (see [2])
\[
L_n^* = \prod_{d|n,(d,b)=1} \left[ (L_{n/d})^{\varepsilon_d} \left(M_{a/d}\right)^{1-\varepsilon_d}\right]^{\mu(d)},
\]
\[
M_n^* = \prod_{d|n,(d,b)=1} \left[ (L_{n/d})^{1-\varepsilon_d} \left(M_{a/d}\right)^{\varepsilon_d}\right]^{\mu(d)},
\]
\[
L_n = \prod_{d|n,(d,b)=1} \left[ (L_{n/d})^{\varepsilon_d} \left(M_{a/d}\right)^{1-\varepsilon_d}\right],
\]
\[
M_n = \prod_{d|n,(d,b)=1} \left[ (L_{n/d})^{1-\varepsilon_d} \left(M_{a/d}\right)^{\varepsilon_d}\right].
\]

We have \( P_n(b) = L_n^2_2^* M_n^2, n \) odd and \( (L_n^*, M_n^*) = 1, L_n^* > 1, M_n^* > 1 \). (It follows from Schinzel’s proof of Theorem \( S_2 \)).

In computing \( L_n^* \) and \( M_n^* \) the following “crossover” theorem (see Kraitchik [16]) is useful
- If \( \left(\frac{b}{n}\right) = 1 \) then \( L_n \mid L_{kn} \) and \( M_n \mid M_{kn} \).
- If \( \left(\frac{b}{n}\right) = -1 \) then \( L_n \mid M_{kn} \) and \( M_n \mid L_{kn} \).

**Definition 7.** Let \( b \) be a natural number, \( L^*(b), M^*(b) \) be primitive parts of \( L_n \) and \( M_n \), respectively.

The pseudoprimes of the form \( L^*M^* \) we shall call Aurifeuillian pseudoprimes of the first kind. The pseudoprimes of the form \( L^* \) or \( M^* \), respectively we shall call Aurifeuillian pseudoprimes of the second kind.

The following theorem holds

**Theorem 3.** If \( b = 2 \) or \( k(b) > 2 \) then there exist infinitely many Aurifeuillian pseudoprimes to the base \( b \) of the first kind. These pseudoprimes coincide with the numbers \( \Phi_s(b), \) where \( s = (2k + 1)\eta(k), k = 3, 4, \ldots \) which do not have intrinsic prime factor.

**Proof.** The above theorem follows from the proofs of Schinzel’s theorems \( S_1 \) and \( S_2 \).
Indeed, from formulas (5), (6) and (7) it follows that if \( n = (2k + 1)\eta k(b) \) then in the cases \( m \) odd, formulas (5) or (6)) or \( m \) even, formula (7)) the \( \Phi_n(x) \) or \( \Phi_{2n}(x) \) for \( m = x \) becomes a difference of squares and from the above we can deduce from Schinzel’s proof of Theorem \( S_1 \) and \( S_2 \) that \( \Phi_s(b) \), where \( s = (2k + 1)\eta k(b), k \geq 3 \) is equal \( L^*(b)M^*(b) \), where \( (L^*(b), M^*(b)) = 1, L^*(b) > 1, M^*(b) > 1 \) and \( \Phi_s(b) = L^*(b)M^*(b) \), where \( s = (2k + 1)\eta k(b), k \geq 3 \) is Aurifeuillian pseudoprime to the base \( b \) if \( \Phi_s(b) \) does not have intrinsic prime factor.

From the fact that the number \( \Phi_s(b) \) does not have the intrinsic prime factor we deduce that every prime factor of \( \Phi_s(b) \) is of the form \( st + 1 \), hence \( L^*(b)M^*(b) \equiv 1 \pmod{s} \), hence

\[
\Phi_s(b) = L(b)M^*(b) \mid bL^*(b)M^*(b) - 1 - 1
\]

and \( L^*(b)M^*(b) \) is Aurifeuillian pseudoprime to the base \( b \) of the first kind.

Since, for example there exist infinitely many primes \( p \) such that \( \eta k(b) \not| p - 1 \), hence every number \( \Phi_{prk(b)}(b) \) \((prk(b) > 20) \) is Aurifeuillian pseudoprime to the base \( b \) of the first kind. Theorem 3 is proved.

**Example.**

\[
\Phi_{4p}(2) = \frac{2^{2p} + 1}{5} = \frac{(2^{p} + 1 - 2^{\frac{p+1}{2}})(2^{p} + 1 + 2^{\frac{p+1}{2}})}{5} = L^* \cdot M^*
\]

is Aurifeuillian pseudoprime for every \( p \geq 7 \). But even if \( \Phi_{4(2k+1)}(2) \) has intrinsic prime factor we can get Aurifeuillian pseudoprime from the last number. The number \( \Phi_{100}(2) = \Phi_{22,52}(2) = L \cdot M = (101 \cdot 8101)(5 \cdot 628501) \) is not Aurifeuillian pseudoprime since is divisible by intrinsic prime factor 5. But if we multiply index \( 2^2 \cdot 5^2 \) by 17 we get Aurifeuillian pseudoprime since \( 2^2 5^2 \not\mid 17^1 \). Indeed, \( \Phi_{1700}(2) = L^* \cdot M^* = (5101 \cdot PRP93) \cdot 8504123101 \), where \( PRP \) indicates that second factor is a probable prime with 93 digits, is Aurifeuillian pseudoprime of the first kind.

**Problem.** Let \( b \) not be a perfect power, \( b = 2 \) or \( k(b) > 2 \). Do there exist infinitely many Aurifeuillian pseudoprimes of the form \( L^*(b) \) or \( M^*(b) \)? (that is pseudoprimes of the second kind to the base \( b \)).

**Remark.** \( M^*_{26}(2) = 53 \cdot 157 \) and \( L^*_{34}(2) = 13 \cdot 953 \) are Aurifeuillian pseudoprimes of the second kind. \( M^*_{25}(5) = 101 \cdot 251 \cdot 401 \) and \( L^*_{45}(5) = 101 \cdot 251 \cdot 401 \) are Aurifeuillian pseudoprimes to the base 5, of the second kind.

Aurifeuillian pseudoprimes to the bases: 2, 3, 5, 6, 7, 10, 11, 12. From Aurifeuillian factorizations (see [2]) we can get Aurifeuillian pseudoprimes.

The numbers \( \Phi_s(2), s = 4(2k+1) \) for \( 3 \leq k \leq 599 \) are Aurifeuillian pseudoprimes except the following cases: \( k = 12, 19, 101, 102, 166, 253, 312, 344, 395 \) in which the numbers \( \Phi_s(2), s = 4(2k+1) \) have the following intrinsic prime factors: 5, 13, 29, 41, 37, 13, 5, 53, 119, respectively.

The least Aurifeuillian pseudoprime of the first kind is \( \Phi_{47}(2) = \frac{2^{41}+1}{2^3} = 29 \cdot 113, L^* = 113, M^* = 29 \).

The numbers \( \Phi_s(3), s = 6(2k+1) \) for \( 1 \leq k \leq 82 \) are Aurifeuillian pseudoprimes to the base 3 of the first kind except the following cases: \( k = 3, 24, 28, 55 \), when the numbers \( \Phi_s(3), s = 6(2k+1) \) have the intrinsic prime factors: 7, 7, 19, 37, respectively.
The numbers \( \Phi_s(5) \), where \( s = 5 \cdot (2k + 1) \) for \( 0 \leq k \leq 31 \) are Aurifeuillian pseudoprimes of the first kind to the base 5 except the case \( k = 5 \), in which the number \( \Phi_{55}(5) \) has the intrinsic prime factor: 11.

The least Aurifeuillian pseudoprime of the first kind to the base 5 is \( \Phi_5(5) = 11 \cdot 71 \), \( L^*(5) = 11 \), \( M^*(5) = 71 \).

The numbers \( \Phi_s(6) \), \( s = 12(2k + 1) \) for \( 0 \leq k \leq 25 \) are Aurifeuillian pseudoprimes of the first kind except the case \( k = 6 \), in which \( \Phi_{12 \cdot 13}(6) \) has the intrinsic prime factor: 13.

The least Aurifeuillian pseudoprime of the first kind to the base 6 is \( \Phi_{12}(6) = 13 \cdot 971 \), \( L^* = 13 \), \( M^* = 97 \).

The numbers \( \Phi_s(7) \), where \( s = 14(2k + 1) \) for \( 0 \leq k \leq 19 \) are Aurifeuillian pseudoprimes of the first kind to the base 7.

The least Aurifeuillian pseudoprime of the first kind to the base 7 is \( \Phi_{14}(7) = 113 \cdot 911 \), \( L^* = 113 \), \( M^* = 911 \).

The numbers \( \Phi_s(10) \), where \( s = 20(2k + 1) \) for \( 0 \leq k \leq 13 \) are Aurifeuillian pseudoprimes of the first kind to the base 10.

The least Aurifeuillian pseudoprime of the first kind to the base 10 is \( \Phi_{20}(10) = 3541 \cdot 27961 \), \( L^* = 3541 \), \( M^* = 27961 \).

The numbers \( \Phi_s(11) \), where \( s = 22(2k + 1) \) for \( 0 \leq k \leq 10 \) are Aurifeuillian pseudoprimes of the first kind to the base 11.

The least Aurifeuillian pseudoprime of the first kind to the base 11 is \( \Phi_{22}(11) = 58167 \cdot 23 \cdot 89 \cdot 11 \), \( L^* = 58367 \), \( M^* = 23 \cdot 89 \cdot 119 \).

The numbers \( \Phi_f(12) \), \( s = 6(2k + 1) \) for \( 0 \leq k \leq 38 \) are Aurifeuillian pseudoprimes of the first kind to the base 12 except the cases: \( k = 3, 9 \) and 24, when the numbers \( \Phi_{42}(12), \Phi_{114}(12) \) and \( \Phi_{294}(12) \) have the intrinsic prime factors: 7, 19, 7, respectively.

The least Aurifeuillian pseudoprime of the first kind to the base 12 is \( \Phi_{6}(12) = 7 \cdot 19 \), \( L^* = 7 \), \( M^* = 19 \).

The first problem on Mersenne numbers \( M_p = 2^p - 1 \), where \( p \) is prime is as follows:

If \( 2^p - 1 \) is a prime, is \( 2^{2^p - 1} - 1 \) prime?

(see Sierpiński [39]).

A counterexample was found for \( p = 13 \), since \( M_{13} = 8191 \) is prime, whereas \( 2^{8191} - 1 \) is composite. In 1976 Keller discovered the prime factor \( p = 3381937559479 \) of \( M_{8191} \) (see Ribenboim [26], p. 97).

The second problem of Catalan (1876), reported in [4], p. 22, is the following. Consider the sequence \( m_{k+1} = 2^{m_k} - 1 \) starting from \( m_1 = 2 \). We have \( m_2 = 2^2 - 1 = 3, m_3 = 2^3 - 1 = 7, m_4 = 2^7 - 1 = 127, m_5 = 2^{127} - 1, \ldots \) Are all numbers \( m_n \) primes? Are there infinitely many which are prime?

At present, it is impossible to test \( m_6 \), which has more than \( 10^{38} \) digits! If the answer for the second question is positive then by the following theorem all numbers of \( m_n \) are primes.

**Theorem 4.** Let \( p \) be any prime number. Consider the sequence of numbers

\[
c_1 = 2^p - 1, c_2 = 2^{c_1} - 1, c_3 = 2^{c_2} - 1, \ldots, c_{n+1} = 2^{c_n} - 1, \ldots
\]  

(19)
Then all numbers of the sequence (19) are primes or there exists such \( k \geq 1 \) that all the numbers \( c_n \) for \( n \geq k \) are pseudoprimes.

**Proof.** Suppose that \( k \) is the number for which \( c_k \) is composite. If \( k = 1 \) then \( 2^p - 1 \) (where \( p \) is prime) is composite and since \( 2^{2^p-2} \equiv 1 \pmod{2^p - 1} \) the number \( 2^p - 1 \) is pseudoprime and all terms \( c_k \) for \( k > 1 \) are also pseudoprime by Sierpiński’s theorem.

If \( k > 1 \) then \( c_{k-1} \) is prime and \( c_k = 2^{k-1} - 1 \) is prime or pseudoprime. But \( c_k \) cannot be prime since \( c_k \) denotes the first term of sequence (19) which is not prime. Thus \( c_k = 2^{c_k - 1} - 1 \) is pseudoprime by Jolivald’s theorem [4] and the next terms \( c_{k+1}, c_{k+2}, \ldots \) would by pseudoprime by Sierpiński [38] theorem. Thus Theorem 4 is proved.

**Conjecture 2.** There are no prime number \( p \geq 2 \) such that all numbers:

\[
p, \quad 2^p - 1, \quad 2^{2^p-1} - 1, \ldots
\]

are prime.

The following reformulation of the conclusion of Dirichlet’s theorem on primes in arithmetic progression appears repeatedly in the literature (see Sierpiński [40] and Knopfmacher & Porubsky [13]).

Let \( (a, b) = 1 \) with \( 0 \leq b < a \). Then \( ax + b \) assumes for \( x = 0, 1, 2, \ldots \) infinitely many prime values if and only if \( ax + b \) assumes here at least one prime.

In [29] I based my proof that there exist infinitely many pseudoprimes of the form \( ax + b \), where \( x \) is a natural number, \( (a, b) = 1 \) on the fact that it is enough to show that there exists at least one pseudoprime number \( p \) of the form \( ak + b \), where \( k \) is natural number.

The same technique was used in the paper [8], [31] and in the paper [35] for strong pseudoprimes.

Knopfmacher and Porubsky [13] with topological tools proved the following very interesting new result:

**Given** \( a, b, s \in \mathbb{N}, \ (a, b) = 1, \) **the arithmetical progression** \( an + b, \ n \in \mathbb{N} \) **contains infinitely many products of** \( s \) **pseudoprimes.**

**References**


[3] Cipolla M., *Su numeri composti \( P \), che verificano la congruenza di Fermat \( \alpha^P - 1 \equiv 1 \pmod{P} \)*, Annali di Matematica (3) 9 (1904), 139–160.


70 A. Rotkiewicz

On pseudoprimes having special forms and a solution of K. Szymiczek’s problem


Author(s) Address(es):

Institute of Mathematics, Polish Academy of Sciences, ul. Śniadeckich 8, 00-956 Warszawa 10, skr. poczt. 21

E-mail address: rotkiewi@impan.gov.pl