FERMAT PSEUDO PRIMES

PROEFSCHRIFT

TER VERKRIJGING VAN DE GRAAD VAN DOCTOR IN DE TECHNISCHE WETENSCHAPPEN AAN DE TECHNISCHE HOGESCHOOL DELFT, OP GEZAG VAN DE RECTOR MAGNIFICUS IR. H. R. VAN NAUTA LEMKE, HOOGLERAAR IN DE AFDELING DER ELEKTROTECHNIEK, VOOR EEN COMMISSIE UIT DE SENAAT TE VERDEDIGEN OP WOENSDAG 21 APRIL 1971 TE 16.00 UUR

DOOR

ERIK LIEUWENS
WISKUNDIG INGENIEUR
GEBOREN TE ROTTERDAM

FERMAT PSEUDO PRIMES

PROEFSCHRIFT

TER VERKRIJGING VAN DE GRAAD VAN DOCTOR IN DE TECHNISCHE WETENSCHAPPEN AAN DE TECHNISCHE HOGESCHOOL DELFT, OP GEZAG VAN DE RECTOR MAGNIFICUS IR. H. R. VAN NAUTA LEMKE, HOOGLERAAR IN DE AFDELING DER ELEKTROTECHNIEK, VOOR EEN COMMISSIE UIT DE SENAAT TE VERDEDIGEN OP WOENSDAG 21 APRIL 1971 TE 16.00 UUR

DOOR

ERIK LIEUWENS
WISKUNDIG INGENIEUR
GEBOREN TE ROTTERDAM

DRUKKERIJ HOOGLAND DELFT — 1971

DIT PROEFSCHRIFT IS GOEDGEKEURD DOOR DE PROMOTOR PROF. DR. H. J. A. DUPARC.

Fermat pseudo primes.

Introduction.

P. de Fermat proved in 1640 that every prime p satisfies $a^p \equiv a \pmod p$. For $(a,p) = 1$ this is equivalent to $a^{p-1} \equiv 1 \pmod p$.
Conversely the relation $a^m \equiv a \pmod m$, then it does not necessarily lead to the conclusion that m is prime.
During the last years a number of articles appeared about odd composite numbers satisfying $2^{m-1} \equiv 1 \pmod m$.
The section 1.1 gives an historical overview of nearly all these papers, moreover some new theorems are added.
Most of the theorems in section 1.1 are generalised in section 1.2. This section deals with composite numbers m, which for a given natural number a satisfy $a^m \equiv a \pmod m$.
A more complicated problem treated in section 1.4 deals with the construction of composite numbers which for all positive integers a satisfy $a^m \equiv a \pmod m$. It is very remarkable, that the perfect numbers come into the picture in this section.
A related more specialized problem namely $\Phi(n) \mid n-1$ is discussed in section 1.4.7.

The first problem, to find composite numbers m which satisfy $2^{m-1} \equiv 1 \pmod m$, might be alternatively formulated: Find composite numbers which satisfy $u_m \equiv u_1 \pmod m$; here the sequence u_n is defined by $u_o = 1$, $u_n = 2.u_{n-1}$ $(n = 1, 2, \ldots)$. This suggest a further generalisation: There are theorems which give information what elements of a second order recurring sequence $u_o = 0$, $u_1 = 1$, $u_{n+2} = au_{n+1} + bu_n$ are divisible by a given prime p. Then it is investigated whether similar properties are satisfied also by composite integers m.

For historical reasons, in section 2.1 the Fibonacci sequence and the associated Fibonacci sequence is investigated. In section 2.2 this matter is generalised to arbitrary second order recurring sequences and in section 2.4 the question is put whether there exist composite numbers which satisfy a prime relation for every second order recurring sequence.

There are properties of second order recurrings sequences, which may be extended to k-th ($k > 2$) order recurrings sequences and again the question can be put "Do there exist composite numbers m, which satisfy a prime relation for every k-th order recurring sequence?"

We could not solve this problem for $k > 1$, even not in the case $k = 2$, but for this special case in section 2.4 some restrictions are given about the divisors of such a possible composite number. Up till now no composite number satisfying the prime relation has been found.

1 Fermat first order pseudo primes.

1.1 Fermat first order pseudo primes with reference to 2.

1.1.1 Introduction.

We call a composite integer m a Fermat first order pseudo prime with reference to 2, if

$$2^m \equiv 2 \pmod{m} \qquad (1)$$

Consider the first order sequence $u_o = 1$, $u_{n+1} = 2u_n$ $(n = 0, 1, \ldots)$. Then (1) is equivalent to $u_m \equiv u_1 \pmod{m}$.
The set of all Fermat first order pseudo-primes with reference to 2, will be denoted by $\Psi(1;2)$.
If m is odd, then (1) is equivalent with:

$$2^{m-1} \equiv 1 \pmod{m} \qquad (2)$$

In 1938 Poulet [58] published a table of nearly all odd numbers $m<10^8$, which satisfy (1). Therefore numbers m, which satisfy (2) are also called Poulet numbers.

Unless stated otherwise all elements $m \in \Psi(1;2)$ in the following sections are odd.

1.1.2 General properties.

F. Sarrus [20] is, to our knowledge, the first who found a number m, namely $341 = 11.31$ and $2^{340} \equiv 1 \pmod{341}$.
V. Bouniakowsky [8] proved that, if $m = p_1 \cdot p_2$ $(p_1 \neq p_2)$ and $m-1$ is divisible by the smallest positive integer e_m, for which holds $2^{e_m} \equiv 1 \pmod{m}$, then $m \in \Psi(1;2)$.
J.H. Jeans [40] noticed, that if $p_1 \neq p_2$, $2^{p_1} \equiv 2 \pmod{p_2}$ and $2^{p_2} \equiv 2 \pmod{p_1}$, then $p_1 \cdot p_2 \in \Psi(1;2)$.

J. Franel [27] and T. Hayashi [36] combined the theorems of Bouniakowsky and Jeans to:

Theorem 1.1.1. If $m = p_1 \cdot p_2$, $p_1 \neq p_2$, $g = (p_1-1, p_2-1)$ and g is divisible by the smallest positive integer e_m, for which holds $2^{e_m} \equiv 1 \pmod{m}$, then $m \in \Psi(1;2)$.

If we call e_{p_i} the smallest positive integer for which holds, that $2^{e_{p_i}} \equiv 1 \pmod{p_i}$, then we can formulate theorem 1.1.1 also as follows:

Theorem 1.1.2. The number $m = p_1 \cdot p_2$, $(p_1 \neq p_2) \in \Psi(1;2)$ if and only if $g \equiv 0 \pmod{\{e_{p_1}, e_{p_2}\}}$; where $g = (p_1-1, p_2-1)$.

Proof: Suppose $m \in \Psi(1;2)$, then holds:

$$2^{m-1} \equiv 1 \pmod{m},$$

so
$$2^{p_1p_2-1} \equiv 1 \pmod{p_1} \tag{3}$$

and
$$2^{p_1p_2-1} \equiv 1 \pmod{p_2}. \tag{4}$$

According to a theorem of Fermat one has

$$2^{p_1-1} \equiv 1 \pmod{p_1} \tag{5}$$

It follows from (3) and (5)

$$2^{p_2-1} \equiv 1 \pmod{p_1} \tag{6}$$

If $g = (p_1-1, p_2-1)$, then it follows from the relations (5) and (6) that $2^g \equiv 1 \pmod{p_1}$, at the same time $g \equiv 0 \pmod{e_{p_1}}$.
Similarly from relation (4) one deduces $g \equiv 0 \pmod{e_{p_2}}$.

Thus $g \equiv 0 \pmod{\{e_{p_1}, e_{p_2}\}}$.

On the other hand, if $g \equiv 0 \pmod{\{e_{p_1}, e_{p_2}\}}$ then

$$2^{p_1-1} \equiv 1 \pmod{p_2}$$

which leads to (4) and a simular argument leads to (3), hence

$$p_1p_2 \in \Psi(1;2).$$

Rotkiewicz [66], [81] proved the following three theorems:

Theorem 1.1.3 For each $p_1 \geq 11$ and $\neq 13$, there exist a $p_2 > p_1$ with $p_1p_2 \in \Psi(1;2)$.
The proof of this theorem uses the fact, that for each $p_1 > 11$ and $\neq 13$ there exist a $p_2 > p_1$, with $2^{p_1} \equiv 2 \pmod{p_2}$ and $p_2 \equiv 1 \pmod{p_1-1}$.

Theorem 1.1.4. $m = p_1 p_2 \in \Psi(1;2)$ if and only if

$$M_{p_1} . M_{p_2} = (2^{p_1}-1)(2^{p_2}-1) \in \Psi(1;2).$$

Theorem 1.1.5. For every $p_1 \geq 11$ and $\neq 13$ there exist $p_2 > p_1$, which satisfies

$$M_{p_1} . M_{p_2} = (2^{p_1}-1)(2^{p_2}-1) \in \Psi(1;2)$$

Theorem 1.1.6. The collection $\Psi(1;2)$ contains an infinite number of elements.

This theorem is already proved by: Duparc [25], Rotkiewicz [73], Steuerwald [96] etc.
We give a simple proof.
Suppose $m \in \Psi(1;2)$, then also $M = 2^m-1 \in \Psi(1;2)$.

$$M = 2^m-1 \mid 2^{2^m-2} - 1 = 2^{M-1} - 1$$

Hence all elements of the sequence

$$m_o = 341; \; m_{n+1} = 2^{m_n} - 1 \quad (n = 0, 1, \ldots.) \text{ belong to } \Psi(1;2).$$

Theorem 1.1.7. If $m = m_1 . m_2$, m_1 and $m_2 \in \Psi(1;2)$, $(m_1, m_2) = 1$, $(m_1-1, m_2-1) = g$ and $g \equiv 0 \pmod{\{e_{m_1}, e_{m_2}\}}$, then $m \in \Psi(1;2)$.

Proof: $g \equiv 0 \pmod{\{e_{m_1}, e_{m_2}\}}$

thus

$$2^{m_1-1} \equiv 1 \pmod{m}$$

and

$$2^{m_2-1} \equiv 1 \pmod{m}.$$

Conclusion $m \in \Psi(1;2)$.

Theorem 1.1.8. Suppose $n \geq 2$ and $p_i \neq p_j$ for $i \neq j$, then

$$m = \prod_{i=1}^{n} p_i \in \Psi(1;2) \text{ if and only if}$$

$$2^{\frac{m}{p_i} - 1} \equiv 1 \pmod{p_i} \quad \text{for} \quad i = 1(1)n.$$

Proof: Suppose $m \in \Psi(1;2)$, thus $2^{m-1} \equiv 1 \pmod{m}$ and also

$$2^{m-1} \equiv 1 \pmod{p_i} \qquad i = 1(1)n$$

p_i is a prime so that: $2^{p_i} \equiv 2 \pmod{p_i}$.

Then

$$2^{p_1 \cdots p_{i-1} p_i p_{i+1} \cdots p_n} \equiv 2^{p_1 \cdots p_{i-1} p_{i+1} \cdots p_n} \pmod{p_i},$$

so

$$2^{\frac{m}{p_i} - 1} \equiv 1 \pmod{p_i}.$$

The proof that the condition is also sufficient, is equally simple.

Theorem 1.1.8 can be generalised to:

Theorem 1.1.9. Suppose that $m_{j_1} \in \Psi(1;2)$,

$$(p_{i_1}, m_{j_1}) = 1, \ (p_{i_1}, p_{i_2}) = 1, \ (m_{j_1}, m_{j_2}) = 1, \ i_1 \neq i_2, \ j_1 \neq j_2$$

for $i_1, i_2 = 1(1)k$ and $j_1, j_2 = 1(1)h$,

then

$$m = \prod_{i=1}^{k} p_i \cdot \prod_{j=1}^{h} m_j \in \Psi(1;2) \text{ if and only if}$$

$$2^{g_i} \equiv 1 \pmod{p_i}, \ g_i = \left(\frac{m}{p_i} - 1, \ p_i - 1\right) \qquad i = 1(1)k$$

$$2^{g_j} \equiv 1 \pmod{m_j}, \ g_j = \left(\frac{m}{m_j} - 1, \ m_j - 1\right) \qquad j = 1(1)h.$$

Proof: Suppose $m \in \Psi(1;2)$, thus $2^{m-1} \equiv 1 \pmod{m}$.

From theorem 1.1.8 it follows that:

$$2^{\frac{m}{p_i} - 1} \equiv 1 \pmod{p_i} \tag{7}$$

From a theorem of Fermat it follows that:

$$2^{p_i - 1} \equiv 1 \pmod{p_i} \tag{8}$$

If $g_i = \left(\frac{m}{p_i} - 1, \ p_i - 1\right)$ then it follows from the relations (7) and (8) that

$$2^{g_i} \equiv 1 \pmod{p_i} \qquad i = 1(1)k.$$

From $2^{m-1} \equiv 1 \pmod{m}$ it follows that $2^{m-1} \equiv 1 \pmod{m_j}$;

$$m_j \in \Psi(1;2)$$

so

$$2^{m_j-1} \equiv 1 \pmod{m_j}$$

and

$$2^{\frac{m}{m_j}-1} \equiv 1 \pmod{m_j}$$

Thus

$$2^{g_j} \equiv 1 \pmod{m_j} \qquad j = 1(1)h,$$

where

$$g_j = \left(\frac{m}{m_j} - 1,\ m_j-1\right).$$

The proof that the conditions are also sufficient is equally simple.

Further Rotkiewicz [61] proved:

Theorem 1.1.10? For every $p\ (\geq 3)$ there exist an infinite number of $m \in \Psi(1;2)$, for which $m \equiv 0 \pmod{p}$

.1.3 Even numbers $m \in \Psi(1;2)$.

D.H. Lehmer is, to our knowledge, the first who found an even number $m \in \Psi(1;2)$, namely $161038 = 2.73.1103$.
After this N.G.W.H. Beeger [6] found three other even numbers $m \in \Psi(1;2)$ and proved the following two theorems:

Theorem 1.1.11. Suppose $n = \prod_{i=1}^{k} p_i$, $k \geq 2$ then $2n \in \Psi(1;2)$ if and only if $2n \equiv p_i \pmod{e_{p_i}}$ $\quad i = 1(1)k$.

Theorem 1.1.12 $\Psi(1;2)$ contains an infinite number of even numbers.

The proof of the last theorem has been based on the fact that for every even number $m_1 = 2n \in \Psi(1;2)$ there exist a prime p, such that

$$m_2 = p.m_1 \in \Psi(1;2).$$

We shall repeat it shortly.
From a theorem of Bang [3] it follows that there exist a prime p, for which holds

$$2^{2n-1} \equiv 1 \pmod{p},\ 2^x \not\equiv 1 \pmod{p} \qquad 1 \leq x < 2n-1$$

and ?

$$p = (2n-1)v+1 \qquad v \geq 2,$$

which leads to $2pn \in \Psi(1;2)$.

1.1.4 Fermat numbers and $\Psi(1;2)$.

A number $F_n = 2^{2^n}+1$ is called a Fermat number.

Theorem 1.1.13. For every integer n, for which F_n is composite, is

$$F_n \in \Psi(1;2).$$

See the proof of theorem 1.2.13.

Duparc [25] proved

Theorem 1.1.14. Every composite divisor m of F_n satisfies $m \in \Psi(1;2)$.

Cipolla [17] proved the following two theorems.

Theorem 1.1.15. If $0 < k \leq 2^n-n-1$ and $m = \prod_{i=n}^{n+k} (2^{2^i}+1)$, then

$$m \in \Psi(1;2).$$

Theorem 1.1.16. If $m = F_{n_1}.F_{n_2}....F_{n_s}$ and $n_1 < \ldots < n_s$, then $m \in \Psi(1;2)$ if and only if

$$2^n > n_s.$$

1.1.5 The number of elements $< N \in \Psi(1;2)$.

Denote by $P(N)$ the number of elements $\in \Psi(1;2)$, which are less than N. Erdös [31] proved

$$c_1 \log N < P(N) < N.e^{-c_2(\log N \log\log N)^{\frac{1}{2}}}$$

1.1.6 The number of prime divisors of $m \in \Psi(1;2)$.

We call $\tau(m)$ the number of prime divisors of m.
In 1936 D.H. Lehmer proved, that there exist an infinite number of elements $m \in \Psi(1;2)$, with $\tau(m) = 2$.
This theorem can be proved by using theorem 1.1.3.

P. Erdös [28] generalised his method and proved

Theorem 1.1.17 For every integer $k \geq 2$ there are an infinite number of elements $m \in \Psi(1;2)$ for which $\tau(m) = k$.

Rotkiewicz [61] reached the same result by proving

Theorem 1.1.18 Suppose a, b and $k \geq 2$ are positive integers, $a > b$ and $(a, b) = 1$, then there exist an infinite number of integers $m \in \Psi(1;a)$ with $a^{m-1} \equiv b^{m-1} \pmod{m}$ and $\tau(m) = k$.

At the same time Rotkiewicz [61] proved

Theorem 1.1.19 For every integer $k \geq 3$ and for every p, there exist an integer $m \in \Psi(1;a)$, such that $m \equiv 0 \pmod{p}$ and $\tau(m) = k$.

C.G. Lekkerkerker [52] generalised a theorem of Bang [3] and proved that for every odd integer n, there exist a prime p, in such a manner that $2^n \equiv 1 \pmod{p}$ and $2^d \not\equiv 1 \pmod{p}$ $1 < d < n$.

With the aid of this, one can prove

Theorem 1.1.20 If the integer $m \in \Psi(1;2)$ has the property $\tau(m) = k$, then for $M = 2^n - 1$ one has $\tau(M) > 2^k - 1$.

With the aid of the proof of theorem 1.1.6 and theorem 1.1.20 we can prove in an elementary way

Theorem 1.1.21 For every integer N there are an infinite number of elements m in $\Psi(1;2)$, with $\tau(m) > N$.

1.1.7 Elements in $\Psi(1;2)$ with square divisors.

Theorem 1.1.22 $m = p^2$ is element of $\Psi(1;2)$, if and only if

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Theorem 1.1.23. $m = p_1^2 . p_2$ is element of $\Psi(1;2)$, $(p_1 > 2, p_2 > 2$ and $p_1 \neq p_2)$ if and only if

$$p_1^2 \in \Psi(1;2),$$

$$2^{p_1^2 - 1} \equiv 1 \pmod{p_2}$$

and

$$2^{p_2 - 1} \equiv 1 \pmod{p_1^2}$$

The proofs of these two theorems is a special case of the proofs of the similar theorems for the set $\Psi(1;a)$ (see section 1.2.7).
To our knowledge there are two numbers, namely $p = 1093$ and $p = 3511$, which satisfy theorem 1.1.22.
With the aid of a result of Birkhoff en Vandiver [7] it is possible to construct numbers which satisfy theorem 1.1.23.

Rotkiewicz [82] proved

Theorem 1.1.24 $m = n^2$ is element of $\Psi(1;2)$ leads for every prime divisor p of n, to $2^{p-1} \equiv 1 \pmod{p^2}$

1.1.8 Arithmetical sequences, which contain an infinite number of elements of $\Psi(1;2)$.

Theorem 1.1.25 Every arithmetical sequence $ax+b$ ($x = 0, 1, 2, \ldots$ and $(a, b) = 1$) contains an infinite number of elements of $\Psi(1;2)$.

The proof was given so far as we know, for the first time by Rotkiewicz [67] in 1963.

Some consequences of this theorem are:

1. Suppose $\{c_i\}$ is a finite ordered set of n positive integers <10, of which $c_1 = 1, 3, 7$ or 9.
   Then there exist an infinite number of elements in $\Psi(1;2)$ of the form $k.10^h + \sum_{i=1}^{h} c_i.10^{i-1}$, in which $h \leq n$, k and h are integers.
2. For every positive integer $k \geq 2$ there exist an element $m > k$ of $\Psi(1;2)$, in such a manner that all the numbers $m \pm 1, \ldots, m \pm k \notin \Psi(1;2)$.
3. There exist an infinite number of elements in $\Psi(1;2)$ of the form $nk+1$, where n is odd and $k=1, 2, \ldots$.

Theorem 1.1.26 There exist an infinite number of triples of different arithmetical sequences $m_{i,j} = a_i k_j + b_i$ $i = 1, 2, 3$; for which there exist an infinite number of integers k_j with $m_{i,j} \in \Psi(1;2)$ for $i = 1, 2, 3$.

The proof of Rotkiewicz [71] is based on

Theorem 1.1.27 If n is odd and n, $2n-1$ and $3n-2 \in \Psi(1;2)$ and $3 \nmid n(2n-1)$ then N, $2N-1$ and $3N-2 \in \Psi(1;2)$, in which $N = \frac{2^{2n}-1}{3}$ and $3 \nmid N(2N-1)$.

The properties hold for $n = \frac{2^{37}+1}{3}$.

Szymiczek [98] proved:

Theorem 1.1.28 For an infinite number of primes p_1 of the form $8k+1$ there exist primes p_2 and p_3, in such a manner that $p_1 \cdot p_2$, $p_1 \cdot p_3$ and $p_2 \cdot p_3 \in \Psi(1;2)$.

1.1.9 Super Fermat first order pseudo-primes with reference to 2.

In 1954 Duparc introduced the Super Poulet numbers. We shall call them Super Fermat first order pseudo primes with reference to 2. The set of all these numbers will be denoted by $\Psi^*(1;2)$.
The elements $M \in \Psi^*(1;2)$ satisfy the following properties

1. $M \in \Psi(1;2)$;
2. For every composite number m, for which holds that $m \mid M$, then $m \in \Psi(1;2)$.

Theorem 1.1.29 The number $m = \prod_{i=1}^{n} p_i$ $(n \geq 2) \in \Psi(1;2)$ is element of $\Psi^*(1;2)$, if and only if $2^g \equiv 1 \pmod{m}$, in which $g = (p_1-1,\ldots,p_n-1)$.

The proof might be illustrated for the case $n = 3$. The proof for $n > 3$ runs similar.

Suppose: $m = p_1p_2p_3 \in \Psi(1;2) \rightarrow 2^{p_1p_2-1} \equiv 1 \pmod{p_3}$

$$p_1 \cdot p_2 \in \Psi(1;2) \rightarrow 2^{p_1-1} \equiv 1 \pmod{p_3} \qquad (9)$$

$$p_2 \cdot p_3 \in \Psi(1;2) \rightarrow 2^{p_2-1} \equiv 1 \pmod{p_3} \qquad (10)$$

$$p_3 \text{ is a prime} \rightarrow 2^{p_3-1} \equiv 1 \pmod{p_3} \qquad (11)$$

From the relations (9), (10) and (11), it follows that

$$2^g \equiv 1 \pmod{p_3} \qquad g = (p_1-1, p_2-1, p_3-1)$$

and similary $2^g \equiv 1 \pmod{p_i}$, $(i = 1, 2)$. So $2^g \equiv 1 \pmod{p_1p_2p_3}$. That the property is also sufficient, is still more simple.

It follows from theorem 1.1.5 and theorem 1.1.29

Theorem 1.1.30 *For every prime* $p \geq 11$ *and* $\neq 13$ *there are only a finite number of elements* $M \in \Psi^*(1;2)$ *for which* $p \mid M$.

Duparc [25] and Szymiczek [100] proved:

Theorem 1.1.31 For every positive integer $n \geq 2$ $\quad F_n.F_{n+1} \in \Psi^*(1;2)$.

Recently Rotkiewicz proved that for every prime $p_1 \geq 11$ and $\neq 13$ there exist two primes p_2 and $p_3 > p_1$ with

$$2^{p_1-1} \equiv 1 \pmod{p_i}$$

and $\qquad p_i \equiv 1 \pmod{p_1} \qquad i = 2, 3.$

From this it follows that

Theorem 1.1.32 There exist an infinite number of elements M of $\Psi^*(1;2)$, for which one has $\upsilon(M) = 3$.

1.1.10 Tables of $\Psi(1;2)$.

In 1819 Sarrus [20] was to our knowledge, the first who found an element of $\Psi(1;2)$.
Banachiewicz [2] found in 1919 7 elements from $\Psi(1;2)$.
Poulet published in 1926 a table of nearly all the odd elements of $\in \Psi(1;2)$, which are smaller than 5.10^7.
In 1936 D.H. Lehmer [48] published a table of odd elements m of $\Psi(1;2)$ for which holds $10^7 < m < 10^8$ and, if $p \mid m$, then $p > 313$.
In 1938 Poulet [58] corrected his table of 1926 and extended it to $m<10^8$.
In 1949 D.H. Lehmer gave 9 corrections on the Poulet's last table and extended his own table to $m < 2.10^8$.
Recently van Zijl [106] and Lieuwens [53] corrected the table of Poulet on three places.

1.2 Fermat first order pseudo primes with reference to a.

1.2.1 Introduction.

We call a composite positive integer m a Fermat first order pseudo prime with reference to a, if

$$a^m \equiv a \pmod{m} \qquad (1)$$

where a is a fixed positive integer ≥ 2.
Consider the first order sequence $u_o = 1$, $u_{n+1} = au_n$, $(n = 0, 1, ..)$.
Then (1) is equivalent to $u_m \equiv u_1 \pmod{m}$.
The set of all Fermat first order pseudo-primes with reference to a, will be denoted by $\Psi(1;a)$.
Unless stated otherwise all elements $m \in \Psi(1;a)$ in the following sections are relative prime to a.

1.2.2 General properties.

Theorem 1.2.1 If $m = p_1 \cdot p_2$, $p_1 \neq p_2$, $g = (p_1-1, p_2-1)$ and g is divisible by the smallest positive integer e_m with: $a^{e_m} \equiv 1 \pmod{m}$, then $m \in \Psi(1;a)$.

If we call e_{p_i} the smallest positive integer satisfying $a^{e_{p_i}} \equiv 1 \pmod{p_i}$ then we can reformulate theorem 1.2.1 as follows:

Theorem 1.2.2 A necessary and sufficient condition for $m = p_1p_2$, $p_1 \neq p_2$, $g = (p_1-1, p_2-1)$ to be an element of $\Psi(1;a)$, is

$$g \equiv 0 \pmod{\left\{e_{p_1}, e_{p_2}\right\}}$$

Proof: Suppose $m \in \Psi(1;a)$, then:

$$a^{m-1} \equiv 1 \pmod{m}$$

thus

$$a^{p_2-1} \equiv 1 \pmod{p_1} \qquad (2)$$

and

$$a^{p_1-1} \equiv 1 \pmod{p_2} \qquad (3)$$

p_1 is a prime and $(p_1, a) = 1$,
thus

$$a^{p_1-1} \equiv 1 \pmod{p_1} \qquad (4)$$

From the relations (2) and (4) it follows that:

$$a^g \equiv 1 \pmod{p_1} \tag{5}$$

in which $g = (p_1-1, p_2-1)$.
Also for p_2:

$$a^g \equiv 1 \pmod{p_2} \tag{6}$$

Because $(p_1, p_2) = 1$ it follows from the relations (5) and (6) that:

$$a^g \equiv 1 \pmod{p_1 \cdot p_2} \tag{7}$$

At the same time:

$$a^k \equiv 1 \pmod{p_1 \cdot p_2} \tag{8}$$

in which $k = \left\{e_{p_1}, e_{p_2}\right\}$. It is simple to prove that k is the smallest positive integer, for which holds that:

$$a^k \equiv 1 \pmod{p_1\, p_2}.$$

It follows from the relations (7) and (8) that $g \equiv 0 \pmod{k}$.
In the opposite case, if $g \equiv 0 \pmod{k}$ then

$$a^g \equiv 1 \pmod{p_1 \cdot p_2} \quad \text{thus} \quad m \in \Psi(1;a).$$

Theorem 1.2.3 There exist an infinite number of elements in $\Psi(1;a)$, which are the product of two different primes.

Lemma For every odd number n there exist at least one pair of primes p_1, p_2 such that:

$$p_1 \mid a^n-1 \qquad p_1 \nmid a^x-1 \qquad 1 \le x < n \qquad p_1 = 2nv_1+1$$

$$p_2 \mid a^n+1 \qquad p_2 \nmid a^x+1 \qquad 1 \le x < n \qquad p_2 = 2nv_2+1$$

Proof of the lemma.
From a result of Birkhoff and Vandiver [7], it follows that there exist primes p_1 and p_2 such that $p_2 \mid a^{2n}-1$ and $p_2 \nmid a^x-1$, if $1 \le x < 2n$ and $p_2 = 2nv_2+1$, thus $p_2 \mid a^n+1$ and $p_2 \neq p_1$ proves the lemma.

Remark that $p_1p_2 \in \Psi(1;a)$.

For $p_1p_2-1 = 2n\,(2nv_1v_2+v_1+v_2)$

and

$$p_1 \mid a^n-1 \mid a^{p_1p_2-1}-1,$$

$$p_2 \mid a^n+1 \mid a^{2n}-1 \mid a^{p_1p_2-1}-1.$$

with this theorem 1.2.3 is proved.

Theorem 1.2.4 $m = p_1p_2 \in \Psi(1;a)$, $p_1 \neq p_2$, if and only if

$$M_{p_1}.M_{p_2} = \left(\frac{a^{p_1}-1}{a-1}\right)\left(\frac{a^{p_2}-1}{a-1}\right) \in \Psi(1;a).$$

Proof: Suppose $p_1p_2 \in \Psi(1;a)$ then:

$$a^{p_2-1} \equiv 1 \pmod{p_1} \quad \text{thus also:} \quad a^{p_2-1} \equiv 1 \pmod{p_1p_2},$$

$$a^{p_2} \equiv a \pmod{p_1p_2} \quad \text{and} \quad \frac{a^{p_2}-1}{a-1} \equiv 1 \pmod{p_1p_2} \tag{9}$$

if

$$p_1 \nmid a-1 \quad \text{and} \quad p_2 \nmid a-1.$$

similarly

$$\frac{a^{p_1}-1}{a-1} \equiv 1 \pmod{p_1p_2} \tag{10}$$

From relation (10) it follows

$$M_{p_1} = \frac{a^{p_1}-1}{a-1} \mid a^{M_{p_1}-1}-1 \tag{11}$$

From relation (9) it follows

$$M_{p_2} = \frac{a^{p_2}-1}{a-1} \mid a^{M_{p}-1}-1 \tag{12}$$

Hence $M_{p_1}.M_{p_2} \in \Psi(1;a)$.

Contrary suppose

$$M_{p_1}.M_{p_2} \in \Psi(1;a)$$

then

$$\frac{a^{p_1}-1}{a-1} \mid a^{M_{p_2}-1}-1.$$

Hence $p_1 \mid \frac{a^{p_2}-1}{a-1} - 1$. Consequently $p_1 \mid a^{p_2-1} - 1$.

Similarly

$$p_2 \mid a^{p_1-1} - 1.$$

Hence $p_1 p_2 \in \Psi(1;a)$.

Theorem 1.2.5 $\Psi(1;a)$ contains at least one element.

Proof: Suppose a is a positive integer ≥ 3, and $m = \frac{a^{2a}-1}{a^2-1}$

It is obvious that

$$2a \mid \frac{a^{2a}-a^2}{a^2-1} = m-1.$$

Thus

$$a^{2a}-1 \mid a^{m-1}-1$$

and

$$m \mid a^{2a}-1$$

consequently

$$m \in \Psi(1;a).$$

Theorem 1.2.6 The set $\Psi(1;a)$ contains an infinite number of elements.

Proof: A number m_1 exists for which $m_1 \in \Psi(1;a)$ and $(m_1, a-1)=1$.

Then $M = \frac{a^{m_1}-1}{a-1} \in \Psi(1;a)$,

for

$$m_1 \mid \frac{a^{m_1}-a}{a-1} = M-1 \quad \text{thus} \quad \frac{a^{m_1}-1}{a-1} \mid a^{M-1}-1.$$

With this it is proved that $\Psi(1;a)$ contains an infinite number of elements.

Theorem 1.2.7 If $m = m_1 \cdot m_2$, m_1 and $m_2 \in \Psi(1;a)$, $(m_1, m_2) = 1$, $g = (m_1-1, m_2-1)$ and g is divisible by the smallest positive integer e_m, for which holds $a^{e_m} \equiv 1 \pmod{m}$, then $m \in \Psi(1;a)$.

Proof: $g \equiv 0 \pmod{e_m}$ and $m_1 \equiv 1 \pmod{g}$. Then it follows

$$a^{m_1-1} \equiv 1 \pmod{m}, \text{ similarly } a^{m_2-1} \equiv 1 \pmod{m}.$$

Hence $m \in \Psi(1;a)$.

Theorem 1.2.8 A necessary and sufficient condition for

$$m = \prod_{i=1}^{k} p_i, \ (k \geq 2) \text{ to be an element of } \Psi(1;a), \text{ is}$$

$$a^{n_i-1} \equiv 1 \pmod{p_i}, \ n_i = \frac{m}{p_i} \qquad i = 1(1)k.$$

Proof: Suppose $m \in \Psi(1;a)$, thus $a^{m-1} \equiv 1 \pmod{m}$; then

$$a^{m-1} \equiv 1 \pmod{p_i} \qquad i = 1(1)k.$$

p_i is a prime thus

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

and

$$a^{m} \equiv a^{n_i} \pmod{p_i}. \text{ Since } (p_i, a) = 1, \text{ it follows that}$$

$$a^{n_i-1} \equiv 1 \pmod{p_i} \qquad i = 1(1)k.$$

The sufficiency of the condition can be proved by a similar simple argument.

The preceding theorem is to be generalized by:

Theorem 1.2.9 Necessary and sufficient conditions, that $m = p_1 \cdots p_k \cdot m_1 \cdots m_\ell$ is an element of $\Psi(1;a)$ are

$$a^{g_i} \equiv 1 \pmod{p_i} \qquad g_i = (\frac{m}{p_i} - 1, p_i - 1) \qquad i = 1(1)k$$

$$a^{g_j} \equiv 1 \pmod{m_j} \qquad g_j = (\frac{m}{m_j} - 1, m_j - 1) \qquad j = 1(1)\ell$$

where

$$m_{j_1} \in \Psi(1;a), \quad (p_{i_1}, m_{j_2}) = 1, \quad (p_{i_1}, p_{i_2}) = 1,$$

$$(m_{j_1}, m_{j_2}) = 1, \ i_1 \text{ and } i_2 = 1(1)k \quad i_1 \neq i_2, \ j_1 \text{ and } j_2 = 1(1)\ell$$

$$j_1 \neq j_2.$$

Proof: Suppose $m \in \Psi(1;a)$,

thus

$$a^{m-1} \equiv 1 \pmod{m}, \text{ then } a^{m-1} \equiv 1 \pmod{p_i} \quad i = 1(1)k;$$

p_i ia a prime, thus $a^{p_i} \equiv a \pmod{p_i}$ then:

$$a^{m} \equiv a^{n_i} \pmod{p_i}, \quad n_i = \frac{m}{p_i}$$

thus

$$a^{n_i-1} \equiv 1 \pmod{p_i}.$$

Hence

$$a^{g_i} \equiv 1 \pmod{p_i}.$$

From $a^{m-1} \equiv 1 \pmod{m}$ it follows, that $a^{m-1} \equiv 1 \pmod{m_j}$;

$m_j \in \Psi(1;a)$ thus $a^{m_j} \equiv a \pmod{m_j}$,

then

$$a^{m} \equiv a^{n_j} \pmod{m_j}, \; n_j = \frac{m}{m_j}$$

thus

$$a^{n_j-1} \equiv 1 \pmod{m_j}.$$

Hence

$$a^{g_j} \equiv 1 \pmod{m_j}.$$

Contrary from

$$a^{g_i} \equiv 1 \pmod{p_i}$$ it follows, that $a^{n_i-1} \equiv 1 \pmod{p_i}$

thus

$$a^{m-1} \equiv 1 \pmod{p_i}.$$

From

$$a^{g_j} \equiv 1 \pmod{m_j}$$ it follows, that $a^{n_j-1} \equiv 1 \pmod{m_j}$

thus

$$a^{m-1} \equiv 1 \pmod{m_j}.$$

Because

$$(p_{i_1}, m_{j_1}) = 1, \; (p_{i_1}, p_{i_2}) = 1, \; (m_{j_1}, m_{j_2}) = 1$$

$i_1, i_2 = 1(1)k$ and $j_1, j_2 = 1(1)\ell$ it follows that

$$a^{m-1} \equiv 1 \pmod{m} \quad \text{thus} \quad m \in \Psi(1;a).$$

Theorem 1.2.10 If there exist a number $m_1 \in \Psi(1;a)$, for which holds that $m_1 \equiv 0 \pmod{p_1}$, then there exist an infinite number of elements $m \in \Psi(1;a)$ such that $m \equiv 0 \pmod{p_1}$.

Proof: Suppose $m \in \Psi(1;a)$, $m \equiv 0 \pmod{p_1}$ and $\tau(m) = k \quad k(>2)$. Then there exist a prime p_2 such that

$$a^{m-1} \equiv 1 \pmod{p_2}, \quad a^x \not\equiv 1 \pmod{p_2} \quad 1 \le x < m-1 \quad \text{and} \quad p_2 = (m-1)v+1.$$

It is simple to prove that $mp_2 \in \Psi(1;a)$.
From this it follows, that $\Psi(1;a)$ contains an infinite number of elements m, for which holds that $p_1 | m$.

1.2.3 Elements $m \in \Psi(1;a)$, for which holds that $m \equiv 0 \pmod{a}$.

This section deals with the case $a|m$, excluded above.

Theorem 1.2.11 $\Psi(1;a)$ contains at least one element m, for which holds that $m \equiv 0 \pmod{a}$.

Proof: For every positive integer $a \ge 3$ there exist a prime p with $(p, a) = 1$, for which holds that:

$$a^2 - a - 1 \equiv 0 \pmod{p}.$$

Thus

$$a^{p+1} - a - 1 \equiv 0 \pmod{p},$$

$$a^{a^{p+1}-a-1} \equiv 1 \pmod{a^p - 1}$$

and

$$a^{a^{p+1}-a} \equiv a \pmod{a(a^p-1)}.$$

Hence

$$a(a^p - 1) \in \Psi(1;a).$$

Theorem 1.2.12 $\Psi(1;a)$ contains an infinite number of elements m, for which holds that $m \equiv 0 \pmod{a}$.

Proof: In the preceding theorem it is proved that $\Psi(1;a)$ contains at least one element $m_o \equiv 0 \pmod{a}$.

By using a result of Birkhoff and Vandiver [7] we are able to find a prime p in such a manner that:

$$a^{m_o-1} \equiv 1 \pmod{p} \quad \text{and} \quad a^x \not\equiv 1 \pmod{p} \quad 1 \le x < m_o-1$$

and

$$p = (m_o-1)v+1.$$

$$pm_o \in \Psi(1;a), \text{ for } pm_o-1 = (m_o-1)(m_o v+1),$$

and

$$p \mid a^{m_o-1}-1 \mid a^{pm_o-1}$$

$$m_o \mid a^{m_o-1}-1 \mid a^{pm_o-1}$$

Because $(p, m_o) = 1$, it holds that:

$$pm_o \mid a^{pm_o-1}-1 \quad \text{thus} \quad pm_o \in \Psi(1;a).$$

Thus it is possible to construct an infinite sequence of elements $m_i \in \Psi(1;a)$, in such a manner that for $i \ge 1$, $m_{i-1} \in \Psi(1;a)$ and

$$a^{m_{i-1}-1} \equiv 1 \pmod{p_i}, \quad a^x \not\equiv 1 \pmod{p_i}, \quad 1 \le x < m_{i-1}-1,$$

$$p_i = (m_{i-1}-1)v_i+1 \quad \text{and} \quad m_i = p_i m_{i-1} \in \Psi(1;a).$$

1.2.4 Generalized Fermat numbers and $\Psi(1;a)$.

We call the number

$$F(a, h) = \frac{a^{a^{h+1}}-1}{a^{a^h}-1} \quad \text{a generalized Fermat number.}$$

$$F(2, h) = F_h = 2^{2^h}+1$$

Theorem 1.2.13 If $F(a, h)$ is composite then

$$F(a, h) \in \Psi(1;a).$$

Proof: $$F(a, h)-1 = \frac{a^{a^{h+1}} - a^{a^h}}{a^{a^h}-1} = a^{a^h} \cdot \frac{a^{a^{h+1}-a^h}-1}{a^{a^h}-1}.$$

Thus

$$a^{h+l} \mid F(a, h)-1,$$

hence

$$a^{F(a, h)-1} \equiv 1 \pmod{F(a, h)},$$

thus

$$F(a, h) \in \Psi(1;a).$$

Theorem 1.2.14 If the positive integers k and ℓ satisfy $k < \ell \leq a^{k-1}$ then $F(a, h) \cdot F(a, \ell) \mid \in \Psi(1;a)$.

Proof: If $k \leq a^{k-1}$ then $a^k \mid a^{a^k} - a^{a^{k-1}} \mid F(a, k)-1$.

Thus

$$F(a, k) \mid a^{F(a, k)-1}-1.$$

Certainly it holds that

$$F(a, k) \mid a^{F(a, \ell)-1}-1$$

$$(F(a, k), F(a, \ell)) = 1.$$

Thus

$$F(a, \ell).F(a, k) \in \Psi(1;a).$$

Theorem 1.2.15 For $n_1 < n_2 < \ldots < n_s < a^{n_1-1} - 1$ one has

$$\prod_{i=1}^{s} F(a, n_i) \in \Psi(1;a).$$

The simple proof runs similar to that of the preceding theorem.

1.2.5 The number of elements $< N \in \Psi(1;a)$.

Denote by $P(N)$ the number of elements $\in \Psi(1;a)$, which are less than N. By the same method as Erdös [31] used for the set $\Psi(1;2)$, it can be proved for the set $\Psi(1;a)$, that

$$P(N) < N.e^{-c(\log N.\log \log N)^{\frac{1}{2}}}$$

1.2.6 The number of prime divisors of $m \in \Psi(1;a)$.

It has been proved in theorem 1.2.6 that if $m \in \Psi(1;a)$, then also

$$M = \frac{a^m-1}{a-1} \in \Psi(1;a).$$

Consequently if m is divisible by s different primes then M is divisible by at least s+1 different prime divisors.

Theorem 1.2.19 For every integer $k \geq 3$ there exist an infinite number of elements $m \in \Psi(1;a)$ in such a manner that $\tau(m) = k$.

Proof: This theorem is correct for k=2 (see theorem 1.2.3).
Suppose it is true for k=h. From the result of Birkhoff and Vandiver [7] it follows that, there exist a prime p_{h+1}, in such a manner that:

$$a^{m_h-1} \equiv 1 \pmod{p_{h+1}} \tag{13}$$

and

$$p_{h+1} \equiv 1 \pmod{m_h-1} \quad \text{and} \quad a^x \not\equiv 1 \pmod{p_{h+1}},\ 1 \leq x < m_h-1.$$

Suppose $p_{h+1} = (m_h-1)v+1$,
then

$$m_h p_{h+1}-1 = (m_h-1)(m_h v+1).$$

Hence

$$m_h \mid a^{m_h-1}-1 \mid a^{m_h p_{h+1}-1}-1. \tag{14}$$

From the relations (13) and (14) it follows that $m_h p_{h+1} \in \Psi(1;a)$, thus the theorem is true for k = h+1.

1.2.7 Elements of $\Psi(1;a)$ with square divisors.

Theorem 1.2.22 The number $m = p^2$ is element of $\Psi(1;a)$ $((a, p)=1)$ if and only if

$$a^{p-1} \equiv 1 \pmod{p^2}$$

Proof: Suppose $m \in \Psi(1;a)$.
Hence

$$a^{p^2-1} \equiv 1 \pmod{p^2}.$$

Because

$$a^{p^2-p} \equiv 1 \pmod{p^2},$$

it follows that

$$a^{p-1} \equiv 1 \pmod{p^2}.$$

Contrary if

$$a^{p-1} \equiv 1 \pmod{p^2}$$

then

$$a^{p^2-1} \equiv 1 \pmod{p^2},$$

thus

$$m \in \Psi(1;a).$$

Theorem 1.2.23 The number $m = p_1^2 \cdot p_2$ is element of $\Psi(1;a)$; with $(p_i, a) = 1$, $(p_1, p_2) = 1$; if and only if

$$a^{p_1^2-1} \equiv 1 \pmod{p_2}, \tag{15}$$

$$a^{p_2-1} \equiv 1 \pmod{p_1^2}, \tag{16}$$

$$a^{p_1-1} \equiv 1 \pmod{p_1^2}. \tag{17}$$

Proof: Suppose $m \in \Psi(1;a)$.

Hence

$$a^{p_1^2p_2-1} \equiv 1 \pmod{p_1^2} \tag{18}$$

$$a^{p_1^2p_2-1} \equiv 1 \pmod{p_2} \tag{19}$$

From the relation (18) and $a^{p_1^2-p_1} \equiv 1 \pmod{p_1^2}$ one finds in virtue of $p_1-1 = x(p_1^2p_2-1)+y(p_1^2-p_1)$ with $x = 1-p_1$ and $y = p_1p_2$ the required relation

$$a^{p_1-1} \equiv 1 \pmod{p_1^2} \tag{20}$$

Because

$$p_2-1 = p_1^2p_2-1-p_2(p_1^2-1)$$

one has

$$a^{p_2-1} \equiv 1 \pmod{p_1^2}. \tag{21}$$

From the relation (19) it follows

$$a^{p_1^2-1} \equiv 1 \pmod{p_2} \tag{22}$$

Moreover from the relations (20) and (21) one obtains

$$a^{p_1^2p_2-1} \equiv 1 \pmod{p_1^2}$$

since

$$p_1^2p_2-1 = p_1^2(p_2-1)+(p_1+1)(p_1-1).$$

From the relation (22) it follows

$$a^{p_1^2p_2-1} \equiv 1 \pmod{p_2}.$$

Hence $p_1^2p_2 \in \Psi(1;a)$.

1.2.8 Arithmetic sequences, which contain an infinite number of elements of $\Psi(1;a)$.

Theorem 1.2.24 There exist an infinite number of elements m of $\Psi(1;a)$, which are of the form $nk+1$.

Proof: Rotkiewicz [85] proved that for every even number n, a^n-1 has a composite divisor of the form $nk+1$, then it can be proved that: $nk+1 \in \Psi(1;a)$. Consider the sequence $a^{n_i}-1$, in which $i = 1, \ldots$ and $n|n_i$, then we can form an infinite number of integer m, in such a manner that $m = nv_i+1$ and $m \in \Psi(1;a)$.
Remark: We don't know whether the sequence $cx+d$, in which $(c, d) = 1$, contains an infinite number of elements of $\Psi(1;a)$.

1.2.9 Super Fermat first order pseudo-primes with reference to a.

We call a number M a Super Fermat first order pseudo-prime with reference to a, if $M \in \Psi(1;a)$ and if, for every composite divisor of m of M, holds that $m \in \Psi(1;a)$.
The set of all these numbers will be denoted by $\Psi^*(1;a)$.
We shall give now some theorems without proving them. The proofs are nearly equivalent to the proofs of the corresponding theorems for $\Psi(1;2)$.

Theorem 1.2.25 A number $m = p_1 \ldots p_n$ $(n \geq 2) \in \Psi^*(1;a)$ if and only if

$$a^g \equiv 1 \pmod{m}$$

in which $g = (p_2-1, \ldots, p_n-1)$.

Theorem 1.2.26 For every prime p there exist only a finite number of elements $\in \Psi^*(1;a)$ with $p|M$.
Remark: It is easy to prove that the numbers $m = p_1^2.p_2 \in \Psi(1;a)$ belong to $\Psi^*(1;a)$.

Theorem 1.2.27 For every positive integer $n \geq 2$

$$F(a, n).F(a, n+1) \in \Psi^*(1;a).$$

1.3 Fermat first order pseudo-primes with reference to a and b.

We call a composite number m a Fermat first order pseudo-prime with reference to a and b, $a \neq b$ if:

$$m \in \Psi(1;a) \quad \text{and} \quad m \in \Psi(1;b)$$

The set of all Fermat first order pseudo-primes with reference to a and b is called $\Psi(1;a,b)$.

$$\Psi(1;a,b) = \Psi(1;a) \cap \Psi(1;b).$$

We don't know whether there exist for every pair a,b one element in the set $\Psi(1;a,b)$. Also we don't know, that if there exist one element in $\Psi(1;a,b)$, that there are an infinite number of elements in $\Psi(1;a,b)$. It is easy to prove, that if $p_1 = 2abk+1$ and $p_2 = 4abk+1$ are simultaneously prime for the same value of k then $p_1p_2 \in \Psi(1;a,b)$.

It is possible to extend this to the set $\Psi(1;a,b,c)$, in which $a \neq b$, $b \neq c$ and $a \neq c$, for if $p_1 = 2abck+1$ and $p_2 = 4abck+1$ are simultaneously prime for the same value of k then $p_1p_2 \in \Psi(1;a,b,c)$. In the two unsolved problems, we have the same difficulty: It is not know whether there exist two arithmetic sequences, in such a manner that there are an infinite number of values of the argument, so that in both sequences there appear a prime.

Table of elements $m \in \Psi(1;2) \cap \Psi(1;3)$ which are $< 10^6$. The numbers, which are marked with an asterisk (*) belong also to $\Psi(1)$.

$561^{*} = 3. 11. 17$
$1105^{*} = 5. 13. 17$
$1729^{*} = 7. 13. 19$
$2465^{*} = 5. 17. 29$
$2701 = 37. 73$
$2821^{*} = 7. 13. 31$
$6601^{*} = 7. 23. 41$
$8911^{*} = 7. 19. 67$
$10585^{*} = 5. 29. 73$
$15841^{*} = 7. 31. 73$
$18721 = 97. 193$
$29341^{*} = 13. 37. 61$
$31621 = 103. 307$
$41041^{*} = 7. 11. 13. 41$
$46657^{*} = 13. 37. 97$
$47197 = 109. 433$
$49141 = 157. 313$
$52633^{*} = 7. 73. 103$
$62745^{*} = 3. 5. 47. 89$
$63973^{*} = 7. 13. 19. 37$
$75361^{*} = 11. 13. 17. 31$
$83333 = 167. 499$
$83665 = 5. 29. 577$
$88561 = 11. 83. 97$
$90751 = 151. 601$
$93961 = 7. 31. 433$
$101101^{*} = 7. 11. 13.101$
$104653 = 229. 457$
$107185 = 5. 13. 17. 97$
$115921^{*} = 13. 37. 241$
$126217^{*} = 7. 13. 19. 73$
$162401^{*} = 17. 41. 233$
$172081^{*} = 7. 13. 31. 61$
$176149 = 19. 73. 127$
$188461^{*} = 7. 13. 19.109$
$204001 = 7. 151. 193$
$226801 = 337. 673$
$228241 = 13. 97. 181$
$252601^{*} = 41. 61. 101$
$276013 = 19. 73. 199$
$278545^{*} = 5. 17. 29.113$
$282133 = 307. 919$
$294409^{*} = 37. 73. 109$
$314821^{*} = 13. 61. 397$
$334153^{*} = 19. 43. 409$
$340561^{*} = 13. 17. 23. 67$
$399001^{*} = 31. 61. 211$
$410041^{*} = 41. 73. 137$
$449065^{*} = 5. 19. 29.163$
$488881^{*} = 37. 73. 181$
$512461^{*} = 31. 61. 271$
$530881^{*} = 13. 97. 421$
$534061 = 11. 47.1033$
$552721^{*} = 13. 17. 41. 61$
$563473 = 37. 97. 157$
$574561 = 13. 193. 229$
$622909 = 7. 23. 53. 73$
$653333 = 467.1399$
$656601^{*} = 3. 11. 101.197$
$658801^{*} = 11. 13. 17.271$
$665281 = 577.1153$
$670033^{*} = 7. 13. 37.199$
$721801 = 601.1201$
$748657^{*} = 7. 13. 19.433$
$786961 = 7. 19. 61. 97$
$825265^{*} = 5. 7. 17. 19. 73$
$838201^{*} = 7. 13. 61.151$
$852841^{*} = 11. 31. 41. 61$
$873181 = 661.1321$
$997633^{*} = 7. 13. 19.577$

1.4 Fermat first order pseudo-primes.

1.4.1 Introduction.

We call a positive composite integer m a Fermat first order pseudo-prime if

$$a^m \equiv a \pmod{m} \text{ for every } a. \qquad (1)$$

They are also called Carmichael numbers.
The set of all Fermat first order pseudo-primes is called $\Psi(1)$.

1.4.2 General properties.

Theorem 1.4.1 If $m \in \Psi(1)$ then m has the following properties:

1. m is odd
2. m is square-free
3. m contains at least 3 different primes.

The proof is elementary, see [56].

Theorem 1.4.2 Necessary and sufficient properties, for

$$m = \prod_{i=1}^{n} p_i \quad (n \geq 3), \text{ to be an element of } \Psi(1), \text{ are}$$

$$m \equiv 1 \pmod{p_i - 1} \qquad i = 1(1)n.$$

For the proof see for instance Duparc [22].

Theorem 1.4.3 The number m, containing n (≥3) primes is of the form $\prod_{i=1}^{n} (2a_i g+1)$, in which every set of n-1 integers a_i are relative prime.

Proof (see also Chernick [15]).
Suppose $m = p_1 \cdot p_2 \cdot \ldots \cdot p_n \in \Psi(1)$ and $2g = (p_1-1, p_2-1, \ldots, p_{n-1}-1)$
then $p_i = 2a_i g+1 \qquad i = 1, \ldots, n-1$.
According to theorem 1.4.2 holds $m \equiv 1 \pmod{p_i-1}$, thus $N_i \equiv 1 \pmod{p_i-1}$,
where $N_i = \frac{m}{p_i}$. Hence $p_n = 2a_n g+1$.

Suppose, that for $i = 1, \ldots, k-1, k+1, \ldots, n$ a_i is a multiple of p.

According to theorem 1.4.2 holds, that

$$\prod_{\substack{i=1\\ i\neq l}}^{n} (2a_i g+1) \equiv 1 \pmod{2a_l g} \qquad (2)$$

Suppose, that $1 \neq k$, then a_k is also a multiple of p. However we supposed, that the a_i's are relative prime, thus $p = 1$.

Theorem 1.4.4 If m is composed of 2n primes, then all the numbers a_i are odd or an even number (<2n) of them are even.

Proof: According to theorem 1.4.3 we can write

$$m = \prod_{i=1}^{2n} (2a_i g+1).$$

According to theorem 1.4.2 it must be satisfied that

$$2a_j g \Bigg| \left(\prod_{\substack{i=1\\ i\neq j}}^{2n} (2a_i g+1)-1 \right) \qquad j = 1(1)2n \qquad (3)$$

$$(a_1, a_2, \ldots, a_{2n}, 2g) = 1$$

and

$$2g \left(\prod_{\substack{i=1\\ i\neq j}}^{2n} (2a_i g+1)-1 \right)$$

so that we can simplify the equation (3) to:

$$a_j \Big| (2g.f(a_1,\ldots,a_{j-1}, a_{j+1},\ldots, a_{2n}, g)+ \sum_{\substack{i=1\\ i\neq j}}^{2n} a_i \qquad (4)$$

in which

$$2g.f(a_1,\ldots, a_{j-1}, a_{j+1},\ldots, a_{2n}, g) = \prod_{\substack{i=1\\ i\neq j}}^{2n} (2a_i g+1)-1-2g \sum_{\substack{i=1\\ i\neq j}}^{2n} a_i.$$

The equation (4) does not hold if a_j is even and $\sum_{i=1}^{2n} a_i$ is odd.

From this theorem 1.4.4 follows.

Theorem 1.4.5 If m is composed of 2n+1 primes, then all the numbers a_i are odd or an odd number (<2n) of them are even.

This theorem can be proved in a similar way.

1.4.3 The extension of an element of $\Psi(1)$ to another element of $\Psi(1)$.

Theorem 1.4.6 If $m_1 = p_1, p_2, \ldots, p_n \in \Psi(1)$ $(n \geq 3)$ and $p_1 < p_2 < \ldots < p_n$; k is the smallest common multiple of the numbers $p_i - 1$ $i = 1(1)n$, then $m_2 = m_1 \cdot p_{n+1} \in \Psi(1)$, if the following properties hold

1. $p_{n+1} - 1 \equiv 0 \pmod{k}$

2. $m_1 - 1 \equiv 0 \pmod{p_{n+1} - 1}$

3. p_{n+1} is a prime $> p_n$.

Proof: See also Chernick [15] and Sispánov [94].

Suppose $m_1 \in \Psi(1)$, then:

$$\frac{m_1}{p_i} - 1 \equiv 0 \pmod{p_i - 1} \qquad i = 1(1)n \tag{5}$$

If $m_2 \in \Psi(1)$ then

$$\frac{m_1 p_{n+1}}{p_i} - 1 \equiv 0 \pmod{p_i - 1} \qquad i = 1(1)n+1 \tag{6}$$

For $i = 1(1)n$ is $\frac{m_1}{p_i} = 1 + V(p_i - 1)$ then equation (6) becomes:

$p_{n+1} - 1 \equiv 0 \pmod{p_i - 1}$ and for $i = n+1$ holds $m_1 - 1 \equiv 0 \pmod{p_{n+1} - 1}$.

From this theorem 1.4.6 follows.

Remarks: The extension of a number m is not always possible, for instance:

$561 = 3.11.17$; $k = 80$ thus $p_4 = 80V+1$

$560 \equiv 0 \pmod{80V}$, $7 \equiv 0 \pmod{V}$, hence:

$V = 1$, $p_4 = 81$

$V = 7$, $p_4 = 561$.

Both numbers are composite.

Thus this number m cannot be extended by the method of theorem 1.4.6.

The following numbers are elements of $\Psi(1)$:

$$2821 = 7.13.31$$
$$172081 = 7.13.31.61$$
$$31146661 = 7.13.31.61.181$$
$$16850343601 = 7.13.31.61.181.541$$
$$36413592521761 = 7.13.31.61.181.541.2161$$
$$235996493133533041 = 7.13.31.61.181.541.2161.6481$$

$$2465 = 5.17.29$$
$$278545 = 5.17.29.113$$
$$93869665 = 5.17.29.113.337$$
$$63174284545 = 5.17.29.113.337.673$$
$$169875651141505 = 5.17.29.113.337.673.2689$$
$$869234892905356934 5 = 5.17.29.113.337.673.2689.231169$$

It is not known, whether this procedure may be repeated infinite number of times.

1.4.4 Perfect numbers and $\Psi(1)$.

Theorem 1.4.7 If n is a perfect number and $n_1, n_2, \ldots, n_k$ are all divisors of n, then

$$m = \prod_{i=1}^{k-1} (n_i.n.h+1) \in \Psi(1),$$

if

$$p_i = n_i.n.h+1 \qquad i = 1(1)k-1 \text{ is prime.}$$

Proof: Since n is perfect, one has $n_1 + \ldots + n_{k-1} = n$.
Suppose $m \in \Psi(1)$, then

$$n_j.n.h \left| \prod_{\substack{i=1 \\ i\neq j}}^{k-1} (n_i.n.h+1)-1 \qquad (j=1(1)\ k-1) \right. \tag{14}$$

Since $n_j.n.h \mid n^2h$ the relation leads to

$$n_j.n.h \left| \left(\sum_{\substack{i=1 \\ i\neq j}}^{k-1} n_i \right).n.h \right. \tag{15}$$

For the last sum one has

$$\sum_{\substack{i=1 \\ i\neq j}}^{k-1} n_i = n-n_j \qquad \text{and because } n_j \mid n, \text{ one concludes to}$$

$$m \in \Psi(1).$$

For the perfect number 6 we take

$$p_1 = 6.n+1$$

$$p_2 = 12.n+1$$

$$p_3 = 18.n+1$$

With this we found the following numbers $m < 2.10^{10}$.

$$1729 = 7 \cdot 13 \cdot 19$$
$$294409 = 37 \cdot 73 \cdot 109$$
$$56052361 = 211 \cdot 421 \cdot 631$$
$$118901521 = 271 \cdot 541 \cdot 811$$
$$172947529 = 307 \cdot 613 \cdot 919$$
$$216821881 = 331 \cdot 661 \cdot 991$$
$$228842209 = 337 \cdot 673 \cdot 1009$$
$$1299963601 = 601 \cdot 1201 \cdot 1801$$
$$2301745249 = 727 \cdot 1453 \cdot 2179$$
$$9624742921 = 1171 \cdot 2341 \cdot 3511$$
$$11346205609 = 1237 \cdot 2473 \cdot 3709$$
$$13079177569 = 1297 \cdot 2593 \cdot 3889$$

For the perfect number 28 we take

$$p_1 = 28.n+1$$

$$p_2 = 56.n+1$$

$$p_3 = 112.n+1$$

$$p_4 = 196.n+1$$

$$p_5 = 392.n+1$$

It appears that the least possible choice, where these $p_1, \ldots, p_5$ are all prime leads to a number $m > 10^{27}$.

Theorem 1.4.8 If n is a perfect number and $n_1, n_2, \ldots, n_k$ are all divisors of n, then

$$m = \prod_{i=1}^{k} (n_i.n.h+1) \in \Psi(1),$$

if

$$p_i = n_i.n.h+1 \qquad i = 1(1)k \text{ is prime.}$$

The proof of this theorem can be given by using theorem 1.4.6.

By using theorem 1.4.6 and 1.4.7 we find, that if the factors $6n+1$, $12n+1$, $18n+1$, $36n+1$, $72n+1$ and $144n+1$ are prime, and if $n \equiv 0 \pmod{20}$ then the product of these 6 factors is element of $\Psi(1)$.
The smallest number of this type is

$$2281 \cdot 4561 \cdot 6841 \cdot 13681 \cdot 27361 \cdot 54721.$$

1.4.5 The number of elements $< N \in \Psi(1)$.

Denote by $P(N)$ the number of elements $\in \Psi(1)$, which are less than N. Erdös proved

$$P(N) < N.e^{-\frac{c.\log N \log\log\log N}{\log\log N}}$$

1.4.6 The number of divisors of $m \in \Psi(1)$.

Theorem 1.4.9 There are only a finite number of elements $m \in \Psi(1)$, which are a product of three primes, from which one prime is given. Beeger [5] was the first who proved this theorem.

Duparc [22] generalized this theorem to

Theorem 1.4.10 There are only a finite number of elements m, which are a product of $s(\geq 3)$ primes, from which $s-2$ primes are given.

1.4.7 Fermat first order pseudo-primes with a special property.

Since $a^{\phi(M)} \equiv 1 \pmod{M}$, obviously all M with $\phi(M) \mid M-1$ belong to $\Psi(1)$. This leads to the problem of finding numbers M which satisfy

$$M-1 = k.\phi(M) \qquad (16)$$

Where k is a given positive integer greater than 1, M a composite integer and $\phi(M)$ is the Euler's totient function. The main purpose is to prove that if the equation (16) has a solution M then M is the product of at least eleven distinct primes.
In 1932 D.H. Lehmer [47] proved that the considered type of numbers M have at least 7 distinct prime numbers, whereas Fr. Schuh [91] in 1944 had the intention to prove that M consists of at least 11 distinct primes. The theorem of Schuh is correct, not however his proof.

First we recall that any solution M of (16) satisfies the following properties:

Theorem 1.4.11 The number M is odd, square-free and a product of at least three different prime factors.

Theorem 1.4.12 If $p|M$, then M contains no prime factor of the form $px+1$.

The (simple) proofs of these two theorems were given by Lehmer [47] and Schuh [91].

Theorem 1.4.13 If $3|M$, then k is of the form $3x+1$.

Proof (from Schuh). Suppose $M = 3p_1p_2\ldots p_n$, the numbers p_i are of the form $3x+2$ (see theorem 1.4.12). M is a solution of equation (16), so

$$3p_1p_2\ldots p_n - 1 \equiv 2k(p_1-1)\ldots(p_n-1) \pmod 3,$$

hence

$$-1 \equiv 2k \pmod 3$$

and

$$k = 3x+1.$$

Since $k=1$ is excluded (this holds only if M is prime), one has $k \geq 4$.

Definition 1. A "S-sequence" is a finite or infinite ordered sequence of prime numbers p_i with the following three properties:

1. The smallest element is ≥ 3;
2. $p_i > p_j$ if and only if $i > j$;
3. $p_i \not\equiv 1 \pmod{p_j}$.

Definition 2. A "primitive" S-sequence with reference to the finite S-sequence $p_1,\ldots, p_n$ is the continuation of the S-sequence $p_1,\ldots, p_n$ in such a manner that each element p_{i+1} $(i \geq n)$ is the smallest prime $> p_i$ for which $p_{i+1} \not\equiv 1 \pmod{p_k}$ $(k = 1,\ldots, i)$.

Definition 3. A sequence $p_1,\ldots, p_n$ is a S-minorant of a sequence $q_1,\ldots, q_n$ if

$$\frac{p_1p_2\cdot\cdots\cdot p_n - 1}{(p_1-1)\ldots(p_n-1)} > \frac{q_1q_2\cdot\cdots\cdot q_n - 1}{(q_1-1)\ldots(q_n-1)}.$$

Remarks.

1. In definition 2 one can take $n = 1$, i.e. we consider a S-sequence which consists of one element only.

2. Primitive S-sequences of any finite number of elements can be constructed.
3. We call $(M-1)|\phi(M)$ the "S-quotient" of M.

One easily verifies the following:

Theorem 1.4.14 If in the index set $\{1,\ldots, n\}$ $(n \geq 2)$ an index k exists such that $p_k < q_k$ and if for all other indices i one has $p_i = q_i$, then

$$\frac{p_1 p_2 \cdot\cdot\cdot\cdot p_n - 1}{(p_1-1)\ldots(p_n-1)} > \frac{q_1 q_2 \cdot\cdot\cdot\cdot q_n - 1}{(q_1-1)\ldots(q_n-1)} .$$

By repeatedly applying this theorem one obtains:

Theorem 1.4.15 If in the index set $\{1,\ldots, n\}$ $(n \geq 2)$ an index k exists such that $p_k < q_k$ and if all other indices i one has $p_i \leq q_i$, then

$$\frac{p_1 \cdot\cdot\cdot\cdot p_n - 1}{(p_1-1)\ldots(p_n-1)} > \frac{q_1 q_2 \cdot\cdot\cdot\cdot q_n - 1}{(q_1-1)\ldots(q_n-1)} .$$

Theorem 1.4.16 If $3|M$, then M is the product of more than 212 prime numbers and $M > 5{,}5.10^{570}$.

Proof: The S-sequence S_1: 3, 5, 17, 23, 29 is S-minorant of any S-sequence of which the smallest element is 3 and which consists of 5 elements. Continuation of S_1 is only possible with prime numbers of the form $6x+29$ $(x = 1, 2, 3, \ldots)$. Consequently the sequence Σ_2: 3, 5, 17, 23, 29, 35, 41, 47, ... is a S-minorant of any S-sequence S_3 with the same number of elements, of which the smallest element is 3. For the S-quotients Q_2 and Q_3 of the sequences Σ_2 and S_3 one has $Q_2 > Q_3$. By theorem 1.4.13 one has $Q_3 \geq 4$, hence $Q_2 > 4$.

Then

$$\frac{3.5.17 \ \ldots \ (17+6n)}{2.3.16 \ \ldots \ (16+6n)} > Q_2 > 4.$$

By easy computation it follows $n \geq 210$, hence

$$M \geq 3 \cdot 5 \cdot \prod_{n=0}^{210} (17+6n) > 5{,}5.10^{570}.$$

Theorem 1.4.17 If the smallest prime factor of M is 5 then M consists of at least 11 primes.

Proof: The primitive S-sequence with reference to 5 is:

$$5, 7, 13, 19, 23, 37, 59, 67, 73, 83, \ldots .$$

A computation learns that:

$$\frac{5.7 \ldots 67.73-1}{4.6 \ldots 66.72} < 2.$$

We now prove, that the finite S-sequence S_4 5, 7, 13, 17, 19, 23, 37, 59, 67, 73 is a S-minorant of any S-sequence of which the smallest element is 5 and which consists of 10 elements. It is obvious that this fact proves theorem 1.4.17.

In order to prove the indicated result, we confer the sequence S_4 with some other sequences. The prime numbers smaller than 83, which can appear in a S-sequence which contains the element 5 are:

$$7, 13, 17, 19, 23, 29, 37, 43, 47, 53, 67, 73, 79.$$

If we remove from S_4 one or more elements ≥ 37 and add the same number of elements in such a way that the new sequences are a S-sequence as well, the new elements are necessarily > 73. Consequently S_4 is a S-minorant of the new sequence.

If we remove from S_3 the elements 23 and/or 29 and add the same number of elements again in such a way that the new sequence is a S-sequence, the new elements are either 47, 59 or > 73. In any case it appears that S_4 is a S-minorant of the then obtained new sequence.

Further a similar procedure will be followed by removing one or more elements 7, 13, 17 and 19; then the elements to be added are either 43, 53 or > 73. In any case the sequences S_4 is also a S-minorant of the new sequence.

Consequently S_4 is S-minorant of any other 10 element S-sequence with smallest element 5.

Remark. Since

$$2 < \frac{5.7.13.17.19.23.37.59.67.73.83-1}{4.6.12.16.18.22.36.58.66.72.82} .$$

The above proof doesnot hold if the sequence S_4 is extended with the additional factor 83, so in the assumption of the theorem the number 11 cannot be replaced by 12.

Theorem 1.4.18 If the smallest prime factor of M is ≥ 7 then M is the product of at least 13 primes.

Proof: The succeeding 13 prime numbers ≥ 7 are:

$$7, 11, 13, 17, \ldots, 41, 43, 47, 53.$$

A computation learns

$$\frac{7.11 \ldots 43.47-1}{6.10 \ldots 42.46} < 2 < \frac{7.11 \ldots 43.47.53-1}{6.10 \ldots 46.52} .$$

Any S-sequence of which the smallest element is ≥ 7 and consists of 13 elements has the sequence 7, 11, ..., 43, 47 as a S-minorant.

From theorems 1.4.16, 1.4.17 and 1.4.18 we derive

Theorem 1.4.19 If there exist a composite number M, which is a solution of equation (16), then M is the product of at least 11 prime numbers.

Remarks. A result of computation is:
If a composite number M, created by a primitive S-sequence with reference to 3 is a solution of the equation (16) then it must be a product of more than 63000 prime factors.

Conjecture. For a S-sequence with elements $p_1, p_2, \ldots$ one has

$$\lim_{n\to\infty} \prod_{i=1}^{n} \frac{p_i}{p_i-1} < 3,$$

which is equivalent to

$$\lim_{n\to\infty} \sum_{i=1}^{n} \frac{1}{p_i} < K \quad (= \text{constant}).$$

2.1 Fermat second order pseudo primes with reference to (1,1).

2.1.1 Introduction.

Consider the second order recurring sequence defined by:

$$u_0 = 0,\ u_1 = 1,\ u_{n+2} = u_{n+1} + u_n \qquad (n = 0, 1, \ldots) \qquad (1)$$

For this sequence the discriminant D of the characteristic polynomial $f(x) = x^2 - x - 1$ is equal to 5.
The sequence satisfies the following properties (where p is a prime):

1. $u_p - \left(\frac{D}{p}\right) \equiv 0 \pmod p$;

2. $u_p \equiv \left(\frac{D}{p}\right) \pmod p$;

3. $v_p \equiv 1 \pmod p$.

Here v_n is an element of the associated recurring sequence defined by:

$$v_0 = 2,\ v_1 = 1,\ v_{n+2} = v_{n+1} + v_n \qquad (n = 0, 1, \ldots),$$

and $\left(\frac{D}{p}\right)$ is the Legendre symbol.

Composite numbers m, which satisfy at least one of the three relations, will be called Fermat second order pseudo primes with reference to (1,1). The sets of these numbers m will be denoted by $\Psi_i(2;1,1)$ respectively. Moreover we define in correspondance with the three above sets the union.

$$\Psi(2;1,1) = \bigcup_{i=1}^{3} \Psi_i(2;1,1).$$

2.1.2 General properties.

For numbers treated in the proceeding section properties hold, some of which are special cases of corresponding properties for more general second order sequences, to be dealt with in section 2.2. So in correspondence with the properties and definitions 2.2.1 - 2.2.4 and 2.2.1 - 2.2.6 one has here similarly 2.1.1 - 2.1.4 and 2.1.1 - 2.1.6.

Moreover one has

Theorem 2.1.7 If $N \neq 1, 2, 6$ or 12, then there is a prime p, such that $N = c(p)$. The proof was given by Carmichael [10].

2.1.3 Composite numbers m belonging to the set $\Psi_1(2;1,1)$.

Also here properties hold which are copies of those of section 2.2.3. we mention theorems 2.1.8 - 2.1.14, which are equivalent to respectively the theorems 2.2.8 - 2.2.14.
By using these theorems we find for instance:

$$29.281 \in \Psi_1(2;1,1)$$

In fact one has

$$c(29) = 14,\ c(281) = 28,$$

thus

$$u_{28} \equiv 0 \pmod{281}$$

and

$$u_{280} \equiv 0 \pmod{29}$$

Remark.
The following connection between prime pairs and $\Psi_1(2;1,1)$ appears to be
If $p \equiv 17 \pmod{60}$ and $q = p+2$ are both prime, then $M = pq \in \Psi_1(2;1,1)$.

2.1.4 Composite numbers m belonging to the set $\Psi_2(2;1,1)$.

The theorem 2.1.15 is equivalent to the theorem 2.2.15.

Further one has the following

Theorem 2.1.16 There exist an infinite number of elements of $\Psi_2(2;1,1)$.

For a proof confer for instance Duparc [24].

2.1.5 Composite numbers m belonging to the set $\Psi_3(2;1,1)$.

The theorem 2.1.17 is equivalent to theorem 2.2.16.

Finally we mention

Theorem 2.1.18 There exist an infinite number of elements $\Psi_3(2;1,1)$.

A proof might be found also in [24].

A table* of all odd square free elements of $\Psi_3(2;1,1)$ which are $< 10^8$ and with a smallest divisor ≥ 23.

99036001	61	541	3001
98467739	139	281	2521
98385377	7013	14029	
98332081	67	919	1597
98158789	229	499	859
97967431	1871	52361	
97894501	1021	95881	
97308121	83	797	1471
97004521	811	119611	
96904081	6961	13921	
95452781	3989	23929	
95451361	5641	16921	
95145751	71	911	1471
94954861	5209	18229	
94913281	167	263	2161
94502701	4861	19441	
93891841	83	421	2687
93591569	7211	12979	
93431521	5581	16741	
93400277	6833	13669	
92625121	181	631	811
91433281	5521	16561	
91418543	3023	30241	
90686777	6733	13469	
89816411	3461	25951	
89784581	5471	16411	
89746073	773	116101	
89190301	1181	75521	
88741171	3331	26641	
87640801	3121	28081	
87581141	3821	22921	
87471017	2957	29581	
87217561	1459	59779	
87160061	2411	36151	
86268781	3511	24571	
86023943	1367	62929	
85903277	6553	13109	
85518229	5849	14621	
85090339	1459	58321	
85015493	4373	19441	
84792811	6091	13921	
84292249	2003	42083	

84188281	31	43	137	461
83967361	3463	24247		
83963177	2089	40193		
83241013	3533	23561		
83168821	1789	46489		
82995421	191	571	761	
82929001	281	421	701	
82597831	139	461	1289	
82291609	4969	16561		
81986581	1531	53551		
81965671	1039	78889		
80918281	6361	12721		
80207381	5171	15511		
80161381	31	61	42391	
79624621	139	691	829	
79525261	31	761	3371	
79465231	79	859	1171	
79398901	6301	12601		
78657721	41	761	2521	
78644611	6271	12541		
78430801	2801	28001		
78318241	29	41	199	331
78249601	89	263	3343	
78033889	2663	29303		
77866381	53	181	8117	
77862391	4651	16741		
77642881	5087	15263		
77337941	5077	15233		
77146831	6211	12421		
76923461	3581	21481		
76753921	23	61	227	241
76461841	31	83	29717	
75983627	6163	12329		
75663451	6151	12301		
75655873	113	607	1103	
75621281	5021	15061		
75606049	3889	19441		
75320341	5011	15031		
75245777	6133	12269		
75239513	2089	36017		
74580767	6529	11423		
73780877	6073	12149		

73693369	2267	32507		
73295777	6053	12109		
73131001	113	227	2851	
72186421	3469	20809		
72052993	43	769	2179	
71760001	139	601	859	
70957921	23	41	47	1601
70894277	5953	11909		
69714481	43	307	5281	
68335921	23	53	61	919
68205061	89	199	3851	
68154001	151	601	751	
67611121	2281	29641		
67237883	3347	20089		
67103401	2731	24571		
67081607	647	103681		
66796529	1783	37463		
66530011	439	151549		
66347849	1777	37337		
66124001	2711	24391		
66007061	4691	14071		
65429569	2089	31321		
65363101	3301	19801		
64709551	541	119611		
64610027	5683	11369		
64514581	4637	13913		
64051681	83	167	4621	
63397751	3251	19501		
62756641	109	241	2389	
62399041	4561	13681		
62289541	5581	11161		
62271311	431	144481		
62176661	131	521	911	
62133377	5573	11149		
61770041	3209	19249		
61218901	4517	13553		
60957361	61	181	5521	
60881921	1033	58937		
60490691	131	409	1129	
59765581	421	141961		
59268827	5443	10889		

59207581	541	109441		
57903361	2447	23663		
57464207	3023	19009		
57385651	1051	54601		
57280081	2861	20021		
57150721	661	86461		
57028949	577	98837		
56052361	211	421	631	
55902881	43	47	139	199
55763161	3049	18289		
55726849	607	91807		
55681841	6581	8461		
55530161	1361	40801		
54760151	1511	36241		
54675571	1021	53551		
54512641	167	449	727	
54459841	4261	12781		
54026029	4649	11621		
53835031	1621	33211		
53697953	4013	13381		
53655551	5981	8971		
53498369	127	223	1889	
52448371	1811	28961		
52326481	31	1069	1579	
51931333	1973	26321		
51803821	31	971	1721	
51803761	5441	9521		
51503671	1669	30859		
51132251	2081	24571		
50581081	3181	15901		
50486941	29	31	89	631
50075027	5003	10009		
49956481	107	541	863	
49476377	4973	9949		
49219673	937	52529		
49019851	4951	9901		
47938021	1951	24571		
47297543	2663	17761		
47219201	3967	11903		
47140601	521	90481		
46724131	2791	16741		
46672291	4831	9661		

46533961	197	199	1187	
46222177	103	443	1013	
46114921	5417	8513		
46112921	5881	7841		
45880213	1597	28729		
45596461	911	50051		
44826541	89	199	2531	
44605201	2161	20641		
44370481	1847	24023		
44236901	113	353	1109	
44111629	2269	19441		
43701901	797	54833		
43259221	3797	11393		
42525773	2089	20357		
42490801	31	41	101	331
42389027	4603	9209		
42149971	4591	9181		
41808581	1181	35401		
41177993	857	48049		
40928627	4523	9049		
40675981	2411	16871		
40629601	2851	14251		
40465501	3181	12721		
40433551	1091	37061		
40341001	29	401	3469	
40110001	31	61	21211	
39891041	281	141961		
39865729	47	769	1103	
39850127	4463	8929		
39440521	83	107	4441	
39247393	2557	15349		
39088169	37	113	9349	
38275301	701	54601		
38248981	3571	10711		
38040433	113	227	1483	
37964809	109	379	919	
37510019	5591	6709		
37011521	2417	15313		
36915301	3001	12301		
36574849	1823	20063		
36067201	101	103	3467	
36061997	1733	20809		

35798491	4231	8461		
35745841	23	79	103	191
35659009	29	37	167	199
35452891	1621	21871		
35365111	2729	12959		
35257249	107	109	3023	
34908721	29	83	14503	
34829761	3407	10223		
34657141	191	421	431	
34379101	811	42391		
34175777	4133	8269		
34134407	1847	18481		
34043101	131	151	1721	
33932089	347	97787		
33816593	73	149	3109	
33796531	4111	8221		
33707521	797	42293		
33666949	211	379	421	
33664651	1451	23201		
33567451	31	71	101	151
33323569	37	821	1097	
33161833	109	307	991	
32817151	4051	8101		
32815361	3307	9923		
32720221	31	541	1951	
32702723	683	47881		
32683201	3301	9901		
32560921	53	271	2267	
32432401	89	307	1187	
32414581	271	119611		
32377591	379	85429		
32167801	31	61	17011	
32092259	2069	15511		
31758371	71	491	911	
31673333	2297	13789		
31622993	233	135721		
31530241	1009	31249		
31513861	1621	19441		
31432381	269	116849		
31405501	71	631	701	
31181581	2111	14771		
31155001	1861	16741		

31150351	2791	11161		
30299333	337	89909		
29971811	2371	12641		
29604893	2909	10177		
29395277	3833	7669		
29111881	211	281	491	
28772641	1171	24571		
27854147	1523	18289		
27799469	37	61	109	113
27485041	43	661	967	
27236311	2131	12781		
27230701	71	421	911	
27012001	3001	9001		
26934121	811	33211		
26417953	43	557	1103	
26274151	151	191	911	
26157121	1321	19801		
25948187	409	63443		
25885421	661	39161		
25707841	2927	8783		
25532501	2917	8753		
25183621	2897	8693		
24994201	29	61	71	199
24930881	3329	7489		
24550241	2861	8581		
24493061	2857	8573		
24236461	1741	13921		
24196849	67	409	883	
24157817	73	149	2221	
24151381	2837	8513		
23759881	571	41611		
23731489	2179	10891		
23307377	3413	6829		
23292361	1171	19891		
22933531	541	42391		
22711873	59	349	1103	
22669501	2381	9521		
22591301	3881	5821		
22556801	761	29641		
22384181	911	24571		
22361327	3343	6689		
22187791	3331	6661		

21988961	2707	8123		
21850951	229	95419		
21813661	61	541	661	
21692189	2237	9697		
21619201	47	383	1201	
21574279	2179	9901		
21496367	1103	19489		
21308197	157	135721		
20754049	3529	5881		
20647441	947	21803		
20623969	113	229	797	
20551301	2617	7853		
20234341	3181	6361		
20036881	31	181	3571	
20018627	3163	6329		
19808821	181	109441		
19168477	433	44269		
18917713	109	197	881	
18673201	2161	8641		
18557951	1061	17491		
18552361	571	32491		
18307381	29	61	79	131
18175361	71	281	911	
18105281	929	19489		
18104129	61	449	661	
17737381	811	21871		
17497127	263	66529		
17461009	53	107	3079	
17438521	43	307	1321	
17236801	151	211	541	
16891981	73	149	1553	
16870961	1061	15901		
16685003	1667	10009		
16675201	101	107	1543	
16628977	23	29	107	233
16538741	37	197	2269	
16485493	1657	9949		
16350337	37	647	683	
16244257	167	211	461	
16233361	1117	14533		
15754007	887	17761		
15752101	911	17291		

~~15748561~~	~~137~~	~~139~~	~~827~~
15287009	547	27947	
~~15247621~~	~~61~~	~~181~~	~~1381~~
14985833	829	18077	
~~14930353~~	~~1597~~	~~9349~~	
14892541	2441	6101	
~~14792971~~	~~3331~~	~~4441~~	
14787181	1453	10177	
~~14676481~~	~~71~~	~~421~~	~~491~~
14671801	79	229	811
~~14646721~~	~~113~~	~~227~~	~~571~~
14609401	31	151	3121
~~14575091~~	~~1559~~	~~9349~~	
14462953	137	229	461
~~14383021~~	~~1433~~	~~10037~~	
14221969	509	27941	
~~14015843~~	~~683~~	~~20521~~	
13695947	827	16561	
~~13647691~~	~~71~~	~~211~~	~~911~~
13455077	2593	5189	
~~13404751~~	~~1831~~	~~7321~~	
13277423	1487	8929	
~~13088461~~	~~661~~	~~19801~~	
13012651	2551	5101	
~~12975691~~	~~1471~~	~~8821~~	
12962291	331	39161	
~~12958081~~	~~1361~~	~~9521~~	
12801491	521	24571	
~~12387799~~	~~3469~~	~~3571~~	
~~12178241~~	~~607~~	~~20063~~	
12119101	1741	6961	
~~12093121~~	~~919~~	~~13159~~	
12049409	2689	4481	
~~11800801~~	~~31~~	~~151~~	~~2521~~
11637583	929	12527	
~~11630081~~	~~43~~	~~307~~	~~881~~
11487961	271	42391	
~~10837601~~	~~1901~~	~~5701~~	
10679131	2311	4621	
~~10604431~~	~~1741~~	~~6091~~	
10403641	2281	4561	
~~10386241~~	~~1861~~	~~5581~~	

10237921	23	241	1847	
~~10054043~~	~~467~~	~~21529~~		
10024561	71	271	521	
~~10009201~~	~~101~~	~~113~~	~~877~~	
9922337	2269	4373		
~~9863461~~	~~2221~~	~~4441~~		
9811891	991	9901		
~~9793313~~	~~1277~~	~~7669~~		
9713027	2203	4409		
~~9594289~~	~~23~~	~~43~~	~~89~~	~~109~~
9476741	1777	5333		
~~9439201~~	~~61~~	~~271~~	~~571~~	
9401893	1877	5009		
~~9264097~~	~~37~~	~~227~~	~~1103~~	
8834641	1123	7867		
~~8834641~~	~~1123~~	~~7867~~		
8655511	1861	4651		
~~8518127~~	~~2063~~	~~4129~~		
~~8327801~~	~~131~~	~~151~~	~~421~~	
8259761	1381	5981		
~~8086231~~	~~2011~~	~~4021~~		
7961801	941	8461		
~~7947701~~	~~191~~	~~41611~~		
7887391	29	211	1289	
~~7879681~~	~~1621~~	~~4861~~		
7640137	29	109	2417	
~~7519441~~	~~41~~	~~241~~	~~761~~	
7405201	1361	5441		
~~7369601~~	~~1567~~	~~4703~~		
7353917	857	8581		
~~7067171~~	~~1231~~	~~5741~~		
6989569	2207	3167		
~~6924061~~	~~233~~	~~29717~~		
6884131	1151	5981		
~~6801661~~	~~349~~	~~19489~~		
6677057	37	113	1597	
~~6580549~~	~~773~~	~~8513~~		
6544561	661	9901		
~~6526369~~	~~557~~	~~11717~~		
6494801	2081	3121		
~~6374111~~	~~809~~	~~7879~~		
6368689	1129	5641		

6359021	709	8969	
6314141	29	239	911
6196129	113	54833	
6192721	941	6581	
6189121	61	241	421
6003923	227	26449	
5942627	1723	3449	
5862341	89	199	331
5800001	463	12527	
5481451	31	151	1171
5328181	1951	2731	
5310241	443	11987	
5208377	1613	3229	
5161201	101	137	373
5148001	41	241	521
5049001	31	271	601
5028577	47	97	1103
4974481	241	20641	
4870847	1087	4481	
4868641	1601	3041	
4828277	1553	3109	
4713361	821	5741	
4475521	211	21211	
4403027	1483	2969	
4250681	67	63443	
4226777	1453	2909	
4187341	773	5417	
4109363	827	4969	
4032337	23	199	881
3944777	43	199	461
3942271	811	4861	
3900797	197	19801	
3828001	101	151	251
3774377	1373	2749	
3663871	479	7649	
3645991	1021	3571	
3636121	313	11617	
3568661	1091	3271	
3452147	587	5881	
3430729	29	281	421
3399527	1303	2609	
3338221	691	4831	

3306493	29	113	1009	
~~3281749~~	~~919~~	~~3571~~		
3277231	331	9901		
~~3241897~~	~~83~~	~~139~~	~~281~~	
3218801	131	24571		
~~3188011~~	~~919~~	~~3469~~		
3181741	37	113	761	
~~3175883~~	~~563~~	~~5641~~		
3011713	47	139	461	
2872321	641	4481		
~~2851201~~	~~43~~	~~61~~	~~1087~~	
2786101	151	18451		
~~2757241~~	~~461~~	~~5981~~		
2747137	97	127	223	
~~2662277~~	~~1153~~	~~2309~~		
2586229	509	5081		
~~2559929~~	~~239~~	~~10711~~		
2509921	23	29	53	71
~~2499841~~	~~61~~	~~107~~	~~383~~	
2476549	137	18077		
~~2465101~~	~~593~~	~~4157~~		
2435423	769	3167		
~~2362081~~	~~887~~	~~2663~~		
2263127	1063	2129		
~~2221811~~	~~1291~~	~~1721~~		
2187841	257	8513		
~~2159389~~	~~991~~	~~2179~~		
2140921	229	9349		
~~1970299~~	~~199~~	~~9901~~		
1909001	41	101	461	
~~1857451~~	~~151~~	~~12301~~		
1857241	31	181	331	
~~1803601~~	~~601~~	~~3001~~		
1735841	761	2281		
~~1697183~~	~~769~~	~~2207~~		
1690501	751	2251		
~~1653601~~	~~47~~	~~151~~	~~233~~	
1626041	521	3121		
~~1536841~~	~~53~~	~~107~~	~~271~~	
1533601	31	61	811	
~~1392169~~	~~257~~	~~5417~~		
1388903	263	5281		

1346269	557	2417	
1325729	47	67	421
1314631	811	1621	
1256293	457	2749	
1203401	401	3001	
1193221	31	61	631
1174889	43	89	307
1149851	59	19489	
1106561	607	1823	
1106327	743	1489	
1084201	521	2081	
1081649	269	4021	
1034881	41	43	587
1033997	293	3529	
999941	577	1733	
925681	23	167	241
853469	239	3571	
851927	881	967	
741751	431	1721	
722261	491	1471	
655201	23	61	467
639539	43	107	139
638189	619	1031	
636641	461	1381	
635627	563	1129	
556421	431	1291	
530611	461	1151	
520801	241	2161	
512461	31	61	271
438751	541	811	
433621	199	2179	
430127	463	929	
399001	31	61	211
330929	149	2221	
303101	101	3001	
302101	317	953	
272611	131	2081	
254321	263	967	
252601	41	61	101
231703	263	881	
219781	271	811	

197209	199	991	
194833	23	43	197
186961	31	37	163
162133	73	2221	
161027	283	569	
146611	271	541	
118441	83	1427	
113573	137	829	
100127	223	449	
97921	181	541	
96049	139	691	
90061	113	797	
75077	193	389	
68251	131	521	
67861	79	859	
64681	71	911	
64079	139	461	
51841	47	1103	
15251	101	151	
13201	43	307	
10877	73	149	
5777	53	109	
4181	37	113	

* This table is a result of a programma written by G.J. Hameetman for an IBM 360/65 computer of the Delft University of Technology.

2.1.6 Super Fermat second order pseudo primes with reference to (1,1).

We call a composite integer M a Super Fermat second order pseudo prime with reference to (1,1) if M satisfies the following properties:

1. $M \in \Psi_3(2;1,1)$
2. For every composite number m, for which holds that $m|M$, then $m \in \Psi_3(2;1,1)$.

The set of all these numbers M will be denoted by $\Psi_3^*(2;1,1)$.

In order to derive properties of this new set we first prove the following

Lemma: If for an odd positive integer n, and a prime p holds that

$$v_n \equiv v_1 \pmod p \quad \text{then}$$

$$v_{m.n} \equiv v_m \pmod p \quad \text{holds for every positive integer m.}$$

Proof:

Suppose the lemma holds for every positive integer k with $1 \le k \le m$. Then it holds that

$$v_{nm} \cdot v_n \equiv v_m \cdot v_1 \pmod p.$$

This is equivalent with

$$v_{n(m+1)} - v_{n(m-1)} \equiv v_{m+1} - v_{m-1} \pmod p$$

and

$$v_{n(m-1)} \equiv v_{m-1} \pmod p.$$

Thus

$$v_{n(m+1)} \equiv v_{m+1} \pmod p.$$

Theorem 2.1.19 The number $m = \prod_{i=1}^{n} p_i$ $(n \ge 2) \in \Psi_3(2;1,1)$ is element of $\Psi_3^*(2;1,1)$, if and only if

$$v_{p_i} \equiv v_1 \pmod m \qquad i = 1(1)n.$$

The proof of this theorem might be illustrated for the case n=3. The proof for n>3 runs similarly.

Suppose

$$m = p_1p_2p_3 \in \Psi_3(2;1,1),$$

then

$p_1p_2 \in \Psi_3(2;1,1)$, hence $v_{p_1} \equiv v_1 \pmod{p_2}$;

$p_1p_3 \in \Psi_3(2;1,1)$, hence $v_{p_1} \equiv v_1 \pmod{p_3}$;

p_1 is a prime, hence $v_{p_1} \equiv v_1 \pmod{p_1}$.

From these relations it follows that

$$v_{p_1} \equiv v_1 \pmod{p_1p_2p_3}$$

and similarly

$$v_{p_i} \equiv v_1 \pmod{p_1p_2p_3} \qquad i = 2, 3.$$

Conversely suppose

$$v_{p_1} \equiv v_1 \pmod{p_1p_2p_3}$$

and

$$v_{p_2} \equiv v_1 \pmod{p_1p_2p_3}$$

Then it follows that

$$v_{p_1} \equiv 1 \pmod{p_2}$$

and using the lemma one obtains

$$v_{p_1p_2} \equiv v_{p_2} \equiv v_1 \pmod{p_2}$$

and similarly

$$v_{p_1p_2} \equiv v_{p_1} \equiv v_1 \pmod{p_1},$$

thus

$$p_1p_2 \in \Psi_3(2;1,1).$$

The proofs that p_1p_3 and $p_2p_3 \in \Psi_3(2;1,1)$ runs similar, thus

$$p_1p_2p_3 \in \Psi_3^*(2;1,1).$$

From theorem 2.1.19 it follows

Theorem 2.1.20 For every prime p only a finite number of elements $M \in \Psi_3^*(2;1,1)$ exist, for which one has $p|M$.

2.2 Fermat second order pseudo primes with reference to (a,b).

2.2.1 Introduction.

Consider the second order recurring sequence defined by:

$$u_0 = 0,\ u_1 = 1,\ u_{n+2} = au_{n+1} + bu_n \qquad (n = 0, 1, \ldots) \qquad (2)$$

Here a and b are fixed given integers.
$D = a^2+4b$ is called the discriminant of the characteristic polynomial $f(x) = x^2-ax-b$.
In either of the cases a=0 or b=0 the second order sequence can be considered essentially equivalent to a first order sequence, so we may suppose $ab \neq 0$.

Also here for a prime p with $p \nmid b$ one has the following properties:

1. $u_{p-\left(\frac{D}{p}\right)} \equiv u_0 \pmod p$;
2. $u_p \equiv \left(\frac{D}{p}\right) \pmod p$;
3. $v_p \equiv v_1 \pmod p$.

Here v_n is an element of the associated recurring sequence defined by:

$$v_0 = 2,\ v_1 = a,\ v_{n+2} = av_{n+1} + bv_n \qquad (n = 0, 1, \ldots)$$

and $\left(\frac{D}{p}\right)$ is the Legendre symbol.

The proofs of the properties are elementary (see for instance Duparc[24]).
Composite numbers m, which satisfy at least one of the three relations will be called Fermat second order pseudo primes with reference to (a,b).
The sets of these numbers m will be called $\Psi_i(2;a,b)$ respectively (i = 1, 2, 3), corresponding to which of the three above relations they satisfy.
Moreover we define

$$\Psi(2;a,b) = \bigcup_{i=1}^{3} \Psi_i(2;a,b).$$

2.2.2 General properties.

Definition 2.2.1 The least positive index c, such that $u_c \equiv 0 \pmod m$ will be denoted by c(m).
It is called "the rank of apparation" or "the restricted period" of the sequence modulo m.

Definition 2.2.2 The least positive index C, such that $u_C \equiv u_o \pmod m$ and $u_{C+1} \equiv u_1 \pmod m$ will be denoted by $C(m)$.
It is called "the period" or "the characteristic number" of the sequence modulo m.

Definition 2.2.3 We shall write

$$d(m) = C(m) \,/\, c(m).$$

Definition 2.2.4 For a given positive integer m, the greatest integer k, such that $u_{c(m)} \equiv u_o \pmod{m^k}$ will be denoted by $k(m)$.

Without proof we shall mention a number of theorems. The proofs can be found in Halton [34] and many others.

Theorem 2.2.1 For every positive integer n_1, there exists a positive integer n_2, such that $u_{n_2} \equiv u_o \pmod{n_1}$.

Theorem 2.2.2 $u_n \equiv u_o \pmod m$ if and only if $c(m) \mid n$.

Theorem 2.2.3 $d(m)$ is an integer.

Theorem 2.2.4 Suppose

$$m = \prod_{i=1}^{n} p_i^{\alpha_i},$$

then

$$c(m) = \{c(p_1^{\alpha_1}), \ldots\ldots, c(p_n^{\alpha_n})\}$$

and

$$C(m) = \{C(p_1^{\alpha_1}), \ldots\ldots, C(p_n^{\alpha_n})\}.$$

Theorem 2.2.5 If p is an odd prime, with $p \nmid D$,
then

$$c(p^n) = p^{n-k(p)}.c(p) \quad \text{for} \quad n > k(p)$$

and

$$c(p^n) = c(p) \quad \text{for} \quad n \le k(p).$$

Duparc [23] proved

Theorem 2.2.6 Let p be an odd prime

$$\text{if } \left(\frac{D}{p}\right) = -1, \text{ then } c(p) \mid p+1,\ C(p) \nmid p+1,\ C(p) \mid p^2-1;$$

if $\left(\frac{D}{p}\right) = +1$, then $c(p) \mid C(p) \mid p-1$;

if $\left(\frac{D}{p}\right) = 0$, then $c(p) = p$; $C(p)\ p(p-1)$.

C.G. Lekkerkerker [53] proved

Theorem 2.2.7 For each positive integer n, with a finite number of exceptions, a prime q exists with

$$u_n \equiv 0 \pmod{q}$$

and

$$u_m \not\equiv 0 \pmod{q} \quad \text{for} \quad m = 1(1)n-1$$

2.2.3 Composite numbers m belonging to the set $\Psi_1(2;a,b)$.

Theorem 2.2.8 An integer $m = \prod_{i=1}^{s} p_i^{\alpha_i}$ (where $p_1, \ldots\ldots, p_s$ are different primes) belongs to $\Psi_1(2;a,b)$ if and only if

$$u_{m_i} - \left(\frac{D}{m_i}\right) \equiv u_o \pmod{p_i^{\alpha_i}},$$

where

$m_i = \frac{m}{p_i}$ and $\left(\frac{D}{m_i}\right)$ is Jacobi symbol $i = 1(1)s$.

A proof was given by Duparc [24].

Theorem 2.2.9 If an integer $m = \prod_{i=1}^{s} p_i^{\alpha_i}$ (where $p_1, \ldots\ldots, p_s$ are different primes) belongs to $\Psi_1(2;a,b)$, then

$$0 < \alpha_i \leq k(p_i) \qquad i = 1(1)s.$$

Proof: From theorem 2.2.8 it follows that

$$u_{m_i} - \left(\frac{D}{m_i}\right) \equiv u_o \pmod{p_i^{\alpha_i}} \quad \text{where} \quad m_i = \frac{m}{p_i} \quad \text{for} \quad i = 1(1)s.$$

From theorem 2.2.2 it follows that

$$u_{m_i} - \left(\frac{D}{m_i}\right) \equiv u_o \pmod{p_i^{\alpha_i}}$$

if and only if

$$m_i - \left(\frac{D}{m_i}\right) \equiv 0 \pmod{c(p_i^{\alpha_i})}.$$

From theorem 2.2.5 it follows for $\alpha_i \geq k(p_i)$, that

$$c(p_i^{\alpha_i}) = p_i^{\alpha_i - k(p_i)} c(p_i).$$

Thus if $\alpha_i > k(p_i) \geq 1$ then $m_i - \left(\frac{D}{m_i}\right) \equiv 0 \pmod{p_i}$.

The last relation contradicts however $m_i \equiv 0 \pmod{p_i}$, which proves the theorem.

Theorem 2.2.10 If there exist an integer m, belonging to $\Psi_1(2;a,b)$ and divisible by p, then $\Psi_1(2;a,b)$ contains, with a finite number of exceptions, an infinite number of such integers.

Proof: Suppose

$$u_m - \left(\frac{D}{m}\right) \equiv u_o \pmod{m} \quad \text{and} \quad m = \prod_{i=1}^{n} p_i^{\alpha_i}.$$

It follows from theorem 2.2.8 that

$$u_{m_i} - \left(\frac{D}{m_i}\right) \equiv u_o \pmod{p_i^{\alpha_i}} \quad \text{where} \quad m_i = \frac{m}{p_i}.$$

By using theorem 2.2.7 we can find, with a finite number of exceptions, a prime p_{n+1} in such a manner that

$$c(p_{n+1}) = m - \left(\frac{D}{m}\right).$$

Because

$$p_{n+1} - \left(\frac{D}{p_{n+1}}\right) \equiv 0 \pmod{c(p_{n+1})},$$

One has

$$p_{n+1} - \left(\frac{D}{p_{n+1}}\right) \equiv 0 \pmod{m - \left(\frac{D}{m}\right)}.$$

Suppose

$$m_{n+1} = p_{n+1} \cdot m$$

From

$$m_i - \left(\frac{D}{m_i}\right) \equiv 0 \pmod{c(p_i^{\alpha_i})},$$

$$p_{n+1} - \left(\frac{D}{p_{n+1}}\right) \equiv 0 \pmod{c(p_i^{\alpha_i})}$$

and

$$m_i\, p_{n+1} - \left(\frac{D}{m_i\, p_{n+1}}\right) \equiv p_{n+1}\left(m_i - \left(\frac{D}{m_i}\right)\right) + \left(\frac{D}{m_i}\right)\left(p_{n+1} - \left(\frac{D}{p_{n+1}}\right)\right)$$

it follows that

$$u_{m_i\, p_{n+1}} - \left(\frac{D}{m_i\, p_{n+1}}\right) \equiv u_o \pmod{p_i^{\alpha_i}} \qquad i = 1(1)n.$$

It is obvious, that holds

$$u_m - \left(\frac{D}{m}\right) \equiv u_o \pmod{p_{n+1}}.$$

Thus

$$u_{m_{n+1}} - \left(\frac{D}{m_{n+1}}\right) \equiv u_o \pmod{m_{n+1}}$$

and

$$m_{n+1} \in \Psi_1(2;a,b).$$

Theorem 2.2.11 For an infinite number of primes p_1 a prime p_2 exists with $p_2 > p_1$ and $p_1 p_2 \in \Psi_1(2;a,b)$.

The proof is essentially equivalent to that theorem 2.2.10.

From theorem 2.2.10 and theorem 2.2.11 it follows

Theorem 2.2.12 For every integer $k \geq 2$ there are an infinite number of elements $m \in \Psi(2;a,b)$ for which $\tau(m) = k$.

From theorem 2.2.11 and theorem 2.2.12 it follows

Theorem 2.2.13 For every integer $k \geq 2$ and for an infinite number of primes p there exist an element $m \in \Psi_1(2;a,b)$ such that $m \equiv 0 \pmod{p}$ and $\tau(m) = k$.

From theorem 2.2.13 it follows

Theorem 2.2.14 For every integer N there are an infinite number of elements in $\Psi_1(2;a,b)$, for which holds that $\tau(m) > N$.

2.2.4 Composite number $m \in \Psi_2(2;a,b)$.

Theorem 2.2.15 An integer $m = \prod_{i=1}^{n} p_i^{\alpha_i}$ (where $p_1, \ldots, p_n$ are different primes) satisfies $u_m \equiv \left(\frac{D}{m}\right) \pmod m$ if and only if

$$u_{m_i} \equiv \left(\frac{D}{m_i}\right) \pmod{p_i^{\alpha_i}} \quad \text{where} \quad m_i = \frac{m}{p_i} \quad \text{and} \quad p_i \nmid D \qquad i = 1(1)n.$$

For a proof see [24].

2.2.5 Composite numbers $m \in \Psi_3(2;a,b)$.

Theorem 2.2.16 An integer $m = \prod_{i=1}^{n} p_i^{\alpha_i}$ (where $p_1, \ldots, p_n$ are different primes) satisfies $v_m \equiv v_1 \pmod m$ if and only if

$$v_{m_i} \equiv v_1 \pmod{p_i^{\alpha_i}} \quad \text{where} \quad m_i = \frac{m}{p_i} \qquad i = 1(1)n.$$

A proof may be found in [24].

Theorem 2.2.17 *There exists for an infinite number of primes p_1 a prime p_2 such that $p_1p_2 \in \Psi_3(2;a,b)$.*

For the proof we have to distinguish 16 cases, obtained by taking all possible alternatives, for each of the 4 relations:

$$\left(\frac{-b}{p_1}\right) = \pm 1, \left(\frac{D}{p_1}\right) = \pm 1, \left(\frac{-b}{p_2}\right) = \pm 1, \left(\frac{D}{p_2}\right) = \pm 1$$

We shall prove the theorem in 4 such cases, and remark that the proofs of the 12 other cases run about similarly.

1. Suppose $\left(\frac{-b}{p_1}\right) = 1$ and $\left(\frac{D}{p_1}\right) = 1$
   then
   $$v_{p_1} - v_1 = D.u_{\frac{1}{2}(p_1-1)}.u_{\frac{1}{2}(p_1+1)}.$$

   By using theorem 2.2.7 there exist with a finite number of exceptions a prime p_2 such that $c(p_2) = \frac{1}{2}(p_1-1)$.

thus

$$p_2 \mid u_{\frac{1}{2}(p_1-1)}$$

and

$$v_{p_1} \equiv v_1 \pmod{p_2}.$$

Now for the prime p_2 4 cases are possible, namely

1.1 $$\left(\frac{-b}{p_2}\right) = +1 \quad \text{and} \quad \left(\frac{D}{p_2}\right) = +1$$

Then one has

$$v_{p_2} - v_1 = D.u_{\frac{1}{2}(p_2-1)} \cdot u_{\frac{1}{2}(p_2+1)}$$

$$p_2 \mid u_{\frac{1}{2}(p_2-1)} \quad \text{thus} \quad c(p_2) \mid \tfrac{1}{2}(p_2-1)$$

and

$$c(p_1) \mid p_1-1 = c(p_2) \mid \tfrac{1}{2}(p_2-1)$$

Hence

$$v_{p_2} \equiv v_1 \pmod{p_1}$$

and

$$p_1 p_2 \in \Psi_3(2;a,b).$$

1.2 $$\left(\frac{-b}{p_2}\right) = +1 \quad \text{and} \quad \left(\frac{D}{p_2}\right) = -1$$

then one has

$$v_{p_2} - v_1 = D.u_{\frac{1}{2}(p_2-1)} \cdot u_{\frac{1}{2}(p_2+1)}$$

$$p_2 \mid u_{\frac{1}{2}(p_2+1)} \quad \text{thus} \quad c(p_2) \mid \tfrac{1}{2}(p_2+1)$$

and

$$c(p_1) \mid p_1-1 = c(p_2) \mid \tfrac{1}{2}(p_2+1)$$

hence

$$v_{p_2} \equiv v_1 \pmod{p_1}$$

and

$$p_1 p_2 \in \Psi_3(2;a,b)$$

1.3 Suppose $\left(\frac{-b}{p_2}\right) = -1$ and $\left(\frac{D}{p_2}\right) = +1$,

then

$$v_{p_2} - v_1 = v_{\frac{1}{2}(p_2+1)} \cdot v_{\frac{1}{2}(p_2-1)} \cdot$$

$$p_2 | v_{\frac{1}{2}(p_2-1)}$$

$$c(p_1) | p_1-1 = c(p_2) | \tfrac{1}{2}(p_2-1)$$

hence

$$v_{p_2} \equiv v_1 \pmod{p_1}$$

and

$$p_1 p_2 \in \Psi_3(2;a,b)$$

1.4 Suppose $\left(\frac{-b}{p_2}\right) = -1$ and $\left(\frac{D}{p_2}\right) = -1$

then

$$v_{p_2} - v_1 = v_{\frac{1}{2}(p_2+1)} \cdot v_{\frac{1}{2}(p_2-1)},$$

$$p_2 | v_{\frac{1}{2}(p_2+1)}$$

and

$$c(p_1) | p_1-1 = c(p_2) | \tfrac{1}{2}(p_2+1),$$

hence

$$v_{p_2} \equiv v_1 \pmod{p_1}$$

and

$$p_1 p_2 \in \Psi_3(2;a,b)$$

2.2.6 Composite numbers $m \in \bigcap_{i=1}^{3} \Psi_i(2;a,b)$.

Theorem 2.2.18 For every positive integer m the relations

$$u_m - \left(\frac{D}{m}\right) \equiv 0 \pmod{m}, \quad u_m - \left(\frac{D}{m}\right) \equiv 0 \pmod{m} \quad \text{and} \quad v_m \equiv v_1 \pmod{m}$$

are lineair dependent (mod m).

Proof: One has

$$A.u_m - \left(\frac{D}{m}\right) + B\left(u_m - \left(\frac{D}{m}\right)\right) + C(v_m - v_1) \equiv 0 \pmod{m}$$

in which

$$A = \alpha^{\left(\frac{D}{m}\right)}\left(\beta - \alpha + \left(\frac{D}{m}\right)(\alpha+\beta)\right) \neq 0, \text{ since } b = f(0) \neq 0$$

$$B = -\left(\frac{D}{m}\right)(\alpha+\beta) \neq 0, \text{ since } a \neq 0$$

$$C = 1$$

and

Bibliotheek TU Delft
Afdeling Leverantie
Prometheusplein 1
2600 MG Delft
Verlenging: 015-2784510
Informatie: 015-2785678

* L O O P B O N V O O R B O E K A A N V R A G E N *

Aangevraagd op: 23 November 1998 Tijd: 1634

Uiterlijk terugbezorgen op (stempel datum):

Documentgegevens (auteur/titel)
Lieuwens, E..: FERMAT PSEUDO PRIMES. Z. plaats z. uitg.
9999. 61 blz..

Plaatsnummer(s)		Exemplaarnummer(s)
- 19475324	CBmg (cB)	647328

Opmerkingen:

Uw aanvraag wordt niet gehonoreerd ivm.

O Afwezig O Alleen ter inzage O U heeft te veel boeken
O Openstaande boete O Overig nl.

Note:

Gebruikers-ID: 69434 Categorie: 02

Demiryurek, R.
Gordonstraat 52 a
3117 MT Schiedam

Bezorglokatie: CBmg (cB)

α and β are the roots of the characteristic polynomial.

Consequently if m is an element of two of the three sets $\Psi_i(2;a,b)$ (i = 1, 2 and 3), then m is also an element of the third set.

Theorem 2.2.19 $\quad m \in \bigcap_{i=1}^{3} \Psi_i(2;a,b)$

if and only if either

$$\left(\frac{D}{m}\right) = 1 \ , \ \beta^m \equiv \beta \pmod m \quad \text{and} \quad \alpha^m \equiv \alpha \pmod m$$

or

$$\left(\frac{D}{m}\right) = -1 \ , \ \beta^m \equiv \alpha \pmod m \quad \text{and} \quad \alpha^m \equiv \beta \pmod m.$$

The proof is elementary.

Corollary.

In the special case of $a = 5$, $b = -6$, one has $D = 1$, hence $\left(\frac{D}{m}\right) = 1$.

If $\quad m \in \bigcap_{i=1}^{3} \Psi_i(2;5,-6),$

then also

$$m \in \Psi(1;2) \cap \Psi(1;3)$$

so that

$$\bigcap_{i=1}^{3} \Psi_i(2;5,-6) \supset \Psi(1;2) \cap \Psi(1;3).$$

In general if $a \neq b$

$$\bigcap_{i=1}^{3} \Psi_i(2;a+b,-ab) \supset \Psi(1;a) \cap \Psi(1;b).$$

2.3 Fermat second order pseudo-primes with reference to both (a,b) and (c,d).

Consider the second order recurring sequences defined by:

$$u_o = 0 \ , \ u_1 = 1 \ , \ u_{n+2} = au_{n+1} + bu_n \qquad (n = 0, 1, \ldots)$$

and

$$u^*_o = 0 \ , \ u^*_1 = 1 \ , \ u^*_{n+2} = cu^*_{n+1} + du^*_n \qquad (n = 0, 1, \ldots)$$

where $(a,b) \neq (c,d)$.

The associated recurring sequences are respectively

$$v_o = 2 \ , \ v_1 = a \ , \ v_{n+2} = av_{n+1} + bv_n \qquad (n = 0, 1, \ldots)$$

and

$$v^*_o = 2 \ , \ v^*_1 = c \ , \ v^*_{n+2} = cv^*_{n+1} + dv^*_n \qquad (n = 0, 1, \ldots).$$

Composite numbers m, which are elements of

$$\Psi(2;a,b) \cap \Psi(2;c,d)$$

are called Fermat second order pseudo-primes with reference to both (a,b) and (c,d).
Van Zijl[106] studied a special case, namely the composite numbers

$$m \in \Psi_3(2;1,1) \cap \Psi_3(2;+3,-2).$$

Remark. One has

$$\Psi_3(2;+3,-2) = \Psi(1;2)$$

and generally

$$\Psi_3(2;+a+1,-a) = \Psi(1;a).$$

By theorem 2.2.17 there exist an infinite number of elements $\in \Psi_3(2;1,1)$ and also an infinite number of elements $\in \Psi_3(2;3,-2)$. We don't know whether there exists an infinite number of elements $\in \Psi_3(2;1,1) \cap \Psi_3(2;3,-2)$.
Van Zijl [106] published a table of Van der Poel numbers m such that $10^7 < m < 10^8$

2.4 Fermat second order pseudo primes.

2.4.1 Introduction.

We call a composite number m a Fermat second order pseudo prime if for all recurring sequences (2) with (m,b) = 1 one of the following properties holds:

1. $u_m - \left(\frac{D}{m}\right) \equiv 0 \pmod{m}$

2. $u_m \equiv \left(\frac{D}{m}\right) \pmod{m}$

3. $v_m \equiv v_1 \pmod{m}$.

The set of all Fermat second order pseudo primes is called $\Psi(2)$.

2.4.2 General properties.

Theorem 2.4.1 There do not exist composite numbers $m \in \Psi(2)$ for which the relation $u_m - \left(\frac{D}{m}\right) \equiv 0 \pmod{m}$ hold.

Theorem 2.4.2 There do not exist composite numbers $m \in \Psi(2)$ for which the relation $u_m \equiv \left(\frac{D}{m}\right) \pmod{m}$ hold.
The proofs were given by Duparc [24].

2.4.3 The existence of Fermat second order pseudo primes.

Whether the set $\Psi(2)$, consisting of all composite m with $v_m \equiv v_1 \pmod m$ for all sequences with $(m,b) = 1$ is empty or not, is not known.
The following theorems might help to solve this problem.

Theorem 2.4.3 A composite number $m \in \Psi(2)$ belongs to $\Psi(2)$, if and only if for every prime divisor p_i of m (with $M = p_i m_i$) either both

$$\frac{m_i-1}{p_i-1} \quad \text{and} \quad \frac{m_i+1}{p_i+1} \quad \text{are odd integers or both}$$

or both

$$\frac{m_i-1}{p_i-1} \quad \text{and} \quad \frac{m_i-1}{p_i+1} \quad \text{are even integers.}$$

Proofs may be found in [24].

Remarks.

1. $\frac{m_i-1}{p_i-1}$ and $\frac{m_i+1}{p_i+1}$ are both odd if and only if $\frac{m-1}{p_i-1}$ and $\frac{m-1}{p_i+1}$ are both even.

2. $\frac{m_i-1}{p_i-1}$ and $\frac{m_i-1}{p_i+1}$ are both even if and only if $\frac{m-1}{p_i-1}$ and $\frac{m+1}{p_i+1}$ are both odd.

3. $\tau(m) \geq 4$.

4. From theorem 2.4.3 it follows that m has to satisfy $p_i-1 \mid m_i-1$ for all $p_i \mid m$ hence $m \in \Psi(1)$, i.e. $\Psi_3(2) \subset \Psi(1)$.

Theorem 2.4.4 Suppose $m = \prod_{i=1} p_i \quad (n \geq 3) \in \Psi(1)$, in which

$$p_i = 2a_i g+1.$$

We call $q_i = (\frac{m}{p_i} - 1) / (p_i - 1)$ for $i = 1(1)n$.

Suppose n is even.
If all the numbers a_i are odd, then for $i = 1(1)n$ the integer q_i is odd.
If an even number ($<n$) a_i are even, no such conclusion about q_i is possible.
Suppose n is odd.
If all the numbers a_i are odd, then the integer q_i for $i = 1(1)n$ is even.
If an odd number ($<n$) a_i are even, no such conclusion about q_i is possible.

The proof is elementary.

Theorem 2.4.5 If $m = \prod_{i=1}^{n} p_i$ $(n \geq 4) \in \Psi(2)$ and

$$\frac{m-1}{p_i-1} \text{ and } \frac{m+1}{p_i+1} \text{ are odd then:}$$

either

$$p_i = 2^s(2n_i+1)+1 \qquad s \geq 2 \qquad i = 1(1)n,$$

or

$$p_i = 2^s(2n_i+1)-1 \qquad s \geq 2 \qquad i = 1(1)n.$$

In both cases one has

$$(p_i, p_j-1) = 1 \ , \ (p_i+1, p_j-1) = 2 \text{ and } (p_i, p_j+1) = 1.$$

Proof: Suppose $p_i = 2^s(2n_i+1)+1$, $m \in \Psi(2)$ and

$$\frac{m}{p_i} - 1 \equiv 0 \pmod{p_i^2-1}$$

Suppose $\frac{m}{p_i} - 1 = (p_i^2-1)v_i$

then

$$m-1 = (p_i-1)(p_i(p_i+1)v_i+1)$$

and

$$m+1 = (p_i+1)(p_i(p_i-1)v_i+1).$$

For $p_j \neq p_i$ both expressions

$$\frac{m-1}{p_j-1} = \frac{(p_i-1)(p_i(p_i+1)v_i+1)}{p_j-1}$$

and

$$\frac{m+1}{p_j+1} = \frac{(p_i+1)(p_i(p_i-1)v_i+1)}{p_j+1}$$

are odd. Hence p_i-1 and p_j-1 resp. p_i+1 and p_j+1 contain the same number s of factors 2, i.e.

$$p_i \equiv p_j \pmod{2^s}.$$

Moreover one easily verifies that both above expressions learn

$$(p_i, p_j-1) = 1, (p_i+1, p_j-1) = 2 \text{ and } (p_i, p_j+1) = 1.$$

In the case that $p_i = 2^s(2n_i+1)-1$ the proof runs similarly.

It is unknown whether there exists numbers $m \in \Psi_3(2)$.

3 Fermat higher order pseudo primes.

3.1 Fermat higher order pseudo primes with reference to $(a_o, \ldots, a_{k-1})$.

3.1.1 Introduction.

Consider the recurring sequence of order $k \geq 3$, defined by

$$u_h = 0,\ h = 0(1)k-2\ ;\ u_{k-1} = 1\ ;\ u_{n+k} = \sum_{i=0}^{k-1} a_i\, u_{n+i} \qquad (n = 0, 1, \ldots)$$

$$D = a_o^k \cdot \prod_{i \neq j} (\alpha_i - \alpha_j)^2$$

is called the discriminant of the characteristic polynomial

$$f(x) = x^k - \sum_{i=0}^{k-1} a_i x^{k-i-1}$$

and α_i, α_j are the roots of $f(x)$.

The associated recurring sequence is defined by:

$$v_i = \sum_{j=1}^{k} \alpha_j^i \qquad i = 0(1)k-1\ ;\ v_{n+k} = \sum_{i=0}^{k-1} a_i v_{n+i} \qquad (n = 0, 1, \ldots).$$

Theorem 3.1.1 For every prime p, this sequence satisfies the property $v_p \equiv v_1 \pmod p$.

Proof. By a theorem of Fermat it is known that

$$a_o^p \equiv a_o \pmod p$$

which is equivalent with

$$\left(\sum_{j=1}^{k} \alpha_j\right)^p \equiv \sum_{j=1}^{k} \alpha_j \pmod p.$$

$\sum_{j=1}^{k} \alpha_j^p$ is a symmetrical polynomial, so that

$$\left(\sum_{j=1}^{k} \alpha_j\right)^p \equiv \sum_{j=1}^{k} \alpha_j^p \pmod p$$

thus

$$\sum_{j=1}^{k} \alpha_j^p \equiv \sum_{j=1}^{k} \alpha_j \pmod p$$

and

$$v_p \equiv v_1 \pmod p.$$

Composite numbers m, which satisfy this property, will be called Fermat k th order pseudo primes with reference to $(a_o, \ldots, a_{k-1})$. The set of these numbers m will be denoted by $\Psi(k; a_o, \ldots, a_{k-1})$.

3.1.2 General properties.

By an observation of G.J. Hameetman, we can prove

Theorem 3.1.2 An integer $m = \prod_{i=1}^{s} p_i$ (where $p_1, \ldots, p_s$ are different primes) belongs to $\Psi(k;a_0, \ldots, a_{k-1})$ if and only if

$$v_{m_i} \equiv v_1 \pmod{p_i}$$

where

$$m_i = \frac{m}{p_i} \qquad i = 1(1)s.$$

Proof. Suppose

$$v_m \equiv v_1 \pmod{m},$$

thus also

$$v_m \equiv v_1 \pmod{p_i},$$

which is equivalent with

$$\sum_{j=1}^{k} \alpha_j^m \equiv \sum_{j=1}^{k} \alpha_j \pmod{p_i}.$$

$\sum_{j=1}^{k} \alpha_j^{m_i} = v_{m_i}$ is an integer, thus by a theorem of Fermat one has

$$\sum_{j=1}^{k} \alpha_j^{m_i p_i} \equiv \sum_{j=1}^{k} \alpha_j^{m_i} \pmod{p_i},$$

so that

$$\sum_{j=1}^{k} \alpha_j^{m_i} \equiv \sum_{j=1}^{k} \alpha_j \pmod{p_i}.$$

That the property is also sufficient, is still more simple.

We now give an example.

We take the sequence

$$w_0 = w_1 = 0,\ w_2 = 1,\ w_{n+3} = w_{n+1} + w_n \qquad (n = 0, 1, \ldots).$$

The characteristic polynomial

$$f(x) = x^3 - x - 1$$

has the discriminant $D = 23$.

The associated recurring sequence is

$$v_0 = 3,\ v_1 = 0,\ v_2 = 2,\ v_{n+3} = v_{n+1} + v_n \qquad (n = 0, 1, \ldots).$$

There do not exist an element $\in \Psi(3;0,1,1)$ which is < 31000, this is very remarkable, because we found the following elements in the sets:

$\Psi(3;\ 1,\ 1,\ 4)$: 25
$\Psi(3;\ 1,\ 1,\ 5)$: 9, 27
$\Psi(3;\ 1,\ 1,\ 6)$: 35, 49
$\Psi(3;\ 1,\ 0,\ 1)$: 4, 14, 18, 22, 46, 58, 74
$\Psi(3;\ 1,\ 0,\ 2)$: 4, 6, 8, 10, 14, 16, 22, 26, 32, 34, 38, 46, 50, 58
$\Psi(3;\ 1,\ 0,\ 3)$: 4, 9, 14, 18, 22, 30, 36, 45, 46, 50
$\Psi(3;\ 1,-\ 1,\ 3)$: 25
$\Psi(3;\ 1,-\ 1,-\ 1)$: 25, 30, 95
$\Psi(3;\ 2,-\ 1,-\ 1)$: 4, 8, 22, 46, 50, 58, 74
$\Psi(3;\ 1,-\ 5,-\ 5)$: 10, 25
$\Psi(3;\ 1,-\ 6,\ 5)$: 4, 25
$\Psi(3;\ 1,\ 10,-11)$: 4
$\Psi(3;\ 0,\ 1,\ 2)$: 42
$\Psi(3;\ 0,\ 1,\ 3)$: 9, 27
$\Psi(3;\ 0,\ 2,-\ 2)$: 4, 8, 16, 24, 32, 48
$\Psi(3;\ 0,-\ 1,\ 1)$: 121

BIBLIOGRAPHY

1. Bachmann, P. Ueber Fermats kleinen Satz, Archiv. Math. Phys. 21 (1913),pp. 185-187.

2. Banachiewicz, T. Comptes rendus de la Soc. des Sc. et de Lettres de Varsovie Classe III 2(1909), pp. 9.

3. Bang, A.S. Tidsskrift for Mat. s.5, v.4 (1886), pp. 70-80, 130-137.

4. Beeger, N.G.W.H. The converse of Fermat's theorem, Nieuw Archief 15 (1928), pp. 330-333.

5. On composite numbers n for which $a^{n-1} \equiv 1 \pmod{n}$ for every a prime to n, Scripta Mathematica Vol. 16 (1950), pp. 133-135.

6. On even numbers m dividing $2^m - 2$, Amer. Math. Monthly 58 (1951), pp. 553-555.

7. Birkhoff, C.D., Vandiver, H.S. On the integral divisors of $a^n - b^n$, Annals of Mathematics (2) 5 (1904), pp. 173-180.

8. Bouniakowsky, V. Mém. Ac. Sc. St. Petersbourg (Math.), 6, 2 (1841) pp. 447.

9. Capelli, A. Sulla irriducibilita della funzione $x^n - A$ in campo qualunque di razionalita, Math. Annalen, 54 (1901), pp. 602-603.

10. Carmichael, R.D. Note on a new number theory function, Bull. Amer. Math. Soc. 16 (1909-10), pp. 232-238.

11. Amer. Math. Monthly 16 (1910), pp. 232-238.

12. On composite numbers P, which satisfy the Fermat congruence $a^{p-1} \equiv 1 \pmod{P}$, Am. Math. Monthly 19 (1912), pp. 22-27.

13. On the numerical factors of the arithmetic form $\alpha^n \pm \beta^n$, Ann. Math. 15 (1913-1914), pp. 30-70.

14. Chapron, R. Sur une proposition erronée de Korselt relative aux nombres composés m qui divisent $a^m - a$, Bull. Sci. Math. 80 (1956), pp. 81-83.

15. Chernick, J. On Fermat's simple theorem. Bull. Am. Math. Soc. 45 (1939), pp. 269-274.

16. Chowla, S. There exist an infinity of 3-combinations of primes in A.P., Proc. Lahore Philos. Soc. 6 (2) (1944), pp. 15-16.

17. Cipolla, M. Sui numeri composti P, che verificano la Congruenza di Fermat $a^{p-1} \equiv 1 \pmod{P}$, Annali di Matematica 9 (1904), pp. 139-160.

18. Corput, J.C. v.d. Wiskundige Opgaven v.11 (1912-14), pp. 483-488.

19. Crocker, R. A theorem on pseudo primes, Amer. Math. Monthly 69 (1962), pp. 540.

20. Dickson, L.E. History of the theory of numbers.

-/2

21. Dickson, L.E. — A new extension of Dirichlets theorem on prime numbers, Messenger of Mathematics 33 (1904), pp. 155-161.

22. Duparc, H.J.A. — On Carmichael numbers, Simon Stevin (1951-52), pp. 21-24.

23. — Divisibility properties of recurring sequences, Doctor thesis.

24. — On almost primes of the second order, Report Z.W. 1955-013, Math. Center Amsterdam 1-13.

25. — Generalisations of the Poulet and Carmichael numbers (Dutch), Math. Center, Report Z.W. 1956-005.

26. — A remark to report Z.W. 1955-013, Math. Center Amsterdam report Z.W. 1956-008.

27. Franel, J. — L'intermédiaire des math. 6 (1899), pp. 142.

28. Erdös, P. — On the converse of Fermat's theorem. Amer. Math. Monthly 56 (1949), pp. 623-624.

29. — Problem 4319, Amer. Math. Monthly 57 (1950), pp. 346.

30. — On almost primes, Amer. Math. Monthly 57 (1950), pp. 404-407.

31. — On pseudo primes and Carmichael numbers, Publicationes Mathematicae Tomus 4, Debrechen (1955-1956) (Hungaria), pp. 201.

32. Grassini, E. — I numeri composti m che verificano la congruenza di Fermat $a^{m-1} \equiv 1 \pmod{m}$. Periodico di Matematiche, vol.43 (1965).

33. Gauss, C.F. — Theoria residuorum biguadraticorum, Commentatio prima, Werke, Band II, Göttingen 1863, pp. 65-92.

34. Halton, J.H. — On the divisibility of Fibonacci numbers, Fib. Quaterly 3 (1966), pp. 217.

35. Hardy, G.H. Wright, E.M. — An Introduction to the theory of numbers, Oxford (1965), pp. 71-73, 81.

36. Hayashi, T. — Jour. of the Ph. School in Tokio 9 (1900), pp. 143, Reprint in Abhand. Geschichte Math. Wiss. 28 (1910), pp. 25.

37. Hausner, M, Sachs, D. — On the congruence $2^p \equiv 2 \pmod{p^2}$, Amer. Math. Monthly 70 (1963), pp. 996.

38. Inkeri, K. Hyyrö, S. — On the congruence $3^{p-1} \equiv 1 \pmod{p^2}$ and the Diophantine Equation $x^2 - 1 = y^p$, Ann. Univ. Turkuensis Sci. An. 50 (1961).

39. Jakobezyk, F. — Les applications de la fonction $\lambda g(n)$ à l'etude des fractions péridiques et de la congruence chinoise $2^n - 2 \equiv 0 \pmod{n}$, Ann. Univ. Mariae Curie - Sklodowska, Lublin, Polonia, vol.5 (1951), pp. 97-138.

-/3

40. Jeans, J.H. — The converse of Fermat's theorem, Messenger of Mathematics 27 (1897-1898), pp. 174.

41. Klee, V.L. — A note on Fermat's congruence, Amer. Math. Monthly 56 (1949).

42. Knödel, W. — Eine obere Schranke für die Anzahl der Carmichaelschen Zahlen kleiner als x, Arch. Math. Vol.4 (1953), pp. 282-284.

43. — Carmichaelsche Zahlen, Math. Nachr. 9 (1953), pp. 343-350.

44. Kraitchik, — Recherches sur la théorie des nombres, v.1, Paris (1924), pp. 131-191.

45. Lehmer, D.H. — Amer. Math. Sc. Bulletin, v.34 (1928), pp. 54-56.

46. — Annals of Math. s.2, v.31 (1930), pp. 419-448.

47. — On Euler's totient function, Bulletin Amer. Math. Soc. 38 (1932), pp. 745.

48. — On the converse of Fermat's theorem, Amer. Math. Monthly 43 (1936),pp. 347-354.

49. — On the Factors of $2^n \pm 1$, Amer. Math. Sc. Bulletin v.33 (1947), pp. 164-167.

50. — Amer. Math. Sc. Bulletin, v.33 (1947), pp. 327-340.

51. — On the converse of Fermat's theorem II, Amer. Math. Monthly 56 (1949), pp. 300-309.

52. Lekkerkerker, C.G. — Prime factors of the elements of certain sequences of integers, Math. Center Z.W. report 1953-003.

53. Lieuwens, E. — Pseudo prime numbers (Dutch).Master thesis Delft(1968).

54. Matulewicz, K. — Sur la solution d'une congruence en nombres composés, Coll. Math. 2 (1951), pp. 261-263.

55. Obláth, R. — Ueber die Zahl $x^2 - 1$, Mathematica B, Zutphen 8, (1940), pp. 161-172.

56. Ore, O. — Number theory and its history, New York (1948) 1st ed., pp. 331-339.

57. Peano, G. — Formulaire de Mathematiques 3, Torino (1901), pp. 96.

58. Poulet, P. — Table des nombres composés vérifant le théorème de Fermat pour le module 2 jusqu'à 100 000 000, Deuxième Congrès Int. d., Récréation Math. Comptes Rendus, Brussel (1937), pp. 42-52.

59. Reutter, O. — Ueber pseudo prim Zahlen, Elem. der Math. (Basel), b.20 (1965), pp. 7.

60. Riesel, H. — Note on the congruence $a^{p-1} \equiv$ (mod p^2), Math. Comp. v.18 (1964), pp.149.

61. Rotkiewicz, A. Sur les nombres composés n qui divisent $a^{n-1}-b^{n-1}$, Rendiconti Circolo Mat. (2), 8 (1959), pp. 115-116.

62. Sur les nombres pairs n pour lesquels les nombres $a^n b-ab^n$ respectivement $a^{n-1}-b^{n-1}$, sont divisibles par n, Rend. del Circ. Mat. (Palermo), s.2,tomo 8, (1959), pp. 341.

63. Sur les nombres pairs n qui divisent $(a+2)^{n-1}-a^{n-1}$, Rendiconti Circolo Mat. Palermo (2), 9 (1960), pp. 78-80.

64. On the properties of the expression a^n-b^n, Prace Mat. 6 (1961), pp. 1-20 (Polish).

65. Demonstration arithmétique de l'existence d'une infinité de nombres premiers de la forme nk+1, Enseignement Mathématique, 7 (1962), pp. 277-280.

66. Sur les nombres premiers p en q telsque $pq/2^{pq}-2$, Rendiconti del Cirolo Matematico di Palermo 9 of 11 (1962), pp. 280-282.

67. Sur les nombres pseudo premiers de la forme ax+b, Comptes Rendus Acad. Sciences, Paris, 257 (1963), pp. 2601-2604.

68. Sur les nombres pseudopremiers relativement à un nombres naturel a contenus dans les progressions arithmetiques, Bull. Soc. Roy. Sci., Liège 32 (1963), pp. 456-458.

69. Sur les diviseurs composés des nombres a^n-b^n, Bull. Soc. Roy. Sci., Liège 32 No 3-4 (1963), pp. 191-195.

70. Sur les nombres composés telsque $n|2^n-2$ et $n|3^n-3$, Bulletin de la Société des mathématiciens et physiciens de la R.S. de Serbie XV, Beograd (1963), pp. 7-11.

71. Sur les progression arithmétiques et géométriques formées de trois nombres pseudopremiers distincts, Acta Arithmetica 10 (1964), pp. 325-328.

72. Sur les formules donnant des nombres pseudopremiers, Colloquium Mathematicum 12 (1964), FASC1.

73. Sur les nombres pseudopremiers triangulaires, El. der Math. (Basel) (1964), no 19.

74. Sur les polynômes en x qui pour une infinité de nombres naturels x donnent des nombres pseudopremiers, Atti. Accad. Naz. Lencei - Rend. Sc. fis. mat. et nat. - 36 (1964), pp. 136-140.

75. Sur les nombres pseudopremiers pentagonaux, Bull. Soc. Roy. Sci., Liège 33 (1964), pp. 261-263.

76. Quelques conséquences de l'existence infinite des nombres pseudopremiers de la forme ax+b, Publ. Inst. Math. (Beograd) 4 (1964), pp. 139-140.

77. Sur les nombres n et k telsque les nombres n et nk sont à la fois pseudopremiers. Atti. Accad. Naz. Lencei. Rend. Cl. Sci. Fis. Mat. Nat. 36 (1964), pp. 816-818.

78. Sur les progressions geométrique formées de k nombre pseudopremiers distincts, Rend. Circ. Mat. Palermo 13 (1964), pp. 369-372.

79. Rotkiewicz,A., Schinzel, A. Sur les nombres pseudopremiers de la forme $ax^2+bxy+cy^2$, C.R. Acad. Sci. Paris 258 (1964), pp. 3617-3620.

80. Rotkiewicz,A. Sur les nombres pseudopremiers n telsque $n/2^{\frac{n-1}{k}} - 1$, Acta Arithmatica 3 (1964).

81. Sur les nombres pseudopremiers de la forme $M_p M_q$. Elemente der Mathematik 20 (1965).

82. Sur les nombres pseudopremiers carrés Elem. Math. 20 (1965), pp. 39-40.

83. Les intervalles contenants les nombres pseudopremiers Rend. Circ. Mat. Palermo 14 (1965), p. 278-280.

84. Sur les polynômes en x du premier degré qui pour une infinité de valeurs de x donnent des nombres pseudo premiers, Matematyka Bechnk 2 (17) (1965), p. 157-161.

85. Sur les nombres pseudopremiers de la forme nk+1, Elem. der Mat. 2 (1966), pp. 32.

86. Rotkiewicz, A., Makowski, A. On pseudoprime numbers of the form $M_p.M_t$, Elem. der Mat. 21 (1966), pp. 133.

87. Rotkiewicz, A. On the prime factors of the number $2^{p-1} - 1$, Glasgow, Math. Journal 9 (1968), pp. 83.

88. Schinzel, A. Sur les nombres composés n qui divisent a^n-a, Rend. Circ. Mat. Palermo 7 (1958), pp. 37-41.

89. Schinzel, A., Sierpinski, W. Sur certaines hypothèses concernant les nombres premiers, Acta Arithmatica, 4 (1958), pp. 185-208.

90. Schinzel, A. On primitive prime factors of $a^n - b^n$, Proc. Cambridge Philos. Soc. (4) 58 (1962), pp. 555-562.

91. Schuh, F. Do there exist numbers n for which $\phi(n)|n-1$? (Dutch) Mathematica B12 (1944), pp. 102.

92. Sierpinski, W. Remarque sur une hypothèse des chinois concernant les nombres $(2^n - 2)/n$, Coll. Math. I (1947), 9.

93. Elementary theory of numbers, pp. 214-219.

94. Sispánov, S. Sobre los numeros pseudo-primos, Boletin Mat 14 (1941), pp. 99-106.

95. Steuerwald, R. Ueber die Kongruenz $2^{n-1} \equiv 1 \pmod n$, sitz. ber. math. nat. Bayer. Akad.Wiss. München (1947),pp.177.

96. Steuerwald, R. Ueber die Kongruenz $a^{n-1} \equiv 1 \pmod{n}$, sitz. ber. math. nat. Bayer. Akad. Wiss. München (1948), pp. 69-70.

97. Sylvester, J.J. Inst. de France, Acad. de Sci., comptes rendus v.90, 1880,pp. 287, 345, 526, 855, 1205.

98. Szymiczek, K. On prime numbers p, q and r such that pq, pr and qr are pseudo primes, Colloquium Mathematicum, v. XIII, 1965, FASC2.

99. A few theorems on pseudo primes, Zeszyty Naukowe Wyzszej Szkoly, Pedagogicznej w Katowicach 5 (1965).

100. Note on Fermat numbers, Elem. Mat. 21 (1966), pp. 59.

101. On pseudo primes which are products of distinct primes, Amer. Math. Monthly 74 (1967), pp. 35-37.

102. Tarry, G. Intermédiaire des Math. (1898), pp. 266; (1899), pp. 142,143.

103. Vahlen, K.H. Ueber reductible Binome, Acta Mathematica 19 (1895), pp. 195-198.

104. Weber, H. Beweis des Satzes, dass jede eigentliche primitieve quadratische Form unendlich viele Primzahlen darzustellen fähig ist, Mathematische Annalen 20 (1882), pp. 103-129.

105. Zsigmondy, K. Zur Theorie der Potenzreste, Monatshefte Math. Phys. 3 (1892), pp. 265-284.

106. Zijl, R.F. v. The numbers of Van der Poel (Dutch). Master thesis Delft(1968).

Samenvatting.

P. de Fermat bewees in 1640, dat voor ieder priemgetal p, geldt dat $a^p \equiv a \pmod{p}$. Omgekeerd als geldt dat $a^m \equiv a \pmod{m}$ dan behoeft m geen priemgetal te zijn.
Gedurende de laatste jaren is een groot aantal artikelen verschenen over oneven samengestelde getallen, die voldoen aan $2^m \equiv 2 \pmod{m}$.
Hoofdstuk 1.1 geeft een historisch overzicht van deze artikelen en verder enkele nieuwe stellingen. De meeste stellingen van dit hoofdstuk 1.1 worden gegeneraliseerd in het volgende hoofdstuk 1.2. Daarin worden samengestelde getallen m beschouwd, waarvoor geldt dat $a^m \equiv a \pmod{m}$ voor een gegeven getal a.
Hierna wordt een meer gecompliceerd probleem bestudeerd, handelend over samengestelde getallen m, die voldoen aan $a^m \equiv a \pmod{m}$ voor alle gehele getallen a.
Het is opmerkelijk, dat hierbij het oude probleem van de volmaakte getallen een rol blijkt te spelen.

Een aanverwant, doch gespecialiseerd probleem namelijk $\phi(n) \mid n-1$ wordt bestudeerd in hoofdstuk 1.4.7.

Het eerstgenoemde probleem, namelijk het vinden van samengestelde getallen m, die voldoen aan $2^m \equiv 2 \pmod{m}$ kan op een andere wijze geformuleerd worden:
Bepaal samengestelde getallen m, welke voldoen aan $u_m \equiv u_1 \pmod{m}$, waarin de rij u_m gedefinieerd is door $u_o = 1$, $u_n = 2u_{n-1}$ $(n = 1, 2, \ldots)$.
Dit kan leiden tot een andere generalisatie: Er bestaan stellingen, die informatie geven welke elementen van een tweede orde recurrente rij $u_o=0$, $u_1 = 1$, $u_{n+2} = au_{n+1} + bu_n$ deelbaar zijn door een gegeven priemgetal p.
In dit proefschrift wordt nu bestudeerd of er samengestelde getallen zijn, die voldoen aan relaties, die gelijkwaardig zijn aan de relaties, die bij dergelijke rijen voor priemgetallen gelden.

Uit historisch oogpunt worden in hoofdstuk 2.1 de rij van Fibonacci en zijn geassocieerde bestudeerd. Een en ander wordt vervolgens gegeneraliseerd voor een willekeurige recurrente rij van de tweede orde. In hoofdstuk 2.4 wordt wederom de vraag gesteld of er samengestelde getallen bestaan, welke voldoen aan een voor priemgetallen geldige relatie voor iedere recurrente rij van de tweede orde.

Tot dusverre schijnen zulke getallen nog niet gevonden te zijn.
Het is echter wel mogelijk om eisen op te stellen, waaraan de delers van deze getallen moeten voldoen.
Er bestaan voorts eigenschappen van tweede orde recurrente rijen, die ook gelden voor recurrente rijen van hoger orde.
Het is niet bekend of er bij iedere recurrente rij van hogere orde een samengesteld getal bestaat, welke voldoet aan de priemrelatie voor deze rij.

Biography

Erik Lieuwens:
Born in Rotterdam at 22 August 1940.
In 1962 he finished the Higher Technical College, department shipbuilding engineering.
During 1962-1965 he was involved at the Ministry of Defence in Submarine design and Construction.
He entered the University of Technology of Delft in 1965 and graduated in mathematics in 1968.
He was appointed as a guest member of staff in the department of mathematics of the University of Technology of Delft in 1969.

STELLINGEN

Stelling 1

Indien er een samengesteld getal m bestaat, zodanig dat $\sigma(^{m}) = 2m + 1$, dan is m ontbindbaar in ten minste 7 verschillende priemfactoren.
Zie voordracht van E. Lieuwens op het 6e Nederlandse Mathematische Congres (1970).

Stelling 2

Beschouw bij een gegeven priemgetal p het produkt

$$P_n = \prod_{i=1}^{n} \frac{p_i - 1}{p_i},$$

waarin de P_i's de opeenvolgende priemgevallen zijn, die voldoen aan $p_i = pv + 1$, $v > 0$.

$$P_{n+1} < \frac{p-1}{p} < P_n$$

noem $p_n = N(p)$.
Beschouw vervolgens de primitieve S-rij met betrekking tot een willekeurig priemgetal $q_1 \geq 5$. Bepaal zodanig dat

$$\prod_{i=1}^{m} \frac{q_i - 1}{q_i} > \tfrac{1}{2} \text{ en } \qquad \prod_{i=1}^{m+1} \frac{q_i - 1}{q_i} < \tfrac{1}{2}.$$

Indien geldt voor iedere $q_i < \frac{q_m}{2}$ dat $N(q_i) > q_m$, dan is de primitieve S-rij met betrekking tot q_1 minorant van iedere andere S-rij met kleinste element gelijk aan q_1.

Voor notatie en begrippen zie hoofdstuk 1.4.7 van dit proefschrift.

Stelling 3

Indien er een getal n bestaat, waarvoor geldt $\Phi(n) \mid n-1$ en waarvan de kleinste priemdeler gelijk is aan 7, dan is het getal n te ontbinden in ten minste 26 verschillende priemfactoren en n is groter dan 10^{84}.
Indien de kleinste priemdeler gelijk is aan 11, dan is het getal n te ontbinden in ten minste 63 verschillende priemfactoren en is dan groter dan 10^{257}.

Stelling 4

Beschouw een eindige matrix M met willekeurige elementen.
Onder een spoor in M wordt verstaan een reeks elementen, die op de volgende wijze wordt geconstrueerd:
Kies, kolomsgewijs een element uit iedere kolom van M, zodanig dat twee elementen, die uit dezelfde rij worden gekozen, identiek zijn.

Een matrix heet spoorbaar, indien hij tenminste één spoor heeft. Er bestaat een 8 bij 4 matrix M, waarvan ieder der 4 rijen ten hoogste 3 verschillende elementen heeft, die niet spoorbaar is.

Zie P. van Emde Boas, D. Kruyswijk
A combinatorial problem on finite abelian groups III
Rapport van Mathematisch Centrum Amsterdam
Afdeling Zuivere Wiskunde WN 31 (1969).

Stelling 5

Bij het onderzoek naar het wel of niet priem zijn van een geheel getal kan men beter gebruik maken van de verzameling $\varphi(3 ; 0, 1, 1,)$ dan van de door van der Poel voorgestelde verzameling $\varphi_3(2 ; 1, 1,)$.

Zie stelling van het proefschrift van W. L. van der Poel, The logical principles of some simple computers.

Zie hoofdstuk 2 en 3 van dit proefschrift.

Stelling 6

Bij de ontwikkeling van nieuwe programmatuur dient de documentatie op standaardwijze te geschieden. Een college over de wijze van documenteren dient door iedere student in de informatica gevolgd te worden.

Stelling 7

Bij een goed gebruik maken van de eigenschappen van het interactief programmeren en de visuele mogelijkheden van een grafisch beeldstation zal de wijze van ontwerpen van een object, met behulp van een grafisch beeldstation een essentiële verandering ondergaan.

Zie E. Lieuwens, H. Haringa
Interactive computer graphics
Intermediair 6, 35 en 6, 36 (1970).

Stelling 8

Ten einde de huidige ontwerp-, plannings- en bouwmethoden te kunnen herzien, is het noodzakelijk, dat een onderzoek wordt ingesteld naar de kriteria, die ten grondslag liggen aan de tijdens het ontwerpproces genomen beslissingen en aan het gebruik van informatie daarbij.

Stelling 9

Het is noodzakelijk een methode te ontwikkelen om grote hoeveelheden gegevens op dusdanige wijze op te kunnen slaan, zodat de hieruit verkregen informatie

— een beter inzicht kan verschaffen in de kompleksiteit van de samenleving

— de mogelijkheid opent de omgeving in een met deze kompleksiteit overeenstemmende verscheidenheid vorm te geven.

Stelling 10

De kosten, die verbonden zijn aan het kosteloos maken van het openbaar vervoer in de grote steden, wegen weliswaar niet op tegen de financiële voordelen, die ontstaan door het wegvallen van de lasten, die in de ruimste zin des woords inherent zijn aan het innen van de vervoersgelden; maar toch zijn er enkele andere argumenten, die er sterk voor pleiten, dat dat openbaar vervoer gratis zal worden. Het laat zich namelijk aanzien dat het particuliere gemotoriseerde verkeer, bij het gratis maken van het openbaar vervoer, in omvang zal afnemen, met als gevolg een drieledig gunstig effect:

1. Het aantal en de omvang van de voorzieningen, die voor het particuliere gemotoriseerde verkeer nodig waren, kunnen worden verminderd;
2. De luchtverontreiniging en geluidshinder, die dat verkeer veroorzaakt, zullen verminderen;
3. Het leefklimaat zal verbeteren en het stadsschoon zal minder worden aangetast, indien minder blikken medebewoners in de grote steden dag en nacht hun stallingsruimte op de openbare weg zullen opeisen.

Stelling 11

Het merendeel van de mensheid neemt de persoonlijkheidsvorm aan, welke hem door zijn culturele omgeving wordt aangeboden, hij doet hierdoor afstand van zijn persoonlijkheid en vervalt bijna tot automaat.

Stelling 12

Het zich in de laatste tijd ontwikkelende gebruik om de laatste van de rij van stellingen, die een proefschrift begeleiden van iets ludieke aard te laten zijn, brengt door de verstarring, die aan elk gebruik inherent is, bepaalde problemen met zich mee.