STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1955-013

On almost primes of the second order

H.J.A. Duparc

1965

The Mathematical Centre at Amsterdam, founded the 11th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

On almost primes of the second order

by

H.J.A. Duparc

Introduction. The well-known theorem of Fermat states that for primes p one has $a^{p-1} \equiv 1 \pmod p$, provided $p \nmid a$. There exist also composite numbers m which satisfy the relation $a^{m-1} \equiv 1 \pmod m$, either for some value of a (for instance a=2; Poulet numbers) or for all a with (a,m)=1 (Carmichael numbers).

If one possesses a table of all Poulet numbers up to a certain limit, then one may conclude that an integer m below this limit is prime if and only if $m \mid 2^{m-1}-1$ and m does not occur in the table. This procedure may be formulated in a slightly different way, which may give suggestions for other ways of investigating primality of a positive integer m. One considers the linear recurring first order sequence defined by

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

and finds out whether its period mod m does or does not divide m-1.

Now a generalization suggests itself. Instead of considering linear recurring sequences of the first order one takes such sequences of the second order. Then one finds out whether a certain property of its elements, valid for primes p, holds for the integer m under consideration. Once the composite numbers which also satisfy that property are tabulated, a new test on primality is obtained.

Now consider a second order recurring sequence defined by

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

Introducing the discriminant $D = a^2+4b$ of its characteristic polynomial $f(x)=x^2-ax-b$ one has for a prime p with $p \nmid b$ the following properties

A. $u_{p-(\frac{D}{p})} \equiv 0 \pmod p$;

B. $v_p \equiv a \pmod p$;

C. $u_p \equiv (\frac{D}{p}) \pmod p$.

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

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

In order to prove these relations the following properties are used

2) $$xu_n+bu_{n-1} = A_n(x) \equiv x^n A_0(x) = x^n \pmod{x^2-ax-b}$$ [1)]

if $(\frac{D}{p}) = 1$, then [2)] $x^{p-1} \equiv 1$ (modd x^2-ax-b,p);

if $(\frac{D}{p}) = -1$, then [3)] $x^{p+1} \equiv -b$ (modd x^2-ax-b,p);

if $(\frac{D}{p}) = 0$, then [3)] $x^p \equiv \frac{1}{2}b$ (modd x^2-ax-b,p);

$$v_n=bu_{n-1}+u_{n+1} = 2u_{n+1}-au_n \quad (n = 0,1,\ldots).$$

The last relation follows from the fact that it holds obviously for $n=0$ and $n=1$ and that the sequences (u) and (v) satisfy the same recurrence relation.

From these properties in the case $(\frac{D}{p})=1$ one derives

$$1 \equiv x^{p-1} \equiv A_{p-1}(x) = xu_{p-1}+bu_{p-2} \text{ (modd } x^2-ax-b,p),$$

thus $u_{p-1} \equiv 0 \pmod p$, $bu_{p-2} \equiv 1 \pmod p$, hence $u_p \equiv 1 \pmod p$ and the relations A,B and C follow immediately in this case. In the case $(\frac{D}{p}) = -1$ one derives similarly

$$-b \equiv x^{p+1} \equiv A_{p+1}(x) = xu_{p+1}+bu_p \text{ (modd } x^2-ax-b,p),$$

thus $u_{p+1} \equiv 0 \pmod p$, $u_p \equiv -1 \pmod p$, whence again the relations A, B and C follow immediately. Finally in the case $(\frac{D}{p})=0$ one has

$$\tfrac{1}{2}b \equiv x^p \equiv A_p(x) = xu_p+bu_{p-1} \text{ (modd } x^2-ax-b,p),$$

thus $u_{p-1} \equiv \frac{1}{2} \pmod p$, $u_p \equiv 0 \pmod p$, whence also here the relations A, B and C follow easily.

Composite numbers M which satisfy at least one of the three relations A,B and C will be called second order almost-primes. Simple examples may show that a composite number satisfying one of these relations does not necessarily satisfy the others. Hence three kinds of second order almost-primes can be distinguished.

---

1) Confer for instance H.J.A. Duparc, Periodicity properties of recurring sequences II, Proc.Kon.Ned.Ak.v.Wetensch. A 57 (1954), 473-485; theorem 30.

2) H.J.A. Duparc, Loc.cit. theorem 36.

3) H.J.A. Duparc, Loc.cit. theorem 37.

In section 1 the second order almost-primes of the types A,B and C will be considered successively. Section 2 is devoted to a special second order sequence, the sequence of Fibonacci. Properties of the almost primes with respect to this sequence are derived. Further a table of all the almost primes of the type B which are < 555200 is given. It was a suggestion of van der Poel to tabulate these numbers in order to obtain a new test on primality. Moreover it will be proved that with respect to the sequence of Fibonacci there exist infinitely many almost primes of each of the types A,B and C. In section 3 it will be investigated whether there exist composite numbers M which satisfy one of the three relations A, B or C for all second order sequences (1) with $(M,b)=1$. These numbers will be called second order Carmichael numbers. It will appear that there are no such numbers of the kinds A and C, whereas a characterization of those of the kind B will be given. Unfortunately the author was unable to prove or disprove the existence of such numbers.

Section 1. Second order almost-primes.

Let $M = p^r m = pm'$ (with p prime, $2 \nmid p$, $p \nmid m$, $r \geq 1$) be a composite number satisfying the relation A for a fixed given sequence (1). Then one has $p^r \mid M \mid u_k$ for $k=M-(\frac{D}{M})$ and moreover by a property of recurring sequences [4] one has $p^r \mid u_h$ with $h=p^{r-1}(p-(\frac{D}{p}))$. Now by a property of the symbol of Jacobion has $k=mh+j(\frac{D}{p})$ where $j=m'-(\frac{D}{m'})$, hence $p^r \mid u_j$. Conversely $p^r \mid u_j$ leads to $p^r \mid u_k$ on account of $p^r \mid u_h$. This proves the following criterium for second order almost-primes of the kind A.

Theorem. An integer $M=p_1^{r_1} \dots p_s^{r_s}$ (where $p_1,\dots,p_s$ are different primes) satisfies $M \mid u_{M-(\frac{D}{M})}$ if and only if

$$p_\sigma^{r_\sigma} \mid u_{j_\sigma}, \text{ where } j_\sigma = M_\sigma - (\frac{D}{M_\sigma}),\ M_\sigma = \frac{M}{p_\sigma} \quad (\sigma = 1,\dots,s).$$

Application. An integer $M=pq$ (where p and q are different primes) satisfies $M \mid u_{M-(\frac{D}{M})}$ if and only if

$$p \mid u_{q-(\frac{D}{q})}, \quad q \mid u_{p-(\frac{D}{p})} .$$

Now second order almost-primes of the type B will be considered. Here the following important relation will be used

---

4) H.J.A. Duparc, Loc.cit. theorem 33.

(3) $$v_h - v_k = D u_{\frac{1}{2}(h+k)} u_{\frac{1}{2}(h-k)} - v_k \left\{ 1-(-b)^{\frac{1}{2}(h-k)} \right\}$$
$$= v_{\frac{1}{2}(h+k)} v_{\frac{1}{2}(h-k)} - v_k \left\{ 1+(-b)^{\frac{1}{2}(h-k)} \right\} .$$

The proof of (3) runs as follows. From the identity

(2) $$x^n \equiv u_n x + b u_{n-1} \pmod{x^2-ax-b}$$

one derives replacing x by a-x

$$(a-x)^n \equiv u_n(a-x) + b u_{n-1} \pmod{x^2-ax-b},$$

hence by subtraction of there relations

(4) $$(2x-a)u_n \equiv x^n-(a-x)^n \pmod{x^2-ax-b}$$

and by addition of them

$$au_n+2bu_{n-1} \equiv x^n+(a-x)^n \pmod{x^2-ax-b}.$$

Then from $v_n=bu_{n-1}+u_{n+1} = au_n+2bu_{n-1}$ one obtains

(5) $$v_n \equiv x^n + (a-x)^n \pmod{x^2-ax-b}.$$

Another proof of the relations (4) and (5) can be given by mathematical induction on n. Now (3) may be found by straight forward substitution of the results (4) and (5) using also the relations $x(a-x) \equiv -b \pmod{x^2-ax-b}$ and $(2x-a)^2 \equiv D \pmod{x^2-ax-b}$. It may here be remarked that a further important relation, to be used later,

(6) $$u_h-u_k = u_{\frac{1}{2}(h+k)} v_{\frac{1}{2}(h-k)} - u_k(1+(-b)^{\frac{1}{2}(h-k)})$$
$$u_{\frac{1}{2}(h-k)} v_{\frac{1}{2}(h+k)} - u_k(1-(-b)^{\frac{1}{2}(h-k)})$$

can be proved in entirely the same way.

<u>Remark.</u> The relations (3) and (6) with k=1 are also given by D. Jarden, Factorization formulae for numbers of Fibonacci's sequence decreased or increased by a unit, Riv. Lemat. 5 (1951), 55-58.

Now let $M=p^r m=pm'$ (with $p \nmid m$) be a second order almost prime of the type B. Then for h=M and k=m' in the case $(-\frac{b}{p})=1$ the relation $(-b)^{\frac{1}{2}p^{r-1}(p-1)} \equiv 1 \pmod{p^r}$, hence $(-b)^{\frac{1}{2}(M-m')} \equiv 1 \pmod{p^r}$, and the relation (3) yield

(7) $$v_M - v_{m'} \equiv D u_{\frac{1}{2}(M+m')} u_{\frac{1}{2}(M-m')} \pmod{p^r}.$$

) = +1 one has 5) $u_{\frac{1}{2}(M-m')} = u_{\frac{1}{2}p^{r-1}(p-1)m} \equiv 0 \pmod{p^r}$,

) = -1 one has 5) $u_{\frac{1}{2}(M+m')} = u_{\frac{1}{2}p^{r-1}(p+1)m} \equiv 0 \pmod{p^r}$

f $(\frac{D}{p})=0$, one has 5) $p|D$ and moreover $u_{\frac{1}{2}(M-m')} \equiv u_{\frac{1}{2}p^{r-1}(p-1)m} \equiv 0 \pmod{p^{r-1}}$

quently in each of these three cases one has $v_M \equiv v_{m'} \pmod{p^r}$.
using (7) the relation $v_M \equiv a \pmod{p^r}$ leads to $v_{m'} \equiv a \pmod{p^r}$ and rsely.

In the case $(-\frac{b}{p}) = -1$ however one has

$$(-b)^{\frac{1}{2}p^{r-1}(p-1)} \equiv -1 \pmod{p^r}, \text{ hence } (-b)^{\frac{1}{2}(M-m')} \equiv -1 \pmod{p^r}.$$

the relation (3) yields

$$v_M - v_{m'} \equiv v_{\frac{1}{2}(M+m')} v_{\frac{1}{2}(M-m')} \pmod{p^r}.$$

) = 1 one has 6) $u_{p^{r-1}(p-1)} \equiv 0 \pmod{p^r}$, $u_{\frac{1}{2}p^{r-1}(p-1)} \equiv 0 \pmod{p^r}$,
using the relation $u_{2n}=u_n v_n$ one obtains $v_{\frac{1}{2}p^{r-1}(p-1)} \equiv 0 \pmod{p^r}$
since $m = \frac{1}{2}(M-m')/\frac{1}{2}p^{r-1}(p-1)$ is odd finally $v_{\frac{1}{2}(M-m')} \equiv 0 \pmod{p^r}$.
e case $(\frac{D}{p}) = -1$ one finds in entirely the same way
-m')$_2 \equiv 0 \pmod{p^r}$. The case $(\frac{D}{p})=0$ does not occur here since
$= a^2+4b$ leads to $-b \equiv (\frac{1}{2}a)^2 \pmod{p}$, hence $(-\frac{b}{p}) = 1$.

Consequently in all possible cases one has $v_M \equiv v_{m'} \pmod{p^r}$ hence
g (8) the relation $v_M \equiv a \pmod{p^r}$ leads to $v_{m'} \equiv a \pmod{p^r}$ and ersely.

This proves the following

rem. A necessary and sufficient condition for $M=p_1^{r_1}\ldots p_s^{r_s}$ (where ..,p_s are different primes) to be a second order almost-prime of B is

$$v_{M_\sigma} \equiv a \pmod{p_\sigma^{r_\sigma}}, \text{ where } M_\sigma = \frac{M}{p_\sigma} \qquad (\sigma = 1,\ldots,s).$$

articular a product $M=pq$ of two different prime factors is second r almost-prime of the kind B if and only if

$$v_p \equiv a \pmod{q}, \quad v_q \equiv a \pmod{p}.$$

.J.A. Duparc, Loc.cit. theorem 33.

.J.A. Duparc, Loc.cit. theorem 3? and 38.

second order almost-primes of the kind C.

Let $M = p^r m = pm'$ $(p \nmid m)$ satisfy

$$u_M \equiv (\tfrac{D}{M}) \pmod{M}.$$

If $(\frac{D}{p}) = +1$ then [7] $u_h \equiv u_k \pmod{p^r}$ if $p^{r-1}(p-1) \mid h-k$. Hence $u_M \equiv u_{m'} \pmod{p^r}$ and one finds $u_{m'} \equiv (\frac{D}{m'}) \pmod{p^r}$. Conversely the last relation leads to $u_M \equiv (\frac{D}{M}) \pmod{p^r}$.

If $(\frac{D}{p}) = -1$ then in the case $(\frac{-b}{p}) = +1$ one has $(-b)^{\frac{1}{2}p^{r-1}(p-1)} \equiv 1 \pmod{p^r}$ and moreover [8] $p^r \mid u_{\frac{1}{2}p^r(p+1)} \mid u_{\frac{1}{2}(M+m')}$. Consequently using (6) one finds $p^r \mid u_M + u_{m'}$. In the case $(\frac{-b}{p}) = -1$ one has

$$(-b)^{\frac{1}{2}p^r(p-1)} \equiv -1 \pmod{p^r} \text{ and moreover [8] } p^r \mid u_{p^r(p+1)},$$

$p^r \nmid u_{\frac{1}{2}p^r(p+1)}$, hence $p^r \mid v_{\frac{1}{2}p^r(p+1)} \mid v_{\frac{1}{2}(M+m')}$ and (6) yields $p^r \mid u_M + u_{m'}$.
In either case one has $u_M \equiv -u_{m'} \pmod{p^r}$ and $u_M \equiv (\frac{D}{M}) \pmod{p^r}$ leads to $u_{m'} \mp (\frac{D}{m'}) \pmod{p^r}$ and conversely.

Finally if $(\frac{D}{p}) = 0$ one has [9] $p \mid u_p$, hence [7] $p^r \mid u_{p^r} \mid u_M$ and the relation $u_M \equiv (\frac{D}{M}) \pmod{p^r}$ is satisfied automatically since both members of this congruence are $\equiv 0 \pmod{p^r}$.

Resuming one finds the following

<u>Theorem</u>. An integer $M = p_1^{r_1} \dots p_s^{r_s}$ $(p_1, \dots, p_s$ different primes) satisfies for a sequence (1) the relation $u_M \equiv (\frac{D}{M}) \pmod{M}$ if and only if

$$u_{M_\sigma} \equiv (\tfrac{D}{M_\sigma}) \pmod{p_\sigma^{r_\sigma}}, \quad M_\sigma = \frac{M}{p_\sigma}, \quad p_\sigma \nmid D \quad (\sigma = 1, \dots, s).$$

<u>Application</u>. An integer $M = pq$ (where p and q are different primes not dividing D) is a second order almost-prime of the kind C if and only if

(9) $$u_p \equiv (\tfrac{D}{p}) \pmod{q}, \quad u_q \equiv (\tfrac{D}{q}) \pmod{p}.$$

<u>Remark.</u>

For all odd primes p dividing D the integer $M = p^r$ $(r = 1, 2, \dots)$ satisfies $p^r \mid u_M$, hence

$$u_M \equiv (\tfrac{D}{M}) \pmod{M},$$

so all these integers are second order almost-primes of the kind C.

<u>Section 2.</u> In this section integers will be investigated which satisfy A, B or C for one of the most simple recurring sequences of the second order, viz. the sequence of Fibonacci:

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

---

7) H.J.A. Duparc, loc.cit. theorem 33.
8) H.J.A. Duparc, loc.cit. theorem 33 and 38.
9) H.J.A. Duparc, loc.cit. theorem 36.

Here almost primes M of the type A satisfy $M \mid u_{M-(\frac{5}{M})}$, those of the type B satisfy $M \mid v_M - 1$ and those of the type C satisfy $M \mid u_M - (\frac{5}{M})$.

It will now be proved that there are infinitely many almost-primes of the type A. For the proof use will be made of the following

<u>Lemma.</u> If $2 \nmid M$, $3 \nmid M$, $5 \nmid M$, $M \mid u_{M-(\frac{5}{M})}$, then $N = u_{2M}$ satisfies the same relations, i.e. $2 \nmid N$, $3 \nmid N$, $5 \nmid N$ and $N \mid u_{N-(\frac{5}{N})}$.

<u>Proof.</u> One has $2 \nmid N$, since $2 \mid N = u_{2M}$ would lead to $3 \mid 2M$, contrary to $3 \nmid M$.

One has further $3 \nmid N$, since $3 \mid N = u_{2M}$ would lead to $4 \mid 2M$, contrary to $2 \nmid M$.

Finally one has $5 \nmid N$, since $5 \mid N = u_{2M}$ would lead to $5 \mid 2M$, contrary to $5 \nmid M$.

Further if c denotes the smallest positive integer with $M \mid u_c$ and $C = C(N)$ the smalles positive integer with $M \mid u_C$, $M \mid u_{C+1} - 1$, then it has been proved[10] that $v = \frac{C}{c}$ is an integer, which is equal to 1,2 or 4. The value $v=4$ only occurs if c is odd. Now by assumption one has $c \mid M-(\frac{5}{M})$, hence $C \mid 2(M-(\frac{5}{M}))$ in the cases $v=1$ or 2. In the case $v=4$ the integer c is odd, hence $c \mid \frac{1}{2}(M-(\frac{5}{M}))$ and also then $C \mid 2(M-(\frac{5}{M}))$. Consequently[11] $u_{2M} \equiv u_{2(\frac{5}{M})} = (\frac{5}{M}) \pmod{M}$, hence $M \mid u_{2M} - (\frac{5}{M}) = N - (\frac{5}{M})$. Since both N and M are odd one has also $2M \mid N - (\frac{5}{M})$, hence $N = u_{2M} \mid u_{N-(\frac{5}{M})}$. Finally $(\frac{5}{M}) = (\frac{5}{N})$. In fact if $(\frac{5}{M}) = 1$, then $M \equiv \pm 1 \pmod{10}$, hence $2M \equiv \pm 2 \pmod{20}$ and $N = u_{2M} \equiv u_{\pm 2} = \pm 1 \pmod{5}$, thus $(\frac{5}{N}) = 1$. If however $(\frac{5}{M}) = -1$ then $M \equiv \pm 3 \pmod{10}$, hence $2M \equiv \pm 6 \pmod{20}$ and $N = u_{2M} \equiv u_{\pm 6} = -8 \equiv 3 \pmod{5}$, hence $(\frac{5}{N}) = -1$. This proofs $N \mid u_{N-(\frac{5}{N})}$.

Now using the lemma one obtains infinitely many almost primes M_h of the type A once one such number $M = M_o$ with $(M,30)=1$ and $M \mid u_{M-(\frac{5}{M})}$ is found. In fact one has only to take

$$M_{h+1} = u_{2M_h} \qquad (h = 0,1,\ldots).$$

Now for M_o one may take any prime $\neq 2,3,5$, for instance $M=7$; then u_{14} is almost-prime in the sense A. Here it has to be remarked that $u_{2k} = u_k v_k$ is certainly composite.

---

10) H.J.A. Duparc, C.G. Lekkerkerker, W. Peremans, Reduced sequences of integers and pseudo random numbers. Rapport ZW 1953-002, Mathem.Centrum; theorem 11.

11) H.J.A. Duparc, C.G. Lekkerkerker, W. Peremans, Loc.cit., theorem 2.

Also one obtains infinitely many numbers of the desired kind from the sequence u_{2p}, where p runs through all infinitely many primes ≥ 7.

Remark. There appears to be the following connection between prime pairs and the almost primes considered here. If $p \equiv 17 \pmod{20}$ and $q=p+2$ are both prime, then $M=pq$ is an almost prime of the kind A.

In fact since $-(\frac{5}{p})=(\frac{5}{q})=1$ one has $p \mid u_{p+1}=u_{q-(\frac{5}{q})}$ and $q \mid u_{q-1}=u_{p+1}=u_{p-(\frac{5}{p})}$.

The almost-primes of the type B were defined by M v_M-1. A table of all such numbers which are $<$ 555200 is given at the end of this paper.

It will now be proved that there are also infinitely many almost-primes of the type B. Here the following lemma will be proved:

Lemma. If $2 \nmid M$, $3 \nmid M$, $M \mid v_M-1$, then $N=v_M$ satisfies the same relations.

Proof. The relation $2 \mid N=v_M$ would lead to $3 \mid M$, contrary to $3 \nmid M$. The relation $3 \mid N=v_M$ would lead to $4 \mid M-2$, contrary to $2 \nmid M$.

If $N \equiv 1 \pmod 4$, then $4M \mid v_M-1$, hence $2M \mid \frac{1}{2}(N-1)$ and using (3)

$$M = v_M \mid u_{2M} \mid u_{\frac{1}{2}(N-1)} \mid 5u_{\frac{1}{2}(N-1)}\, u_{\frac{1}{2}(N+1)} = v_N-1.$$

If $N \equiv 3 \pmod 4$, then $\frac{1}{2}(N-1)$ is odd. Since $M \mid \frac{1}{2}(N-1)$ one finds again using (3)

$$M = v_M \mid v_{\frac{1}{2}(N-1)} \mid v_{\frac{1}{2}(N-1)}\, v_{\frac{1}{2}(N+1)} = v_N-1.$$

From this lemma it appears that any number of the sequence defined by

$$M_{h+1} = v_{M_h} \qquad (h = 0,1,\dots)$$

is a number of the desired type, once it is now that M_o is so. Here for M_o one may take for instance $M_o=4181=37.113$, which number satisfies $M_o \mid v_{M_o}-1$, as may be easily verified by making use of the second theorem of section 2.

Finally the almost-primes of the type C are considered. These composite integers satisfy $M \mid u_M-(\frac{5}{M})$. Of course it will be proved that there exist also infinitely many pseudo-primes of this type and also here a lemma will be used.

Lemma. If $M \equiv 1$ (120) and $M \mid u_M-(\frac{5}{M})$, then these relations hold also for $N=u_M$.

Proof. One has $C(8)=12$, hence $N=u_M \equiv u_1=1 \pmod 8$. Also $C(3)=8$, hence $N=u_M \equiv u_1 \pmod 3$. Finally $C(5)=20$, hence $N=u_M \equiv u_1=1 \pmod 5$. Consequently $N \equiv 1 \pmod{120}$ and $(\frac{5}{M})=(\frac{5}{N})=1$. Since both N and M are odd the relation $M \mid u_M-(\frac{5}{M}) = N-1$ leads to $M \mid \frac{1}{2}(N-1)$. Then using (6) one finds

$$N=u_M \mid u_{\frac{1}{2}(N-1)} \mid u_{\frac{1}{2}(N-1)} v_{\frac{1}{2}(N+1)} = u_N - 1 = u_N - (\tfrac{5}{N}).$$

From this lemma it follows immediately that any element of the sequence defined by

$$M_{h+1} = u_{M_h} \qquad (h = 0,1,\ldots)$$

is a number of the desired type provided M_0 is so. For M_0 one can take for instance 13201 = 43.307.

Section 3. Second order Carmichael numbers.

A second order Carmichael number of the type A is a composite number M which satisfies $M \mid u_{M-(\frac{D}{M})}$ for all recurring sequences (1) with $(M,b)=1$. It will be shown however that such numbers do not exist.

Let $M=p^r m$ with $p \nmid m$ be a second order Carmichael number of the type A. Now first take a recurring sequence (1) with characteristic polynomial $f(x)=(x-1)(x-g)$, where g is a primitive root mod p^r. Then for $u_n = \frac{g^n-1}{g-1}$ one has $p^r \mid u_n$ if and only if $p^{r-1}(p-1) \mid n$. Consequently the first theorem of section 1 gives $p^{r-1}(p-1) \mid p^{r-1}m-(\frac{D}{p^{r-1}m})$, hence $r=1$. Further consider a recurring sequence for which the characteristic polynomial $f(x) = x^2-ax-b$ is a mod p irreducible divisor of the cyclotomic polynomial of degree p^2-1. Then one has $p \mid u_n$ if and only if $p+1 \mid n$. In fact $p+1 \mid n$ leads obviously to [12] $p \mid u_{p+1} \mid u_n$. Conversely if $p \mid u_{n'}$ with $p+1 \nmid n'$, then an integer h exists such that $p \mid u_h$ with $0<h<p+1$. Hence using (2) $x^h \equiv bu_{h-1}$ (modd $f(x)p$) and $x^{h(p-1)} \equiv 1$ (modd $f(x),p$) where $0<h(p-1)<p^2-1$, contrary to the construction of $f(x)$. Then the immediate consequence $p \mid M \mid u_{m-(\frac{D}{m})}$ of the assumption on M leads to $p+1 \mid m-(\frac{D}{m})$. Now consider another such sequence with polynomial x^2-ax-b_1 where $b_1 \equiv b \pmod p$. Hence $p+1 \mid m-(\frac{D_1}{m})$. If one chooses b_1 such that $b_1 \equiv b \pmod q$ for every divisor q of m apart from one divisor q_1 and that $(\frac{a^2+4b}{q}) = -(\frac{a^2+4b_1}{q_1})$, then $(\frac{D}{m}) = -(\frac{D_1}{m})$. This leads to the contradiction $p+1 \mid m+1$ and $p+1 \mid m-1$.

Now first second order Carmichael numbers of the type C will be considered, i.e. composite numbers M satisfying $u_M \equiv (\frac{D}{M}) \pmod M$ for all recurring sequences (1) with $(M,b)=1$. It will be proved that these numbers do not exist neither.

Suppose $M=p^r m$ with $p \nmid m$ is a second order Carmichael number of the type C. Now first take a recurring sequence (1) with charactertistic polynomial $f(x)=(x-1)(x-g)$ where g is a primitive root mod p^r. Then for $u_n = \frac{g^n-1}{g-1}$ one has $p^r \mid u_n$ if and only if $p^{r-1}(p-1) \mid n$. Consequently the

---

12) H.J.A. Duparc, Loc.cit. theorem 36.

third theorem of section 1 gives $p^r | u_{p^r m} - 1 = \frac{g(g^{p^r m-1}-1)}{g-1}$ and $p^{r-1}(p-1) | p^r m-1$ hence $r=1$ and $p-1 | m-1$. Further a special recurring sequence (1), necessary to disprove the existence of the second order Carmichaelnumbers of the type C will be constructed. First the following lemma is proved.

Lemma. For every prime $p \geq 7$ there exist integers r,s and t such that $t=r+s$ and $(\frac{r}{p})=(\frac{s}{p})=(\frac{t}{p})=1$.

Proof. Let h be an arbitrary odd quadratic residu $\neq 1$ of p. Such an integer h exists since $p \geq 7$. Take $s=(\frac{h-1}{2})^2$, $t=(\frac{h+1}{2})^2$, then $r=t-s=h$ and also s and t are quadratic residues mod p with $t=r+s$.

Now the special recurring sequence (1) necessary to disprove the existence of the second order Carmichael numbers of the type C will be constructed. If r,s and t denote the above found integers, first take $a^2 \equiv t \pmod p$, $b' \equiv -\frac{1}{4}s \pmod p$. Then for $D'=a^2+4b'$ one has $D' \equiv t-s = r \pmod p$, hence $(\frac{-b}{p}) = (\frac{D'}{p}) = 1$. Now take $b' \equiv b \pmod p$ such that $D = a^2+4b$ is a non-residu mod m. (This can be obtained by the Chinese remainder theorem; for b one has to satisfy $b \equiv b' \pmod p$ and $b \equiv \frac{1}{4}(d-a^2) \pmod m$, where d is a fixed integer with $(\frac{d}{m})=-1$). Then one has $(\frac{D}{p})=(\frac{D'}{p})=1$ and $(\frac{D}{m})=-1$. Consequently for this sequence one has using (6)

$$u_m - 1 = u_{\frac{1}{2}(m-1)} \, v_{\frac{1}{2}(m+1)} - (1-(-b)^{\frac{1}{2}(m-1)}),$$

hence $u_m - 1 \equiv u_{\frac{1}{2}(m-1)} \, v_{\frac{1}{2}(m+1)} \pmod p$ on account of $(\frac{-b}{p})=1$ and $p-1 | m-1$. Moreover one has [13] $p | u_{\frac{1}{2}(p-1)}$, hence $p | u_{\frac{1}{2}(m-1)}$, thus $p | u_m - 1$ and $p \nmid u_m - (\frac{D}{m})$. This disproves the existence of the second order Carmichael numbers of the kind C and only those of the kind B may exist.

Finally an attempt will be made to construct second order Carmichael numbers of the type B, i.e. numbers M satisfying

$$v_M \equiv a \pmod M$$

for all recurring sequences (1) with $(M,b)=1$.

First consider a sequence with $f(x)=(x-1)(x-g)$ where $(g,M)=1$. Then one has $v_n=g^n+1$, hence

$$v_M - a = g^M+1 - (g+1) = g(g^{M-1}-1)$$

and $M | v_M - a$ if and only if $M | g^{M-1}-1$ for all introduced g, i.e. for all g with $(M,g)=1$. Consequently M is certainly an ordinary Carmichael number, hence M is odd, quadratfrei and a product of at least three different prime factors. Moreover by taking for g a primitive root mod p one finds $p-1 | M-1$. For $M=pm$, where p is one of the prime factors of M and

----

13) H.J.A. Duparc, Loc.cit. theorem 38.

$p-1 \mid m-1$ further conditions are derived now.

a. First consider the case $\frac{m-1}{p-1}$ is odd. In this case consider, as before, a sequence for which $p \mid u_n$ if and only if $p+1 \mid n$. Then $(\frac{-b}{p})=-1$ since otherwise [14] already $p \mid u_{\frac{1}{2}(p+1)}$. Hence $(-b)^{\frac{1}{2}(p-1)} \equiv -1 \pmod p$, consequently $(-b)^{\frac{1}{2}(m-1)} \equiv -1 \pmod p$. Then (3) yields $v_m - a \equiv v_{\frac{1}{2}(m-1)} v_{\frac{1}{2}(m+1)} \pmod p$ and $p \mid v_m - a$ is equivalent to $p \mid v_{\frac{1}{2}(m-1)} v_{\frac{1}{2}(m+1)}$. Again using the fact that the considered sequence satisfies $p \mid u_n$ if and only if $p+1 \mid n$ one finds using $u_{2n}=u_n v_n$

(10) either $p+1 \mid m-1,\ p+1 \nmid \frac{1}{2}(m-1)$ or $p+1 \mid m+1,\ p+1 \nmid \frac{1}{2}(m+1)$.

Again two cases are distinguished. If $p \equiv 1 \pmod 4$, then $4 \mid p-1 \mid m-1$, Hence $p+1 \mid m-1,\ p+1 \nmid \frac{1}{2}(m-1)$ is excluded on account of $p+1 \equiv 2 \pmod 4$. Consequently the second relation (10) holds i.e. $p+1 \mid m+1,\ p+1 \mid \frac{1}{2}(m+1)$, hence $\frac{m+1}{p+1}$ is an odd integer. In the case $p \equiv 3 \pmod 4$ one has $4 \nmid p-1$, hence $4 \nmid m-1$ and $m \equiv 3 \pmod 4$. Now $p+1 \mid m-1$ is again excluded since $4 \mid p+1,\ 4 \nmid m-1$. Then (10) yields again $p+1 \mid m+1,\ p+1 \nmid \frac{1}{2}(m+1)$, and again $\frac{m+1}{p+1}$ appears to be an odd integer.

b. In the second case to be considered the integer $\frac{m-1}{p-1}$ is even, hence $4 \mid m-1$. Since here $p-1 \nmid \frac{1}{2}(m-1)$ one has $(-b)^{\frac{1}{2}(m-1)} \equiv 1 \pmod p$ and (3) yields $p \mid u_{\frac{1}{2}(m+1)} u_{\frac{1}{2}(m-1)}$. Again considering the above used sequence for which $p \mid u_n$ if and only if $p+1 \mid n$ one finds either $p+1 \mid \frac{1}{2}(m+1)$ or $p+1 \mid \frac{1}{2}(m-1)$. Now $4 \mid m-1$, hence $\frac{1}{2}(m+1)$ is odd and $p+1 \mid \frac{1}{2}(m+1)$ excluded. Consequently $p+1 \mid \frac{1}{2}(m-1)$.

Resuming the results a second order Carmichael number M of the type B is certainly an ordinary Carmichael number and further if $p \mid M$, $M=pm$, either both $\frac{m-1}{p-1}$ and $\frac{m+1}{p+1}$ are odd integers or both $\frac{m-1}{p-1}$ and $\frac{m-1}{p+1}$ are even.

It will now be proved that also the reversed property holds. Let M be a Carmichael number. Consider a prime factor p of M and put $M=pm$.

First suppose that both $\frac{m-1}{p-1}$ and $\frac{m+1}{p+1}$ are odd integers. Then for all recurring sequences with $(\frac{-b}{p})=1$ one has $(-b)^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$ and [14] if $p \nmid D$ one has either $p \mid u_{\frac{1}{2}(p+1)}$ or $p \mid u_{\frac{1}{2}(p-1)}$. Hence $(-b)^{\frac{1}{2}(m-1)} \equiv 1 \pmod p$ and moreover either $p \mid u_{\frac{1}{2}(m+1)}$ or $p \mid u_{\frac{1}{2}(m-1)}$. Then (3) yields $p \mid v_m - a$. In the case $p \mid D$ one has obviously $p \mid D\, u_{\frac{1}{2}(m+1)} u_{\frac{1}{2}(m-1)}$, hence $v_m \equiv a \pmod p$. For all sequences with $(\frac{-b}{p})=-1$ however one has $(-b)^{\frac{1}{2}(p-1)} \equiv -1 \pmod p$ and, as remarked in section 2, here $p \nmid D$, Then [15] either $p \mid v_{\frac{1}{2}(p+1)}$ or $p \mid v_{\frac{1}{2}(p-1)}$, consequently $(-b)^{\frac{1}{2}(m-1)} \equiv -1 \pmod p$ and moreover either $p \mid v_{\frac{1}{2}(m+1)}$ or $p \mid v_{\frac{1}{2}(m-1)}$. Then (3) gives again $p \mid v_m - a$.

----

14) H.J.A. Duparc, Loc.cit. theorem 38.

15) H.J.A. Duparc, Loc.cit. theorem 38.

In the case both $\frac{m-1}{p-1}$ and $\frac{m-1}{p+1}$ are even the integer p-1 divides $\frac{1}{2}(m-1)$ hence $(-b)^{\frac{1}{2}(m-1)p} \equiv 1 \pmod p$. Since both p-1 and p+1 divide $\frac{1}{2}(m-1)$ one has $p \mid Du_{p-1}\, u_{p+1} \mid Du_{\frac{1}{2}(m-1)}\, u_{\frac{1}{2}(m+1)}$ and (3) yields also here $p \mid v_m - a$. This completes the proof of the following

Theorem. An integer M is a second order Carmichael number of the type B if and only if for every prime divisor p of M (with M=pm) either both $\frac{m-1}{p-1}$ and $\frac{m+1}{p+1}$ are odd integers or both $\frac{m-1}{p-1}$ and $\frac{m-1}{p+1}$ are even integers.

Some more properties for the number M can be derived.

First it has to be remarked that the integers $\frac{m-1}{p-1}$ and $\frac{m+1}{p+1}$ are both odd if and only if $\frac{M-1}{p-1}$ and $\frac{M-1}{p+1}$ are both even. In fact $\frac{M-1}{p-1} - \frac{m-1}{p-1} = m$ is odd and so is $\frac{M-1}{p+1} + \frac{m+1}{p+1} = m$.

Similarly $\frac{m-1}{p-1}$ and $\frac{m-1}{p+1}$ are both even if and only if $\frac{M-1}{p-1}$ and $\frac{M+1}{p+1}$ are both odd. Here the relation $\frac{M+1}{p+1} + \frac{m-1}{p+1} = m$ is used.

Further it will be shown that M contains at least 4 different prime factors.

In fact consider the largest prime factor p of M. If for p one is in the first case i.e. if both $\frac{m-1}{p-1}$ and $\frac{m+1}{p+1}$ are odd, then $\frac{m-1}{p-1} - \frac{m+1}{p+1} = \frac{2(m-p)}{p^2-1}$ is even. Since $p-1 \mid m-1$ one has $p < m$, hence $\frac{2(m-p)}{p^2-1} > 0$ and consequently $\frac{2(m-p)}{p^2-1} \geqq 2$, hence $m \geqq p^2+p-1$. If however $\frac{m-1}{p-1}$ and $\frac{m-1}{p+1}$ are both even then $p^2-1 \mid m-1$, hence $p^2 \leqq m$. In either case from $p^2 \leqq m$ one deduces that m must have more than two different prime factors, which proves the assertion.

Moreover one has $3 \nmid M$, for above it was found that either $p^2-1 \mid m^2-1$ or $p^2-1 \mid M^2-1$. Taking $p \neq 3$ one has $3 \mid p^2-1$, hence in the first case $3 \nmid m$, thus $3 \nmid M$, whereas in the second case the relation $3 \nmid M$ follows immediately.

Finally in the first case (where both $\frac{m-1}{p-1}$ and $\frac{m+1}{p+1}$ are odd) one finds after a little discussion $m \equiv p \pmod{24}$, hence $M = pm \equiv p^2 \equiv 1 \pmod{24}$. In the second case by the above remark both $\frac{M-1}{p-1}$ and $\frac{M+1}{p+1}$ are odd, hence $M \equiv p \pmod{24}$ and $m \equiv 1 \pmod{24}$.

If $M \not\equiv 1 \pmod{24}$ the number of prime factors of M is odd. In fact putting $M = p_1 \ldots p_s$ for every prime factor of M one is in the second case (since in the first case it was found that $24 \mid M-1$). Hence

$$M \equiv p_\sigma \pmod{24} \quad (\sigma = 1, \ldots, s)$$

and after multiplication of these relations

$$M^s \equiv M \not\equiv 1 \pmod{24}.$$

Hence $2 \nmid s$.

As a consequence of this fact it appears that in the case $M \not\equiv 1 \pmod{24}$ the number M must have at least 5 different prime factors.

Up till now the author has not been able to prove or to disprove the existence of second order Carmichael numbers of the kind B. Since every such number is certainly an ordinary Carmichael number all Carmichael numbers $< 10^8$ are investigated [16] but none of them appeared to be a second order Carmichael number. So there are no second order Carmichael numbers $< 10^8$.

Table of all almost primes < 555200 of the type B with respect to the sequence of Fibonacci.
The Poulet numbers occurring in this table are indicated by P apart from the Carmichael numbers, which are denoted by C.

705 = 3.5.47		
1605 = 5.7.107		
2465 = 5.17.29	C	
2737 = 7.17.23		
4181 = 37.113		
5777 = 53.109		
6721 = 11.13.47		
10877 = 73.149		
13201 = 43.307		
15251 = 101.151		
24465 = 3.5.7.233		
34561 = 17.19.107		
35785 = 5.17.421		
51841 = 47.1103		
54705 = 3.5.7.521		
64079 = 139.461		
64681 = 71.911		
67251 = 131.521		
67861 = 79.859		
75077 = 193.389		
90061 = 113.797		
96049 = 139.691		
97921 = 181.541		
100065 = 3.5.7.953		
100127 = 223.449		
105281 = 11.17.563		
113573 = 137.829		
118441 = 83.1427		
146611 = 271.541		
161027 = 283.569		
162133 = 73.2221		
163081 = 17.53.181		
186961 = 31.37.163		
194833 = 29.43.197		
197209 = 199.991		
209665 = 5.19.2207		
217257 = 3.139.521		
219781 = 271.811	P	
228241 = 13.97.181	P	
229445 = 5.109.421		
231703 = 263.881		
252601 = 41.61.101	C	
254321 = 263.967		
257761 = 7.23.1601		
268801 = 13.23.29.31		
272611 = 131.2081		
302101 = 317.953		
303101 = 101.3001		
323301 = 3.11.97.101		
330929 = 149.2221		
399001 = 31.61.211	C	
430127 = 463.929		
433621 = 199.2179		
447145 = 5.37.2417		
455961 = 3.11.41.337		
490841 = 13.17.2221		
497761 = 11.37.1223		
512461 = 31.61.271	C	
520801 = 241.2161		

Litterature

H.J.A. Duparc, On Carmichael numbers, Simon Stevin 29 (1952), 21-24.

H.J.A. Duparc, C.G. Lekkerkerker, W. Peremans, Reduced sequences of integers and pseudo random numbers, Rapport ZW 1953-002, Mathem.Centrum.

H.J.A. Duparc, Periodicity properties of recurring sequences I and II, Proc.Kon.Ned.Ak.v.Wet. A57 (1954),331-342 and 473-485.

D. Jarden, Factorization formulae for numbers of Fibonacci's sequence decreased or increased by a unit, Riv.Lemat.5(1951),55-58

P. Poulet, Table des nombres composés vérifiant le théorème de Fermat pour le module 2 jusqu'à 100000000, Sphinx 8(1938),42-52.