STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1956-008

A remark to "rapport ZW 1955-013"

H.J.A. Duparc

1956

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.

A remark to "rapport ZW 1955-013"

H.J.A. Duparc

In the "rapport ZW 1955-013" it has been proved that there exist infinitely many composite numbers m such that $m \mid v_m - 1$, where (v) is the sequence which is associated with the sequence of Fibonacci, i.e. where

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

Here it will be proved that the similar assertion $m \mid v_m - a$ also holds for any sequence (v) defined by

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

where a is a fixed given integer and b=1 or -1.

In the proof one may restrict oneself to the case that the discriminant $D=a^2+4b$ of the quadratic form $f(x)=x^2-ax-b$ differs from zero. In fact otherwise a is even (=2c) and one has $v_n=2c^n$ and it is known that for every given c there exist infinitely many composite m with $m \mid c^{m-1}-1$, hence $m \mid v_m - a$.

In order to obtain the result in the case $D \neq 0$ the following lemma will be proved first.

<u>Lemma.</u> If m is composite, $m \equiv 1 \pmod{24}$, $(m,D)=1$ and $x^{m-1} \equiv 1 (\text{modd } f(x), m)$ then the same properties hold for the integer $M=u_m=\frac{\alpha^m-\beta^m}{\alpha-\beta}$; here α and β are the roots of $f(x)=0$.

<u>Proof</u>. One has $(D,M)=1$. In fact, if a prime p dividing D should satisfy $p \mid u_m$, then [1] one would have $p \mid m$, contrary to $(m,D)=1$.

Further one has $M \equiv 1 \pmod{24}$, i.e. $u_m \equiv u_1 \pmod{24}$. In fact if $(\frac{D}{2})=1$ one has [2] $u_h \equiv u_k \pmod 8$ as soon as $12 \mid h-k$; if $(\frac{D}{2})=0$ one has [2] $u_h \equiv u_k \pmod 8$ as soon as $8 \mid h-k$, hence $24 \mid m-1$ leads to $u_m \equiv u_1 \pmod 8$. Further if $(\frac{D}{3})=-1$ one has [1] $u_h \equiv u_k \pmod 3$ as soon as $8 \mid h-k$, if $(\frac{D}{3})=0$ one has [1] $u_h \equiv u_k \pmod 3$ as soon as $6 \mid h-k$ and if $(\frac{D}{3})=1$ one has [1] $u_h \equiv u_k \pmod 3$ as soon as $2 \mid h-k$, hence $24 \mid m-1$ leads to $u_m \equiv u_1 \pmod 3$. Consequently $M \equiv 1 \pmod{24}$.

Now from the assumption one has

$$\alpha^{m-1} \equiv 1 \pmod m, \quad \beta^{m-1} \equiv 1 \pmod m,$$

hence

$$M(\alpha-\beta) = \alpha^m - \beta^m \equiv \alpha - \beta \pmod m$$

and since $(M,D)=1$ one finds $M \equiv 1 \pmod m$. Since $4 \nmid m$ and $24 \mid M-1$ one has further $4m \mid M-1$.

Then the relation $M \mid \alpha^m - \beta^m$ leads to

$$\alpha^{2m} \equiv \alpha^m \beta^m = \pm 1 \pmod{M}, \text{ hence } \alpha^{4m} \equiv 1 \pmod{m}$$

and

$$M \mid \alpha^{4m}-1 \mid \alpha^{M-1}-1$$

This proves the lemma.

Remark. In the proof the following property has been used: if $h \equiv k \pmod{24}$, then $u_h \equiv u_k \pmod{24}$. In the same way one may deduce the further property (to be used below) if $h \equiv k \pmod{3.2^{r+3}}$, then $u_h \equiv u_k \pmod{3.2^{r+3}}$, $v_h \equiv v_k \pmod{3.2^{r+3}}$.

From the lemma it follows that once one composite integer m_0 with the above properties is known, then infinitely many such integers $m_0, m_1, \ldots$ are found by the relation

$$m_{h+1} = u_{m_h} \qquad (h = 0,1,\ldots).$$

Each such integer satisfies $m \mid \alpha^m - \alpha$, $m \mid \beta^m - \beta$, hence also $m \mid \alpha^m + \beta^m - \alpha - \beta = v_m - a$. It remains therefore to find an initial composite integer $m = m_0$ with the above properties.

Suppose that $D = q_1^{r_1} \ldots q_s^{r_s}$ be the canonical decomposition of D. Let the integer a contain exactly r factors 2. Now let p be a prime satisfying

(1) $\quad p \nmid a, \quad p \equiv 1 \pmod{3.2^{r+3}}, \; p \equiv 1 \pmod{q_\sigma} \qquad (\sigma = 1,\ldots,s)$

Then the integer $m = \dfrac{\alpha^{2p} - \beta^{2p}}{\alpha^2 - \beta^2} = u_p v_p / a$ has the required properties.

In fact one has $\left(\frac{p}{q_\sigma}\right) = 1$, hence $\left(\frac{q_\sigma}{p}\right) = 1$ $(\sigma = 1,\ldots,s)$ in virtue of $4 \mid p-1$. Consequently $\left(\frac{D}{p}\right) = 1$.

Then one has [2] $\alpha^{p-1} \equiv 1 \pmod{p}$, $\beta^{p-1} \equiv 1 \pmod{p}$, hence $\alpha^{2p} - \beta^{2p} \equiv \alpha^2 - \beta^2 \pmod{p}$ and since $p \nmid D$, $p \nmid a$ one deduces $m \equiv 1 \pmod{p}$. Further from $3.2^{r+3} \mid p-1$ it follows by the above remark that $u_p \equiv u_1 = 1 \pmod{3.2^{r+3}}$, $v_p \equiv v_1 = a \pmod{3.2^{r+3}}$, hence

$$am = u_p v_p \equiv a \pmod{3.2^{r+3}}, \quad m \equiv 1 \pmod{24}.$$

Consequently $4p \mid m-1$. Then finally one obtains from $\alpha^{2p} \equiv \beta^{2p} \pmod{m}$ the result

$$\alpha^{4p} \equiv \alpha^{2p} \beta^{2p} = (\pm 1)^{2p} = 1 \pmod{m}, \text{ hence } m \mid \alpha^{4p} - 1 \mid \alpha^{m-1} - 1$$

Remark. Since there exist infinitely many primes p satisfying (1) the last argument itself gives the existence not only of one integer m with the required properties but even of infinitely many.

1) H.J.A. Duparc, Periodicity properties of recurring sequences I, II, Proc.Kon.Ned.Ak.v.Wet.57 (1954), 331-342, 473-485; theorem 36.

2) Loc.cit., theorem 36 (remark) and 34 (remark).