Divisibility properties in second order recurrences

By PÉTER KISS and BUI MINH PHONG (Eger)

1. Introduction

We define the generalized second order recurrences G by integers G_0, G_1 and

$$G_n = A \cdot G_{n-1} - B \cdot G_{n-2} \tag{1}$$

for $n > 1$ where A and B are fixed integers with $A \cdot B \neq 0$. We shall denote the sequence G by R if $G_0 = 0$ and $G_1 = 1$. So $R_0 = 0$, $R_1 = 1$ and

$$R_n = A \cdot R_{n-1} - B \cdot R_{n-2}$$

for $n > 1$.

Throughout this paper, the integers A and B will be fixed.

An integer $g = g(m) > 0$ is called the rank of apparition of m in the sequence G if $m | G_g$ and $m \nmid G_n$ for $0 < n < g$. In particular if $G = R$, the rank of an integer m in the sequence R is denoted by $r = r(m)$.

Note that $g(m)$ and $r(m)$ are not sure to exist for every integer m. In the following, we shall say $g(m)$ (resp. $r(m)$) exists in a sequence G if G (resp. R) has a term G_n (resp. R_n) with $m | G_n$ (resp. $m | R_n$) and $n \neq 0$.

The purpose of this paper is to study the conditions of the existence of $r(m)$ and $g(m)$ and to find connections between $g(m)$ and $r(m)$.

We improve a theorem of V. E. HOGGATT JR. and C. T. LONG [4] concerning the existence of $r(m)$ (Theorem 2.1.), furthermore we give a necessary and sufficient condition for $m | G_n$ (Theorem 3.1. and 4.1.). We give a necessary and sufficient condition for the existence of $g(m)$ in every sequence G with fixed A and B (Theorem 5.1. and Corollary 5.1.), generalizing some theorems of P. A. CATLIN [11] and D. M. BLOOM [8]. These theorems were proved only for prime m and for the case $A = -B = 1$ respectively. Furthermore we show that the solution of Fermat's Last Theorem is related to the properties of $r(m)$.

2. Preliminary results and lemmas

Let us denote the discriminant of the polynomial x^2-Ax+B by $D=A^2-4B$. It is known that $r(m)$ exists for any integer m for which $(m, B)=1$. Moreover

$$m|R_n \quad \text{if and only if} \quad r(m)|n \tag{2}$$

$$r(p)\,|\,(p-(D/p)) \tag{3}$$

$$r(p^e) = p^{e-k}\cdot r(p) \tag{4}$$

$$r(p_1^{e_1}\cdot p_2^{e_2}\dots p_t^{e_t}) = [r(p_1^{e_1}), r(p_2^{e_2}), \dots, r(p_t^{e_t})] \tag{5}$$

where p and p_i $(0<i\leqq t)$ are primes; $p\nmid B$; $p_i\nmid B$; $[a, b, \dots]$ denotes the l.c.m. of $a, b, \dots$; $e\geqq k$ and p^k is the highest power of p for which $p^k|R_{r(p)}$ (thus $r(p)=\dots$ $\dots=r(p^k)\neq r(p^{k+1})$); furthermore (D/p) is the Kronecker-symbol. (see e.g. D. H. Lehmer [1], H. J. A. Duparc [2] or J. H. Halton [3]).

First we prove the condition $(m, B)=1$ to be sufficient but not necessary for the existence of $r(m)$.

Theorem 2.1. *An integer m divides one of the terms of the sequence R different from $R_0=0$ if and only if m does not contain any prime p among its primefactors for which $p|B$ and $p\nmid A$.*

Corollary 2.1. *The rank of apparition exists in the sequence R for every integer m if $B|A$.*

Corollary 2.2. *In the case $(A, B)=1$ $r(m)$ exists if and only if $(m, B)=1$.*

Proof of Theorem 2.1. The condition is necessary. For if $p|B$ and $p\nmid A$ for one prime p and $p|R_t$ for $t>1$ then $R_t=A\cdot R_{t-1}-B\cdot R_{t-2}$ implies $p|R_{t-1}$ and this leads to $p|R_1=1$ which is a contradiction.

Now we shall show that the condition of Theorem 2.1. is sufficient. It is enough to study the case $(m, B)\neq 1$ because the statement of the theorem is well known in the case $(m, B)=1$ (see e.g. V. E. Hoggatt Jr. and C. T. Long [4]). Let $m=d\cdot m'$ where $(m', B)=1$, $d=p_1^{e_1}\dots p_s^{e_s}$ and $p_i|B$. By the conditions of the theorem $p_i|A$ for $i=1, \dots, s$. Let us consider the equation

$$R_n = \sum_{i=0}^{[(n-1)/2]} \binom{n-1-i}{i} A^{n-1-2i}(-B)^i \tag{6}$$

which was proved by V. E. Hoggatt Jr. and C. T. Long [4].

In (6) $n-1-2i+i\geqq n-1-\left[\frac{n-1}{2}\right]\geqq\left[\frac{n-1}{2}\right]$, which implies $(p_1\dots p_s)^{\left[\frac{n-1}{2}\right]}|R_n$. So $d|R_k$ for any integer k for which $\left[\frac{k-1}{2}\right]\geqq\max(e_1, \dots, e_s)$. But on account of $(m', B)=1$, there is an integer t for which $m'|R_t$. Furthermore it is known that $R_u|R_{uv}$ for any integers u and v (see e.g. P. Bundschuh and J. S. Shiue [5]), and so $R_k|R_{kt}$ and $R_t|R_{kt}$ which implies $m=d\cdot m'|R_{kt}$. This proves our statement.

We shall need some lemmas. For any integers k, n, t and for any sequences G,

Lemma 1. $G_{t+k}=R_t\cdot G_{k+1}-B\cdot R_{t-1}\cdot G_k=R_{t+1}\cdot G_k-B\cdot R_t\cdot G_{k-1}$ *or in particular*

$$R_{t+k}=R_t\cdot R_{k+1}-B\cdot R_{t-1}\cdot R_k=R_{t+1}\cdot R_k-B\cdot R_t\cdot R_{k-1}$$

and

$$G_k=R_k\cdot G_1-B\cdot R_{k-1}\cdot G_0.$$

Lemma 2. $R_{kt+1}\equiv R_{t+1}^k \pmod{R_t^2}$.

Lemma 3. $R_{kt}\equiv k\cdot R_t\cdot R_{t+1}^{k-1} \pmod{R_t^2}$.

Lemma 4. $G_{kt+n}\equiv G_n\cdot R_{t+1}^k \pmod{R_t}$.

Lemma 5. *If p is a prime, $(G_0, G_1, p)=1$ and $p|(G_{k-1}, G_k)$ then $p|(A, B)$ or $p|B$, $p|G_1$ and $p\nmid A$.*

Lemma 1. was proved by D. JARDEN [7] (p. 46).

PROOF OF LEMMA 2. We shall prove it by induction on k. The lemma is obvious for $k=1$. If the lemma is true for one integer i, then using Lemma 1. and the relation $R_t|R_{it}$

$$R_{(i+1)\cdot t+1}=R_{(it+1)+t}=R_{it+1}\cdot R_{t+1}-B\cdot R_{it}\cdot R_t\equiv$$
$$\equiv R_{it+1}\cdot R_{t+1}\equiv R_{t+1}^{i+1} \pmod{R_t^2},$$

and from this the statement follows.

PROOF OF LEMMA 3. The proof again goes by induction on k. The statement is obviously true for $k=1$. If the lemma is true for one integer i then using (1), Lemmas 1 and 2, we get

$$R_{(i+1)t}=R_{it+t}=R_{it+1}\cdot R_t-B\cdot R_{it}\cdot R_{t-1}\equiv$$
$$\equiv R_{t+1}^i\cdot R_t-B\cdot i\cdot R_t\cdot R_{t+1}^{i-1}\cdot R_{t-1}=$$
$$=R_{t+1}^{i-1}\cdot R_t\cdot(R_{t+1}-i\cdot B\cdot R_{t-1})\equiv R_{t+1}^{i-1}\cdot R_t\cdot(i+1)\cdot R_{t+1}=$$
$$=(i+1)\cdot R_t\cdot R_{t+1}^i \pmod{R_t^2}$$

which proves the statement of Lemma 3.

PROOF OF LEMMA 4. We get by Lemma 1. and Lemma 2. using the relation $R_t|R_{kt}$

$$G_{kt+n}=R_{kt+1}\cdot G_n-B\cdot R_{kt}\cdot G_{n-1}\equiv R_{kt+1}\cdot G_n\equiv G_n\cdot R_{t+1}^k \pmod{R_t}$$

which proves the lemma.

PROOF OF LEMMA 5. Let p be a prime and $p|(G_{k-1}, G_k)$. If $p\nmid B$ then (1) implies $p|G_{k-2}$ which leads to $p|G_1$ and $p|G_0$. But this contradicts the condition $(G_0, G_1, p)=1$, thus $p|B$. If $p\nmid A$ then $G_{k-1}=A\cdot G_{k-2}-B\cdot G_{k-3}$ implies $p|G_{k-2}$ for $k\geqq 3$ and this leads to $p|G_1$ (the relation $p|G_0$ does not follow because R_{-1} is not sure to exist). So $p|A$ or $p\nmid A$ and $p|G_1$.

3. Connection between $r(m)$ and $g(m)$

It is known for the sequence R that if $r(m)$ exists and $(m, B)=1$ then $m|R_n$ if and only if $r(m)|n$; furthermore we know an upper bound for $r(m)$ (see part 2). For similar questions in sequences G only sufficient conditions are known. It was mentioned in [11] by P. A. Catlin that if $m|G_g$ then $m|G_{g+k\cdot r(m)}$. In this part we show that if $g=g(m)$ exists then $m|G_n$ if and only if $n=g+k\cdot r(m)$, furthermore we give an upper bound for $g(m)$. As an application of this result we generalize a theorem of D. M. Bloom [8]. If there exist integers b and d for the sequences G and G' such that $G'_n=(-1)^d\cdot G_{n+b}$ for all n (i.e. G' can be obtained from G "by translation" together with a possible uniform sign change) then G and G' are called equivalent. By definition (1) we may extend the definition of the sequence G for negative subscripts, too. D. M. Bloom proved; if $A=-B=1$ and every positive integer divides at least one term of a sequence G, then G is equivalent ot the sequence R. We extend this theorem to general sequences.

We prove two theorems.

Theorem 3.1. *Let G be a sequence given by the integers A, B, G_0 and G_1 and let m be an integer. If $(m, B)=(G_0, G_1, m)=1$ and the sequence G has terms divisible by m (i.e. $g(m)$ exists), then $g(m)\leqq r(m)$ and $m|G_n$ if and only if $n=g(m)+k\cdot r(m)$ for one integer k.*

Corollary 3.1. *Let $m=p_1^{e_1}\cdot p_2^{e_2}\dots p_s^{e_s}$ be an integer (the p_i's are distinct primes) and $(m, B)=(G_0, G_1, m)=1$. The sequence G has terms divisible by m if and only if $g(p_i^{e_i})$ exists for $i=1, 2, \dots, s$ and the system of congruences*

$$\begin{aligned} x &\equiv g(p_1^{e_1}) \pmod{r(p_1^{e_1})} \\ x &\equiv g(p_2^{e_2}) \pmod{r(p_2^{e_2})} \\ &\vdots \\ x &\equiv g(p_s^{e_s}) \pmod{r(p_s^{e_s})} \end{aligned}$$

is solvable.

Theorem 3.2. *Let us define a sequence G by the integers A, B, G_0 and G_1, where $A>0$, $B<0$, $(A, B)=(G_0, G_1)=1$ and let the sequence G be monotone from a subscript n_0 onwards. If for any integer m $g(m)$ exists if and only if $r(m)$ does, then the sequences G and R are equivalent.*

Proof of Theorem 3.1. Let us suppose that G has term divisible by the integer m, i.e. $g=g(m)$ exists. $(m, B)=1$ so $r=r(m)$ also exists. If $g>r$ $(\geqq 2)$ then g has the form $g=tr+s$ where $0\leqq s<r$. On account of (2), Lemma 1. and Lemma 5.

$$0\equiv G_g=R_{tr}\cdot G_{s+1}-B\cdot R_{tr-1}\cdot G_s\equiv -B\cdot R_{tr-1}\cdot G_s\equiv G_s \pmod m$$

which does not contradict the definition of g only in the case $s=0$. But $s=0$ i.e. $m|G_0$ shows that the sequence G is the sequence R multiplied by G_1 modulo m and from this follows $G_r\equiv 0 \pmod m$. So $g>r$ is impossible. Thus $g\leqq r$ and $g=r$ only if $m|G_0$.

By Lemma 4. we get

$$G_{kr+g}\equiv G_g\cdot R_{r+1}^k\equiv 0 \pmod m$$

thus $m|G_n$ if $n=g+kr$. So it suffices to prove that $m|G_n$ implies $n=g+kr$. We may assume $n=g+s$ and $s>0$. By Lemma 1. we get

$$0 \equiv G_n = G_{g+s} = R_s \cdot G_{g+1} - B \cdot R_{s-1} \cdot G_g \equiv R_s \cdot G_{g+1} \pmod m,$$

and so $R_s \equiv 0 \pmod m$ since $(m, B)=1$, $m|G_g$ and Lemma 5. together imply $(m, G_{g+1})=1$. Using (2) we obtain from this $s=kr$ for one integer k, which completes the proof of Theorem 3.1.

PROOF OF COROLLARY 3.1. Now $m=p_1^{e_1}\dots p_s^{e_s}$ and $(m, B)=1$, so $r(p_i^{e_i})$ exists for $i=1, 2, \dots, s$. But $m|G_x$ implies $p_i^{e_i}|G_x$ and by Theorem 3.1. x has the form $x=g(p_i^{e_i})+k\cdot r(p_i^{e_i})$ which implies the statement.

PROOF OF THEOREM 3.2. We may assume that the terms of G are positive for positive subscripts and the sequence G is increasing. Namely, if G is decreasing, we may replace G by $-G$ (G and $-G$ are equivalent) and G may be generated by two arbitrary consecutive positive terms as initial terms G_0, G_1. The sequence R is also increasing by our conditions. So

$$g(G_t) = t \quad \text{and} \quad r(R_s) = s \tag{7}$$

for any t and s. Let G_n be an arbitrary term of G. By our conditions $G_n|G_n$ leads to $G_n|R_k$ for some integer k and this implies, using Corollary 2.2., $(G_n, B)=1$. From this follows, as in the proof of Lemma 5., $(G_0, G_1, G_n)=1$. Let us use the following notations; $r=r(G_n)$ (and so $G_n|R_r$), $g=g(R_r)$ (and so $R_r|G_g$). We get from (7) $r(R_r)=r$ and $g(G_n)=n$, furthermore using Theorem 3.1. $0<n\leqq r$, $0<g\leqq r$ and we have only one subscript i with $m|G_i$ and $0<i\leqq r(m)$. Therefore $G_n|R_r$ and $R_r|G_g$ imply $G_n|G_g$ and from this $n=g$ follows. Thus $G_n|R_r$ and $R_r|G_n$ and so $G_n=R_r$. We get similarly $G_{n+1}=R_t$ and $G_{n+2}=R_s$ for some integers t and s with $r<t<s$.

Thus $0<G_n=R_r<G_{n+1}=R_t<G_{n+2}=R_s$, and from this

$$R_{t+1} = A\cdot R_t - B\cdot R_{t-1} \geqq A\cdot R_t - B\cdot R_r = G_{n+2} = R_s$$

follows since $B<0$. But it is true only if $t+1=s$, i.e. G_{n+1} and G_{n+2} are consecutive terms of the sequence R, so that the sequences R and G are equivalent.

Remarks. a) The statement $g(m)\leqq r(m)$ in Theorem 3.1. cannot be improved in general since the sequence G may be generated by initial terms $G_0=R_k$ and $G_1=R_{k+1}$ with any integers k.

b) The condition $(G_0, G_1)=1$ in Theorem 3.2. is necessary. In fact, e.g. if $G_0=0$, $|G_1|>1$ and $(G_1, B)=1$ then $G_n=G_1\cdot R_n$ for all integers n and so the sequences G and R are not equivalent but the conditions of Theorem 3.2. hold, except $(G_0, G_1)=1$.

4. On terms of G divisible by prime powers

In part 2 we have given the condition for the existence of terms in the sequence R which are divisible by an integer m (Theorem 2.1.). This raises the following question; what is the condition for the existence of terms in G divisible by m? The question has been studied for primes p.

Let α and β be the roots of the polynomial

$$f(x) = x^2 - Ax + B.$$

It is well-known that the terms of the sequence R have the form $R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ for $\alpha \neq \beta$. M. HALL [9] has given the terms of the sequences G in a similar form; $G_n = P \cdot \alpha^n - Q \cdot \beta^n$ where $P = \frac{G_0 \cdot \beta - G_1}{\beta - \alpha}$ and $Q = \frac{G_0 \cdot \alpha - G_1}{\beta - \alpha}$, furthermore he studied the existence of $g(p)$ with help of another sequence. M. WARD [10] proved that if the ratio of α by β is not a root of unity, then the sequence G has terms divisible by p for infinitely many primes p, furthermore he proved that $g(p)$ exists if and only if the rank of p in the sequence $\frac{P^n - Q^n}{P - Q}$ is a divisor of $r(p)$.

Now, and in the next part we generalize some theorems of P. A. CATLIN [11]. He proved that if a and b are the solutions of the congruence $x^2 - Ax + B \equiv 0 \pmod{p}$, then $g(p)$ exists for every sequence G, except when $G_1 \equiv G_0 \cdot a$ and $G_1 \equiv G_0 \cdot b$ modulo p, if and only if $r(p) = p - 1$. Furthermore he proved that if $r(p) = p + 1$ then $g(p)$ exists for all sequences G regardless of initial values G_0 and G_1, and conversely. We give a condition for the existence of $g(p^n)$, and using this we extend P. A. CATLIN's theorems to the case of prime powers.

Theorem 4.1. *Let p be an odd prime, let $(p, B) = (p, G_0, G_1) = 1$ and let the sequence G have terms divisible by p (i.e. $g(p)$ exists). Furthermore let s be an integer for which $g(p) = \ldots = g(p^s) \neq g(p^{s+1})$. There are terms in G divisible by p^{s+n} for any $n > 0$ if and only if $r(p^s) \neq r(p^{s+1})$.*

Corollary 4.1. *Let p be an odd prime with $p \nmid B$ and $(p, G_0, G_1) = 1$ for a sequence G. If $g(p)$ exists and $r(p) \neq r(p^2)$ then there are terms in G divisible by p^n for any positive integer n.*

Corollary 4.2. *Let p be an odd prime. There are terms in G divisible by p^n for any integer n and for every sequence G if and only if $p \mid (A, B)$ or $r(p) = p + 1 \neq r(p^2)$.*

Corollary 4.3. *Let p be an odd prime for which $p \nmid B$ and let α and β be the roots of the congruence $x^2 - Ax + B \equiv 0 \pmod{p}$. There are terms in every sequence G, divisible by p^n for any $n > 0$, except when $G_1 \equiv \alpha \cdot G_0$ or $G_1 \equiv \beta \cdot G_0$ modulo p, if and only if $r(p) = p - 1 \neq r(p^2)$. The condition $r(p) \neq r(p^2)$ is necessary only in the case $n > 1$.*

PROOF OF THEOREM 4.1. Let p be an odd prime, $p \nmid B$, $(p, G_0, G_1) = 1$, $g(p) = \ldots$ $\ldots = g(p^s) = g$ and $r(p^s) = r$. $r(p^s)$ exists by the condition $p \nmid B$. By Theorem 3.1. $p^s \mid G_n$ if and only if $n = rx + g$ for some integer x. So if $g(p^{s+1})$ exists then it has the form $g(p^{s+1}) = rx + g$, too. By Lemmas 1, 2 and 3 we get

$$G_{rx+g} = R_{rx+1} \cdot G_g - B \cdot R_{rx} \cdot G_{g-1} \equiv$$

$$\equiv R_{r+1}^x \cdot G_g - x \cdot B \cdot G_{g-1} \cdot R_{r+1}^{x-1} \cdot R_r =$$

$$= R_{r+1}^{x-1} \cdot (G_g \cdot R_{r+1} - B \cdot R_r \cdot G_{g-1} \cdot x) \pmod{R_r^2}.$$

But $p^s|R_r$ implies $p^{s+1}|R_r^2$ and $p\nmid R_{r+1}$ ($p|R_r$ and $p|R_{r+1}$ leads to a contradiction with the conditions), therefore $p^{s+1}|G_{rx+g}$ if and only if

$$G_g \cdot R_{r+1} - B \cdot R_r \cdot G_{g-1} \cdot x \equiv 0 \pmod{p^{s+1}}. \tag{8}$$

(8) does not hold for any integers x if $p^{s+1}|R_r$ that is $r(p^s)=r(p^{s+1})$, and so the condition of Theorem 4.1. is necessary.

We prove that the condition is sufficient. If $r(p^s)\neq r(p^{s+1})$ then dividing the congruence (8) by p^s, the coefficient of x will be coprime to the modulus p, therefore (8) is soluble for x and so $g(p^{s+1})$ exists. But on account of (4) $r(p^s)\neq r(p^{s+1})$ implies $r(p^{s+n})\neq r(p^{s+n+1})$ for any integers $n>0$, therefore the condition of Theorem 4.1. is indeed sufficient.

Remark. We note that $g(p^s)\neq g(p^{s+1})$ does not always imply $r(p^s)\neq r(p^{s+1})$. For example, if $A=4$, $B=3$, $G_0=2$ and $G_1=1$ then $R=\{0, 1, 4, 13, 40, 121, \ldots\}$ and $G=\{2, 1, -2, -11, \ldots\}$. Here $g(11)=3\neq g(11^2)$ but $r(11)=r(11^2)=5$.

PROOF OF COROLLARY 4.1. It follows immediately from Theorem 4.1, since by (4) $r(p)\neq r(p^2)$ implies $r(p^n)\neq r(p^{n+1})$ for any integers $n>1$.

PROOF OF COROLLARY 4.2. If in every sequence G there are terms divisible by p^n then by Theorem 2.1. $p|(A, B)$ or $p\nmid B$.

If $p|(A, B)$ then by Lemma 1

$$G_i = R_i \cdot G_1 - B \cdot R_{i-1} \cdot G_0$$

and from this $p^n|G_i$ follows for large enough integers i (see the proof of Theorem 2.1.).

Now let us study the case $p\nmid B$. If every sequence G has terms divisible by p^n then by P. A. Catlin's theorem (see above) $r(p)=p+1$. We must yet show that $r(p)\neq r(p^2)$. For this, by Theorem 4.1., it is enough to give a sequence G for which $g(p)\neq g(p^2)$. There exists such a sequence, for example the sequence generated by the initial terms $G_0=1$, $G_1=p$ has such properties. So the first part of our statement is true.

The second part of the statement is also true. For if $r(p)=p+1\neq r(p^2)$ then $p\nmid B$ and we may assume $(p, G_0, G_1)=1$, and in this case Corollary 4.1. and P. A. Catlin's theorem imply the statement. Namely if $p|B$ then $(D/p)=1$ or 0, and this contradicts $r(p)=p+1$. Furthermore if $(p, G_0, G_1)\neq 1$ then we may examine the sequence G', for which $G_0'=\dfrac{G_0}{p^i}$, $G_1'=\dfrac{G_1}{p^i}$, instead of the sequence G where G_0' and G_1' are integers and $(G_0', G_1')=1$.

PROOF OF COROLLARY 4.3. Let $r(p)=p-1$. Then by P. A. Catlin's theorem (see above) every sequence G has terms divisible by p except when $G_1\equiv G_0\cdot\alpha$ or $G_1\equiv G_0\cdot\beta \pmod p$. In this case, by Corollary 4.1., if $r(p)\neq r(p^2)$ then the statement is true. We may use Corollary 4.1. since $p\nmid B$ and we may assume that $(p, G_0, G_1)=1$. Namely if the statement is true for the case $(p, G_0, G_1)=1$ then it is true for all cases.

Conversely, let us suppose that every sequence G has terms divisible by p^n $(n=1, 2, \dots)$ except when $G_1 \equiv G_0 \cdot \alpha$ or $G_1 \equiv G_0 \cdot \beta \pmod p$. In this case p has similar properties and so $r(p)=p-1$ (using P. A. Catlin's theorem). Now we have only to show that $r(p) \neq r(p^2)$. By Theorem 4.1. it is sufficient to find a sequence G for which $g(p) \neq g(p^2)$ and the conditions hold. The sequence G generated by $G_0=1$ and $G_1=p$ has such properties. In this sequence obviously $g(p) \neq g(p^2)$ and $G_1 \not\equiv G_0 \cdot \alpha$, $G_1 \not\equiv G_0 \cdot \beta \pmod p$ since otherwise $\alpha \equiv 0$ or $\beta \equiv 0 \pmod p$ which contradicts the condition $p \nmid B$.

5. The divisors of all sequences G

In part 4 we quoted a theorem of P. A. Catlin [11]: if p is a prime and $r(p)=p+1$ then in every sequence G there exist terms divisible by p, and conversely. D. M. Bloom [8] has studied a similar problem in the sequences G for which $A=-B=1$. He proved that all sequences S have terms divisible by an integer m if and only if $r(m)=m \cdot \prod_{p|m} \left(1+\frac{1}{p}\right)$. Here the sequence S is defined by $S_n=S_{n-1}+S_{n-2}$ with any S_0 and S_1, and in this case $r(m)$ is the rank of apparition of m in the Fibonacci sequence F $(F_0=0,\ F_1=1$ and $F_n=F_{n-1}+F_{n-2}$ for $n>1)$.

In this part we show that D. M. Bloom's theorem can be extended to general sequences G and our result includes P. A. Catlin's theorem, too. As a consequence we give all integers m for which any sequence G has terms divisible by m.

Theorem 5.1. *Let m be an integer with condition $(m, B)=1$. All sequences G with arbitrary initial values G_0 and G_1 have terms divisible by m if and only if*

$$r(m) = m \cdot \prod_{p|m} \left(1+\frac{1}{p}\right)$$

(p runs through the distinct prime divisors of m).

Corollary 5.1. *Let m be an integer, $e>1$ any integer and $(m, B)=1$. Every sequence G has terms divisible by m if and only if*

a) *$m=p$ and $r(p)=p+1$; or*

b) *$m=p^e$ and $r(p)=p+1 \neq r(p^2)$; or*

c) *$m=2p^e$, $p \neq 3$, $3 \nmid (p+1)$, $r(p)=p+1 \neq r(p^2)$ and $r(2)=3$; or*

d) *$m=2p$, $r(2)=3$, $3 \nmid (p+1)$ and $r(p)=p+1$; or*

e) *$m=2$ and $r(2)=3$; or*

f) *$m=2^e$ and $r(2^e)=2^{e-1} \cdot 3$,*

where p is any odd prime.

Proof of Theorem 5.1. Suppose that every sequence G independently of the initial values G_0 and G_1 has terms divisible by m, that is $g(m)$ and $r(m)$ exist for every sequence G. So we can replace every sequence G with another sequence which is equivalent to G and in which $m|G_0$. Let us consider only those sequences for which $(G_0, G_1)=1$. By Theorem 3.1. in these sequences $g(m)=r(m)$. Let us reduce the terms of the sequences modulo m, these reduced terms being denoted by $\overline{G}_n$, and let us consider the sequences $[0; \overline{G}_1]$, $[\overline{G}_1; \overline{G}_2]$, ..., $[\overline{G}_{r(m)-1}; 0]$. The number of pairs is $r(m)$ in every pair-sequence and $0 < \overline{G}_i < m$ for $i=1, 2, \dots, r(m)-1$ since $\overline{G}_i=0$ contradicts Theorem 3.1. Furthermore by Lemma 5, $(m, \overline{G}_j, \overline{G}_{j+1})=1$ for every integer j. It has been supposed that $(G_0, G_1)=1$ and $m|G_0$, which imply $(m, \overline{G}_1)=1$ and so we have $\varphi(m)$ distinct pair-sequences modulo m (φ denotes the Euler totient function). In a pair-sequence evidently there do not exist identical pairs. Furthermore two distinct pair-sequences have no common pair. For if $[\overline{G}'_i; \overline{G}'_{i+1}]=[\overline{G}''_k; \overline{G}''_{k+1}]$ for sequences G' and G'' then by $(m, B)=1$ we get $[\overline{G}'_{i-1}; \overline{G}'_i]=[\overline{G}''_{k-1}; \overline{G}''_k]$ that leads to $[0; \overline{G}'_1]=[\overline{G}''_{k-i}; \overline{G}''_{k-i+1}]$ and so $k=i$ that is G' and G'' cannot be distinct modulo m. This implies that we have written $r(m)\cdot\varphi(m)$ distinct pairs in the pair-sequences.

Now we show that every pair $[a; b]$ for which $(a, b, m)=1$ and $0 \leqq a, b < m$ occurs among the $r(m)\cdot\varphi(m)$ pairs. Let us consider the sequence G for which $G_0=a$ and $G_1=b$. P. Bundschuh and J. S. Shiue [6] proved that if $(m, B)=1$ then G is purely periodic modulo m and for the length $h(m)=h$ of the period $h \geqq r(m)=r$. Thus $G_h \equiv a=\overline{G}_h$ and $G_{n+1} \equiv b=\overline{G}_{h+1}$ modulo m. But G has a term divisible by m (on account of our supposition), i.e. $g(m)=g$ exists and so by Theorem 3.1., $G_{g+kr} \equiv 0 \pmod m$ for every integer k and $g \leqq r \leqq h$. From this follows that there is an integer t for which $g+tr \leqq h < h+1 \leqq g+(t+1)r$, and so the pair $[a; b]=[\overline{G}_h; \overline{G}_{h+1}]$ occurs in the pair-sequence for which the initial term is $[0; \overline{G}_{g+tr+1}]$ and here, by Lemma 5, $(m, G_{g+tr+1})=1$.

Thus the $r(m)\cdot\varphi(m)$ pairs exhaust each possibility. But D. M. Bloom [8] proved that the number of pairs $[a; b]$, for which $(a, b, m)=1$ and $0 \leqq a, b < m$, is $\varphi_2(m)=m^2\cdot \prod_{p|m}\left(1-\frac{1}{p^2}\right)$, so we get

$$r(m)\cdot\varphi(m) = m^2\cdot \prod_{p|m}\left(1-\frac{1}{p^2}\right)$$

which implies $r(m)=m\cdot \prod_{p|m}\left(1+\frac{1}{p}\right)$. This proves the first part of the statement of Theorem 5.1.

Conversely, assume that $(m, B)=1$ and $r(m)=m\cdot \prod_{p|m}\left(1+\frac{1}{p}\right)$, and let us study the sequences G for which $G_0=0$, $G_1=a$, $0<a<m$ and $(a, m)=1$ (in this case $G_n=a\cdot R_n$ for any integer n). Forming the pair-sequences modulo m from these sequences, as above, we get distinct pairs and the number of these pairs is $r(m)\cdot\varphi(m)=\varphi_2(m)$. So we got each pair $[a; b]$ in the pair-sequences. From this follows that every sequence G, for which $(G_0, G_1)=1$, is equivalent modulo m to one of the $\varphi(m)$ sequences, that is if $(G_0, G_1)=1$ then G has terms divisible by m. But if $(G_0, G_1)=d\neq 1$ then $G_n=d\cdot G'_n$ for every integer n where the sequence G' is defined by $G'_0=\frac{G_0}{d}$, $G'_1=\frac{G_1}{d}$ and on account of $(G'_0, G'_1)=1$ G' has terms divisible by m, so the sequence G has terms divisible by m, too.

Thus if $r(m)=m\cdot \prod_{p|m}\left(1+\frac{1}{p}\right)$ then every sequence G has terms divisible by m, which proves the second part of the statement of Theorem 5.1.

PROOF OF COROLLARY 5.1. If $(m, B)=1$ and $m=\prod_{i=1}^{s} p_i^{e_i}$ (the p_i's are distinct primes) then by (3), (4) and (5) we get

$$r(m)=[r(p_1^{e_1}), \dots, r(p_s^{e_s})] \leqq \prod_{i=1}^{s} p_i^{e_i-1}(p_i+1) = m \cdot \prod_{i=1}^{s}\left(1+\frac{1}{p_i}\right).$$

By Theorem 5.1. every sequence G has terms divisible by m if and only if equality holds. But equality holds if and only if $r(p_i)=p_i+1$ and $(r(p_i), r(p_j))=1$ for $1\leqq i, j\leqq s$ and $i\neq j$ furthermore $r(p_i)\neq r(p_i^2)$ for $e_i>1$. Therefore if every G has terms divisible by m then m cannot have two distinct odd prime factors. Similarly m cannot have the form $m=2^{e_0}\cdot p^e$ with $e_0>1$ or $p=3$ and $e>1$. From these the statement follows.

6. Connection between $r(p)$ and Fermat's Last Theorem

In part 5 we have seen that every sequence G has terms divisible by a power p^e of a prime p only if $r(p)\neq r(p^2)$. The study of the condition $r(p)\neq r(p^2)$ is difficult since it leads to the study of Fermat's Last Theorem, as we are going to show. We shall prove a theorem:

Theorem 6.1. *Let p be an odd prime and $(p, B)=1$. $r(p)=r(p^2)$ if and only if $p^2 | R_{p-(D/p)}$.*

Let q be an integer and let us consider the sequence R for which $A=q+1$, $B=q$. In this case the equation $x^2-Ax+B=0$ has roots $x_1=q$ and $x_2=1$ so the terms of R are

$$R_n=\frac{q^n-1}{q-1}.$$

Now $D=A^2-4B=(q-1)^2$ therefore $(D/p)=1$ for all primes p if $p\nmid(q-1)$. From this follows by Theorem 6.1. that if $p\nmid(q-1)$ then $p^2|R_{p-1}$ if and only if $r(p)=r(p^2)$ that is $q^{p-1}\equiv 1 \pmod{p^2}$ if and only if $r(p)=r(p^2)$.

On the other hand it is well known that the equation $x^p+y^p=z^p$ in case $p\nmid xyz$ has integral solution only if $q^{p-1}\equiv 1 \pmod{p^2}$ for every prime $q\leqq 43$ (this was proved by A. WIEFERICH, D. MIRIMANOFF, H. S. VANDIVER, G. FROBENIUS, F. POLLACZEK, T. MORISHIMA and J. N. ROSSER; see [12], p. 225).

Comparing the two results we get that the equation $x^p+y^p=z^p$ in case $p\nmid xyz$ has integral solution only if in the sequences R, for which $A=q+1$ and $B=q$, $r(p)=r(p^2)$ for every prime $q\leqq 43$ and $p\nmid(q-1)$.

Finally we prove Theorem 6.1.

PROOF OF THEOREM 6.1. We know that $r(p)\big|(p-(D/p))$ and so $p-(D/p)=s\cdot r(p)$ for some integer s (see (3) in part 2). By Lemma 3 we get

$$R_{s\cdot r(p)} \equiv s\cdot R_{r(p)}\cdot R_{r(p)+1}^{s-1} \pmod{R_{r(p)}^2}$$

But $p^2|R_{r(p)}^2$, $p|R_{s\cdot r(p)}$ and $(p, R_{r(p)+1})=(p, s)=1$ therefore $p^2|R_{s\cdot r(p)}=R_{p-(D/p)}$ if and only if $p^2|R_{r(p)}$, that is $r(p)=r(p^2)$.

References

[1] D. H. LEHMER, An Extended Theory of Lucas' Functions, *Ann. of Math.*, **31** (1930), 419—448
[2] H. J. A. DUPARC, Divisibility Properties of Recurring Sequences, *Doctoral thesis*, 1952.
[3] J. H. HALTON, On the Divisibility of Fibonacci Numbers, *Fibonacci Quart.*, **3** (1966), 217.
[4] V. E. HOGGATT, JR. and C. T. LONG, Divisibility Properties of Generalized Fibonacci Polynomials, *Fibonacci Quart.*, **12** (1974), 113—120.
[5] P. BUNDSCHUH and J. S. SHIUE, Solution of a Problem on the Uniform Distribution of Integers, *Atti Accad. Naz. Lincei, Rend. Cl. Sci. Fis. Mat. Nat.* Ser II, **55** (1973), 172—177.
[6] P. BUNDSCHUH and J. S. SHIUE, A Generalization of a Paper by D. D. Wall, *Atti Accad. Naz. Lincei, Rend. Cl. Sci. Fis. Mat. Nat. Ser* II, **56** (1974), 135—144.
[7] D. JARDEN, Recurring Sequences, *Riveon Lematematika, Jerusalem*, 1958.
[8] D. M. BLOOM, On Periodicity in Generalized Fibonacci Sequences, *Amer. Math. Monthly*, **72** (1965), 856—861.
[9] M. HALL, Divisor of Second Order Sequences, *Bull. Amer. Math. Soc.*, **43** (1937), 78—80.
[10] M. WARD, Prime Divisor of Second Order Recurring Sequences, *Duke Math. J.* **21** (1956), 607—614.
[11] P. A. CATLIN, On the Divisor of Second Order Recurrences, *Fibonacci Quart.*, **12** (1974), 175—178.
[12] Z. I. BOREVICH and I. R. SHAFAREVICH, Number Theory, *New York* and *London*, 1967.

(Received May 5, 1976.)