Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

# Rendiconti

Peter Bundschuh, Jau-Shyong Shiue

## A Generalization of a paper by D. D. Wall

*Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8*, Vol. **56** (1974), n.2, p. 135–144.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1974_8_56_2_135_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1974.

RENDICONTI
DELLE SEDUTE
DELLA ACCADEMIA NAZIONALE DEI LINCEI

**Classe di Scienze fisiche, matematiche e naturali**

*Seduta del 9 febbraio 1974*

*Presiede il Presidente della Classe* BENIAMINO SEGRE

## SEZIONE I

**(Matematica, meccanica, astronomia, geodesia e geofisica)**

**Teoria dei numeri.** — *A Generalization of a paper by D. D. Wall.* Nota di PETER BUNDSCHUH e JAU-SHYONG SHIUE (*), presentata (**) dal Socio B. SEGRE.

RIASSUNTO. — Vengono studiate alcune successioni che generalizzano quelle di Fibonacci modulo un intero $m \geq 2$.

In this Note we study sequences $\{G_n\}$ of the following type. Let $A, B, a, b$ be fixed rational integers, let the equation $x^2 - Ax + B = 0$ have distinct nonzero roots, which means $B \neq 0$ and $D = A^2 - 4B \neq 0$, and moreover let $a, b$ be not both equal to zero. Then let $\{G_n\}$ be defined by

$$G_0 = a \quad , \quad G_1 = b \quad , \quad G_{n+1} = AG_n - BG_{n-1} \qquad (n = 1, 2, \cdots) \tag{1}$$

and let $\{R_n\}$ denote the special sequence of $\{G_n\}$ with $a = 0, b = 1$.

Let $m \geq 2$ be a fixed natural number. In this note we are concerned with the periods of $\{G_n\}$ modulo $m$ and we generalize results proved by D. D. Wall [3] in case of Fibonacci sequences; these occur in (1) by taking $A = -B = 1$.

THEOREM 1. $\{G_n\}$ *is periodic* mod $m$, *i.e. there exists a rational integer* $h = h(a, b, m) > 0$ *such that* $G_{n+h} \equiv G_n \pmod m$ *for all* $n \geq n_0(a, b, m) \geq 0$. *Especially if* $(B, m) = 1$, *then* $\{G_n\}$ *is purely periodic* mod $m$, *which means that* $n_0(a, b, m) = 0$.

*Proof*. Consider the $m^2 + 2$ least nonnegative residues $\tilde{G}_i$ of $G_i$ mod $m$ for $0 \leq i \leq m^2 + 1$ and consider further the $m^2 + 1$ ordered pairs $(\tilde{G}_i, \tilde{G}_{i+1})$, $0 \leq i \leq m^2$. Then there exist $j, k$ with $0 \leq j < k \leq m^2$ such that $(\tilde{G}_j, \tilde{G}_{j+1}) =$

(*) This paper was written while the second Author was a Humboldt Stiftung fellow visiting University of Göttingen.

(**) Nella seduta del 9 febbraio 1974.

$= (\tilde{\tilde{G}}_k , \tilde{\tilde{G}}_{k+1})$. From the recursion formula in (1) one sees that $G_{k+t} \equiv G_{j+t}$ (mod $m$) for $t = 0, 1, 2, \cdots$, which gives

$$G_{k-j+n} \equiv G_n \pmod m \tag{2}$$

for $n \geq j$, which completes the proof of the first part of Theorem 1 and shows that $n_0(a, b, m) \leq j < m^2$, $h \mid (k-j)$ and so $h \leq m^2$.

If $(B, m) = 1$, then $G_j \equiv G_k$, $G_{j+1} \equiv G_{k+1}(m)$ imply $BG_{j-1} \equiv BG_{k-1}(m)$ and so $G_{j-1} \equiv G_{k-1}(m)$. Thus by induction we get (2) for each $n \geq 0$.

*Remark.* Take $A = 1$, $B = 2$, $m = 4$. We have that $\{R_n \pmod 4\}$ begins with $0, 1, 1, 3, 1, 3, \cdots$ This shows that $h(0, 1, 4) = 2$, $n_0(0, 1, 4) = 2$ for these A, B, and so it can in fact happen that the sequences are not purely periodic if $(B, m) \neq 1$. *From now on we assume* $(B, m) = 1$ *for the rest of this paper*, and so $\{G_n \pmod m\}$ is always purely periodic.

COROLLARY 1. *If* $a = 0$, *then* $G_{h(0,b,m)} \equiv 0 \pmod m$ *and in particular* $R_{H(m)} \equiv 0 \pmod m$, *where* $H(m) = h(0, 1, m)$ *denotes the least period of* $\{R_n \pmod m\}$.

THEOREM 2. *If m has the prime factorization* $m = \prod_{i=1}^{c} p_i^{k_i}$, *then* $h(a, b, m)$ *is the least common multiple of the* $h(a, b, p_i^{k_i})$, $1 \leq i \leq c$.

*Proof.* We refer to the proof of Theorem 2 of [3].

In virtue of this theorem, it is clear that we can assume $m$ to be a prime power. We note that if $x_1 = (A + \sqrt{D})/2$, $x_2 = (A - \sqrt{D})/2$ are the (distinct nonzero) roots of $x^2 - Ax + B = 0$, then we have $R_n = (x_1^n - x_2^n)/(x_1 - x_2)$ and we define $S_n$ by $S_n = x_1^n + x_2^n$ for $n = 0, 1, \cdots$.

The next eight theorems contain results on the least periods of the special sequences $\{R_n \pmod m\}$ under various conditions. For several proofs we need certain relations between the $R_n$'s and the $S_n$'s, which we collect in the following lemma whose proof is very simple if one uses the trivial formulas $x_1 + x_2 = A$, $x_1 x_2 = B$, $x_1 - x_2 = \sqrt{D}$.

LEMMA. *For* $n, t, j \geq 0$ *one has the relations*

$$R_{n+t} = R_{n+1} R_t - BR_n R_{t-1}, \quad \textit{where} \quad R_{-1} = -B^{-1} R_1, \tag{3}$$

$$R_{jn} = 2^{1-j} R_n (jS_n^{j-1} + KR_n^2), \tag{4}$$

$$R_{jn+1} = 2^{-j} (S_n^j + jAR_n S_n^{j-1} + LR_n^2) \tag{5}$$

(*with certain rational integers* K, L),

$$S_n = 2R_{n+1} - AR_n = R_{n+1} - BR_{n-1}, \tag{6}$$

$$S_n^2 = DR_n^2 + 4B^n, \tag{7}$$

$$R_{2n} = R_n S_n, \quad R_{2n+1} = R_{n+1}^2 - BR_n^2 = S_n R_{n+1} - B^n = R_n S_{n+1} + B^n, \tag{8}$$

$$R_{n-1} R_{n+1} - R_n^2 = -B^{n-1}, \quad S_{n-1} S_{n+1} - S_n^2 = DB^{n-1}, \tag{9}$$

$$S_{2n} = S_n^2 - 2B^n. \tag{10}$$

*Remark.* The proof of (4) is given in [1, Lemma 2] and that of (5) runs in an analogous way.

THEOREM 3. *The terms of* $\{R_n\}$ *which are divisible by* $m$, *have subscripts which are exactly the multiples of a certain natural number* $f$ *depending only on* $m$.

*Proof.* Assume $R_i \equiv R_j \equiv 0\,(m)$ with $i \geq j$, say. Then from (3) we have $R_{i+j} \equiv 0\,(m)$. On the other hand take $n + t = i$, $n = j$ in (3); we get $m \mid R_{j+1}R_{i-j}$ from which we have $R_{i-j} \equiv 0\,(m)$, since $(R_{j+1}\,, m) = 1$. Namely if we had $(R_{j+1}\,, m) = M > 1$, then $M \mid m \mid R_j$ and $M \mid R_{j+1}$ and so $M \mid R_\nu$ for each $\nu \geq j$. But we have $R_{tH(m)+1} \equiv 1$ (mod $m$) and so also (mod M) for all natural $t$. Lef $f$ be the smallest natural number with $R_f \equiv 0\,(m)$. Then, by the preceding remark on $R_{i+j}$, we have $R_{rf} \equiv 0\,(m)$ for $r = 1\,, 2\,, \cdots$. On the other hand, if there exists $n$ such that $R_n \equiv 0\,(m)$, then divide $n$ by $f$: $n = rf + g$ with $0 \leq g < f$ and the preceding result concerning $R_{i-j}$ shows $R_{n-rf} = R_g \equiv 0\,(m)$, from which we have $g = 0$ by the minimal condition of $f$.

The following theorem can be proved along the same lines.

THEOREM 4. *If in the sequence* $\{R_n\}$ *there are terms (with* $n > 0$*) being zero, then these terms have subscripts which are exactly the multiples of a certain natural number* $g$, *say.*

In the next theorem all sequences $\{R_n\}$ in dependence of A , B are determined, in which zero-terms with subscripts $> 0$ occur.

THEOREM 5. $\{R_n\}$ *has zero-terms other than* $R_0$ *if and only if exactly one of the following conditions is satisfied*: (i) $A = 0$; (ii) $B = A^2$; (iii) $2B = A^2$; (iv) $3B = A^2$ *and the* $g$ *of Theorem 4 is then* $g = 2\,, g = 3\,, g = 4\,, g = 6$ *respectively.*

*Proof.* Assume first that $\{R_n\}$ has zero-terms with subscripts $> 0$ and let $g$ be the smallest such subscript. $R_g = 0$ is equivalent to $(x_1/x_2)^g = 1$, where $x_1$ and $x_2$ denote the roots of $x^2 - Ax + B = 0$ mentioned above. Now

$$x^g - 1 = \prod_{h \mid g} \Phi_h(x)\,,$$

where the $\Phi_h$ denote the cyclotomic polynomials, which are known to be irreducible over the rational field and of exact degree $\varphi(h)$, $\varphi$ Eulers totient function. $y = x_1/x_2$ is algebraic of degree two at most and a zero of $x^g - 1$. Therefore at least one of the numbers $\Phi_h(y)$ with $h \mid g$ is zero. But if $\Phi_{g'}(y) = 0$ for a certain $g' \mid g$, $1 \leq g' < g$, then obviously $\prod_{h \mid g'} \Phi_h(y) = y^{g'} - 1 = 0$. This implies $R_{g'} = 0$ against the minimality condition of $g$. Therefore we have $\Phi_g(x_1/x_2) = 0$ and so $\Phi_g(x)$ must be of degree $\varphi(g) \leq 2$. It is easily checked that $g = 1\,, 2\,, 3\,, 4\,, 6$ are the only natural numbers satisfying this condition.

Since $\Phi_1(x_1/x_2) = (x_1 - x_2)/x_2 \neq 0$ the value $g = 1$ is impossible. $0 = \Phi_2(x_1/x_2) = (x_1 + x_2)/x_2 = A/x_2$ implies $A = 0$ and the remaining cases 3, 4, 6 for $g$ are treated in an analogous manner using the form of $\Phi_g(x)$.

By $R_2 = A$, $R_3 = A^2 - B$, $R_4 = A(A^2 - 2B)$, $R_6 = A(A^2 - B)(A^2 - 3B)$, we know that the converse is also true.

COROLLARY 2. *If* $A \neq 0$ *and* $B < 0$, *then* $R_n \neq 0$ *for all* $n > 0$. *If* $n \equiv \pm 1 \pmod 6$, *then* $R_n \neq 0$ *for all admissible* A, B.

Now we begin to study $H(m)$. The simplest result is contained in

THEOREM 6. *The order of* B mod $m$ *divides* $H(m)$.

*Proof.* Writing H for $H(m)$ the congruences $R_H \equiv 0$, $R_{H+1} \equiv 1\ (m)$ show $1 \equiv -BR_{H-1}\ (m)$, such that we have

$$R_x \equiv -B^x R_{H-x} \pmod m \tag{11}$$

for $x = 0, 1$. Assume that (11) is proved for $0 \leq x \leq y$ where $y < H$, then

$$-B^{x+1} R_{H-(x+1)} = B^x R_{H-(x-1)} - AB^x R_{H-x} \equiv -BR_{x-1} + AR_x = R_{x+1} \pmod m.$$

Thus (11) is proved for all $x$ with $0 \leq x \leq H$. Taking $x = H - y$ in (11), one gets $R_{H-y} \equiv -B^{H-y} R_y \pmod m$ and so $-B^y R_{H-y} \equiv B^H R_y \equiv R_y \pmod m$. $y = 1$ (for example) shows $B^H \equiv 1\ (m)$ giving the result.

COROLLARY 3. *If* $m > 2$ *is such that* $B \equiv -1\ (m)$, *then* $H(m)$ *is even. Especially* $H(m)$ *is even for each* $m > 2$, *if* $B = -1$.

Note that $H(m)$ can be odd in both cases $(D, m) = 1$ and $(D, m) \neq 1$. If $A = 3$, $B = 2$, $m = 7$, then $D = 1$, $(D, m) = 1$, the order of B mod $m$ is 3 and $H(m) = 3$. If $A = 1$, $B = 2$, $m = 7$, then $D = -7$, $(D, m) = 7$, the order of B mod $m$ is once more 3 and $H(m) = 21$.

THEOREM 7. *If* [1] $p \mid D$, $p > 2$, *then one has* $H(p) = 2dp$ *if* $H(p)$ *is even. If* $H(p)$ *is odd, then* $H(p) = dp$. *Here* d *denotes the exact order of* B mod $p$.

*Proof.* By $p \mid D$ we have for $\nu = 0, 1, \cdots$

$$R_{2\nu} \equiv \nu AB^{\nu-1} \quad , \quad R_{2\nu+1} \equiv (2\nu + 1) B^\nu \pmod p \tag{12}$$

the proof of which can be found in [1] in the beginning of § 3. Taking $\nu = dp$ in (12), one sees that $R_{2dp} \equiv 0$, $R_{2dp+1} \equiv 1 \pmod p$, such that $H(p) \mid 2dp$.

In virtue of $p \nmid A$ (since $p \mid D$, $p \nmid 2B$) one has from (12) that $p \mid H(p)$. Namely, if $H(p) = 2S$, then $0 \equiv R_{H(p)} \equiv SAB^{S-1}\ (p)$ and so $p \mid S$ and if $H(p) = 2S + 1$, so $0 \equiv R_{H(p)} \equiv H(p)\, B^S\ (p)$ and so once more $p \mid H(p)$. Since $d \mid (p - 1)$, we have $(d, p) = 1$ and so from Theorem 6 we know $dp \mid H(p)$. In case $H(p)$ is odd the assertion follows from this and $H(p) \mid 2dp$. In case $H(p)$ is even, 2 S say, we have from (12)

$$1 \equiv R_{H(p)+1} \equiv (H(p) + 1)\, B^S \equiv B^S \pmod p,$$

giving $d \mid S$ and so $2d \mid H(p)$, from which the other assertion of Theorem 7 can be derived.

THEOREM 8. *If* (1) $p > 2$ *and* $H(p^2) \neq H(p)$, *then* $H(p^k) = H(p)\, p^{k-1}$ *for* $k = 1, 2, \cdots$.

*Proof.* The theorem is obviously true for $k = 1$ and we make induction on $k$. Assume that the theorem is yet proved up to (and including) a certain $k \geq 1$. Denote for shortness $H(p^k) = H_k$. Since $R_{H_{k+1}} \equiv 0$, $R_{H_{k+1}+1} \equiv 1\ (p^{k+1})$ these congruences are also true mod $p^k$ such that $H_k \mid H_{k+1}$. On the other hand we have by (4) and (5), inserting $j = p$, $n = H_k$ and observing $p \neq 2$

$$R_{pH_k} \equiv 0 \quad , \quad R_{pH_k+1} \equiv (S_{H_k}/2)^p \quad (\mathrm{mod}\ p^{k+1}).$$

By (6) we have $S_{H_k} \equiv 2\,(p^k)$ and so $(S_{H_k}/2)^p \equiv 1\,(p^{k+1})$, showing that $pH_k$ is a period of $\{R_n\,(\mathrm{mod}\ p^{k+1})\}$, which means $H_{k+1} \mid pH_k$. So we have $H_{k+1} = tH_k$ with $t$ either $p$ or 1. If $k = 1$, then $t = p$ by the assumption of Theorem 8. Now let $k \geq 2$. If we had $t = 1$ or equivalently $H_{k+1} = H_k = p^{k-1} H_1 = pH_{k-1}$ (using the induction hypothesis), then from

$$R_{H_{k+1}} = R_{pH_{k-1}} \equiv 0 \quad , \quad R_{pH_{k-1}+1} \equiv 1\ (p^{k+1})$$

one would get by (4) and (5) (taking $j = p$, $n = H_{k-1}$)

$$(13) \qquad 0 \equiv R_{H_{k-1}}(pS_{H_{k-1}}^{p-1} + KR_{H_{k-1}}^2)\,(p^{k+1}),$$

$$(14) \qquad 1 \equiv (S_{H_{k-1}}/2)^p + 2^{-p}\, pAR_{H_{k-1}}\, S_{H_{k-1}}^{p-1} + 2^{-p}\, LR_{H_{k-1}}^2\,(p^{k+1}).$$

From (13) we have $p^k \mid R_{H_{k-1}} S_{H_{k-1}}^{p-1}$, since $p^{k+1} \mid p^{3k-3} \mid R_{H_{k-1}}^3$ for $k \geq 2$. Since $p \mid p^{k-1} \mid R_{H_{k-1}}$ and $p \nmid 2B$ we have from (7) that $p \nmid S_{H_{k-1}}$, such that we can conclude

$$(15) \qquad R_{H_{k-1}} \equiv 0\,(p^k).$$

Inserting this in (14) one sees that $(S_{H_{k-1}}/2)^p \equiv 1\,(p^{k+1})$. Now from Eulers criterion [2, Satz 46] we conclude that $S_{H_{k-1}} \equiv 2\,(p^k)$ and so, by (6) and (15), $R_{H_{k-1}+1} \equiv 1\,(p^k)$. This together with (15) shows that $H_k \mid H_{k-1}$, or equivalently $pH_{k-1} \mid H_{k-1}$ (by $H_k = pH_{k-1}$), and this is impossible. Therefore we have $t = p$ and $H_{k+1} = pH_k = p^k H_1$ and so the proof is complete.

*Remark.* It should be noted that Theorem 8 is in general non correct in case $p = 2$, as it is shown by the following example. Take $A = B = 1$, then $R_n$ is $0, 1, 1, 0, -1, -1, 0, 1, \cdots$ such that $H(2) = 3 \neq H(4) = 6$ and also $H(2^k) = 6$ for each $k \geq 2$.

COROLLARY 4. *If* (1) $p \mid D$, $p > 2$, *then* $H(p^k) = p^{k-1} H(p)$ *for* $k = 1, 2, \cdots$. *In case* $p = 3$, *this is only true under the extra condition* $H(9) \neq H(3)$.

(1) It should be noted that on account of the remark after Theorem 1 we assume also $(B, p) = 1$, such that instead of $p > 2$ we could have written $p \nmid 2B$.

COROLLARY 5. *If* (1) $p \mid D$, $p > 2$, *then we have* $H(p^k) = 2\,dp^k$ *for* $k = 1, 2, \cdots$ *if* $H(p)$ *is even, and* $H(p^k) = dp^k$ *if* $H(p)$ *is odd. Here* d *denotes the exact order of* B mod $p$.

*Proof of the corollaries.* From [1, Lemma 5] one knows that $p^2 \mid R_{H(p^2)}$ implies $p^2 \mid H(p^2)$ in case $p \neq 3$. If we had $H(p^2) = H(p)$, then $p^2 \mid H(p) = fdp$ (with $f$ either 1 or 2) in virtue of Theorem 7. But $p \mid d$ is impossible, and so $H(p^2) \neq H(p)$ if $p \neq 3$ and in case $p = 3$ this is true by an assumption of Corollary 4. Now Theorem 8 gives all. Note that in the example of the remark after Theorem 8 we have $D = -3$ and taking $p = 3$ we get $H(3^k) = 6$ for $k = 1, 2, \cdots$, which shows that the extra condition $H(9) \neq H(3)$ of Corollary 4 cannot be omitted. Corollary 5 follows now immediately from Theorem 7. The first part of it was stated without proof in [1] after the formulation of the main theorem.

THEOREM 9. *Let* (1) $p > 2$, $p \nmid D$ *and the Legendre-symbol* $(D/p) = 1$. *Then* $H(p) \mid (p-1)$.

*Proof.* If $x^2 - Ax + B$ has a double root $r$ mod $p$, i.e. if $x^2 - Ax + B \equiv (x-r)^2\ (p)$, then $A \equiv 2r$, $B \equiv r^2 \pmod p$ and so $p \mid D$ against an assumption. Now we have

$$4(x^2 - Ax + B) = (2x - A)^2 - D \equiv 0\ (p) \qquad \text{if and only if } (2x-A)^2 \equiv D\ (p)$$

and since $(D/p) = 1$, $p > 2$ we have in virtue of the preceding remark two mod $p$ different rational integers $y_1, y_2$ which are solutions of $x^2 - Ax + B \equiv 0\ (p)$. Obviously we have

$$(16) \qquad R_n \equiv R'_n = (y_1^n - y_2^n)/(y_1 - y_2) \pmod p$$

for $n = 0$ and $n = 1$. Now we have mod $p$

$$R_{n+1} \equiv AR'_n - BR'_{n-1} = ((Ay_1^n - By_1^{n-1}) - (Ay_2^n - By_2^{n-1}))/(y_1 - y_2) \equiv$$
$$\equiv (y_1^{n+1} - y_2^{n+1})/(y_1 - y_2) = R'_{n+1},$$

proving (16) for all $n \geq 0$. Now by Fermats theorem

$$y_i^{p-1} \equiv 1 \quad , \quad y_i^p \equiv y_i \qquad \pmod p \quad \text{for } i = 1, 2,$$

since $p \nmid y_i$ by $p \nmid B$. So we have from (16)

$$R_{p-1} \equiv 0 \quad , \quad R_p \equiv 1 \qquad \pmod p,$$

which gives the result.

THEOREM 10. *Let* $p > 2$ *and* $(D/p) = -1$. *Then* $H(p) \mid d(p+1)$, *where* d *is the exact order of* B mod $p$.

*Proof.* Note first that here we have automatically $p \nmid B$ and $p \nmid D$. By Eulers criterion [2, Satz 57] we have $-1 = (D/p) \equiv D^{(p-1)/2}\ (p)$ and so we get

$$(17) \qquad R_p \equiv -1 \quad , \quad R_{p+1} \equiv 0 \quad , \quad R_{p+2} \equiv B \quad (p).$$

Namely we have mod $p$

$$R_p \equiv 2^{p-1} R_p = \sum_{j=0}^{(p-1)/2} \binom{p}{2j+1} A^{p-2j-1} D^j \equiv D^{(p-1)/2} \equiv -1 \, ,$$

giving the first congruence in (17). The second we get from

$$2^p R_{p+1} = \sum_{j=0}^{(p-1)/2} \binom{p+1}{2j+1} A^{p-2j} D^j \equiv \sum_{j=1}^{(p-3)/2} \left(\binom{p}{2j} + \binom{p}{2j+1}\right) A^{p-2j} D^j \equiv 0 \, (p)$$

and the third follows from the recursion formula.

Applying (4) and (5) with $j = \mathrm{d}$, $n = p + 1$ gives by (17)

$$(18) \qquad R_{\mathrm{d}(p+1)} \equiv 0 \quad , \quad R_{\mathrm{d}(p+1)+1} \equiv (S_{p+1}/2)^{\mathrm{d}} \qquad (\mathrm{mod}\ p).$$

By (6) and (17) we have $S_{p+1} \equiv 2\,B\,(p)$, and so $(S_{p+1}/2)^{\mathrm{d}} \equiv B^{\mathrm{d}} \equiv 1 \ (\mathrm{mod}\ p)$, which together with (18) gives the result.

The Theorems 3 up to 10 gave information on the periods $H(m)$ of the special sequence $\{R_n \ (\mathrm{mod}\ m)\}$ under various conditions. In the next three theorems we study the connections between $H(m)$ and the periods $h(a, b, m)$ of the general sequences $\{G_n \ (\mathrm{mod}\ m)\}$.

THEOREM 11. *Let* $E = b^2 - abA + a^2 B$ *and* $(E, m) = 1$, *then* $h(a, b, m) = H(m)$. *In particular, if* $(D, m) = 1$, *then* $\{S_n \ (\mathrm{mod}\ m)\}$ *has period* $H(m)$.

*Proof.* By $G_n = bR_n - aBR_{n-1}$ (see for example [1, formula (2)]) it is clear that $h(a, b, m) \mid H(m)$. To prove the converse, let $h$ denote $h(a, b, m)$ and consider the system mod $m$

$$G_h - a = bR_h - a(1 + BR_{h-1}) \equiv 0$$

$$G_{h+1} - b = (bA - aB)\,R_h - b(1 + BR_{h-1}) \equiv 0 \, ,$$

in $R_h$, $1 + BR_{h-1}$, whose determinant is $-E$. In virtue of $(E, m) = 1$ this system has only the trivial solution

$$R_h \equiv 0 \quad , \quad BR_{h-1} \equiv -1 \ (m),$$

or equivalently $R_h \equiv 0$, $R_{h+1} \equiv 1 \ (m)$, giving $H(m) \mid h$. For $\{S_n\}$ we have $a = S_0 = 2$, $b = S_1 = A$ and so $E = -D$, from which the special case follows.

*Remark.* Note that, if $(E, m) \neq 1$, both cases $h(a, b, m) = H(m)$ and $h(a, b, m) \mid H(m)$, but $h(a, b, m) \neq H(m)$ can occur as the following example shows: Take $A = 3$, $B = -1$, $m = 9$; then $H(9) = 6$ and $h(1, 1, 9) = 6$, but $h(1, 7, 9) = 3$ (in both cases $3 \mid E$).

COROLLARY 6. *If* [(1)] $p \mid D$, $p > 2$, $p \nmid (bA - 2aB)$, *then* $h(a, b, p^k) = H(p^k)$.

*Proof*. This is Lemma 1 of [1]. Note that $4\,BE = (2\,aB - bA)^2 - Db^2$, and so under the conditions $p \mid D$, $p \nmid 2B$ we have the equivalence $(m = p^k, E) = 1$ if and only if $p \nmid (2\,aB - bA)$; and now the corollary is immediate from Theorem 11.

COROLLARY 7. *If* $p > 2$, $(D/p) = -1$, *then* $h(a, b, p^k) = H(p^k)$ *in case* $(a, b, p) = 1$.

*Proof*. We have $4E = (2b - aA)^2 - a^2 D$. Take $m = p^k$. If we had $(E, p^k) \neq 1$, then $p \mid E$ and so

$$(2b - aA)^2 \equiv a^2 D \qquad (\mathrm{mod}\ p)\,. \tag{19}$$

If $p \mid a$, then by $p \mid E$ we have $p \mid b$ and so $p \mid (a, b, p)$. So $p \nmid a$ and from (19) we see that D is a quadratic residue mod $p$ against $(D/p) = -1$. Hence $(E, p^k) = 1$ and Theorem 11 gives the assertion.

THEOREM 12. *If $m$ is odd and $a, b$ are such that $(a, b, m) = 1$, $h = h(a, b, m)$ is odd and* $B^h \equiv -1$ (mod $m$), *then* $H(m) = 2h$ *in case* $H(m)$ *is even and* $H(m) = h$ *in case* $H(m)$ *is odd.*

*Proof*. Regarding now

$$\begin{aligned} G_h - a &= R_h b - (1 + BR_{h-1})\, a \equiv 0 \\ G_{h+1} - b &= (R_{h+1} - 1)\, b - BR_h\, a \equiv 0 \end{aligned} \qquad (\mathrm{mod}\ m) \tag{20}$$

as a system in $a, b$, one has from $(a, b, m) = 1$ mod $m$

$$\begin{aligned} 0 \equiv (R_{h+1} - 1)(BR_{h-1} + 1) - BR_h^2 = B\,(R_{h+1} R_{h-1} - R_h^2) + \\ + (R_{h+1} - BR_{h-1}) - 1 = -B^h + S_h - 1 \end{aligned}$$

in virtue of (6) and (9). So $S_h \equiv 0$ (mod $m$) by assumption and $R_{2h} \equiv 0\ (m)$ by (8). Furthermore, we have by (6) and (10)

$$2\,R_{2h+1} = AR_{2h} + (R_{2h+1} - BR_{2h-1}) \equiv S_{2h} \equiv -2\,B^h \equiv 2 \qquad (\mathrm{mod}\ m)$$

and so $R_{2h} \equiv 0$, $R_{2h+1} \equiv 1$ (mod $m$), which gives $H(m) \mid 2h$. From $h \mid H(m)$ (see the beginning of the proof of Theorem 11) the result follows immediately.

The next corollary comes easily from Theorem 12 and Corollary 3.

COROLLARY 8. *If $m$ is odd and* B *such that* $B \equiv -1$ (mod $m$), *if further $a, b$ are such that $(a, b, m) = 1$ and $h(a, b, m)$ is odd, then* $H(m) = 2\,h(a, b, m)$.

THEOREM 13. *If* $(D, m) = 1$, $B \equiv -1$ (mod $m$) *and $a, b$ are such that $(a, b, m) = 1$ and $h = h(a, b, m)$ is even, then* $H(m) = h$.

*Proof.* We now write the system (20) of congruences as equations and since $B \equiv -1 \pmod m$ we obtain

$$
(21) \qquad \begin{aligned} R_h \cdot b + (R_{h-1} - 1)\, a &= \varkappa\, m \\ (R_{h+1} - 1)\, b + R_h\, a &= \lambda\, m \end{aligned}
$$

with certain rational integers $\varkappa$, $\lambda$.

First let $h/2$ be odd. Then by (8) we have

$$
R_{h+1} \equiv S_{h/2}\, R_{h/2+1} + 1 \quad , \quad R_{h-1} \equiv R_{h/2-1}\, S_{h/2} + 1 \qquad (\text{mod } m).
$$

Inserting this and $R_h = R_{h/2}\, S_{h/2}$ in (21) we get with certain rational integers $\varkappa'$, $\lambda'$

$$
(22) \qquad \begin{aligned} R_{h/2}\, b + R_{h/2-1}\, a &= \varkappa'\, m\, S_{h/2}^{-1} \\ R_{h/2+1}\, b + R_{h/2}\, a &= \lambda'\, m\, S_{h/2}^{-1} \; . \end{aligned}
$$

Now by (9) we have $R_{h/2}^2 - R_{h/2-1}\, R_{h/2+1} = B^{h/2-1} \equiv 1 \pmod m$. So from (22) we see that $m \mid a\, S_{h/2}$ and $m \mid b\, S_{h/2}$. If $m \nmid S_{h/2}$, then $m$ has a prime factor $q$ with $q \nmid S_{h/2}$, but $q \mid a$ and $q \mid b$ against our condition $(a, b, m) = 1$. So $S_{h/2} \equiv 0 \pmod m$ and by (8)

$$
R_h = R_{h/2}\, S_{h/2} \equiv 0 \quad , \quad R_{h+1} = S_{h/2}\, R_{h/2+1} - B^{h/2} \equiv 1 \qquad (\text{mod } m)
$$

and so $H(m) \mid h$.

Now let $h/2$ be even; then by (8) we have

$$
R_{h+1} \equiv R_{h/2}\, S_{h/2+1} + 1 \quad , \quad R_{h-1} \equiv R_{h/2}\, S_{h/2-1} + 1 \qquad (\text{mod } m).
$$

From (21) we get with rational integers $\varkappa''$, $\lambda''$

$$
\begin{aligned} S_{h/2}\, b + S_{h/2-1}\, a &= \varkappa''\, m\, R_{h/2}^{-1} \\ S_{h/2+1}\, b + S_{h/2}\, a &= \lambda''\, m\, R_{h/2}^{-1} \end{aligned}
$$

and by (9) we have $S_{h/2}^2 - S_{h/2-1}\, S_{h/2+1} \equiv D \pmod m$. Therefore we have $m \mid a D R_{h/2}$ and $m \mid b D R_{h/2}$, and so $m \mid a R_{h/2}$, $m \mid b R_{h/2}$ by $(D, m) = 1$. Now we have $R_{h/2} \equiv 0 \pmod m$, by an analogous reasoning as above, and so by (8)

$$
R_h = R_{h/2}\, S_{h/2} \equiv 0 \quad , \quad R_{h+1} \equiv R_{h/2}\, S_{h/2+1} + B^{h/2} \equiv 1 \qquad (\text{mod } m),
$$

giving $H(m) \mid h$ also in case $h/2$ is even. Since $h \mid H(m)$, our proof is complete.

*Remark.* It should be noted that our Theorem 13 is a generalization of Theorem 12 in [3], whose proof is however not clear to us. Furthermore, we do not need the condition that $m$ is odd as in [3]. One may ask whether in our Theorem 13 one can replace the condition $B \equiv -1 \pmod{m}$ by the weaker condition $(B, m) = 1$. The following example shows that this is not possible in general: Take $m = 9$, $A = 3$, $B = -4$, then $D = 4$ and $(D, m) = 1$, $(B, m) = 1$ is satisfied. For $a = 1$, $b = 2$ we have $(a, b, m) = 1$ and $h = h(a, b, m) = 2$. But $H(m) = 6$.

## References


[1] BUNDSCHUH P. and SHIUE J.-S., *Solution of a problem on the uniform distribution of integers*, « Atti Accad. Naz. Lincei, Rend. Cl. Sci. Fis. Mat. Natur. », *55*, 172–177 (1973).

[2] SCHOLZ A. and SCHOENEBERG B., *Einführung in die Zahlentheorie*, 3. Aufl., Berlin: de Gruyter, 1961.

[3] WALL D. D., *Fibonacci series modulo m.*, « Amer. Math. Monthly », *67*, 52–61 (1961).