Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
17 (2001), 19–24
www.emis.de/journals

MORE ON THE DISTRIBUTION OF THE FIBONACCI NUMBERS MODULO 5c

GYULA DARVASI

ABSTRACT. The Fibonacci sequence $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$ is purely periodic modulo m with $2 \leq m \in \mathbb{N}$. Take any shortest full period and form a frequency block $B_m \in \mathbb{N}^m$ to consists of the residue frequencies within any full period. The purpose of this paper is to show that such frequency blocks can nearly always be produced by repetition of some multiple of their first few elements a certain number of times. The four theorems contain our main results where we show when this repetition does occur, what elements will be repeated, what is the repetition number and how to calculate the value of the multiple.

Let $F_0 = 0$, $F_1 = 1$ and define the Fibonacci sequence $\{F_n\}$ to satisfy the recurrence relation $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. For an integer $m > 1$, the sequence $\{F_n\}$ considered modulo m is purely periodic (see [3], [15]). Define $h(m)$ to be the length of a shortest period of $\{F_n \pmod m\}$, and $S(m)$ to be the set of residue frequencies within any full period of $\{F_n \pmod m\}$ (see [11]), as well as $A(m,d)$ to denote the number of times the residue d appears in a full period of $\{F_n \pmod m\}$ (see [12]). Hence for a fixed m, the range of $A(m,d)$ is the same as the set $S(m)$, that is $\{A(m,d) | 0 \leq d < m\} = S(m)$.

We say that $\{F_n\}$ is uniformly distributed modulo m if all residues modulo m occur with the same frequency in any full period. In this case the length of any period will be a multiple of m, moreover $\|S(m)\| = 1$ and $A(m,d)$ is a constant function (see [7]). It is known that $\{F_n\}$ is uniformly distributed modulo 5^k with $k \geq 1$ and $h(5^k) = 4 \cdot 5^k$ (see [3], [9], [15]). Thus, $\|S(5^k)\| = 1$ and $A(5^k, d) = 4$.

For a fixed m form a number block $B_m \in \mathbf{N}^n$ to consist of frequency values of the residues d when d runs through the complete residue system modulo m. This number block B_m will be called the frequency block modulo m, which has properties like $(qB_m)^r = q(Bm)^r$ and $((B_m)^r)^s = (B_m)^{rs}$ with $q, r, s \in \mathbf{N}$ and $(B_m)^r =: (B_m, \ldots, B_m)$ taking B_m in the brackets r times. Here are some examples for B_m with $m \in \{2, 3, 4, 11, 10, 15, 20, 55\}$:

$$
\begin{aligned}
B_2 &= (1,2) \\
h(2) &= 3 \\
B_{10} &= (4,8,4,8,4,8,4,8,4,8) = (4B_2, 4B_2, 4B_2, 4B_2, 4B_2) = \\
&\qquad (4B_2)^5 = 4(B_2)^5 \\
h(10) &= 60 = 4 \cdot 5 \cdot h(2)
\end{aligned}
$$

2000 *Mathematics Subject Classification.* 11B39.

Key words and phrases. Second-order linear recurrences, uniform distribution.

$$\begin{aligned}
B_3 &= (2,3,3)\\
h(3) &= 8\\
B_{15} &= (2,3,3,2,3,3,2,3,3,2,3,3,2,3,3) = (B_3,B_3,B_3,B_3,B_3) =\\
&\qquad (B_3)^5\\
h(15) &= 40 = 1\cdot 5\cdot h(3)
\end{aligned}$$

$$\begin{aligned}
B_4 &= (1,3,1,1)\\
h(4) &= 6\\
B_{20} &= (2,6,2,2,2,6,2,2,2,6,2,2,2,6,2,2,2,6,2,2) =\\
&\qquad (2B_4,2B_4,2B_4,2B_4,2B_4) = (2B_4)^5 = 2(B_4)^5\\
h(20) &= 60 = 2\cdot 5\cdot h(4)
\end{aligned}$$

$$\begin{aligned}
B_{11} &= (1,3,2,1,0,1,0,0,1,0,1)\\
h(11) &= 10\\
B_{55} &= (2,3,2,1,0,2,0,0,1,0,0,0,0,2,\ldots) \neq q(B_{11})^5\\
&\qquad \text{for any } q\in\{1,2,4\}\\
h(55) &= 20 \neq q\cdot 5\cdot h(11) \text{ for any } q\in\{1,2,4\}
\end{aligned}$$

All examples except the last one show a kind of repetation in the frequency blocks for $m = 5c$ with $c \in \{2, 3, 4\}$, that means, such frequency blocks can be produced by repetition of their first few elements a whole number of times, moreover the first few repeating elements of B_m are the elements of B_c or some multiple of them. Letting $0 \le x < c$, $0 \le y < m$ and $y = x \pmod c$, this fact can be expressed by $A(m, y) = q \cdot A(c, x)$ for $q \in \{1, 2, 4\}$. A similar result in connection with the uniform distribution was found in [7] for the Fibonacci numbers. The purpose of this paper is to investigate such kind of repetition properties in the frequency block of $\{F_n \pmod 5)c\}$ with $2 \le c \in \mathbf{N}$. The questions to answer at first are when this repetition does occur and how to calculate the value of the factor q. This will be answered in our theorems, but now let's see some necessary lemmas.

Lemma 1. *Let $m, n \in \mathbf{N}$, $0 < |m - n| < h(5) = 20$ and $m = n \pmod s$ with $1 < s \mid 4$. Then $F_m \neq F_n \pmod 5$.*

Proof. The characteristic polynomial of $\{F_n\}$ is $x^2 - x - 1 = 0$, whose roots are

$$r_1 = \frac{1+\sqrt5}{2} \text{ and } r_2 = \frac{1-\sqrt5}{2}.$$

Then by the Binet equation

$$F_n = \frac{r_1^n - r_2^n}{r_1 - r_2}$$

we have

$$F_n = \frac{2^{-n}}{\sqrt5}\left(\left(1+\sqrt5\right)^n - \left(1-\sqrt5\right)^n\right) = \frac{2^{1-n}}{\sqrt5}\sum_{\substack{j\text{ odd}\\ j=1}}^{2\left[\frac{n-1}{2}\right]+1}\binom{n}{j}\sqrt5^{\,j}.$$

Let $s = 4$ and assume $m > n$, that can be done without loss of generality. From $m = n \pmod 4$ and $0 < |m - n| < 20$ results $m = n + 4t$ with $t \in \{1, 2, 3, 4\}$.

Therefore

$$F_m - F_n = \frac{2^{1-m}}{\sqrt{5}} \sum_{\substack{j \text{ odd} \\ j=1}}^{2\left[\frac{m-1}{2}\right]+1} \binom{m}{j} \sqrt{5}^j - \frac{2^{1-n}}{\sqrt{5}} \sum_{\substack{j \text{ odd} \\ j=1}}^{2\left[\frac{n-1}{2}\right]+1} \binom{n}{j} \sqrt{5}^j =$$

$$= 2^{1-n-4t} \left(\sum_{\substack{j \text{ odd} \\ j=1}}^{2\left[\frac{n+4t-1}{2}\right]+1} \binom{n+4t}{j} \sqrt{5}^{j-1} - 2^{4t} \sum_{\substack{j \text{ odd} \\ j=1}}^{2\left[\frac{n-1}{2}\right]+1} \binom{n}{j} \sqrt{5}^{j-1} \right)$$

whence

$$2^{n+4t-1}(F_m - F_n) = \left(\binom{n+4t}{1} - 2^{4t} \binom{n}{1} \right) +$$

$$+ 5 \left(\sum_{\substack{j \text{ odd} \\ j=3}}^{2\left[\frac{n+4t-1}{2}\right]+1} \binom{n+4t}{j} \sqrt{5}^{j-3} - 2^{4t} \sum_{\substack{j \text{ odd} \\ j=3}}^{2\left[\frac{n-1}{2}\right]+1} \binom{n}{j} \sqrt{5}^{j-3} \right) =$$

$$=: K + 5L,$$

where K and L are integers. Now we state that $5 \nmid K$. The reason for this is

$$K = n + 4t - 2^{4t} \cdot n = 4t - (16^t - 1)n = 4t \pmod 5$$

and $t \in \{1,2,3,4\}$. All these yield $5 \nmid (F_m - F_n)$, that is $F_m \neq F_n \pmod 5$. The remaining case $s = 2$ can be carried out in a similar way. □

We note that in this paper from now on (a, b) and $[a, b]$ will denote the greatest common divisor and the least common multiple of the integers a and b respectively.

Now let $v_5(z)$ denote the greatest power of 5 in the integer z, that means $5^{v_5(z)} \mid z$ but $5^{v_5(z)+1} \nmid z$.

Lemma 2. *For $2 \le c \in \mathbf{N}$, $(c, 5) = 1$, $v_5(h(c)) \le k - 1$ and*

$$q =: \frac{h(5^k c)}{5h(5^{k-1}c)}$$

with $0 < k \in \mathbf{N}$, we have $q \mid 4$.

Proof. Because of $(c, 5) = 1$ follows

$$q = \frac{\left[h(5^k), h(c)\right]}{5\left[h(5^{k-1}), h(c)\right]}$$

for all $0 < k \in \mathbf{N}$ (see Theorem 2 in [15]). The case $k = 1$ yields

$$q = \frac{[h(5), h(c)]}{5\,[h(1), h(c)]} = \frac{[20, h(c)]}{5h(c)} = \frac{4}{(20, h(c))} = \frac{4}{(4, h(c))},$$

since $v_5(h(c)) = 0$, that is $5 \nmid h(c)$ for $k = 1$. Hence $q \cdot (4, h(c)) = 4$, that is $q \mid 4$. The case $k > 1$ results

$$q = \frac{\left[4 \cdot 5^k, h(c)\right]}{5\left[4 \cdot 5^{k-1}, h(c)\right]} = \frac{\left(4 \cdot 5^{k-1}, h(c)\right)}{\left(4 \cdot 5^k, h(c)\right)},$$

whence $q = 1$ because of $v_5(h(c)) \le k - 1$, and therefore $q \mid 4$ is obviously true. □

Corollary 1. *For $2 \le c \in \mathbf{N}$, $(c, 5) = 1$ and $0 < k \in \mathbf{N}$,*

$$q = \frac{h(5^k c)}{5 \cdot h(5^{k-1}c)}$$

is an integer iff $v_5(h(c)) \le k - 1$.

The possible cases are as follows:

$$k = 1 \implies q = \begin{cases} 4 & \text{if } (4, h(c)) = 1 \iff h(c) \text{ is odd} \\ 2 & \text{if } (4, h(c) = 2 \iff 2 \mid h(c) \text{ but } 4 \nmid h(c) \\ 1 & \text{if } (4, h(c)) = 4 \iff 4 \mid h(c) \end{cases}$$
$$k > 1 \implies q = 1$$

Corollary 2. *For $2 \le c = 5^r \cdot s$ with $0 < r, s \in \mathbf{N}$ and $(s, 5) = 1$, we have $q = \frac{h(5c)}{5h(c)}$ is an integer iff $v_5(h(s)) \le r$.*

The only possible case is $q = 1$.

We note here that $q \in \left\{\frac{4}{5}, \frac{2}{5}, \frac{1}{5}\right\}$ for $k = 1$ and $v_5(h(c)) > 0$, moreover $q = \frac{1}{5}$ for $k > 1$ and $v_5(h(c)) > k - 1$. This happens for example for $c \in \{11, 22, 33, 44, \dots\}$.

Further on we make use of the fact that the purely periodic property of $\{F_n \pmod{c}\}$ yields the identity of the values $F_{w+jh(c)}$ modulo c for all $w, j \in \mathbf{N}$ and $2 \le c \in \mathbf{N}$.

Theorem 1. *For $2 \le c \in \mathbf{N}$, $(c, 5) = 1$, $v_5(h(c)) = 0$ and $q =: \frac{h(5c)}{5h(c)}$, we have $B_{5c} = q(B_c)^5$.*

Proof. According to Corollary 1 for $k = 1$, we have to consider the three cases when $q \in \{1, 2, 3\}$.

Case 1. $q = 1 \iff (4, h(c)) = 4$, that is $4 \mid h(c)$.

Now $h(5c)) = 5h(c)$ and it is to prove that for all $w \in \mathbf{N}$ and $j \in \{0, 1, 2, 3, 4\}$, the five values of $F_{w+jh(c)}$ are pairwise different modulo 5, and therefore also modulo $5c$. Assume that $F_{w+j_1h(c)} = F_{w+j_2h(c)} \pmod{5}$ for some $j_1, j_2 \in \{0, 1, 2, 3, 4\}$ and $0 < |j_1 - j_2| < 5$, furthermore let k_1 and k_2 denote the modulo 20 reduced values of $w + j_1h(c)$ and $w + j_2h(c)$ respectively, that is $0 \le |k_1 - k_2| = |j_1 - j_2|h(c) < 20$. This gives $F_{k_1} = F_{k_2} \pmod{5}$, since $h(5) = 20$. Now $0 < |j_1 - j_2| < 5$ and $v_5(h(c)) = 0$ yield $20 \nmid (j_1 - j_2)h(c)$ and therefore $k_1 \ne k_2$, that is $0 < |k_1 - k_2|$. From $4 \mid h(c)$ results that the values of $w + j_1h(c)$ and $w + j_2h(c)$ are in the same residue class modulo 4, and so are also k_1 and k_2. But this fact contradicts Lemma 1.

Case 2. $q = 2 \iff (4, h(c)) = 2$, that is $2 \mid h(c)$ but $4 \nmid h(c)$.

Now $h(5c) = 10h(c)$, and it is to prove that for all $w \in \mathbf{N}$ and $j \in \{0, 1, \dots, 9\}$ among the ten values of $F_{w+jh(c)}$ there are at most two identical ones modulo 5, and therefore also modulo $5c$. Assume that there are at least three identical ones modulo 5, which are say

$$F_{w+j_1h(c)},\ F_{w+j_2h(c)},\ F_{w+j_3h(c)}$$

with $j_1, j_2, j_3 \in \{0, 1, \dots, 9\}$ and $0 < |j_1 - j_2|, |j_1 - j_3|, |j_2 - j_3| < 10$. Let k_1, k_2 and k_3 denote the modulo 20 reduced values of $w + j_1h(c)$, $w + j_2h(c)$ and $w + j_3h(c)$ respectively. This yields –as in Case 1 before– that k_1, k_2 and k_3 are pairweise different, and fall in the same residue class modulo 20. This contradicts Lemma 1 again.

Case 3. $q = 4 \iff (4, h(c)) = 1$, that is $2 \nmid h(c)$.

Now $h(5c) = 20h(c)$, and it is to prove that for all $w \in \mathbf{N}$ and $j \in \{0, 1, \dots, 19\}$ among the twenty values of $F_{w+jh(c)}$ with pairwise different indices modulo 20, there are at most four identical ones modulo 5. But this fact yields immediately from the uniform distribution of the sequence $\{F_n \pmod{5}\}$. Since for $m > 2$, the range of $h(m)$ is the set of all even integers greater than 4 (see [13]), the condition $2 \nmid h(c)$ in Case 3 yields $c = 2$, and one can go on proving by a simple computation. □

Theorem 2. *For $2 \le c = 5^r \cdot s$, $0 \le r, 1 \le s \in \mathbf{N}$, $(s, 5) = 1$, $v_5(h(s)) \le r$ and $q = \frac{h(5c)}{5h(c)}$, we have $B_{5c} = q(B_c)^5$.*

Proof. We'll consider the following three cases.

Case 1. $r=0$ This gives back our Theorem 1.

Case 2. $r \geq 1$ and $s=1$ This is the well known uniform distribution. Now $q=1$ and $B_{5^{r+1}} = 1 \cdot (B_{5^r})^5$ is true (see [8],[9]).

Case 3. $r \geq 1$ and $s>1$. Now $q=1$ again, and $B_{5^{r+1} \cdot s} = 1 \cdot (B_{5^r \cdot s})^5$ is to prove. Then it's to show that for any $w \in \mathbf{N}$ and $j \in \{0,1,2,3,4\}$, the numbers $F_{w+jh(c)}$ are pairwise different modulo $5c$. Since $(s,5)=1$ and $v_5(h(s)) \leq r$, we get

$$h(c) = h(5^r \cdot s) = [h(5^r), h(s)] = h(5^r) \cdot \frac{h(s)}{(h(5^r), h(s))} = h(5^r) \cdot z$$

for some $0 < z \in \mathbf{N}$ and $5 \mid z$. Hence for any $w \in \mathbf{N}$ and $j \in \{0,1,2,3,4\}$, the values $w + jh(c)$ and $w + jh(5^r)$ are always in the same residue class modulo $h(5^r)$, therefore the numbers $F_{w+jh(c)}$ and $F_{w+jh(5^r)}$ are in the same residue class modulo 5^r too. But the numbers $F_{w+jh(5^r)}$ are pairwise different modulo 5^{r+1} because of Lemma 8 in [1], and for this reason so are the numbers $F_{w+jh(c)}$ modulo $5c$ too. □

Theorem 3. *For* $2 \leq c \in \mathbf{N}$, $(c,5)=1$, $v_5(h(c)) \leq k-1$ *and* $q = \frac{h(5^k \cdot c)}{5 \cdot h(5^{k-1} \cdot c)}$ *with* $0 < k \in \mathbf{N}$, *we have* $B_{5^k \cdot c} = q\left(B_{5^{k-1} \cdot c}\right)^5$.

Proof. We proceed by induction on k. When $k=1$, we get back to Theorem 1. Assume the statement is true for all $k>1$. Then in consequence of Case $k>1$ in Lemma 2, it is $q=1$ to take, whence

$$\begin{aligned} B_{5^{k+1} \cdot c} = B_{5(5^k \cdot c)} = 1 \cdot \left(B_{5^k \cdot c}\right)^5 = \left(q\left(B_{5^{k-1} \cdot c}\right)^5\right)^5 = \\ = q\left(\left(B_{5^{k-1} \cdot c}\right)^5\right)^5 = q\left(B_{5^k \cdot c}\right)^5 . \end{aligned}$$

□

Corollary 3. *For* $2 \leq c \in \mathbf{N}$, $(c,5)=1$, $v_5(h(c)) \leq k-1$ *and* $q = \frac{h(5^k \cdot c)}{5 \cdot h(5^{k-1} \cdot c)}$ *with* $0 < k \in \mathbf{N}$, *we have* $B_{5^k \cdot c} = q\left(B_c\right)^{5^k}$.

Proof.

$$\begin{aligned} B_{5^k \cdot c} = q\left(B_{5^{k-1} \cdot c}\right)^5 = q\left(B_{5(5^{k-2} \cdot c)}\right)^5 = q\left(B_{5^{k-2} \cdot c}\right)^{5^2} = \ldots \\ = q\left(B_{5c}\right)^{5^{k-1}} = q\left(B_c\right)^{5^k} . \end{aligned}$$

□

Corollary 4. *For* $2 \leq c \in \mathbf{N}$, $(c,5)=1$, $v_5(h(c)) \leq k-1$ *and* $q = \frac{h(5^k \cdot c)}{5 \cdot h(5^{k-1} \cdot c)} \in \{1,2,4\}$ *with* $0 < k \in \mathbf{N}$,*we have* $\|S(5^k c)\| = \|S(c)\|$.

Theorem 4. *For* $2 \leq c = 5^r \cdot s$, $0 \leq r, 1 \leq s \in \mathbf{N}$, $(s,5)=1$, $v_5(h(s)) \leq r$ *and* $q = \frac{h(5c)}{5h(c)}$, *we have* $B_{5^{r+1} \cdot s} = q(B_s)^{5^{r+1}}$.

Proof. If $r=0$, then $c=s$, and hence we get back to the case $k=1$ in Corollary 3, that means $B_{5s} = q(B_s)^5$ is true. Assume the statement is true for all integer $r \geq 1$. Then Corollary 2 yields $q=1$, and therefore

$$\begin{aligned} B_{5^{(r+1)+1} \cdot s} = B_{5(5^{r+1} \cdot s)} = 1 \cdot \left(B_{5^{r+1} \cdot s}\right)^5 = \left(q(B_s)^{5^{r+1}}\right)^5 = \\ = q\left((B_s)^{5^{r+1}}\right)^5 = q(B_s)^{5^{(r+1)+1}} \end{aligned}$$

□

Corollary 5. *For* $2 \leq c = 5^r \cdot s$, $0 \leq r$, $1 \leq s \in \mathbf{N}$, $(s,5)=1$, $v_5(h(s)) \leq r$ *and* $q = \frac{h(5c)}{5 \cdot h(c)}$, *we have* $q=1$ *and therefore* $\|S(5^{r+1} \cdot s)\| = \|S(s)\|$.

References

[1] Bundschuh, P., On the distribution of Fibonacci numbers, *Tamkang Journal of Mathematics*, Vol. 5, No. 1, 1974, 75–79.

[2] Bundschuh, P. and Shiue, J.-S., Solution of a problem on the uniform distribution of integers, *Atti della Accademia Nazionale dei Lincei*, Vol. LV (1973), 172–177.

[3] Bundschuh, P. and Shiue, J.-S., A generalization of a paper by D. D. Wall, *Atti della Accademia Nazionale dei Lincei*, Vol. LVI (1974), 135–144.

[4] Darvasi, Gy., Computerunterstützte Behandlung von Resten der Fibonacci-Folge mod $5c$, *Praxis der Mathematik*, Nr. 4, 1989, 242–244.

[5] Darvasi, Gy. and Eckmann, S., Zur Verteilung der Reste der Fibonacci-Folge modulo $5c$, *Elemente der Mathematik*, Nr. 2, 1995, 76–80.

[6] Göttsch, G., Über die mittlere Periodenlänge der Fibonacci-Folgen modulo p, Dissertation, Hannover 1982.

[7] Jacobson, E., The distribution of residues of two-term recurrence sequences, *Fibonacci Quarterly*, Aug. 1990, 227–229.

[8] Kuipers, L. and Shiue, J.-S., A distribution property of the sequence of Fibonacci numbers, *Fibonacci Quarterly*, 10, 1972, 375–376, 392.

[9] Niederreiter, H., Distribution of Fibonacci numbers mod 5^k, *Fibonacci Quarterly*, 10, 1972, 373–374.

[10] Niven, I., Uniform distribution of sequences of integers, *Trans. Amer. Math. Soc.*, 98, 1961, 52–61.

[11] Schinzel, A., Special Lucas Sequences, *Including the Fibonacci Sequence, Modulo a Prime*, A Tribute to Paul Erdős, Eds. A. Baker, B. Bollobás and A. Hajnal, Cambridge University Press 1990, 349–357.

[12] Somer, L., Distribution of Residues of Certain Second-Order Linear Recurrences Modulo p – II, *Fibonacci Quarterly*, 29, 1991, 72–78.

[13] Stanley, T. E., Some remarks on the periodicity of the sequences of Fibonacci numbers, *Fibonacci Quarterly*, 14, 1976, 52–54.

[14] Vince, A., The Fibonacci sequence modulo n, *Fibonacci Quarterly*, 16, 1978, 403–407.

[15] Wall, D. D., Fibonacci series modulo m, *Amer. Math. Monthly*, 67, 1960, 525–532.

Received September 6, 2000.

E-mail address: darvasi@zeus.nyf.hu

Department of Mathematics and Computer Science
College of Nyíregyháza
Po Box 166, Nyíregyháza,
Hungary, H-4401