ON THE PERIODS OF THE FIBONACCI SEQUENCE MODULO M

Amos Ehrlich
School of Education, Tel-Aviv University, Israel
(Submitted May 1986)

This article deals with Fibonacci's sequence

$$u_0 = 0,\ u_1 = 1,\ u_{n+2} = u_{n+1} + u_n$$

and with the arithmetical function

$K(m)$ = length of the period of Fibonacci's sequence when reduced modulo m.

In the last few years I had some occasions to guide activities in a mathematics-with-computer club for 15-year-olds, where we investigated the function $K(m)$. Theorems 1 and 2 of the present article were found (without proofs) by members of these clubs. To be more specific, these are those of the students' results, which I was not able to find in the literature either before or after they have emerged in the club. The rest of the students' discoveries can be found either in [1] or in [4]. One of these is the following lemma which was suggested by the student Oded Farago.

Lemma: For any m and n, $K([m, n]) = [K(m), K(n)]$.

Proof: Follows from [5], Lemma 13.

Theorem 2 in [1] says almost the same, but only for m and n that are relatively prime, so Oded's present version is more symmetric. (The lemma holds for every sequence that becomes periodical when reduced modulo a natural number.)

Theorem 1: For any fixed m let $\lambda_m(n) = K(m^{n+1})/K(m^n)$. Then:

I. $\lambda_m(n) \mid m$ for all n;

II. $\lambda_m(n) \mid \lambda_m(n+1)$ for all n;

III. there exists t such that $\lambda_m(n) = m$ for all $n \geq t$.

This theorem emerged from the work of four girls: Shoshi Pashkes, Sigalit Teshuva, Mali Gana, and Chenit Lotan.

Proof:

(i) If p is prime and t is the largest integer such that $K(p^t) = K(p)$, then Theorem 5 in [1] implies

$$\lambda_p(n) = \begin{cases} 1 \text{ if } 1 \leq n \leq t-1 \\ p \text{ if } n \geq t \end{cases},$$

from which I, II, and III immediately follow.

(ii) If $m = p^e$, then the conclusion follows from (i), since

$$\lambda_m(n) = \lambda_p(ne)\lambda_p(ne+1)\ \dots\ \lambda_p(ne+e-1).$$

(iii) Now let $(a, b) = 1$ and assume that the theorem holds for $m = a$ and $m = b$. By hypothesis and the lemma,

$$\lambda_a(n)\,|\,a,\ \lambda_b(n)\,|\,b,\ K(a^n b^n) = [K(a^n), K(b^n)],$$

also

$$K(a^{n+1}b^{n+1}) = [\lambda_a(n)K(a^n), \lambda_b(n)K(b^n)].$$

Let $\lambda_{ab}(n) = K(a^{n+1}b^{n+1})/K(a^n b^n)$. Then $\lambda_{ab}(n)\,|\,\lambda_a(n)\lambda_b(n)$. Thus, $\lambda_{ab}(n)\,|\,ab$.

Let p be a prime such that $p^{z_n}\|\lambda_{ab}(n)$. Then $p|ab$; without loss of generality, let $p|a$.

Let $p^{x_n}\|\lambda_a(n)$, $p^{y_n}\|K(a^n)$, $p^c\|K(b)$.

Since $p\nmid b$, by part I we have $p\nmid\lambda_b(n)$, so $p^c\|K(b^n)$ for all n. Therefore,

$$z_n = \mathrm{Max}\{x_n + y_n, c\} - \mathrm{Max}\{y_n, c\},$$

that is, $z_n = x_n$, $x_n + y_n - c$, or 0. By hypothesis, $x_n \le x_{n+1}$ and $y_n \le y_{n+1}$. Therefore, $z_n \le z_{n+1}$, so $p^{z_n}|\lambda_{ab}(n+1)$. Since p is arbitrary, we have

$$\lambda_{ab}(n)\,|\,\lambda_{ab}(n+1).$$

By hypothesis, there exists t_a such that $\lambda_a(n) = a$ for all $n \ge t_a$. Since $\lambda_a(n) = a$ means that $K(a^{n+1}) = aK(a^n)$ this implies that $y_{n+1} \ge y_n + 1$. It follows that there exists a $T > t_a$ such that for all $n \ge T$ we have $y_n > c$ and thus $z_n = x_n$.

Since, for such an n, $\lambda_a(n) = a$, it follows from $z_n = x_n$ that $p^{z_n}\|a$.

Since $p\nmid b$, it follows that, for all $n \ge T$, $p^{z_n}\|ab$.

For n sufficiently large, this holds for every prime p that divides ab; for such an n, $\lambda_{ab}(n) = ab$.

Theorem 2: For any even $i > 3$, $K(u_i) = 2i$. For any odd $i > 4$, $K(u_i) = 4i$.

Remark 1: Amihai and Moshe, the boys who found this, used different words. They said that the elements of the sequence $K(u_4)$, $K(u_5)$, $K(u_6)$, ... are, alternatively, the elements of two arithmetical sequences, one with the difference 4 and one with the difference 8.

Remark 2: The second part of Theorem 2 follows from Theorem 3 in [3].

Proof: $K(m)$ is the first i after 0 such that $u_i \equiv 0$ and $u_{i+1} \equiv 1 \pmod{m}$.

Theorem 3 in [1] says: For every m there is a d such that $u_j \equiv 0 \pmod{m}$ if and only if $d|j$.

If $m = u_i > 1$ then $d = i$, since the elements before u_i are not changed when reduced modulo u_i. [This proves that $K(u_i)$ is a multiple of i.]

For the same reason, if $i > 3$ then $u_{i-1} \not\equiv 1 \pmod{u_i}$.

Now $u_{i+1} \equiv u_{i-1} \pmod{u_i}$; therefore, if $i > 3$, then the i^{th} element of the Fibonacci sequence modulo u_i does not start a new period, instead, it starts a sequence of u_{i-1} multiples $(\text{mod } u_i)$ of the original sequence. Hence,

$$u_{2i+1} \equiv u_{2i-1} \equiv u_{i-1}^2 \pmod{u_i}.$$

For every i, $u_{i-1}^2 = u_{i-2}u_i + (-1)^i$; therefore, if i is even, then $u_{2i+1} \equiv 1 \pmod{u_i}$ and $K(u_i) = 2i$.

For odd i, $u_{2i+1} \equiv -1$; therefore, $u_{4i+1} \equiv 1$, so $u_{3i+1} \not\equiv 1$ and $K(u_i) = 4i$.

References

1. D. D. Wall. "Fibonacci Series Modulo m." *American Math. Monthly* 67 (1960):525-532.
2. S. E. Mamangakis. "Remarks on Fibonacci Series Modulo m." *American Math. Monthly* 68 (1961):648-649.
3. John Vinson. "The Relation of the Period Modulo to the Rank of Apparition of m in the Fibonacci Sequence." *Fibonacci Quarterly* 1.2 (1963):37-46.
4. T. E. Stanley. "Powers of the Period Function for the Sequence of Fibonacci Numbers." *Fibonacci Quarterly* 18.1 (1980):44-45.
5. John H. Halton. "On the Divisibility Properties of Fibonacci Numbers." *Fibonacci Quarterly* 2 (1964):217-240.

*****