FIBONACCI SEQUENCE MODULO m

A. P. SHAH
Gujarat University, Ahmedabad 9, India

Wall [1] has discussed the period k(m) of Fibonacci sequence modulo m. Here we discuss a somewhat related question of the existence of a complete residue system mod m in the Fibonacci sequence.

We say that a positive integer m is <u>defective</u> if a complete residue system mod m does not exist in the Fibonacci sequence.

It is clear that not more than k(m) distinct residues mod m can exist in the Fibonacci sequence, so that we have:

<u>Theorem 1.</u> If $k(m) < m$, then m is defective.

<u>Theorem 2.</u> If m is defective, so is every multiple of m.

<u>Proof.</u> Suppose tm is not defective. Then for every r, $0 \le r \le m - 1$, there exists a Fibonacci number u_n (which, of course, depends on r) for which $u_n \equiv r \pmod{tm}$. But then $u_n \equiv r \pmod{m}$, so that m is not defective.

Remark: The converse is not true; i.e., if m is a composite defective number, it does not follow that some proper divisor of m is defective. For example, 12 is defective, but none of 2, 3, 4 and 6 is.

<u>Theorem 3.</u> For $r \ge 3$ and m odd, $2^r m$ is defective.

<u>Proof.</u> The Fibonacci sequence (mod 8) is

$$1,\ 1,\ 2,\ 3,\ 5,\ 0,\ 5,\ 5,\ 2,\ 7,\ 1,\ 0,\ 1,\ 1,\ 2,\ 3,\ 5, \cdots .$$

The sequence is periodic and $k(8) = 12$. It is seen that the residues 4 and 6 do not occur. This proves that 8 is defective. Since for $r \ge 3$, $2^r m$ is a multiple of 8, the theorem follows from Theorem 2.

<u>Theorem 4.</u> If a prime $p \equiv \pm 1 \pmod{10}$, then p is defective.

<u>Proof.</u> For $p \equiv \pm 1 \pmod{10}$, $k(p)\ (p - 1)$ ([1]), and hence $k(p) \le p - 1 < p$. Therefore by Theorem 1, p is defective.

<u>Theorem 5.</u> If a prime $p \equiv 13$ or $17 \pmod{20}$, then p is defective.

<u>Proof.</u> Let u_n denote the n^{th} Fibonacci number. Since [1] for $p \equiv \pm 3 \pmod{10}$, $k(p) \mid 2(p + 1)$, it is clear that all the distinct residues of p that

(Received February 1967)

occur in the Fibonacci sequence are to be found in the set $\{u_1, u_2, u_3, \cdots, u_{2(p+1)}\}$. We shall prove that for each t, $1 \le t \le 2(p+1)$,

$$u_t \equiv 0 \quad \text{or} \quad u_t \equiv \pm u_r \pmod{p}, \tag{5.1}$$

for some r, where $1 \le r \le (p-1)/2$.

Granting for the moment that (5.1) has been proved, it follows that all the distinct residues of p occurring in the Fibonacci sequence are to be found in the set

$$\{0, \pm u_1, \pm u_2, \pm u_3, \cdots, \pm u_m\}, \tag{5.2}$$

where $m = (p-1)/2$; or, since $u_1 = u_2 = 1$, the set (5.2) may be replaced by

$$\{0, \pm 1, \pm u_3, \pm u_4, \cdots, \pm u_m\}. \tag{5.3}$$

But this set contains at most $2(m-1)+1 = p-2$ distinct elements. Thus the number of distinct residues of p occurring in the Fibonacci sequence is not more than $p-2$. Therefore p is defective.

Proof of (5.1). It is easily proved inductively that for $0 \le r \le p-1$,

$$u_{p-r} \equiv (-1)^{r+1} u_{r+1} \pmod{p} \tag{5.4}$$

and that for $1 \le r \le p+1$

$$u_{p+1+r} \equiv -u_r \pmod{p}. \tag{5.5}$$

We note that since $p \equiv \pm 3 \pmod{10}$, $p \mid u_{p+1}$, $u_p \equiv -1 \pmod{p}$ [2, Theorem 180]. (5.4) and (5.5) are valid for all such primes. Replacing r by $(p-1)/2 - s$ in (5.4), we get for $0 \le s \le (p-1)/2$.

$$u_{h+s} \equiv (-1)^{s+1} u_{h-s} \pmod{p}, \text{ where } h = (p+1)/2. \tag{5.6}$$

In particular, we note that $p \mid u_m$ for $m = (p+1)/2$, $p+1$, $3(p+1)/2$ and $2(p+1)$.

(5.5) and (5.6) clearly imply (5.1). This completes the proof. Combining Theorems 4 and 5, we have

Theorem 6. If a prime $p \equiv 1, 9, 11, 13, 17$ or $19 \pmod{20}$, then p is defective.

Remarks: This implies that if p is a non-defective odd prime, then $p = 5$ or $p \equiv 3$ or $7 \pmod{20}$. While it is easily seen that 2, 3, 5 and 7 are non-defective, the author has not been able to find any other non-defective primes.

From Theorems 2 and 6, we have

Theorem 7. If $n > 1$ is non-defective, then n must be of the form $n - 2^t m$, m odd, where $t = 0, 1$, or 2 and all prime divisors of m (if any) are either 5 or $\equiv 3$ or $7 \pmod{20}$. Finally, we prove

Theorem 8. If a prime $p \equiv 3$ or $7 \pmod{20}$, then a necessary and sufficient condition for p to be non-defective is that the set

$$\{0, \pm 1, \pm 3, \pm 4, \cdots, \pm u_h\} ,$$

where $h = (p + 1)/2$, is a complete residue system mod p.

Proof. The formulae (5.5) and (5.6) still remain valid. However, for primes $p \equiv 3 \pmod 4$, we cannot prove that $p | u_h$ (in fact, $p \nmid u_h$). So that all distinct residues of p occurring in the Fibonacci sequence must be found in the set

$$\{0, \pm 1, \pm u_3, \pm u_4, \cdots, \pm u_h\} .$$

Since this set contains only p numbers, it can possess all the p distinct residues of p if and only if it is a complete residue system mod p.

The author wishes to express his gratitude to Professor A. M. Vaidya for suggesting the problem and for his encouragement and help in the preparation of this note.

REFERENCES

1. D. D. Wall, "Fibonacci Series Modulo m," Amer. Math. Monthly, 67 (1960), pp. 525-532.
2. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford, 1960 (Fourth Edition).

* * * * *