ON MODULI FOR WHICH THE FIBONACCI SEQUENCE CONTAINS A COMPLETE SYSTEM OF RESIDUES

S. A. BURR
Bell Telephone Laboratories, Inc., Whippany, New Jersey

Shah [1] and Bruckner [2] have considered the problem of determining which moduli m have the property that the Fibonacci sequence $\{u_n\}$, defined in the usual way, contains a complete system of residues modulo m. Following Shah we say that m is defective if m does not have this property.

The results proved in [1] include: (I) If m is defective, so is any multiple of m; in particular, 8n is always defective. (II) if p is a prime not 2 or 5, p is defective unless $p \equiv 3$ or 7 (mod 20). (III) If p is a prime $\equiv 3$ or 7 (mod 20) and is not defective, then the set $\{0, \pm 1, \pm u_3, \pm u_4, \pm u_5, \cdots, \pm u_n\}$, where $h = (p + 1)/2$, is a complete system of residues modulo p. In [2], Bruckner settles the case of prime moduli by showing that all primes are defective except 2, 3, 5, and 7.

In this paper we complete the work of Shah and Bruckner by proving the following result, which completely characterizes all defective and nondefective moduli.

Theorem. A number m is not defective if and only if m has one of the following forms:

$$5^k, \quad 2\cdot 5^k, \quad 4\cdot 5^k,$$
$$3^j\cdot 5^k, \quad 6\cdot 5^k,$$
$$7\cdot 5^k, \quad 14\cdot 5^k,$$

where $k \geq 0$, $j \geq 1$.

Thus almost all numbers are defective. We will prove a series of lemmas, from which the theorem will follow directly. We first make some useful definitions.

We say a finite sequence of integers $(a_1, a_2, \cdots, a_r)$ is a Fibonacci cycle modulo m if it satisfies $a_i + a_{i+1} \equiv a_{i+2} \pmod m$, $i = 1, \cdots, r - 2$, as well as $a_{r-1} + a_r \equiv a_1 \pmod m$ and $a_r + a_1 \equiv a_2 \pmod m$, and furthermore $(a_1, a_2, \cdots, a_q)$ does not have these properties for any $q < r$. (As

the name implies, it is convenient to regard the cycles as circular.) We say r is the length of the cycle. For any m, we also call (km) a Fibonacci cycle modulo m of length 1. We call two Fibonacci cycles equivalent if one is congruent termwise modulo m to a cyclic permutation of the other. Finally, we define a complete Fibonacci system modulo m to be a maximal set of pairwise inequivalent Fibonacci cycles modulo m. Note that the total number of terms appearing in such a system is m^2.

The idea behind this definition is simple; it is a compact way of representing all possible Fibonacci sequences modulo m. For example, the following are complete Fibonacci systems modulo 2, 3, 4, and 5, respectively:

$\{(0, 1, 1), (0)\}$,

$\{(0, 1, 1, 2, 0, 2, 2, 1), (0)\}$,

$\{0, 1, 1, 2, 3, 1), (0, 3, 3, 2, 1, 3), (0, 2, 2), (0)\}$,

$\{(0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1), (1, 3, 4, 2), (0)\}$.

For larger m the structure of these systems can become quite intricate and is worthy of study in itself. We will not undertake such a study here. Instead, we will proceed to the lemmas. The first lemma gives another proof of the result of Bruckner; it is included to illustrate the above ideas..

Lemma 1. If p is a prime which is not defective, then p = 2, 3, 4, or 7.

Proof. Assume the contrary, and let $p > 7$ be a nondefective prime. Then $p \equiv 3$ or 7 (mod 20), and (III) holds. From this it is easily seen either directly or from (5.5) and (5.6) of [1] that

$$C_1 = (0, 1, 1, \cdots, u_{h-2}, u_{n-1}, u_h, -u_{h-1}, u_{h-2}, \cdots, 1, -1,$$
$$0, -1, -1, \cdots, -u_{h-2}, -u_{h-1}, -u_h, u_{h-1}, -u_{h-2}, \cdots, -1, 1)$$

is a Fibonacci cycle of length $2p + 2$ modulo p.

Let C_k, $k = 1, \cdots, (p - 1)/2$, be the finite sequence formed by multiplying the terms of C_1 by k. Clearly each C_k is a Fibonacci cycle modulo p. But they are all inequivalent, since C_j equivalent to C_k implies

$j \equiv \pm k \pmod{p}$, which implies $j = k$. Since all the $(p - 1)/2$ sequences C_k are inequivalent, the set

$$\{C_1, \cdots, C_{(p-1)/2}, (0)\}$$

is a complete Fibonacci system (modulo p) because the total number of terms appearing is

$$\frac{p - 1}{2} \cdot (2p + 2) + 1 = p^2 .$$

Consider the finite sequence of integers 5, -2, 3, 1, 4, 5. This satisfies the Fibonacci difference equation, and hence must be congruent term-by-term to a portion of some C_k (possibly wrapped end around). Thus some C_k has two congruent terms five steps apart. Therefore, multiplying each term by the inverse of k, we see that C_1 has two congruent terms five steps apart. But examination of the definition of C_1 shows that this implies that for some $3 \leq j \leq h$ either $u_j \equiv \pm 1 \pmod{p}$ or $u_j \equiv \pm u_k \pmod{p}$ for some $k \neq j$, $3 \leq k \leq h$. (Note that here we have used $p > 7$.) But this contradicts (III), so the lemma is proved.

By property (I) it suffices to consider moduli divisible only by 2, 3, 5, and 7. We first deal with the powers of 3.

Lemma 2. No power of three is deficient.

Proof. We begin by determining a complete Fibonacci system modulo 3^n. It is well known that the rank and period of 3^n are $4 \cdot 3^{n-1}$ and $8 \cdot 3^{n-1}$ respectively. That is, the smallest $m > 0$ for which $3^n \mid u_m$ is $4 \cdot 3^{n-1}$, and for all m,

$$u_m \equiv u_{m+8\cdot 3^{n-1}} \pmod{3^n} .$$

Thus

$$C = (0, 1, 1, 2, \cdots, u_{8\cdot 3^{n-1}})$$

is a Fibonacci cycle modulo 3^n. But it is easily from the above facts that

$$u_{4\cdot 3^{n-1}+1} \equiv -1 \pmod{3^n},$$

so that

$$C_1 = \left(0, 1, 1, 2, \cdots, 0, -1, -1, -2, \cdots, u_{8\cdot 3^{n-1}-1}\right)$$

is an equivalent Fibonacci cycle.

For each integer k prime to 3 in the range $0 < k < \frac{1}{2}\cdot 3^n$, let C_k be the sequence formed by multiplying each term of C_1 by k. As in the previous lemma, the C_k are all inequivalent Fibonacci cycles. The total number of such C_k is $\frac{1}{2}\phi(3^n) = 3^{n-1}$, where ϕ is the Euler function. Hence, the total number of terms appearing in the C_k is $8 \cdot 3^{m-2}$. Consider also the sequences formed by multiplying by 3 every term of a complete Fibonacci system modulo 3^{n-1}. This clearly forms a set of inequivalent Fibonacci cycles modulo 3^n, and the total number of terms appearing in the cycles is 3^{2n-2}. Furthermore, none of these cycles is equivalent to any C_k. Therefore, these cycles, together with the C_k, form a complete Fibonacci system modulo 3^n, since the total number of terms is then

$$8\cdot 3^{2n-2} + 3^{2n-2} = 3^{2n}.$$

It is well known that the expression $\left|a^2 + ab - b^2\right|$, where a and b are two consecutive terms of a sequence satisfying the Fibonacci difference equation, is an invariant of the sequence. Consequently, an invariant of any such sequence modulo m is the pair of residue classes corresponding to $\pm(a^2 + ab - b^2)$, and the same applies to Fibonacci cycles.

We now show that any Fibonacci cycle modulo 3^n with invariant corresponding to ± 1 is equivalent to C_1. Certainly such a cycle must be equivalent to some C_k, since the invariants of the other cycle are divisible by 3. Such a C_k must satisfy $k^2 \equiv \pm 1 \pmod{3^n}$. But

$$k^2 \equiv -1 \pmod{3^n}$$

is impossible, so $(k + 1)(k - 1) \equiv 0 \pmod{3^n}$, so that $k = 1$ and the cycle is equivalent to C_1.

From this, we see that the lemma will be proved if it can be shown that for any a there is a b such that

$$a^2 + ab - b^2 \equiv \pm 1 \pmod{3^n}.$$

In fact, we will even show this for

$$a^2 + ab - b^2 \equiv -1.$$

This is obvious for $n = 1$. Now suppose the above to have been proved for some value $n \geq 1$, and let b be such that

$$a^2 + ab - b^2 \equiv -1 \pmod{3^n},$$

let

$$a^2 + ab - b^2 = A \cdot 3^n - 1.$$

We will determine an $x = 3^n t + b$ such that

$$a^2 + ax - x^2 \equiv -1 \pmod{3^{n+1}}.$$

We have

$$\begin{aligned} a^2 + ax - x^2 &\equiv a^2 + 3^n at + ab + 2 \cdot 3^n bt + b^2 \\ &\equiv 3^n(a + 2b)t + (a^2 + ab - b^2) \\ &\equiv 3^n(a + 2b)t + 3^n A - 1 \pmod{3^{n+1}}. \end{aligned}$$

Thus x will have the desired property if

$$(a + 2b)t + A \equiv 0 \pmod{3}.$$

But $3 \nmid a + 2b$, for otherwise $a \equiv b$, and

$$a^2 \equiv a^2 + ab - b^2 \equiv -1 \pmod 3 ,$$

which is impossible. Therefore, the above congruence has a solution and the lemma is proved.

We now consider the effect of the prime 5. We will prove a general lemma which is of some interest in itself.

Lemma 3. Suppose that the Fibonacci sequence $\{u_n\}$ has period k modulo m, and that it has period 5k modulo 5m. For some n and a let $u_n \equiv a \pmod m$. Then $u_n, u_{k+n}, \cdots, u_{4k+n}$ are congruent to a, m + a, $\cdots$, 4m + a (mod 5m) in some order.

Proof. We consider two cases, depending on whether or not $5 \mid m$. We first assume $5 \nmid m$. Then the period of 5m is the g. c. d. of k and the period of 5, which is 20. Since this period is to equal 5k, we have $k \equiv 4, 8, 12, 16 \pmod{20}$. Now, a cycle modulo 5 which corresponds to the standard Fibonacci sequence is

$$(0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1).$$

From this it may be verified that $u_n, u_{k+n}, \cdots, u_{4k+n}$ are congruent modulo 5 to 0, 1, 2, 3, 4 in some order. For instance, if $n \equiv 0 \pmod{20}$ they are congruent respectively to 9, 3, 1, 4, 2. Since each of these is congruent to a modulo m, they are congruent in some order to a, m + a, $\cdots$, 4m + a. This completes the first case.

We now assume $5 \mid m$. Since the Fibonacci sequence has period k modulo m, $u_n, u_{k+n}, \cdots, u_{4k+n}$ are all congruent to a modulo m and hence are each congruent to im + a modulo 5m for some choice of $0 \le i \le 4$. Our object is to show that the value of i is different for each of the five terms. Set $u_{n+1} \equiv b \pmod m$. Then $u_{n+1}, u_{m+n+1}, \cdots, u_{4m+n+1}$ are each congruent to jm + b for some $0 \le j \le 4$. Speaking in terms of the concept we have defined, there are 25 pairs congruent modulo 5m to (im + a, jm + b) appearing within a complete Fibonacci system modulo 5m, of which 5 appear in the cycle corresponding to the standard Fibonacci sequence. Our object is to show that each of these 5 gives a different value of i.

Since

$$a^2 + ab - b^2 \equiv \pm 1 \pmod{m},$$

we may set

$$a^2 + ab - b^2 = mA \pm 1.$$

Applying this same invariant to the pair $(im + n,\ jm + b)$, we have

$$\begin{aligned}(im + a)^2 &+ (im + a)(jm + b) - (jm + b)^2 \\ &= i^2m^2 + ijm^2 - j^2m^2 + ((2a + b)i + (a - 2b)j)m + a^2 + ab - b^2 \\ &= m^2(i^2 + ij - j^2) + m((2a + b)i + (a - 2b)j) + mA \pm 1.\end{aligned}$$

This last expression will be congruent to ± 1 (modulo $5m$) if and only if

$$(2a + b)i + (a - 2b)j + A \equiv 0 \pmod{5}.$$

However, $2a + b \not\equiv 0 \pmod{5}$ since otherwise

$$\pm 1 \equiv a^2 - ab - b^2 \equiv a^2 - 2a^2 - 4a^2 \equiv 0 \pmod{5};$$

similarly $a - 2b \not\equiv 0 \pmod{5}$.

Consequently, for each of the 5 possible choices of i, there is exactly one j satisfying the above congruence. Hence only these 5 pairs could appear as consecutive pairs in the Fibonacci sequence. Since i is different in each case, the lemma is proved.

We now deal with the other primes, and combinations thereof.

Lemma 4. The numbers 8, 12, 18, 21, 28, and 49 are deficient; the numbers 4, 6, 14, and 20 are nondeficient.

Proof. The arithmetic involved in verifying these facts is left to the reader.

We now can easily prove the main result.

Proof of Theorem. Lemmas 1 and 4, along with (I), show that the numbers of the theorem are the only possible nondeficient numbers. All numbers 3^j are nondeficient by Lemma 2. Furthermore, the periods of 6, 14, 20,

and 30 are 24, 48, 60, and $8 \cdot 3^{j-1}$, respectively, so that by Lemma 3, all numbers $6 \cdot 5^k$, $14 \cdot 5^k$, $20 \cdot 5^k$, $3^j \cdot 5^k$ are all nondeficient. Applying (I) again we see that all numbers of the theorem are nondeficient. Thus, the theorem is proved.

It would be interesting to extend this work by considering more generally the problem of characterizing, at least partially, the residue classes that appear in the Fibonacci sequence with respect to a general modulus, as well as their multiplicities. A small start on this large problem has been made by [1], [2], and the present work, especially Lemma 3. Also of interest, both as an aid to the above and for itself, would be a systematic study of complete Fibonacci systems, whose structure can be quite complicated. In particular, it would be useful to know the set of lengths and multiplicities of the cycles. Considerable information, especially for prime moduli, bearing on this problem exists in various places; see for instance [3], [4]. Of course, these problems can be generalized to sequences satisfying other recurrence relations.

REFERENCES

1. A. P. Shah, "Fibonacci Sequence Modulo m," Fibonacci Quarterly, Vol. 6, 1968, pp. 139-141.
2. G. Bruckner, "Fibonacci Sequence Modulo A Prime $p \equiv 3 \pmod 4$," Fibonacci Quarterly, Vol. 8, 1970, pp. 217-220.
3. D. D. Wall, "Fibonacci Series Modulo m," Amer. Math Monthly, Vol. 67, 1960, pp. 525-532.
4. D. M. Bloom, "On Periodicity in Generalized Fibonacci Sequences," Amer. Math. Monthly, Vol. 72, 1965, pp. 856-861.

NINTH ANNUAL FALL CONFERENCE OF THE FIBONACCI ASSOCIATION

Nov. 13, 1971 COLLEGE OF THE HOLY NAMES, Oakland, California

Morning Session

A Triangle for the Fibonacci Powers
Charles Pasma, San Jose State College, San Jose, California
On the Number of Primitive Solutions of $x^2 - xy - y^2 = a$ in Positive Relatively Prime Integers, Professor V. E. Hoggatt, Jr., San Jose State College
Free Discussion Period

[Continued on page 526.]