FIBONACCI SEQUENCES MODULO M

AGNES ANDREASSIAN
American University of Bierut, Bierut, Lebanon

Most of the questions concerning the length of the period of the recurring sequence obtained by reducing a general Fibonacci sequence by a modulus m have been answered by D. D. Wall [1]. The problem discussed in this paper is to determine the number of ordered pairs (a, b) with $0 \leq a < m$ and $0 \leq b < m$ that produce these various possible lengths.

The results that have been used in this study are summarized below. The proofs of these theorems are omitted here except for "Theorem 12" whose proof in [1] is incorrect. The outline of a correct proof of "Theorem 12" was proposed by D. D. Wall in answer to a letter sent to him asking for clarification.

SUMMARY OF KNOWN RESULTS

Using the notation in [1], let f_n denote the n^{th} term of the Fibonacci sequence where $f_0 = a$, $f_1 = b$, and $f_{n+1} = f_n + f_{n-1}$. Let $h = h(a,b,m)$ denote the length of the period of this sequence when it is reduced modulo m, taking least non-negative residues. When h does not depend on a and b we may write $h = h(m)$ instead. The special Fibonacci sequence which starts with the pair (0, 1) will be denoted by $\{u_n\}$ and its period when reduced modulo m by k(m). The sequence which starts with (2, 1) will be denoted by $\{v_n\}$. The letter p will be used to denote a prime and e a positive integer. In studying the possible values of h(a, b, m) we may assume, without any loss of generality, that $(a,b,m) = 1$.

1. If

$$m = \Pi p_i^{e_i} \quad \text{and} \quad h\left(a,\ b,\ p_i^{e_i}\right) = h_i\ ,$$

then $h(a,b,m) = \text{LCM}[h_i]$ [1, Theorem 2].

2. If t is the largest integer such that $k(p^t) = k(p)$ then $k(p^e) = p^{e-t}k(p)$ for $e \geq t$ [1, Theorem 5].

Remark. The proof of this theorem as given in [1] is rather incomplete. It is possible to give a complete proof by using induction on e as suggested, but a much neater proof for the case when p is an odd prime is given by Robinson [2], by the use of matrix algebra.

For $p = 2$, Robinson's proof that $k(p^{e+1})$ is either $k(p^e)$ or $pk(p^e)$ still holds, and the proof that shows that if $k(p^{e+1}) = pk(p^e)$, then $k(p^{e+2}) = pk(p^{e+1})$ is still applicable for $e > 1$. The case $p = 2$ and $e = 1$ is verified by direct computations since we have $k(2) = 3$, $k(2^2) = 6$, and $k(2^3) = 12$.

In particular, if $k(p^2) \neq k(p)$, we obtain $k(p^e) = p^{e-1}k(p)$. In [3] Mamangakis has shown that (1) if c and p are relatively prime and cp occurs in $\{u_n\}$, then $k(p^2) \neq k(p)$, and (2) if c and p are relatively prime, $e \leq d$, and $u_j = cp^d$ is the first multiple of p to occur in $\{u_n\}$, then $k(p^e) = k(p)$ if and only if u_{j-1} has the same order mod p and mod p^e. For all p up to 10,000 it has been shown that $k(p^2) \neq k(p)$. However, it has not yet been proved that $k(p^2) = k(p)$ is impossible.

3. If $m > 2$, then $k(m)$ is even [1, Theorem 4].

4. If $(b^2 - ab - a^2, p^e) = 1$, then $h(p^e) = k(p^e)$ [1, Corollary to Theorem 8].

5. If $p \equiv \pm 3 \pmod{10}$, then $h(p^e) = k(p^e)$ [1, Theorem 8].

6. $h(2^e) = k(2^e)$ [1, Theorem 9].

7. If $b^2 - ab - a^2 \not\equiv 0 \pmod 5$, then $h(5^e) = k(5^e)$; and if $b^2 - ab - a^2 \equiv 0 \pmod 5$, then $h(5^e) = (1/5)k(5^e)$ [1, Theorem 9].

8. If $m = p^e$, $p > 2$, and if there is a pair (a,b) which gives $h(a,b,p^e) = 2t + 1$, then $k(p^e) = 4t + 2$ [1, Theorem 10].

9. If $m = p^e$, $p > 2$, and if $k(p^e) = 4t + 2$ then $h(a,b,p^e) = 2t + 1$ for some pair (a,b) [1, Theorem 11].

10. If $m = p^e$, $p > 2$, $p \neq 5$, and h is even, then $h(p^e) = k(p^e)$ [1, Theorem 12].

Proof. Since $f_h = u_{h-1}a + u_h b$, we have

$$f_h - a = bu_h + a(u_{h-1} - 1) \equiv 0 \pmod{p^e}; \tag{1}$$

$$f_{h+1} - b = b(u_{h+1} - 1) + au_h \equiv 0 \pmod{p^e}. \tag{2}$$

Since we are assuming that $(a,b,p^e) = 1$, considering a and b as the unknowns, the determinant must be zero. Hence $u_h^2 - (u_{h+1} - 1)(u_{h-1} - 1) \equiv 0 \pmod{p^e}$. But it is known that $u_h^2 - u_{h+1}u_{h-1} = (-1)^{h-1}$, and so $u_{h+1} + u_{h-1} \equiv 1 + (-1)^h \pmod{p^e}$. Since h is even and $u_{h+1} = u_h + u_{h-1}$, this gives $2u_{h-1} + u_h \equiv 2 \pmod{p^e}$, or $u_h \equiv 2(1 - u_{h-1}) \pmod{p^e}$. It has been shown that if $b^2 - ab - a^2 \not\equiv 0 \pmod p$ we obtain the unique solution $u_h \equiv 0$ and $u_{h-1} \equiv 1 \pmod{p^e}$, and so $h(p^e) = k(p^e)$. Next consider the cases for which $b^2 - ab - a^2 \equiv 0 \pmod p$. Since $u_h \equiv 2(1 - u_{h-1}) \pmod{p^e}$, substituting in (1) we obtain

$$2b(1 - u_{h-1}) + a(u_{h-1} - 1) \equiv 0 \pmod{p^e}, \quad \text{or} \quad (2b - a)(1 - u_{h-1}) \equiv 0 \pmod{p^e}.$$

We will show that $(2b - a, p^e) = 1$. The condition $b^2 - ab - a^2 \equiv 0 \pmod p$ can be written in the equivalent form $(2b - a)^2 \equiv 5a^2 \pmod p$. Now if $p \mid (2b - a)$, then $p \mid 5a^2$; but $p \neq 5$, hence $p \mid a$. Therefore $p \mid 2b$, and since $p > 2$, $p \mid b$. Thus $(a,b,p^e) \neq 1$ contrary to assumption. Hence $p \nmid (2b - a)$, and so we may cancel $2b - a$ from the above congruence obtaining $1 - u_{h-1} \equiv 0 \pmod{p^e}$, or $u_{h-1} \equiv 1 \pmod{p^e}$. Since $u_h \equiv 2(1 - u_{h-1}) \pmod{p^e}$, this implies that $u_h \equiv 0 \pmod{p^e}$, and so again $h(p^e) = k(p^e)$.

11. If $h(a,b,p) = k(p)$, then $h(a,b,p^e) = k(p^e)$ [1, Corollary 2 to Theorem 12].

12. Let $f(m)$ denote the smallest positive integer, n, for which $u_n \equiv 0 \pmod m$, and let p be an odd prime. If $2/f(p)$, then $k(p^e) = 4f(p^e)$ [4].

THE PROBLEM

For any given modulus m, there are m^2 possible ordered pairs in sequence. Of these m^2 ordered pairs we would like to determine the number of pairs corresponding to each of the various possible lengths for that modulus. For example, if $m = 7$ we obtain

$0, 0, \cdots$	length 1	(1 pair)
$0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, \cdots$	length 16	(16 pairs)
$0, 2, 2, 4, 6, 3, 2, 5, 0, 5, 5, 3, 1, 4, 5, 2, 0, \cdots$	length 16	(16 pairs)
$0, 3, 3, 6, 2, 1, 3, 4, 0, 4, 4, 1, 5, 6, 4, 3, 0, \cdots$	length 16	(16 pairs)

Hence 1 pair produces a sequence of length 1 and 48 pairs produce sequences of length 16. Viewing these as infinite sequences extending to the right as well as to the left, some of these sequences become indistinguishable. Thus instead of number of pairs it is convenient to talk about number of distinct sequences of a given length. In the above example, there is 1 distinct sequence of length 1 and there are 3 distinct sequences of length 16.

Let $n(h,m)$ denote the number of distinct sequences of length h when the sequence is reduced mod m. This will be abbreviated to $n(h)$ when it is clear what modulus is used. Thus the problem is to determine the values of $n(h)$ corresponding to the various possible values of h for any given modulus m.

Since the results summarized from [1] hold when $(a,b,p^e) = 1$, we must consider what happens when $(a,b,p^e) \neq 1$. When $m = p$, there is only one pair, namely $(0,0)$, with $(a,b,p) \neq 1$ and it produces a sequence of length 1. When $m = p^2$, then sequences for which $(a,b,p^e) = 1$ are all the sequences for mod p multiplied throughout by p. When $m = p^3$, the sequences for which $(a,b,p^3) \neq 1$ are all the sequences for mod p^2 multiplied throughout by p. Thus, in general when $m = p^e$ we can trace back all the sequences except the one arising from $(0,0)$ to pairs for mod $p^e, p^{e-1}, p^{e-2}, \cdots, p$ where the condition of being relatively prime holds. The pair $(0,0)$ will always have length 1 no matter what the modulus is.

We shall henceforth abbreviate $k(p)$ as k.

Theorem 1. Let $m = p^e$ where $p = 2$ or $p \equiv \pm 3 \pmod{10}$. If $k(p^2) \neq k(p)$ then $n(1) = 1$ and

$$n(p^i k) = \frac{p^i(p^2 - 1)}{k}$$

for $i = 0, 1, \cdots, e - 1$.

Proof. By 5 and 6, if $p = 2$ or $p \equiv \pm 3 \pmod{10}$ and if $(a,b,p^e) = 1$, then $h(a,b,p^e) = k(p^e)$. If $(a,b,p^e) \neq 1$, then we still have $h(a,b,p^e) | k(p^e)$. Since $k(p^e) = p^{e-1}k$, the possible values of $h(a,b,p^e)$ are $1, k, pk, p^2k, \cdots, p^{e-1}k$. We know that there is always one sequence of length 1, namely when $a = 0$ and $b = 0$. Thus $n(1) = 1$. We will show that all of the $n(p^{e-1}k)$ sequences come from cases where $(a,b,p^e) = 1$. We know that the sequences for which $(a,b,p^e) \neq 1$ are the same sequences as for mod p^{e-1} multiplied throughout by p, and these sequences have the same lengths as the corresponding sequences for mod p^{e-1}. Since none of the sequences for mod p^{e-1} has a length greater than $k(p^{e-1}) = p^{e-2}k$, no sequence for which $(a, b, p^e) \neq 1$ can have a length of $p^{e-1}k$. Moreover, all the sequences for which $(a, b, p^e) = 1$ have lengths of $p^{e-1}k$ and so are included in $n(p^{e-1}k)$.

Since $\sum n(h_i)\cdot h_i = m^2$ where h_i are the different possible lengths, we must have

$$1 + \sum_{i=0}^{e-1} n(p^i k) \cdot p^i k = p^{2e}$$

and

$$1 + \sum_{i=0}^{e-2} n(p^i k) \cdot p^i k = p^{2e-2} .$$

Subtracting we obtain

$$n(p^{e-1}k) \cdot p^{e-1}k = p^{2e-2}(p^2 - 1)$$

and so

$$n(p^{e-1}k) = \frac{p^{e-1}(p^2 - 1)}{k} .$$

Now since $n(p^{e-2}k)$, $n(p^{e-3}k)$, $\cdots$, $n(p^0k)$ represent the numbers of the sequences for which $(a, b, p^e) \neq 1$, they correspond to the sequences for mod p^{e-1}. But for mod p^{e-1}, the sequences that have lengths of $p^{e-2}k$ are those for which $(a', b', p^{e-1}) = 1$ where $a = pa'$ and $b = pb'$. The number of these sequences gives $n(p^{e-2}k)$. Hence we may use the formula derived above and obtain

$$n(p^{e-2}k) = \frac{p^{e-2}(p^2 - 1)}{k}$$

Thus in general for mod p^e we have

$$n(p^i k) = \frac{p^i(p^2 - 1)}{k}$$

for $i = 0, 1, \cdots, e-1$.

Since $k(2) = 3$ and $k(2^2) \neq k(2)$ we have:

Corollary. For mod 2^e, $n(1) = 1$ and $n(3 \cdot 2^i) = 2^i$ for $i = 0, 1, \cdots, e-1$.

Theorem 1'. Let $m = p^e$ where $p \equiv \pm 3 \pmod{10}$. If t is the largest integer such that $k(p^t) = k(p)$ with $t > 1$, then (1) for $e \leq t$, $n(1) = 1$ and

$$n(k) = \frac{p^{2e} - 1}{k} ,$$

and (2) for $e > t$, $n(1) = 1$,

$$n(k) = \frac{p^{2t} - 1}{k}, \qquad \text{and} \qquad n(p^{i-t+1}k) = \frac{p^{i+t-1}(p^2 - 1)}{k}$$

for $i = t, \cdots, e-1$.

Proof.

(1) For $e \leq t$, $k(p^e) = k(p)$ and so all the sequences except the $(0,0)$ sequence have length k. Since $\Sigma h_i n(h_i) = p^{2e}$ this means

$$n(k) = \frac{p^{2e} - 1}{k} .$$

(2) For $e > t$, the possible lengths are $1, k, pk, \cdots, p^{e-t}k$. Since all the lengths of the sequences for mod p^e can be identified as the lengths for mod $p^e, p^{e-1}, \cdots, p, p^0$ where $(a, b, m) = 1$, we have:

For mod p^0, $n(1) = 1$.

For mod p , $n(1) = 1$ and $n(k) = (p^2 - 1)/k$.

For mod p^t, $n(1) = 1$ and $n(k) = (p^{2t} - 1)/k$.

For mod p^{t+1}, $n(1) = 1$, $n(k) = (p^{2t} - 1)/k$, and $n(pk) = (p^{2t+2} - p^{2t})/pk = (p^{2t-1}(p^2 - 1))/k$.

For mod p^{t+2}, $n(1) = 1$, $n(k) = (p^{2t} - 1)/k$,

$$n(pk) = \frac{p^{2t-1}(p^2 - 1)}{k} \qquad \text{and} \qquad n(p^2k) = \frac{p^{2t+4} - p^{2t+2}}{p^2k} = \frac{p^{2t}(p^2 - 1)}{k} .$$

$$\cdots$$

Therefore, for mod p^e, $n(1) = 1$, $n(k) = (p^{2t} - 1)/k$, and

$$n(p^{i-t+1}k) = \frac{p^{i+t-1}(p^2 - 1)}{k} \quad \text{for} \quad i = t, \cdots, e - 1 .$$

Theorem 2. If $m = 5^e$, then $n(1) = 1$, $n(4) = 1$, $n(4 \cdot 5^i) = 6 \cdot 5^{i-1}$ for $i = 1, \cdots, e - 1$, and $n(4 \cdot 5^e) = 5^{e-1}$.

Proof. We always have $n(1) = 1$. With the assumption that $(a, b, 5^e) = 1$ we know by 7 that if $(b^2 - ab - a^2, 5) = 1$ then $h(5^e) = k(5^e)$, and if $(b^2 - ab - a^2, 5) \neq 5$ then $h(5^e) = (1/5)k(5^e)$.

It can be shown that the assumption $(a, b, 5^e) = 1$ is superfluous in the first case because if $(a, b, 5^e) \neq 1$, then $5|a$ and $5|b$; hence $5|(b^2 - ab - a^2)$ contradicting $(b^2 - ab - a^2, 5) = 1$. Thus, if $(b^2 - ab - a^2, 5) = 1$, then $(a, b, 5^e) = 1$.

In general, we know that there are $p^{2e} - p^{2e-2}$ pairs (a,b) with $(a,b,p^e) = 1$. We wish to determine how many of these $5^{2e} - 5^{2e-2}$ pairs give $(b^2 - ab - a^2, 5) = 5$. This is equivalent to $b^2 - ab - a^2 \equiv 0 \pmod 5$, or $(2a + b)^2 \equiv 5b^2 \pmod 5$, or $(2a + b) \equiv 0 \pmod 5$. Hence $b \equiv -2a \pmod 5$, or $b \equiv 3a \pmod 5$. Thus if $(a, b, 5^e) = 1$ and

$$(b^2 - ab - a^2, 5) = 5,$$

a can take $5^e - 5^{e-1}$ different values and corresponding to each value of a, b can have 5^{e-1} values. Therefore, there will be $5^{e-1}(5^e - 5^{e-1}) = 4 \cdot 5^{2e-2}$ such pairs (a,b). Since the total number of pairs (a,b) for which $(a,b,5^e) = 1$ is $5^{2e} - 5^{2e-2}$ and all the cases for which $(b^2 - ab - a^2, 5) = 1$ arise from these, the number of pairs (a,b) such that $(b^2 - ab - a^2, 5) = 1$ is given by $5^{2e} - 5^{2e-2} - 4 \cdot 5^{2e-1} = 4 \cdot 5^{2e-1}$. This is the number of pairs that produce sequences of length $k(5^e)$. Since $k = k(5) = 20$, $k(5^e) = 5^{e-1}k = 4 \cdot 5^e$ and so

$$n(4 \cdot 5^e) = \frac{4 \cdot 5^{2e-1}}{4 \cdot 5^e} = 5^{e-1} .$$

We have $4 \cdot 5^{2e-2}$ pairs with $(a, b, 5^e) = 1$ producing sequences of length $\frac{1}{5}k(5^e) = 4 \cdot 5^{e-1}$. There are also the cases for which $(a, b, 5^e) \neq 1$. But there are the sequences for mod 5^{e-1} multiplied throughout by 5. Since $k(5^{e-1}) = 4 \cdot 5^{e-1}$ the number of pairs that produce sequences of length $4 \cdot 5^{e-1}$ is given by $4 \cdot 5^{2e-2} + 4 \cdot 5^{2(e-1)-1}$ and so

$$n(4 \cdot 5^{e-1}) = \frac{4 \cdot 5^{2e-2} + 4 \cdot 5^{2e-3}}{4 \cdot 5^{e-1}} = 6 \cdot 5^{e-2} .$$

We have $\frac{1}{5}k(5^{i+1}) = k(5^i) = 4 \cdot 5^i$ for $i = 1, 2, \cdots, e - 1$ and so

$$n(4 \cdot 5^i) = \frac{4 \cdot 5^{2(i+1)-2} + 4 \cdot 5^{2(i+1)-3}}{4 \cdot 5^i} = 6 \cdot 5^{i-1}$$

for $i = 1, 2, \cdots, e-1$. In addition to these there are the pairs that produce sequences of length $\frac{1}{5}k(5) = 4$. The number of such pairs is $4 \cdot 5^{2e-2}$, where $e = 1$. Hence,

$$n(4) = (4 \cdot 5^0)/4 = 1 .$$

Theorem 3. Let $m = p^e$ where $p \equiv \pm 1 \pmod{10}$. If $k(p^2) \neq k(p)$ then

(1) If $4|k$, $n(1) = 1$ and

$$n(p^i k) = \frac{p^i(p^2 - 1)}{k}$$

for $i = 0, 1, \cdots, e-1$ and

(2) if $4\not|k$, $n(1) = 1$,

$$n(p^i k/2) = \frac{2(p-1)}{k}$$

and

$$n(p^i k) = \frac{(p-1)(p^{i+1} + p^i - 1)}{k}$$

for $i = 0, 1, \cdots, e-1$.

Proof. By 3, $k(p^e)$ is even, and so it is either of the form $4t$ or of the form $4t+2$.

(1) If $k(p^e) = 4t$, by 8, $h(p^e)$ cannot be odd; and if h is even then by 10, $h(p^e) = k(p^e)$. Thus on condition $(a, b, p^e) = 1$, $h(p^e) = k(p^e) = p^{e-1}k$, and so the proof of Theorem 1 is applicable here. We also note that the condition $4|k(p^e)$ is equivalent to that of $4|k$ since $k(p^e) = p^{e-1}k$ and $2\not|p^{e-1}$.

(2) If $k(p^e) = 4t+2$, by 9 $h(p^e) = 2t+1$ for some (a,b). By 4 if $(b^2 - ab - a^2, p^e) = 1$, then $h(p^e) = k(p^e)$. Now consider $(b^2 - ab - a^2, p^e) \neq 1$; if $h(a, b, p^e)$ is even, by 10 $h(a, b, p^e) = k(p^e)$; and if $h(a, b, p^e)$ is odd, by 8, $h(a, b, p^e) = \frac{1}{2}k(p^e)$.

Let us first consider the case for mod p. To determine the number of pairs (a,b) for which $(b^2 - ab - a^2, p) \neq 1$, consider $b^2 - ab - a^2 \equiv 0 \pmod p$, or $(2b - a)^2 \equiv 5a^2 \pmod p$. Since 5 is a quadratic residue of primes of this form, $x^2 \equiv 5 \pmod p$ has two solutions $\pm c$. Thus the above condition is equivalent to $2b - a \equiv \pm ca \pmod p$, or

$$b \equiv \left(\frac{1 \pm c}{2}\right) a \pmod p ,$$

or $b_1 \equiv ra$ and $b_2 \equiv sa \pmod p$, where $r \equiv (1+c)/2$ and $s \equiv (1-c)/2 \pmod p$. Note that $r \not\equiv s \pmod p$ for this would imply $c \equiv 0$ and hence $c^2 \equiv 0 \pmod p$.

To have $(a, b, p) = 1$, we must have $(a, p) = 1$ because if $(a,p) \neq 1$, then $p|a$; but

$$b \equiv \left(\frac{1 \pm c}{2}\right) a \pmod p ,$$

and so $b \equiv 0 \pmod p$ and $p|b$; hence $(a, b, p) \neq 1$. Therefore for mod p there are $p - 1$ possible values of a that will give $(a, b, p) = 1$ and $(b^2 - ab - a^2, p) \not| 1$; and corresponding to each value of a, there are two values of b. Hence, there are $2(p - 1)$ pairs (a,b) with $(a,b,p) = 1$ and $(b^2 - ab - a^2, p) \neq 1$. We obtain:

If $a \equiv 1$, $b_1 \equiv r$ and $b_2 \equiv s \pmod{p}$;

If $a \equiv 2$, $b_1 \equiv 2r$ and $b_2 \equiv 2s \pmod{p}$;

...

If $a \equiv p - 1$, $b_1 \equiv (p - 1)r$ and $b_2 \equiv (p - 1)s \pmod{p}$.

It is clear that no matter what a is, for mod p, the pairs (a, ar) will all produce sequences of the same length as the pair $(1,r)$, and similarly the pairs (a, as) will all produce sequences of the same length as the pair $(1,s)$.

Now, we know that since $k(p) = 4t + 2$ there exist (a,b) such that $h(a,b,p) = \frac{1}{2}k(p) = 2t + 1$. But if there is one pair (a,b) satisfying this, there are at least $p - 1$ pairs (a,b) with $h(a,b,p) = 2t + 1$. We will show that there are only $p - 1$ such pairs.

Without any loss of generality we may assume a to be 1. We will show that either $(1,r)$ or $(1,s)$ but not both, will produce a sequence of length $2t + 1$ when reduced mod p. Now suppose that both $(1,r)$ and $(1,s)$ produce sequences of length $2t + 1$. We have

$$1,\ r,\ 1 + r,\ 1 + 2r,\ 2 + 3r,\ \cdots,\ u_{n-1} + u_n r,\ \cdots \pmod{p};$$

$$1,\ s,\ 1 + s,\ 1 + 2s,\ 2 + 3s,\ \cdots,\ u_{n-1} + u_n s,\ \cdots \pmod{p}.$$

Therefore, we must have $u_{2t} + u_{2t+1}r \equiv 1$ and $u_{2t} + u_{2t+1}s \equiv 1 \pmod{p}$. Hence $u_{2t+1}(r-s) \equiv 0 \pmod{p}$. By 12, $f(p)$ must be even for if $f(p)$ is odd, then $4 | k(p^e)$. This gives $u_{2t+1} \not\equiv 0 \pmod{p}$ for otherwise $f(p) | (2t + 1)$ which is impossible. Hence we have $r \equiv s \pmod{p}$, and we have shown that this is impossible. Thus, the pairs $(1,r)$ and $(1,s)$ cannot both produce sequences of length $2t + 1$.

An alternative proof is the following. Since $b^2 - ab - a^2 \equiv 0 \pmod{p}$ we must have $r^2 - r - 1 \equiv 0 \pmod{p}$, or $1 + r \equiv r^2 \pmod{p}$. Using the recurrence relation $f_n = f_{n-1} + f_{n-2}$ we may obtain $r + r^2 = r(1 + r) \equiv r^3 \pmod{p}$, $r^2 + r^3 = r(r + r^2) \equiv r^4 \pmod{p}$, etc. Thus the sequence

$$1,\ r,\ 1 + r,\ 1 + 2r,\ 2 + 3r,\ \cdots \pmod{p}$$

may be written as $1, r, r^2, r^3, r^4, \cdots \pmod{p}$. Similarly, the sequence $1, s, 1 + s, 1 + 2s, 2 + 3s, \cdots \pmod{p}$ may be written as $1, s, s^2, s^3, s^4, \cdots \pmod{p}$.

Therefore, the assumption that these two sequences have periods of length $2t + 1$ when reduced mod p, implies that $r^{2t+1} \equiv 1$ and $s^{2t+1} \equiv 1 \pmod{p}$. Multiplying these two congruences we obtain $(rs)^{2t+1} \equiv 1 \pmod{p}$. But

$$rs \equiv \frac{1 - c^2}{4} \equiv -1 \pmod{p}$$

because $c^2 \equiv 5 \pmod{p}$, and so $(-1)^{2t+1} \equiv 1 \pmod{p}$ which is impossible. Hence $(1,r)$ and $(1,s)$ cannot both produce sequences of length $\frac{1}{2}k(p) = 2t + 1$.

Therefore of the $2(p-1)$ pairs (a,b) for which $(b^2 - ab - a^2, p) \neq 1$ and $(a,b,p) = 1$, $p - 1$ pairs produce sequences of length $\frac{1}{2}k$ and the other $p - 1$ pairs produce sequences of length k.

Since the total number of pairs (a,b) with $(a,b,p) = 1$ is given by $p^2 - 1$, we can now find the number of pairs (a,b) for which $(a,b,p) = 1$ and $(b^2 - ab - a^2, p) = 1$. We obtain $(p^2 - 1) - 2(p-1) = (p-1)^2$. All of these produce sequences of length k. Therefore for mod p we have

$$n(1) = 1, \qquad n\left(\frac{k}{2}\right) = \frac{2(p-1)}{k}$$

and

$$n(k) = \frac{(p-1) + (p-1)^2}{k} = \frac{p(p-1)}{k} \quad .$$

We shall next consider the case for mod p^e. The condition $(b^2 - ab - a^2, p^e) \neq 1$ is equivalent to $(b^2 - ab - a^2, p) \neq 1$. Therefore we must again have

$$b \equiv \left(\frac{1 \pm c}{2}\right) a \qquad (\text{mod } p) \ .$$

We know that $(a, b, p^e) = 1$ if and only if $(a, p^e) = 1$. Hence there are $p^e - p^{e-1}$ possible values of a, and corresponding to each value of a there are $2p^{e-1}$ values of b. Thus there are $2p^{e-1}(p^e - p^{e-1})$ pairs (a,b) with $(a,b,p^e) = 1$ and $(b^2 - ab - a^2, p^e) \neq 1$. If $a \equiv 1$, $b_1 \equiv r + jp$ and $b_2 \equiv s + jp \pmod{p^e}$ where $j = 0, 1, 2, \cdots, p^{e-1} - 1$. If $a \equiv 2$, $b_1 \equiv 2r + jp$ and $b_2 \equiv 2s + jp \pmod{p^e}$, where $j = 0, 1, 2, \cdots, p^{e-1} - 1$. These are equivalent to $b_1 \equiv 2(r + jp)$ and $b_2 \equiv 2(s + jp) \pmod{p^e}$, where $j = 0, 1, 2, \cdots, p^{e-1} - 1$.

Since for any a, the sequences $(a, a(r + jp))$ and $(a, a(s + jp))$ will all have the same length as $(1, r + jp)$ and $(1, s + jp)$, respectively, for $j = 0, 1, \cdots, p^{e-1} - 1$, it is sufficient to consider the sequences $(1, r + jp)$ and $(1, s + jp)$ for $j = 0, 1, \cdots, p^{e-1} - 1$.

Since $k(p^e) = 4t + 2$, we know that for at least one value of j, at least one of $(1, r + jp)$ and $(1, s + jp)$ produces a sequence of length $2t + 1$. Suppose for some value of j, $h = h(1, r + jp, p^e) = 2t + 1$. We will show that then for any i where i is one of $0, 1, 2, \cdots, p^{e-1} - 1$, $h(1, s + ip, p^e) \neq 2t + 1$. Suppose for some i,

$$h = h(1, r + jp, p^e) = h(1, s + ip, p^e) = \tfrac{1}{2}k = 2t + 1.$$

We have

$$1,\ r + jp,\ \cdots,\ u_{n-1} + u_n(r + jp),\ \cdots \qquad (\text{mod } p^e);$$

$$1,\ s + ip,\ \cdots,\ u_{n-1} + u_n(s + ip),\ \cdots \qquad (\text{mod } p^e);$$

and so

$$u_{h-1} + u_h(r + jp) \equiv 1 \equiv u_{h-1} + u_h(s + ip) \pmod{p^e},$$

or $u_h(r + jp) \equiv u_h\,(s + ip) \pmod{p^e}$. Since by 12 $u_h \not\equiv 0 \pmod{p}$, we may cancel u_h and obtain $r + jp \equiv s + ip \pmod{p^e}$, or $r \equiv s \pmod{p}$ which is impossible.

Hence if for some value of j, $h(1 + r + jp, p^e) = 2t + 1$ then for no value of i can $h(1, s + ip, p^e)$ be equal to $2t + 1$. Similarly, if for some value of j,

$$h(1, s + jp, p^e) = 2t + 1,$$

then for no value of i can $h(1, r + ip, p^e)$ be equal to $2t + 1$.

Next, we will show that only one value of j gives a length of $2t + 1$. Suppose both $(1, r + jp)$ and $(1, r + ip)$ produce sequences of length $h = 2t + 1$, where i and j are two different numbers from $0, 1, \cdots, p^{e-1} - 1$. Therefore

$$u_{h-1} + u_h(r + jp) \equiv 1 \equiv u_{h-1} + u_h(r + ip) \pmod{p^e},$$

or

$$u_h(r + jp) \equiv u_h(r + ip) \pmod{p^e}.$$

Since by 12, $u_h \not\equiv 0 \pmod{p}$, we have $r + jp \equiv r + ip \pmod{p^e}$, or $jp \equiv ip \pmod{p^e}$, or $j \equiv i \pmod{p^{e-1}}$ which is impossible. Therefore of the $2p^{e-1}$ values corresponding to each value of a, only one can produce a sequence of length $2t + 1$. But there are $p^e - p^{e-1}$ possible values of a. Hence there are $p^e - p^{e-1}$ or $p^{e-1}(p - 1)$ pairs (a, b) that produce sequences of length $\frac{1}{2}k(p^e)$. The remaining $2p^{e-1}(p^e - p^{e-1}) - (p^e - p^{e-1})$ or $p^{e-1}(p - 1)(2p^{e-1} - 1)$ pairs (a, b) that have $(a, b, p^e) = 1$ and $(b^2 - ab - a^2, p^e) \neq 1$ produce sequences of length $k(p^e)$. Also since there are $p^{2e} - p^{2e-2}$ pairs (a, b) for which $(a, b, p^e) = 1$, we have

$$(p^{2e} - p^{2e-2}) - 2p^{e-1}(p^e - p^{e-1})$$

or $p^{2e-2}(p - 1)^2$ pairs with $(b^2 - ab - a^2, p^e) = 1$. All of these produce sequences of length $k(p^e)$. In addition to these, there are the sequences for which $(a, b, p^e) \neq 1$. Thus for mod p^e we have $n(1) = 1$,

$$n(p^i k/2) = \frac{p^i(p - 1)}{p^i k/2} = \frac{2(p - 1)}{k}$$

and

$$n(p^i k) = \frac{p^i(p - 1)(2p^i - 1) + p^{2i}(p - 1)^2}{p^i k} = \frac{(p - 1)(p^{i+1} + p^i - 1)}{k} \qquad (i = 0, 1, \cdots, e - 1).$$

Theorem 3'. Let $m = p^e$ where $p \equiv \pm 1 \pmod{10}$ and let t be the largest integer such that $k(p^t) = k(p)$ with $t > 1$.

(1) if $4|k$, then (a) for $e \leq t$, $n(1) = 1$ and

$$n(k) = \frac{p^{2e} - 1}{k} ,$$

and (b) for $e > t$, $n(1) = 1$,

$$m(k) = \frac{p^{2t} - 1}{k} ,$$

and

$$n(p^{i-t+1}k) = \frac{p^{i+t-1}(p^2 - 1)}{k} \quad \text{for } i = t, \cdots, e - 1.$$

(2) if $4 \nmid k$, then (a) for $e \leq t$, $n(1) = 1$,

$$n\left(\frac{k}{2}\right) = \frac{2(p^e - 1)}{k}$$

and

$$n(k) = \frac{p^e(p^e - 1)}{k}$$

and (b) for $e > t$, $n(1) = 1$,

$$n\left(\frac{k}{2}\right) = \frac{2(p^t - 1)}{k} ,$$

$$n(k) = \frac{p^t(p^t - 1)}{k} ,$$

$$n(p^{i-t+1}k/2) = \frac{2p^{t-1}(p - 1)}{k} ,$$

and

$$n(p^{i-t+1}k) = \frac{p^{t-1}(p - 1)(p^{i+1} + p^i - 1)}{k}$$

for $i = t, \cdots, m - 1$.

Proof. (1) Same as the proof for Theorem 1'.

(2) We have shown in Theorem 3 that if $(a, b, p^e) = 1$, for mod p^e, $p^{e-1}(p - 1)$ pairs (a,b) produce sequences of length $\frac{1}{2}k(p^e)$ and

$$p^{e-1}(p - 1)(2p^{e-1} - 1) + p^{2e-2}(p - 1)^2$$

or

$$p^{e-1}(p - 1)(p^e + p^{e-1} - 1)$$

pairs (a,b) produce sequences of length $k(p^e)$. Thus we have:

For mod p^0, $n(1) = 1$.

For mod p, $n(1) = 1$,

$$n\left(\frac{k}{2}\right) = \frac{2(p - 1)}{k} ,$$

and

$$n(k) = \frac{p(p - 1)}{k} .$$

For mod p^2, $n(1) = 1$,

$$n\left(\frac{k}{2}\right) = \frac{2(p - 1)}{k} + \frac{2p(p - 1)}{k} = \frac{2(p^2 - 1)}{k} ,$$

and

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

...

For mod p^t, $n(1) = 1$,

$$n\left(\frac{k}{2}\right) = \sum_{i=0}^{t-1} \frac{2p^i(p - 1)}{k} = \frac{2(p^t - 1)}{k} ,$$

and

$$n(k) = \sum_{i=0}^{t-1} \frac{p^i(p - 1)(p^{i+1} + p^i - 1)}{k} = \frac{p^t(p^t - 1)}{k} .$$

For mod p^{t+1}, $n(1) = 1$,

$$n\left(\frac{k}{2}\right) = \frac{2(p^t - 1)}{k} ,$$

$$n(k) = \frac{p^t(p^t - 1)}{k} ,$$

$$n(pk/2) = \frac{2p^{t-1}(p - 1)}{k} ,$$

and

$$n(pk) = \frac{p^{t-1}(p - 1)p^{t+1} + p^t - 1)}{k} .$$

For mod p^{t+2}, $n(1) = 1$,

$$n\left(\frac{k}{2}\right) = \frac{2(p^t - 1)}{k}, \qquad n(k) = \frac{p^t(p^t - 1)}{k}, \qquad n(pk/2) = \frac{2p^{t-1}(p - 1)}{k},$$

$$n(pk) = \frac{p^{t-1}(p - 1)(p^{t+1} + p^t - 1)}{k}, \qquad n(p^2k/2) = \frac{2p^{t-1}(p - 1)}{k},$$

and

$$n(p^2k) = \frac{p^{t-1}(p - 1)(p^{t+2} + p^{t+1} - 1)}{k} .$$

$$\cdots$$

Thus for $e \leq t$, we have $n(1) = 1$,

$$n\left(\frac{k}{2}\right) = \sum_{i=0}^{e-1} \frac{2p^i(p - 1)}{k} = \frac{2(p^e - 1)}{k}$$

and

$$n(k) = \sum_{i=0}^{e-1} \frac{p^i(p - 1)(p^{i+1} + p^i - 1)}{k} = \frac{p^e(p^e - 1)}{k} ;$$

and for $e > t$ we have $n(1) = 1$,

$$n\left(\frac{k}{2}\right) = \frac{2(p^t - 1)}{k}, \qquad n(k) = \frac{p^t(p^t - 1)}{k}, \qquad n(p^{i-t+1}k/2) = \frac{2p^{t-1}(p - 1)}{k},$$

and

$$n(p^{i-t+1}k) = \frac{p^{t-1}(p - 1)(p^{i+1} + p^i - 1)}{k} \quad \text{for } i = t, \cdots, e - 1 .$$

<u>Theorem 4.</u> Let $N(h,m) = h \cdot n(h,m)$. If

$$m = \prod_{i=1}^{n} p_i^{e_i} ,$$

then

$$n(h,m) = \sum_{\mathrm{LCM}[h_i]=h} \frac{\prod_{i=1}^{n} N(h_i, p_i^{e_i})}{h} ,$$

where $h_i = h(a, b, p_i^{e_i})$.

Proof. Consider the equivalent problem for which the modulus is of the form $\prod_{i=1}^{n} m_i$ where the m_i are pairwise relatively prime. Suppose first that $m = m_1m_2$ and $(m_1, m_2) = 1$. By 1, if $h(a,b,m_1) = h_1$ and $h(a,b,m_2) = h_2$ then $h(a, b, m_1m_2)$ is the least common multiple of h_1 and h_2. Also, by the Chinese Remainder Theorem, we know that each pair $(a,b) \pmod{m_1}$ and each pair $(c,d) \pmod{m_2}$ gives rise to a unique pair (e,f) $\pmod{m_1m_2}$ such that $e \equiv a$, $f \equiv b \pmod{m_1}$, and $e \equiv c$, $f \equiv d \pmod{m_2}$. By 1, $h(e, f, m_1m_2)$ is the least common multiple of $h(e, f, m_1)$ and $h(e, f, m_2)$. But $e \equiv a$ and $f \equiv b \pmod{m_1}$ imply that $h(e, f, m_1) = h(a, b, m_1) = h_1$, and similarly $h(e, f, m_2) = h_2$; and so $h(e, f, m_1m_2)$ is the least common multiple of h_1 and h_2.

Let $[h_1, h_2]$ denote the least common multiple of h_1 and h_2. We have seen that each pair of pairs $(a,b) \pmod{m_1}$ and $(c,d) \pmod{m_2}$ gives a unique pair $(e,f) \pmod{m_1m_2}$, of length $h = [h_1, h_2]$. Therefore there are $N(h_1, m_1)\cdot N(h_2, m_2)$ such pairs (e,f) with length $h_1 \pmod{m_1}$ and length $h_2 \pmod{m_2}$. Now any pair $(e,f) \pmod{m_1m_2}$ with length h when reduced mod m_1 produces a sequence of length h_1 and when reduced mod m_2 produces a sequence of length h_2 such that $[h_1, h_2] = h$. Hence

$$N(h, m_1m_2) = \sum_{[h_1,h_2]=h} N(h_1,m_1)\cdot N(h_2,m_2), \quad \text{and so} \quad n(h, m_1m_2) = \sum_{[h_1,h_2]=h} \frac{N(h_1,m_1)\cdot N(h_2,m_2)}{h}.$$

By induction, this result is now easily extended to the case $m = \prod_{i=1}^{n} m_i$, where $n > 2$, and all the m_i are pairwise relatively prime. Thus we obtain

$$n(h,m) = \sum_{\mathrm{LCM}[h_i]=h} \frac{\prod_{i=1}^{n} N(h_i, m_i)}{h}.$$

In particular, if $m_i = p_i^{e_i}$ for $i = 1, \cdots, n$, we have

$$n(h,m) = \sum_{\mathrm{LCM}[h_i]=h} \frac{\prod_{i=1}^{n} N(h_i, p_i^{e_i})}{h}.$$

These four theorems cover all possible values of m. Thus if $k(p^e)$ is known, the values of $h(a, b, m)$ as well as $n(h,m)$ can be determined.

I would like to acknowledge the assistance Prof. D. Singmaster gave me with his criticisms and suggestions in putting this paper in its final form.

REFERENCES

1. D. D. Wall, "Fibonacci Series Modulo m," Amer. Math. Monthly, 67 (1960), 525-532.
2. D. W. Robinson, "The Fibonacci Matrix Modulo m," Fibonacci Quarterly, 1 (1963), pp. 29-35.
3. S. E. Mamangakis, "Remarks on the Fibonacci Series Modulo m," Amer. Math. Monthly, 68 (1961), pp. 648-649.
4. J. Vinson, "The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence," Fibonacci Quarterly, 1 (1963), pp. 37-45.