AMERICAN UNIVERSITY OF BEIRUT

FIBONACCI SEQUENCES MODULO m

By

Agnes Andreassian

Approved:

David Singmaster
Advisor

Robert J. Fraga
Member of Committee

Amin Muwafi
Member of Committee

Member of Committee

Date of Thesis Presentation: Feb. 5, 1968.

FIBONACCI SEQUENCES MODULO m

By

Agnes Andreassian

Submitted in Partial Fulfillment for the Requirements

of the Degree Master of Arts

in the Mathematics Department of the

American University of Beirut

Beirut, Lebanon

1968

FIBONACCI SEQUENCES MODULO m

By

Agnes Andreassian

CONTENTS

INTRODUCTION

The Fibonacci numbers are named after the thirteenth century mathematician, Leonardo Pisano. In his work, Liber Abacci, he proposed the famous rabbit problem which is stated in the following form:

"Someone placed a pair of rabbits in a certain place, enclosed on all sides by a wall, to find out how many pairs of rabbits will be born there in the course of one year, it being assumed that every month a pair of rabbits produces another pair, and that rabbits begin to bear young two months after their own birth." [1]

Listing the total number of pairs of rabbits at the end of each month produced the following sequence of numbers:

$$\{1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377\}$$

This gave rise to the recurrent sequence called the Fibonacci sequence defined by $u_0 = 0$, $u_1 = 1$, and $u_n = u_{n-1} + u_{n-2}$. The numbers in the sequence are called Fibonacci numbers.

Many other Fibonacci type sequences can be produced by starting with any two integers a and b and using the same recurrence relation. Thus, general Fibonacci sequences are of the form

$$a, b, a + b, a + 2b, 2a + 3b, 3a + 5b, \ldots$$

which may be defined by $f_0 = a$, $f_1 = b$, and $f_n = f_{n-1} + f_{n-2}$.

We can show by mathematical induction that $f_n = u_{n-1}\, a + u_n\, b$. It is clear that $f_1 = b = u_0 a + u_1 b$. Assuming that the formula holds

for all positive integers less than n, we have

$$f_{n-2} = u_{n-3}a + u_{n-2}b$$

and

$$f_{n-1} = u_{n-2}a + u_{n-1}b$$

But

$$f_n = f_{n-1} + f_{n-2} = (u_{n-2} + u_{n-3})a + (u_{n-1} + u_{n-2})b$$

and so

$$f_n = u_{n-1}a + u_nb.$$

Hence the formula holds for all positive integers n.

Also the recurrence relation used to define Fibonacci sequences $\{f_n\}$ can be used to extend the sequences to terms with negative subscripts. Thus $f_{-1} = f_1 - f_0$, $f_{-2} = f_0 - f_{-1}$, $f_{-3} = f_{-1} - f_{-2}$, etc. We can show that $f_{-n} = (-1)^n (u_{n+1}a - u_nb)$. It is clear that this is true for $n = 1$. Now assume that the formula holds for all positive integers less than n. We have $f_{-n+2} = (-1)^{n-2} (u_{n-1}a - u_{n-2}b)$ $= (-1)^n (u_{n-1}a - u_{n-2}b)$ and $f_{-n+1} = (-1)^{n-1} (u_na - u_{n-1}b)$. Since $f_{-n} = f_{-n+2} - f_{-n+1}$ we obtain

$$f_{-n} = a\left[(-1)^n u_{n-1} - (-1)^{n-1} u_n\right] - b\left[(-1)^n u_{n-2} - (-1)^{n-1} u_{n-1}\right],$$

or

$$f_{-n} = a\left[(-1)^n(u_{n-1} + u_n)\right] - b\left[(-1)^n (u_{n-2} + u_{n-1})\right],$$

or

$$f_{-n} = (-1)^n(u_{n+1}a - u_nb).$$

In particular if $a = 0$ and $b = 1$, this becomes $u_{-n} = (-1)^{n+1}u_n$. Using this result we see that the formula for f_{-n} is a special case of $f_n = u_{n-1}a + u_nb$ where n has been replaced by -n.

Now suppose a general Fibonacci sequence is reduced modulo m, using least non-negative residues. It is sufficient to perform the

division for two consecutive terms and then work directly with the remainders using the same recurrence relation.

When we divide by m, there can only be m possible remainders, and two remainders in a given order determine what happens in the rest of the sequence. Since m quantities can be paired among themselves in m^2 ways, there can only be m^2 possible pairs in sequence. So we will eventually arrive at a pair that we had before thus resulting in periodicity of the sequence. Now, for any Fibonacci sequence there are many values of n which give $f_{r+n} \equiv f_r$ and $f_{r+n+1} \equiv f_{r+1} \pmod{m}$. The smallest value of n satisfying these will be called the period of the sequence mod m. It follows that all other values of n satisfying these congruences will be multiples of the period.

Let $k = k(m)$ denote the length of the period of the Fibonacci sequence $\{u_n\}$ for which $u_0 = 0$ and $u_1 = 1$. The lengths of the periods of the general Fibonacci sequences depend on a and b as well as m, and will be denoted by $h = h(a,b,m)$. Since $f_n = u_{n-1}a + u_n b$, f_n repeats after k terms. Hence $h(a,b,m)$ is a divisor of $k(m)$.

Our problem is to determine the number of ordered pairs (a,b), with $0 \leq a < m$, $0 \leq b < m$, that produce the various possible values of h when reduced modulo m.

In Chapter I, basic material relevant to the problem is presented, including preliminary results concerning Fibonacci sequences and what is known about the lengths of the periods of Fibonacci sequences modulo m. Chapter II discusses the problem for moduli of different forms.

CHAPTER I

BASIC FACTS

In the first section of this chapter a number of lemmas concerning Fibonacci sequences are presented. These results are used in the second section to establish the properties of the lengths of the periods of Fibonacci sequences modulo m. The lemmas and theorems are numbered for easy reference and proofs are given for completeness.

In writing Chapter I, the paper by D.D. Wall, "Fibonacci Series Modulo m" [2] has been used as a guide and his methods of proof have been used in establishing properties of the lengths of the periods of Fibonacci sequences modulo m. There are a number of other mathematical papers that deal with the properties of k(m), the period of the Fibonacci sequence $\{u_n\}$ with $u_0 = 0$ and $u_1 = 1$ [3 - 10]. These have not been used directly but are of interest. The preliminary results concerning Fibonacci sequences can be found in various forms in all elementary texts discussing Fibonacci numbers [1] , [11] .

Preliminary Results Concerning Fibonacci Sequences:

General Fibonacci sequences with $f_0 = a$, $f_1 = b$, and $f_n = f_{n-1} + f_{n-2}$ will be denoted by $\{f_n\}$. The Fibonacci sequence with $u_0 = 0$, $u_1 = 1$ will be denoted by $\{u_n\}$. Another special Fibonacci sequence, called the Lucas sequence, will be denoted by $\{v_n\}$ where $v_0 = 2$ and $v_1 = 1$. The letter p will be used to represent a prime and e a positive integer. $k = k(m)$ will denote the length of the period of $\{u_n\}$ reduced mod m.

The length of the period of $\{f_n\}$ will in general depend on a and b as well as m, and will be denoted by $h = h(a,b,m)$. In some cases, if it depends only on m we will write $h = h(m)$. "The length of $\{f_n\}$ mod m" will mean the length of the period of $\{f_n\}$ when reduced mod m.

Consider now the Fibonacci sequence $\{f_n\}$ reduced modulo m, using least non-negative residues.

Lemma 1: If the greatest common divisor of a,b, and m is g, let $a = ga'$, $b = gb'$, and $m = gm'$ so that a',b',m' are relatively prime, then $h(a,b,m) = h(a',b',m')$.

Proof: If $h = h(a,b,m)$ is the length of the period of $\{f_n\}$ mod m, then $f_h \equiv f_0$ and $f_{h+1} \equiv f_1 \pmod m$. Also if $h' = h(a',b',m')$ is the length of the period of $\{f'_n\}$ mod m', then $f'_{h'} \equiv f'_0$ and $f'_{h'+1} \equiv f'_1 \pmod{m'}$. But $f_0 = gf'_0$, $f_h = gf'_h$, $f_1 = gf'_1$, and $f_{h+1} = gf'_{h+1}$, and so $gf'_h \equiv gf'_0$ and $gf'_{h+1} \equiv gf'_1 \pmod{gm'}$. Hence $f'_h \equiv f'_0$ and $f'_{h+1} \equiv f'_1 \pmod{m'}$ and thus $h(a',b',m') \mid h(a,b,m)$. Also $f'_{h'} \equiv f'_0$ and $f'_{h'+1} \equiv f'_1 \pmod{m'}$ imply that $m' \mid (f'_{h'} - f'_0)$ and $m' \mid (f'_{h'+1} - f'_1)$ and so $gm' \mid g(f'_{h'} - f'_0)$ and $gm' \mid g(f'_{h'+1} - f'_1)$. Therefore $gf'_{h'} \equiv gf'_0$ and $gf'_{h'+1} \equiv gf'_1 \pmod{gm'}$, or $f_{h'} \equiv f_0$ and $f_{h'+1} \equiv f_1 \pmod m$. Hence $h(a,b,m) \mid h(a',b',m')$. Therefore $h(a,b,m) = h(a',b',m')$.

Thus in the discussion of h(a,b,m) we may assume a,b,m relatively prime. This will be denoted by $(a,b,m) = 1$. In the rest of this paper, unless stated explicitly, it will be assumed that $(a,b,m) = 1$.

The Fibonacci formulas given in the following lemmas will be proved for terms with non-negative subscripts. However, the proofs can easily be extended to show that they apply for negative subscripts

as well.

Lemma 2: Any two consecutive terms in $\{u_n\}$ are relatively prime.

Proof: Since u_0 and u_1 are relatively prime, we can use induction. Assuming that $(u_{n-1}, u_n) = 1$ we shall show that $(u_n, u_{n+1}) = 1$. Suppose $g \mid u_n$ and $g \mid u_{n+1}$ where $g > 1$. We have $u_{n+1} = u_{n-1} + u_n$. Hence $g \mid u_{n-1}$ and $(u_{n-1}, u_n) \neq 1$ contrary to assumption. Hence $(u_n, u_{n+1}) = 1$.

Lemma 3: $u_{n+t} = u_{n+1}\, u_t + u_n\, u_{t-1}$

Proof: We shall use induction on t. For $t = 0$, we get $u_n = u_{n+1}\, u_0 + u_n\, u_{-1} = u_n$ because $u_0 = 0$ and $u_{-1} = 1$. For $t = 1$, the result is $u_{n+1} = u_{n+1}\, u_1 + u_n\, u_0 = u_{n+1}$ since $u_1 = 1$ and $u_0 = 0$. Now, assume that the formula holds for all positive integers less than t. Therefore

$$u_{n+t-2} = u_{n+1}\, u_{t-2} + u_n\, u_{t-3}$$

and

$$u_{n+t-1} = u_{n+1}\, u_{t-1} + u_n\, u_{t-2}$$

But

$$u_{n+t} = u_{n+t-2} + u_{n+t-1} = u_{n+1}(u_{t-2} + u_{t-1}) + u_n(u_{t-3} + u_{t-2})$$

and so $u_{n+t} = u_{n+1}\, u_t + u_n\, u_{t-1}$ for all positive integers t.

Lemma 4: The subscripts of the terms for which $u_n \equiv 0 \pmod{m}$ form a simple arithmetic progression.

Proof: If $u_i \equiv 0$ and $u_j \equiv 0 \pmod{m}$, using the formula in Lemma 3, we obtain

$$u_{i+j} = u_{i+1}\, u_j + u_i\, u_{j-1} \equiv 0 \pmod{m}$$

and

$$u_i = u_{j+1}\, u_{i-j} + u_j\, u_{i-j-1} \quad \text{where } i \geq j.$$

Hence $u_{j+1}\, u_{i-j} \equiv 0 \pmod{m}$. But by Lemma 2 $(u_j, u_{j+1}) = 1$ and since $u_j \equiv 0 \pmod{m}$, $(u_{j+1}, m) = 1$. Therefore $u_{i-j} \equiv 0 \pmod{m}$.

We have shown that the subscripts of the terms for which $u_n \equiv 0 \pmod{m}$ are closed under addition and subtraction. They form the non-negative terms of an ideal and so are of the form $n = xd$. Since the sequence is periodic, u_0 is not the only $u_n \equiv 0 \pmod{m}$, and so $d > 0$. That is, $n = xd$ for $x = 0,1,2,\ldots$ and some positive integer $d = d(m)$ gives all n for which $u_n \equiv 0 \pmod{m}$.

Lemma 5: If r and s are the roots of $x^2 = x + 1$, then

$$u_n = \frac{r^n - s^n}{r - s}.$$

Proof: We shall use induction. Since the formula is true for $n = 0$ and $n = 1$, assume that it holds for all positive integers less than n. Hence

$$u_{n-2} = \frac{r^{n-2} - s^{n-2}}{r - s} \quad \text{and} \quad u_{n-1} = \frac{r^{n-1} - s^{n-1}}{r - s}$$

Therefore
$$u_n = u_{n-1} + u_{n-2} = \frac{(r^{n-2} + r^{n-1}) - (s^{n-2} + s^{n-1})}{r - s}$$

But r and s satisfy the equation $x^2 = x + 1$ and so $r^2 = r + 1$ and $s^2 = s + 1$. Multiplying the first by r^{n-2} and the second by s^{n-2} we obtain $r^n = r^{n-1} + r^{n-2}$ and $s^n = s^{n-1} + s^{n-2}$. Hence $u_n = \frac{r^n - s^n}{r-s}$.

Lemma 6: If r and s are the roots of $x^2 = x + 1$, then $v_n = r^n + s^n$.

Proof: We have $v_0 = r^0 + s^0 = 2$ and $v_1 = r + s = \frac{1+\sqrt{5}}{2} + \frac{1-\sqrt{5}}{2} = 1$. We shall use induction. Assuming that the formula holds for all positive

integers less than n, we have

$$v_{n-2} = r^{n-2} + s^{n-2} \quad \text{and} \quad v_{n-1} = r^{n-1} + s^{n-1}.$$

We find by addition

$$v_n = v_{n-2} + v_{n-1} = (r^{n-2} + r^{n-1}) + (s^{n-2} + s^{n-1}) = r^n + s^n$$

as was shown in the proof of Lemma 5.

Lemma 7: $u_{an} = 2^{1-a}\, u_n(Ku_n^2 + av_n^{a-1})$ where K is an integer.

Proof: Since $r = \frac{1+\sqrt{5}}{2}$ and $s = \frac{1-\sqrt{5}}{2}$, $r - s = \sqrt{5}$ and the result of Lemma 5 can be written as $u_n = \frac{r^n - s^n}{\sqrt{5}}$. Using this and Lemma 6 we may solve for r^n and s^n in terms of u_n and v_n. We obtain

$$r^n = \tfrac{1}{2}(v_n + \sqrt{5}\, u_n) \quad \text{and} \quad s^n = \tfrac{1}{2}(v_n - \sqrt{5}\, u_n)$$

Hence

$$u_{an} = \frac{r^{an} - s^{an}}{\sqrt{5}} = \frac{\left[2^{-a}(v_n + \sqrt{5}\, u_n)^a - 2^{-a}(v_n - \sqrt{5}\, u_n)^a\right]}{\sqrt{5}}.$$

By using the binomial theorem and combining similar terms we obtain

$$u_{an} = 2^{1-a} \sum_{j \text{ odd}} \binom{a}{j} 5^{(j-1)/2}\, u_n^{\,j}\, v_n^{a-j}$$

and so

$$u_{an} = 2^{1-a}\, u_n(Ku_n^2 + av_n^{a-1})$$

where K is an integer.

Lemma 8: $u_{an+1} = 2^{-a}(Ku_n^2 + au_n v_n^{a-1} + v_n^a)$ where K is an integer.

Proof: We have $u_{an+1} = \frac{r^{an+1} - s^{an+1}}{\sqrt{5}}$. Using the values of r^n and s^n found in the proof of Lemma 7, we obtain

$$u_{an+1} = \frac{\left[2^{-a-1}(1+\sqrt{5})(v_n + \sqrt{5}\, u_n)^a - 2^{-a-1}(1-\sqrt{5})(v_n - \sqrt{5}\, u_n)^a\right]}{\sqrt{5}},$$

or,

$$u_{an+1} = \frac{2^{-a-1}}{\sqrt{5}} \left\{ \left[(v_n + \sqrt{5}\, u_n)^a - (v_n - \sqrt{5}\, u_n)^a \right] + \sqrt{5} \left[(v_n + \sqrt{5} u_n)^a + (v_n - \sqrt{5}\, u_n)^a \right] \right\}.$$

By using the binomial theorem and combining similar terms, we find

$$u_{an+1} = 2^{-a} \sum_{j \text{ odd}} \binom{a}{j} 5^{(j-1)/2} u_n^j v_n^{a-j} + 2^{-a} \sum_{j \text{ even}} \binom{a}{j} 5^{j/2} u_n^j v_n^{a-j},$$

or,

$$u_{an+1} = 2^{-a} \sum_{j=0}^{a} \binom{a}{j} 5^{(j-1)/2} u_n^j v_n^{a-j} \left[\frac{(1+\sqrt{5}) - (-1)^j (1 - \sqrt{5})}{2} \right]$$

and so

$$u_{an+1} = 2^{-a}(K u_n^2 + a u_n v_n^{a-1} + v_n^a)$$

where K is an integer.

Lemma 9: $v_n = u_{n+1} + u_{n-1}$

Proof: We have $v_n = r^n + s^n = \frac{1}{r-s}(r^n + s^n)(r-s)$

and so

$$v_n = \frac{1}{r-s}\left[r^{n+1} - s^{n+1} - rs(r^{n-1} - s^{n-1}) \right].$$

But

$$-rs = -\frac{1}{4}(1+\sqrt{5})(1-\sqrt{5}) = 1.$$

Hence

$$v_n = \frac{1}{r-s}\left[(r^{n+1} - s^{n+1}) + (r^{n-1} - s^{n-1}) \right] = u_{n+1} + u_{n-1}.$$

Lemma 10: The congruence $x^2 \equiv x + 1 \pmod{p}$ has a double root only when $p = 5$.

Proof: If we have $x^2 - x - 1 \equiv (x - r)^2 = x^2 - 2rx + r^2$ then $2r \equiv 1$ and $r^2 \equiv -1$. Hence $4r^2 \equiv 1$ and $4r^2 \equiv -4$. Subtracting we find $5 \equiv 0$ and so $p = 5$.

Lemma 11: $u_n = 2^{1-n} \sum_{j \text{ odd}} \binom{n}{j} 5^{(j-1)/2}$

Proof: We know that $u_n = \frac{r^n - s^n}{r - s}$ when $r = \frac{1+\sqrt{5}}{2}$

and $s = \frac{1-\sqrt{5}}{2}$. Substituting, using the binomial theorem, and combining similar terms we obtain:

$$u_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] = \frac{2^{-n}}{\sqrt{5}}\left[2\binom{n}{1}\sqrt{5} + 2\binom{n}{3}5\sqrt{5} + 2\binom{n}{5}5^2\sqrt{5} + \ldots\right],$$

or

$$u_n = 2^{1-n}\left[\binom{n}{1} + 5\binom{n}{3} + 5^2\binom{n}{5} + \ldots\right] = 2^{1-n}\sum_{j \text{ odd}}\binom{n}{j}5^{(j-1)/2}.$$

Lemma 12: $u_n^2 - u_{n+1}u_{n-1} = (-1)^{n-1}$

Proof: For $n = 1$, this becomes $u_1^2 - u_2 \cdot u_0 = (-1)^0$ which is true. Assuming that the formula holds for some positive integer $n - 1$, we have

$$u_{n-1}^2 - u_n u_{n-2} = (-1)^{n-2}$$

We know that $u_{n+1} = u_n + u_{n-1}$ and $u_{n-2} = u_n - u_{n-1}$ and so $u_n^2 - u_{n+1}u_{n-1} = u_n^2 - (u_n + u_{n-1})u_{n-1}$, or, $u_n^2 - u_{n+1}u_n - 1 = u_n(u_n - u_{n-1}) - u_{n-1}^2 = u_n u_{n-2} - u_{n-1}^2$. Using the hypothesis, this becomes

$$u_n^2 - u_{n+1}u_{n-1} = -(-1)^{n-2},$$

or,

$$u_n^2 - u_{n+1}u_{n-1} = (-1)^{n-1}.$$

Lemma 13: The number 5 is a quadratic residue for primes of the form $p = 10x \pm 1$ and is a quadratic non-residue for primes of the form $p = 10x \pm 3$.

Proof: By the law of quadratic reciprocity [12, p.68], if p is an odd prime, $p \neq 5$, then

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{(p-1)/2 \cdot (5-1)/2},$$

or

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{p-1} = \left(\frac{p}{5}\right).$$

This gives the following possibilities:

1. If $p \equiv 1 \pmod 5$, $(\frac{p}{5}) = (\frac{1}{5}) = 1$.

2. If $p \equiv 2 \pmod 5$, $(\frac{p}{5}) = (\frac{2}{5}) = -1$

3. If $p \equiv 3 \pmod 5$, $(\frac{p}{5}) = (\frac{3}{5}) = -1$

4. If $p \equiv 4 \pmod 5$, $(\frac{p}{5}) = (\frac{4}{5}) = 1$

Since p is an odd prime, this implies

$$(\frac{5}{p}) = 1 \text{ if and only if } p \equiv \pm 1 \pmod{10}$$

and

$$(\frac{5}{p}) = -1 \text{ if and only if } p \equiv \pm 3 \pmod{10}.$$

Thus, 5 is a quadratic residue of primes of the form $p = 10x \pm 1$ and is a quadratic nonresidue of primes of the forms $p = 10x \pm 3$.

Lengths of Periods of Fibonacci Series Modulo m:

The results in the first section will now be used to establish the properties of the lengths of the periods of Fibonacci series modulo m.

Theorem 1: If $m > 2$, then $k(m)$ is an even number.

Proof: Suppose k is odd; let $k = 2x + 1$. By working both ends to the middle we then have for mod m:

$$-u_k \equiv 0 = u_0$$

$$u_{k-1} \equiv 1 = u_1$$

$$-u_{k-2} = -u_k + u_{k-1} \equiv u_0 + u_1 = u_2$$

. . . . . .

$$(-1)^{t-1} u_{k-t} \equiv (-1)^{t-1} u_{k-t+2} + (-1)^{t} u_{k-t+1} \equiv u_{t-2} + u_{t-1} \equiv u_t$$

. . . . . .

$$(-1)^{x-2} u_{x+2} \equiv u_{x-1}$$

$$(-1)^{x-1} u_{x+1} \equiv u_x .$$

Now, if x is odd $u_{x+1} \equiv u_x$ but $u_{x+1} = u_x + u_{x-1}$ and so $u_{x-1} \equiv 0$; and if x is even $-u_{x+1} \equiv u_x$ but $u_{x+2} = u_{x+1} + u_x$ and so $u_{x+2} \equiv 0$; and since $(-1)^{x-2} u_{x+2} \equiv u_{x-1}$ we have again $u_{x-1} \equiv 0$. Since all n for which $u_n \equiv 0 \pmod m$ are multiples of some positive integer $d = d(m)$, we must have $d \mid (x-1)$ and so $d \mid (2x - 2)$; also $d \mid k$ and so $d \mid (2x + 1)$. Hence $d \mid (2x + 1 - 2x + 2)$ and so $d = 3$. Therefore $u_d = u_3 = 2 \equiv 0 \pmod m$. Thus the assumption that k is odd gives $m = 2$. Hence if $m > 2$, k must be even.

The next two theorems give upper bounds for $k(p)$ for primes of the form $p = 10x \pm 1$ and $p = 10x \pm 3$. However no nontrivial lower bounds can be given for $k(p)$.

Theorem 2: If $p = 10x \pm 1$, then $k(p) \mid (p - 1)$.

Proof: By Lemma 10, we know that the congruence $x^2 \equiv x + 1 \pmod p$ where p is of the form $10x \pm 1$ cannot have a double root. This congruence is equivalent to $(2x - 1)^2 \equiv 5 \pmod p$. By Lemma 13, we know that 5 is a quadratic residue for primes of this form. Hence this congruence has distinct roots r and s. By extending Lemma 5 to congruences (mod p) we have $u_n \equiv \frac{r^n - s^n}{r - s} \pmod p$.

Let g represent the least common multiple of the order of $r \pmod p$ and the order of $s \pmod p$. Hence $r^g \equiv 1$ and $s^g \equiv 1 \pmod p$. Now,

$$u_{n+g} \equiv \frac{r^{n+g} - s^{n+g}}{r - s} = \frac{r^n \cdot r^g - s^n \cdot s^g}{r - s} \equiv \frac{r^n - s^n}{r - s} \equiv u_n \pmod p$$

$$\text{and } u_{n+g+1} \equiv \frac{r^{n+g+1} - s^{n+g+1}}{r-s} = \frac{r^{n+1}\cdot r^{g} - s^{n+1}\cdot s^{g}}{r-s}$$

$$\equiv \frac{r^{n+1} - s^{n+1}}{r-s} \equiv u_{n+1} \pmod{p}.$$

Thus $u_n \pmod p$ repeats after g terms and so $k(p) \mid g$. But since $p \nmid r$ and $p \nmid s$, $r^{p-1} \equiv 1$ and $s^{p-1} \equiv 1 \pmod p$ by Fermat's Theorem. But g is the least common multiple of the orders of r and $s \pmod p$. Hence $g \mid (p-1)$. Therefore $k(p) \mid (p-1)$.

Theorem 3: If $p \equiv 10x \pm 3$, then $k(p) \mid (2p+2)$ and $k(p) \equiv 0 \pmod 4$.

Proof: By Lemma 13, 5 is a quadratic nonresidue of primes of the form $10x \pm 3$ and hence $\left(\frac{5}{p}\right) \equiv -1 \pmod p$. But $\left(\frac{5}{p}\right) \equiv 5^{(p-1)/2} \pmod p$, and so $5^{(p-1)/2} \equiv -1 \pmod p$.

By Lemma 11, $u_n \equiv 2^{1-n} \sum_{j \text{ odd}} \binom{n}{j} 5^{(j-1)/2}$. If we let $n \equiv p$, we obtain $u_p \equiv 2^{1-p}\cdot 5^{(p-1)/2} \cdot \left(\frac{p}{p}\right) \pmod p$ because for $1 \le j < p$, $\binom{p}{j} \equiv 0 \pmod p$. But $2^{p-1} \equiv 1 \pmod p$ by Fermat's Theorem. Hence $u_p \equiv 5^{(p-1)/2} \equiv -1 \pmod p$.

Now, if we substitute $n \equiv p+1$, we obtain $u_{p+1} \equiv 2^{-p}\left[\binom{p+1}{1} + \binom{p+1}{p} 5^{(p-1)/2}\right] \pmod p$ because for $1 < j < p$, $\binom{p+1}{j} \equiv 0 \pmod p$. Since $5^{(p-1)/2} \equiv -1$ and $2^{p-1} \equiv 1 \pmod p$, we have $u_{p+1} \equiv 2^{-1}\left[\binom{p+1}{1} - \binom{p+1}{p}\right] \equiv 0 \pmod p$. Hence, for mod p, $u_{p+2} \equiv u_p + u_{p+1} \equiv -1 \equiv -u_1$

$$u_{p+3} \equiv u_{p+1} + u_{p+2} \equiv -1 \equiv -u_2$$

$$u_{p+4} \equiv u_{p+2} + u_{p+3} \equiv -2 \equiv -u_3$$

. . . . . .

and so

$$u_{2p+1} = u_p + (p+1) \equiv -u_p \equiv 1$$

$$u_{2p+2} = u_{p+}(p+2) \equiv -u_{p+1} \equiv u_0 \equiv 0$$

$$u_{2p+3} = u_p + (p+3) \equiv -u_{p+2} \equiv u_1 \equiv 1$$

Thus

$$u_{2p+2} \equiv u_0 \quad \text{and} \quad u_{2p+3} \equiv u_1$$

indicating that $u_n \pmod p$ repeats beginning with u_{2p+2}. Hence $k(p) \mid (2p+2)$.

This also shows that $k(p) \equiv 0 \pmod 4$, for otherwise $k(p) \mid (p+1)$. Thus $u_{p+1} \equiv 0$ and $u_{p+2} \equiv 1$ which implies that $u_p \equiv +1$ contrary to $u_p \equiv -1$ as proved above.

Theorem 4: If t is the largest integer with $k(p^t) = k(p)$, then $k(p^e) = p^{e-t} k(p)$ for $e \geq t$. In particular if $t = 1$, then $k(p^2) \neq k(p)$ so $k(p^e) = p^{e-1} k(p)$.

Proof: The proof is by induction. The case where p is an odd prime will be discussed first, and then the proof for $p = 2$ will be given separately.

(1) Let p be an odd prime.

If $e = t$, we have $k(p^t) = p^0 k(p)$ which is true by hypothesis. Now we wish to show that $k(p^{t+i}) = p^i k(p)$ for i any positive integer. Let us first show that this is true for $i = 1$. That is, we must prove $k(p^{t+1}) = pk(p)$.

Let u_n be the first term $\equiv 0 \pmod{p^t}$. Hence $k(p^t) = nx$ for some x. We know that $k(p^{t+1}) \neq k(p^t)$. Since $k(p^t) \mid k(p^{t+1})$, we have $k(p^{t+1}) = ck(p^t)$ where $c > 1$. Hence $k(p^{t+1}) = cnx$ with $c > 1$.

We have $u_{nx} = 0$ and $u_{nx+1} = 1 \pmod{p^t}$. We will show that

$k(p^{t+1})$ pnx. By Lemma 7, $u_{an} = 2^{1-a}\, u_n(Ku_n^2 + av_n^{a-1})$. If we replace a by p and n by nx, we obtain

$$u_{pnx} = 2^{1-p}\, u_{nx}\,(Ku_{nx}^2 + pv_{nx}^{p-1}).$$

Since $p^t \mid u_{nx}$ and $p \mid (Ku_{nx}^2 + pv_{nx}^{p-1})$, we have $p^{t+1} \mid u_{nx}(Ku_{nx}^2 + pv_{nx}^{p-1})$ and so $u_{pnx} \equiv 0 \pmod{p^{t+1}}$. Now, by Lemma 8, $u_{an+1} = 2^{-a}(Ku_n^2 + au_nv_n^{a-1} + v_n^a)$. Putting 1 for a and nx for n we obtain

$$u_{nx+1} = \frac{Ku_{nx}^2 + u_{nx} + v_{nx}}{2}$$

And so $u_{nx} \equiv 0$ and $u_{nx+1} \equiv 1 \pmod{p^t}$ implies $\frac{v_{nx}}{2} \equiv 1 \pmod{p^t}$. Hence $(\frac{v_{nx}}{2})^p \equiv 1 \pmod{p^{t+1}}$ [13, p. 50]. Using again the formula $u_{an+1} = 2^{-a}\,(Ku_n^2 + au_nv_n^{a-1} + v_n^a)$ and putting p for a and nx for n we have

$$u_{pnx+1} = 2^{-p}\left[u_{nx}\,(Ku_{nx} + pv_{nx}^{p-1}) + v_{nx}^p\right].$$

Since

$$p^t \mid u_{nx} \quad \text{and} \quad p \mid (Ku_{nx} + pv_{nx}^{p-1}),$$

this gives $u_{pnx+1} \equiv (\frac{v_{nx}}{2})^p \pmod{p^{t+1}}$. And so $u_{pnx+1} \equiv 1 \pmod{p^{t+1}}$. Therefore since $u_{pnx} \equiv 0$ and $u_{pnx+1} \equiv 1 \pmod{p^{t+1}}$, $k(p^{t+1}) \mid pnx$. But $k(p^{t+1}) = cnx$ with $c > 1$. Thus $cnx \mid pnx$, or $c \mid p$ and since $c > 1$, $c = p$. Therefore $k(p^{t+1}) = pnx = pk(p^t) = pk(p)$.

Now, let us assume that $k(p^{t+i}) = p^i\, k(p)$ for all positive integers less than or equal to j. That is, we assume

$$k(p^{t+1}) = pk(p^t) = pk(p)$$

$$k(p^{t+2}) = pk(p^{t+1}) = p^2k(p^t) = p^2k(p)$$

$$k(p^{t+3}) = pk(p^{t+2}) = p^3k(p^t) = p^3k(p)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$k(p^{t+j}) = pk(p^{t+j-1}) = p^jk(p^t) = p^jk(p).$$

We must prove that

$$k(p^{t+j+1}) = pk(p^{t+j}) = p^{j+1}\,k(p^t) = p^{j+1}\,k(p).$$

Let u_n be the 1st term $\equiv 0 \pmod{p^{t+j-1}}$. Hence $k(p^{t+j-1}) = nx$ for some x. Therefore $k(p^{t+j}) = pk(p^{t+j-1}) = pnx$. Since $k(p^{t+j}) \mid k(p^{t+j+1})$, we must have $k(p^{t+j+1}) = pnxy$, for some y. Since $k(p^{t+j}) = pnx$, we have

$$u_{pnx} \equiv 0 \quad \text{and} \quad u_{pnx+1} \equiv 1 \pmod{p^{t+j}}.$$

In the formula $u_{an+1} = 2^{-a}(Ku_n^2 + au_n v_n^{a-1} + v_n^a)$ put 1 for a and pnx for n. We obtain

$$u_{pnx+1} = \frac{Ku_{pnx}^2 + u_{pnx} + v_{pnx}}{2}$$

and so $\frac{v_{pnx}}{2} \equiv 1 \pmod{p^{t+j}}$. Hence $(\frac{v_{pnx}}{2})^p \equiv 1 \pmod{p^{t+j+1}}$ [13, p.50]. Now, in the same formula if we put p for a and pnx for n, we obtain

$$u_{p^2nx+1} = 2^{-p}\left[u_{pnx}\,(Ku_{pnx} + pv_{pnx}^{p-1}) + v_{pnx}^{p}\right].$$

Since

$$p^{t+j} \mid u_{pnx} \quad \text{and} \quad p \nmid (Ku_{pnx} + pv_{pnx}^{p-1}),$$

this gives

$$u_{p^2nx+1} \equiv (\frac{v_{pnx}}{2})^p \pmod{p^{t+j+1}}$$

and so

$$u_{p^2nx+1} \equiv 1 \pmod{p^{t+j+1}}.$$

Also, putting p for a and pnx for n in the formula

$$u_{an} = 2^{1-a}\,u_n(Ku_n^2 + pv_n^{p-1})$$

we obtain

$$u_{p^2nx} \equiv 2^{1-p}\, u_{pnx}\,(Ku_{pnx}^2 + pv_{pnx}^{p-1})$$

and so

$$u_{p^2nx} \equiv 0 \pmod{p^{t+j+1}}.$$

Therefore

$$k(p^{t+j+1}) \mid p^2nx, \quad \text{or} \quad pnxy \mid p^2nx, \quad \text{or} \quad y \mid p.$$

Now, either $y = 1$ or $y = p$. We will show that if $y = 1$, we arrive at a contradiction.

If $y = 1$, $k(p^{t+j+1}) = pnx$, and so

$$u_{pnx} \equiv 0 \quad \text{and} \quad u_{pnx+1} \equiv 1 \pmod{p^{t+j+1}}$$

Now either

(a) $p^{t+j} \mid u_n$

or

(b) $p^{t+j} \nmid u_n$

(a) If $p^{t+j} \mid u_n$, $u_n \equiv 0 \pmod{p^{t+j}}$ and so $u_{nx} \equiv 0 \pmod{p^{t+j}}$.

(b) If $p^{t+j} \nmid u_n$ we will show that u_{pn} is the first term $\equiv 0 \pmod{p^{t+j}}$ and not $\equiv 0 \pmod{p^{t+j+1}}$. Let g be the greatest common divisor of u_n and v_n. By Lemma 9, $v_n = u_{n+1} + u_{n-1}$ and so $g \mid u_n$ and $g \mid u_{n+1} + u_{n-1}$. But $u_{n+1} = u_n + u_{n-1}$ and so $g \mid 2u_{n-1} + u_n$. Since $g \mid u_n$, we must have $g \mid 2u_{n-1}$. But by Lemma 2, $(u_{n-1}, u_n) = 1$, and so $g \nmid u_{n-1}$. Hence $g \mid 2$, and so g is either 1 or 2.

Putting p for a in the formula $u_{an} = 2^{1-a}\, u_n(Ku_n^2 + av_n^{a-1})$ we obtain $u_{pn} = 2^{1-p}u_n(Ku_n^2 + pv_n^{p-1})$. Now $p^{t+j-1} \mid u_n$ and $p \mid (Ku_n^2 + pv_n^{p-1})$. Therefore $p^{t+j} \mid u_{pn}$, but since $(u_n, v_n) = 1$ or 2, $p^{t+j+1} \nmid u_{pn}$.

To show that u_{pn} is the first term $\equiv 0 \pmod{p^{t+j}}$, let r be the first subscript such that $u_r \equiv 0 \pmod{p^{t+j}}$. Then $r \mid pn$. But

$u_r \equiv 0 \ (p^{t+j-1})$ and so $n \mid r$, and since $u_n \not\equiv 0 \pmod{p^{t+j}}$, $n \neq r$. Hence $r = pn$.

Similarly since u_{pn} is the first term $\equiv 0 \pmod{p^{t+j}}$ and not $\equiv 0 \pmod{p^{t+j+1}}$, u_{p^2n} is the first term $\equiv 0 \pmod{p^{t+j+1}}$ and not $\equiv 0 \pmod{p^{t+j+2}}$. Hence for this value of n the terms u_{pnz} for $z = 0, 1, 2, \ldots$ are the terms $\equiv 0 \pmod{p^{t+j}}$ and u_{p^2nz} gives all terms $\equiv 0 \pmod{p^{t+j+1}}$.

Now if $k \ (p^{t+j+1}) = pnx$ then $pnx = p^2nz$ for some value of z. And so for this value of z, $x = pz$ and $u_{nx} = u_{pnz}$. But $u_{pnz} \equiv 0 \pmod{p^{t+j}}$; hence $u_{nx} \equiv 0 \pmod{p^{t+j}}$.

Thus, in both cases we have shown $u_{nx} \equiv 0 \pmod{p^{t+j}}$. We will now show that $u_{nx+1} \equiv 1 \pmod{p^{t+j}}$.

We have

$$u_{pnx} \equiv 0 \quad \text{and} \quad u_{pnx+1} \equiv 1 \pmod{p^{t+j+1}}.$$

Putting p for a and nx for n in the formula

$$u_{an+1} = 2^{-a}(Ku_n^2 + au_nv_n^{a-1} + v_n^a),$$

we obtain

$$u_{pnx+1} = 2^{-p}\left[u_{nx}(Ku_{nx} + pv_{nx}^{p-1}) + v_{nx}^p\right].$$

We have

$$p^{t+j} \mid u_{nx} \quad \text{and} \quad p \mid (Ku_{nx} + pv_{nx}^{p-1}),$$

and so

$$p^{t+j+1} \mid u_{nx}(Ku_{nx} + pv_{nx}^{p-1}).$$

This gives $u_{pnx+1} \equiv (\frac{v_{nx}}{2})^p \pmod{p^{t+j+1}}$. Hence $(\frac{v_{nx}}{2})^p \equiv 1 \pmod{p^{t+j+1}}$. Therefore, since p is an odd prime $\frac{v_{nx}}{2} \equiv 1 \pmod{p^{t+j}}$ [13, p. 50]. Also, putting 1 for a and nx for n in

$$u_{an+1} = 2^{-a}\,(Ku_n^2 + au_nv_n^{a-1} + v_n^a)$$

we obtain

$$u_{nx+1} = \frac{Ku_{nx}^2 + u_{nx} + v_{nx}}{2}$$

Hence

$$u_{nx+1} \equiv \frac{v_{nx}}{2} \pmod{p^{t+j}}.$$

This gives $u_{nx+1} \equiv 1 \pmod{p^{t+j}}$.

Therefore $k(p^{t+j}) \mid nx$. This is impossible because $k(p^{t+j}) = pnx$. Thus $y = 1$ leads to a contradiction. Hence $y = p$, and so

$$k(p^{t+j+1}) = p^2nx = pk(p^{t+j}) = p^{j+1}\,k(p).$$

(2) For $p = 2$, we first observe that $k(2) = 3$, $k(2^2) = 6$, and $k(2^3) = 12$. Therefore $k(2^2) \neq k(2)$; moreover $k(2^2) = 2k(2)$ and $k(2^3) = 2k(2^2) = 2^2k(2)$. We have thus verified the formula $k(2^e) = 2^{e-1}\,k(2)$ for $e = 1$, 2, and 3. Suppose the formula holds for all positive integers less than or equal to j. That is, we assume that

$$k(2^2) = 2k(2)$$

$$k(2^3) = 2k(2^2) = 2^2k(2)$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$k(2^j) = 2k(2^{j-1}) = 2^{j-1}\,k(2).$$

We wish to prove that $k(2^{j+1}) = 2k(2^j) = 2^j\,k(2)$.

Let u_n be the first term $\equiv 0 \pmod{2^{j-1}}$. Therefore $k(2^{j-1}) = nx$ for some x. Hence $k(2^j) = 2k(2^{j-1}) = 2nx$. This gives $u_{2nx} \equiv 0$ and $u_{2nx+1} \equiv 1 \pmod{2^j}$. We will first show that $k(2^{j+1}) \mid 4nx$.

By Lemma 3, $u_{n+t} = u_{n+1}\,u_t + u_n\,u_{t-1}$. Putting 2nx for n as well as for t we obtain $u_{4nx} = u_{2nx}\,(u_{2nx+1} + u_{2nx-1})$. We know that $2^j \mid u_{2nx}$. Since $(u_{2nx}, u_{2nx+1}) = 1$ and $(u_{2nx-1}, u_{2nx}) = 1$ u_{2nx+1} and u_{2nx-1} are both odd and so their sum is even and $2 \mid u_{2nx+1} + u_{2nx-1}$. Hence $2^{j+1} \mid u_{4nx}$, or $u_{4nx} \equiv 0 \pmod{2^{j+1}}$. Now, if we put 2nx for n and 2nx+1 for t in the formula $u_{n+t} = u_{n+1}\,u_t + u_n\,u_{t-1}$, we obtain

$$u_{4nx+1} = u_{2nx+1}^2 + u_{2nx}^2.$$

We know that $2^{j+1} \mid u_{2nx}^2$. Therefore $u_{4nx+1} \equiv u_{2nx+1}^2 \pmod{2^{j+1}}$. But $2^j \mid u_{2nx+1} - 1$ and $2 \mid u_{2nx+1} + 1$. Hence $2^{j+1} \mid u_{2nx+1}^2 - 1$ and so $u_{2nx+1}^2 \equiv 1 \pmod{2^{j+1}}$. This gives $u_{4nx+1} \equiv 1 \pmod{2^{j+1}}$.

Thus we have shown that $k(2^{j+1}) \mid 4nx$. But $k(2^j) \mid k(2^{j+1})$ and $k(2^j) = 2nx$. Therefore $k(2^{j+1})$ is either 2nx or 4nx. We will show that $k(2^{j+1}) = 2nx$ leads to a contradiction.

Suppose $k(2^{j+1}) = 2nx$, then

$$u_{2nx} \equiv 0 \quad \text{and} \quad u_{2nx+1} \equiv 1 \pmod{2^{j+1}}.$$

Putting nx for n as well as for t in the formula $u_{n+t} = u_{n+1}\,u_t + u_n\,u_{t-1}$, we obtain $u_{2nx} = u_{nx}(u_{nx+1} + u_{nx-1})$. Now, either (a) $2^j \mid u_n$, or (b) $2^j \nmid u_n$.

(a) If $2^j \mid u_n$, $u_n \equiv 0 \pmod{2^j}$ and $u_{nx} \equiv 0 \pmod{2^j}$.

(b) If $2^j \nmid u_n$, we will show that again, $u_{nx} \equiv 0 \pmod{2^j}$. We have $2^{j+1} \mid u_{nx}(u_{nx+1} + u_{nx-1})$, or $2^{j+1} \mid u_{nx}\,v_{nx}$ and $2 \mid v_{nx}$. But $(u_{nx}, v_{nx}) = 1$ or 2. Hence for $j \geq 3$, $2^{j-1} \mid u_{nx}$ implies that $2^2 \nmid v_{nx}$. Since we have $2^{j+1} \mid u_{nx}\,v_{nx}$, this gives $2^j \mid u_{nx}$ and so $u_{nx} \equiv 0 \pmod{2^j}$.

Thus in either case we have shown that $u_{nx} \equiv 0 \pmod{2^j}$. We will now show that $u_{nx+1} \equiv 1 \pmod{2^j}$.

The formula $u_{n+t} = u_{n+1}\, u_t + u_n\, u_{t-1}$ gives $u_{2nx+1} = u_{nx+1}^2 + u_{nx}^2$ if we put nx for n and nx+1 for t. Since $u_{2nx+1} \equiv 1 \pmod{2^{j+1}}$ and $u_{nx}^2 \equiv 0 \pmod{2^{j+1}}$, we have $u_{nx+1}^2 \equiv 1 \pmod{2^{j+1}}$, or $(u_{nx+1} + 1)(u_{nx+1} - 1) \equiv 0 \pmod{2^{j+1}}$. We know that $2 \mid u_{nx+1} + 1$. We will show that $2^2 \nmid u_{nx+1} + 1$.

Now, since $j > 1$, $u_{nx} \equiv 0 \pmod{2^j}$ implies $u_{nx} \equiv 0 \pmod{2^2}$. If $2^2 \mid u_{nx+1} + 1$, we have $u_{nx+1} \equiv -1 \pmod{2^2}$, or $u_{nx+1} \equiv 3 \pmod{2^2}$. But for mod 2^2 we have the sequence

$$0, 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, \ldots .$$

Thus, u_{6y} for $y = 0, 1, 2, \ldots$ gives all the terms that are $\equiv 0 \pmod{2^2}$, and u_{6y+1} is always $\equiv 1 \pmod{2^2}$. Hence $2^2 \nmid u_{nx+1} + 1$. Therefore the congruence $(u_{nx+1} + 1)(u_{nx+1} - 1) \equiv 0 \pmod{2^{j+1}}$ implies $u_{nx+1} - 1 \equiv 0 \pmod{2^j}$, or $u_{nx+1} \equiv 1 \pmod{2^j}$.

We have thus shown that if $k(2^{j+1}) = 2nx$ then $k(2^j) \mid nx$. But this is impossible because $k(2^j) = 2nx$. Therefore $k(2^{j+1}) \neq 2nx$. Hence $k(2^{j+1}) = 4nx = 2k(2^j) = 2^j\, k(2)$.

For all p up to 10,000 it has been shown that $k(p^2) \neq k(p)$, but it has not been proved that $k(p^2) = k(p)$ is impossible.

Theorems 1 to 4 have given us some properties of k(m). Theorems 5 through 12 will discuss the relationship of h(m), the period of $\{f_n\} \pmod m$, to k(m).

Theorem 5: If $(b^2 - ab - a^2, m) = 1$, then $h(m) = k(m)$.

Proof: We know that $f_n = au_{n-1} + bu_n$. If $h = h(m)$ is the length of the period of $\{f_n\} \pmod m$, then we have $f_h \equiv a$ and

$f_{h+1} \equiv b \pmod{m}$, which may be written as

$$f_h - a = bu_h + a(u_{h-1} - 1) \equiv 0 \pmod{m}$$

and

$$f_{h+1} - b = (a+b)u_h + b(u_{h-1} - 1) \equiv 0 \pmod{m}.$$

If we consider a and b as coefficients, the determinant of the system is

$$D = \begin{vmatrix} b & a \\ a+b & b \end{vmatrix} = b^2 - ab - a^2$$

Now if $(b^2 - ab - a^2, m) = 1$, then $D \not\equiv 0 \pmod{m}$ and so the system has the unique solution

$$u_h \equiv 0 \quad \text{and} \quad u_{h-1} \equiv 1 \pmod{m}.$$

Hence $k \mid h$. But also $h \mid k$ and so $h(m) = k(m)$.

Theorem 6: If $p = 10x \pm 3$, then $h(p^e) = k(p^e)$.

Proof: We must show that $(D, p^e) = 1$. Now $D \equiv 0 \pmod{p}$ is equivalent to $(2a+b)^2 \equiv 5b^2 \pmod{p}$. We require $(a,b,p^e) = 1$, and so if $D \equiv 0 \pmod{p}$ then $b \not\equiv 0 \pmod{p}$ because otherwise we would have $a \equiv 0 \pmod{p}$ and so $(a, b, p^e) \neq 1$. Hence if $D \equiv 0 \pmod{p}$, then 5 is a quadratic residue of p. But $p = 10x \pm 3$ and 5 is not a quadratic residue of primes of this form. Hence $p \nmid D$, and so $(D, p^e) = 1$. Therefore by Theorem 5, $h(p^e) = k(p^e)$.

Theorem 7: $h(2^e) = k(2^e)$.

Proof: We must have $(a,b,2) = 1$ and so we cannot have $a \equiv 0$ and $b \equiv 0 \pmod{2}$. We may have $a \equiv 1$ and $b \equiv 1 \pmod{2}$ in which case $D = b^2 - ab - a^2 \equiv 1 \pmod{2}$; or we may have one of a or $b \equiv 1 \pmod{2}$ and the other $\equiv 0 \pmod{2}$, and again $D = b^2 - ab - a^2 \equiv 1 \pmod{2}$.

Hence in all cases, $2 \nmid D$ and so $(D, 2^e) = 1$ and by Theorem 5, $h(2^e) = k(2^e)$.

Theorem 8: If $(b^2 - ab - a^2, 5) = 1$, then $h(5^e) = k(5^e)$, and if $(b^2 - ab - a^2, 5) = 5$, then $h(5^e) = \frac{1}{5} k(5^e)$.

Proof: The first statement is a direct consequence of Theorem 5. In the second statement we have $D \equiv 0 \pmod 5$ which is equivalent to $(2a + b)^2 \equiv 5b^2 \pmod 5$. Since we require $(a,b,5^e) = 1$, $b \not\equiv 0 \pmod 5$ and so $D \not\equiv 0 \pmod{5^2}$. Consider now the congruences $f_h - a \equiv 0$ and $f_{h+1} - b \equiv 0 \pmod{5^e}$. Assuming $e > 1$, we obtain the solution $u_h \not\equiv 0$ and $u_{h+1} \equiv 1 \pmod{5^{e-1}}$, and so $k(5^{e-1}) \mid h(a,b,5^e)$ and hence $h(a,b,5^e)$ is either $k(5^e)$ or $\frac{1}{5} k(5^e)$. We will show that the second value always holds.

$$D \equiv 0 \pmod 5 \quad \text{implies} \quad b = -2a + 5t.$$

Since $k(5) = 20$ and $k(5^e) = 5^{e-1} k(5)$ we have $\frac{1}{5} k(5^e) = 4 \cdot 5^{e-1}$. If we take $n = \frac{1}{5} k(5^e)$ in the formula $u_n = 2^{1-n} \sum_{j \text{ odd}} \binom{n}{j} 5^{(j-1)/2}$ we obtain

$$u_{\frac{1}{5}k(5^e)} \equiv 2^{1-4\cdot 5^{e-1}} \binom{4\cdot 5^{e-1}}{1} \pmod{5^e}.$$

But by Euler's generalization of Fermat's Theorem $2^{4\cdot 5^{e-1}} \equiv 1 \pmod{5^e}$. Therefore

$$u_{\frac{1}{5}k(5^e)} \equiv 2 \cdot 4 \cdot 5^{e-1} \equiv (3+5)5^{e-1} \equiv 3 \cdot 5^{e-1} \pmod{5^e}.$$

Now take $n = \frac{1}{5}k(5^e) + 1$, or $n = 4 \cdot 5^{e-1} + 1$ in the same formula. We obtain

$$u_{\frac{1}{5}k(5^e)+1} \equiv 2^{-4\cdot 5^{e-1}} \binom{1 + 4\cdot 5^{e-1}}{1} \pmod{5^e}.$$

Since $2^{4\cdot 5^{e-1}} \equiv 1 \pmod{5^e}$, we get $u_{\frac{1}{5}k(5^e)+1} \equiv 1 + 4 \cdot 5^{e-1} \pmod{5^e}$.

This gives

$$u_{\frac{1}{5}k(5^e)-1} = u_{\frac{1}{5}k(5^e)+1} - u_{\frac{1}{5}k(5^e)} \equiv 1 + 5^{e-1} \pmod{5^e}.$$

Therefore

$$f_{\frac{1}{5}k(5^e)} \equiv (-2a + 5t)\cdot 3\cdot 5^{e-1} + a(1+5^{e-1}) \pmod{5^e},$$

or,

$$f_{\frac{1}{5}k(5^e)} \equiv 3t\cdot 5^e - a\cdot 5^e + a \equiv a \pmod{5^e};$$

and

$$f_{\frac{1}{5}k(5^e)+1} \equiv (-2a + 5t)(1+4\cdot 5^{e-1}) + a(3\cdot 5^{e-1}) \pmod{5^e},$$

or,

$$f_{\frac{1}{5}k(5^e)+1} \equiv (-2a + 5t) + 4t\cdot 5^e - a\cdot 5^e \pmod{5^e},$$

or,

$$f_{\frac{1}{5}k(5^e)+1} \equiv -2a + 5t \equiv b \pmod{5^e}.$$

Since these formulas require $e > 1$, consider now the case $e = 1$. We are interested in the cases where $D \equiv 0 \pmod 5$. Enumerating all such cases we find $h(5) = 4 = \frac{1}{5}k(5)$.

Hence whenever $D \equiv 0 \pmod 5$ we have $h(5^e) = \frac{1}{5}k(5^e)$.

Theorem 9: If for $p > 2$, there exist a, b such that $h = h(a, b, p^e) = 2t + 1$, then $k(p^e) = 4t + 2$.

Proof: We have

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

and

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

Since $(a, b, p^e) = 1$, considering a and b as the unknowns, the determinant must be zero. Hence $u_h^2 - (u_{h+1} - 1)(u_{h-1} - 1) \equiv 0 \pmod{p^e}$. Using Lemma 12, this becomes

$$(-1)^h + u_{h+1} + u_{h-1} - 1 \equiv 0 \pmod{p^e},$$

or

$$u_{h+1} + u_{h-1} \equiv 1 + (-1)^h \pmod{p^e}.$$

But by Lemma 3, putting n for t we obtain $u_{2n} = u_n(u_{n+1} + u_{n-1})$ and hence we have $\frac{u_{2h}}{u_h} \equiv 1 + (-1)^h \pmod{p^e}$. Therefore if h is odd, $u_{2h} \equiv 0 \pmod{p^e}$. Now since $\{f_n\} \pmod{p^e}$ repeats after h terms, it also repeats after $2h$ terms. Had we started with this condition we would have obtained $u_{2h+1} + u_{2h-1} \equiv 1 + (-1)^{2h} = 2 \pmod{p^e}$. We have $u_{2h} \equiv 0 \pmod{p^e}$, and so $u_{2h+1} + u_{2h-1} = 2u_{2h+1} - u_{2h} \equiv 2u_{2h+1} \equiv 2$ and hence $u_{2h+1} \equiv 1 \pmod{p^e}$. Therefore $k \mid 2h$. But for $m > 2$, k is even and since h is odd and $h \mid k$ we must have $k = 2h = 4t + 2$.

Theorem 10: If $m = p^e$ with $p > 2$ and if $k = 4t + 2$, then $h = 2t + 1$ for some a, b.

Proof: If $k(p^e) = 4t + 2$, we have $u_{4t+2} \equiv u_0$ and $u_{4t+3} \equiv u_1 \pmod{p^e}$. By working both ends to the middle as in the proof of Theorem 1, but now with k even, we obtain $u_{2t+2} \equiv -u_{2t} \pmod{p^e}$. Now if we let $a = f_0 \equiv -u_{2t+1} - u_0 \pmod{p^e}$ and

$$b = f_1 \equiv u_{2t} - u_1 \pmod{p^e}$$

we have

$$f_n \equiv (-u_{2t+1} - u_0)u_{n-1} + (u_{2t} - u_1)\, u_n \pmod{p^e},$$

or

$$f_n \equiv -u_{2t+1}\, u_{n-1} + u_{2t}\, u_n - u_n \pmod{p^e}.$$

Using the formulas $u_{n+t} = u_{n+1}\, u_t + u_n\, u_{t-1}$ and $u_{-n} = (-1)^{n+1} u_n$, we may write

$$f_n \equiv (-1)^{n-1} u_{2t+1-n} - u_n$$

Thus

$$f_{2t+1} \equiv u_0 - u_{2t+1} = -u_{2t+1} - u_0 = f_0$$

and

$f_{2t+2} \equiv - u_{-1} - u_{2t+2} \equiv - u_1 + u_{2t} \equiv f_1$. Therefore $h \mid 2t + 1$ and this implies by Theorem 9 that $k = 2h = 4t + 2$, and so $h = 2t + 1$ for these values of a and b.

Finally we must show that $(a, b, p^e) = 1$. Since $a \equiv - u_{2t+1} - u_0$ and $b \equiv u_{2t} - u_1$, if $a \equiv b \equiv 0 \pmod{p}$ we must have $u_{2t} \equiv u_1$ and $u_{2t+1} \equiv - u_0 \pmod{p}$, and hence $k(p) = 2t+1$ which is impossible for $p > 2$.

The following theorem and its proof are quoted from the paper by D.D. Wall, "Fibonacci Series Modulo m" [2, p. 531] .

Theorem 11: "If $m = p^e$, $p > 2$, $p \neq 5$, and h is even, then $h = k$.

Proof: We use the condition $v_h \equiv 1 + (-1)^h \pmod{m}$, from Theorem 10 [Theorem 9 in our paper] , and the relation $v_n = r^n + s^n$ where r and s are the real roots of the equation $x^2 = x + 1$. Then, since h is even, and since $rs = -1$,

$$r^h + s^h - 2 \equiv 0 \pmod{m},$$

$$r^{2h} + s^{2h} + 4 + 2(rs)^h - 4r^h - 4s^h \equiv 0 \pmod{m^2},$$

$$r^{2h} - 2 + s^{2h} \equiv (r^h - s^h)^2 \equiv 0 \pmod{m^2}.$$

Now $r^h - s^h$ is not an integer, but is of the form $x\sqrt{5}$; and since $p \neq 5$ assures $5 \not\equiv 0 \pmod{m}$, we may divide by $5 = (r - s)^2$ to obtain

$$\left[(r^h - s^h)/(r - s)\right]^2 = u_h^2 \equiv 0 \pmod{m^2},\ u_h \equiv 0 \pmod{m}.$$

Finally $u_h \equiv 0$ and $v_h \equiv 2$ imply $u_{h-1} \equiv u_{h+1} \equiv 1$, which is turn implies $h = k$."

There is one step in this proof which does not seem to follow;

namely the step which asserts that $r^{2h} - 2 + s^{2h} \equiv 0 \pmod{m^2}$. Since $r^{2h} - 2 + s^{2h} \equiv 4(r^h + s^h - 2) \pmod{m^2}$ and $r^h + s^h - 2 \equiv 0 \pmod{m}$, it is clear that $r^{2h} - 2 + s^{2h} \equiv 0 \pmod{m}$, but the conclusion that it is $\equiv 0 \pmod{m^2}$ does not seem to be justified.

The possibilities for some misprint in the proof have been investigated, but nothing has been found. We have also written to the author asking for clarification, but we have not received any answer. (See appendix)

Even if the proof of the theorem as given is incorrect, the statement of the theorem seems to be true, and we shall assume this in the rest of this paper. This assumption is used specifically in the discussion of moduli of the form p^e where $p = 10x \pm 1$ on p. 44 and on p. 46 as well as in Theorem 12.

Theorem 12: If $h(a, b, p) = k(p)$, then $h(a, b, p^e) = k(p^e)$.

Proof: We know that $h(a, b, p^e)$ must be a multiple of $h(a, b, p) = k(p)$ and a divisor of $k(p^e) = p^{e-t} k(p)$ where t is the largest integer with $k(p^t) = k(p)$. Therefore $h(a, b, p^e)$ must be of the form $p^{-c} k(p^e)$ for $c \geq 0$. But in Theorems 9 and 11 it was shown that for $p \neq 2$ and $p \neq 5$ if h is odd then $h = \frac{k}{2}$ and if h is even then $h = k$. We know that for $p > 2$, $k(p)$ is even and hence $h(a, b, p)$ is even. Therefore $h(a, b, p^e)$ is even and so $h(a, b, p^e) = k(p^e)$. The cases $p = 2$ and $p = 5$ are covered by Theorems 7 and 8.

Theorem 13: If $h_i = h(a, b, p_i^{e_i})$ denotes the length of the period of $\{f_n\} \pmod{p_i^{e_i}}$ then $h = h(a, b, \prod_{i=1}^{n} p_i^{e_i})$, the length of the period of $\{f_n\} \pmod{\prod_{i=1}^{n} p_i^{e_i}}$, is the least common multiple of the h_i.

Proof: Since the length of the period of $\{f_n\} \pmod{\prod_{i=1}^{n} p_i^{e_i}}$ is h, $\{f_n\} \pmod{p_i^{e_i}}$ repeats after h terms for all values of i.

But the length of the period of $\{f_n\}$ (mod $p_i^{e_i}$) is h_i, and so $\{f_n\}$ (mod $p_i^{e_i}$) can repeat only after blocks of length ch_i. Hence $h_i \mid h$ for all values of i. But $\{f_n\}$ (mod $\prod_{i=1}^{n} p_i^{e_i}$) will repeat after any multiple of all the h_i. Hence $h(a, b, \prod_{i=1}^{n} p_i^{e_i})$ is the least common multiple of the h_i.

We also conclude that for any two moduli m_1 and m_2 such that $(m_1, m_2) = 1$, $h(a, b, m_1 m_2)$ is the least common multiple of $h(a, b, m_1)$ and $h(a, b, m_2)$. Or more generally, if m_i for $i = 1,\ldots,n$, are pairwise relatively prime, then $h(a, b, \prod_{i=1}^{n} m_i)$ is the least common multiple of the $h(a, b, m_i)$ where $i = 1, \ldots, n$.

Now, let $f(m)$ denote the smallest positive integer, n, for which $u_n \equiv 0 \pmod{m}$. The next two theorems, which are proved by Vinson [5], show the relationship of $k(m)$ and $f(m)$.

Theorem 14: For $m > 2$

(1) if $f(m)$ is even, then $k(m) = f(m)$ or $k(m) = 2f(m)$,

and

(2) if $f(m)$ is odd, then $k(m) = 4f(m)$.

Also

$$k(1) = f(1) \qquad \text{and} \qquad k(2) = f(2).$$

Conversely, $k(m) = 4f(m)$ implies $f(m)$ is odd, $k(m) = 2f(m)$ implies $f(m)$ is even, and $k(m) = f(m)$ implies $f(m)$ is even or $m = 1$ or 2.

Proof: For $m = 1$ and $m = 2$, we verify that $k(m) = f(m)$. Now suppose $m > 2$. By Lemma 12, $u_n^2 - u_{n+1} u_{n-1} = (-1)^{n-1}$. Putting $f(m)$ for $n + 1$ we obtain

$$u_{f(m)-1}^2 \equiv u_{f(m)} u_{f(m)-2} + (-1)^{f(m)} \equiv (-1)^{f(m)} \pmod{m}.$$

If $f(m)$ is even we have $u_{f(m)-1}^2 \equiv 1 \pmod{m}$. Now by Lemma 5,

$$u_j = \frac{r^j - s^j}{r - s} \quad \text{and} \quad u_{j+1} = \frac{r^{j+1} - s^{j+1}}{r - s}.$$

Solving the system for r^j and s^j and using the relation $r + s = 1$, we obtain

$$r^j = u_{j+1} - su_j = (1-s)u_j + u_{j-1} = ru_j + u_{j-1}$$

$$s^j = u_{j+1} - ru_j = (1-r)u_j + u_{j-1} = su_j + u_{j-1}.$$

We also have

$$u_{nj+i} = \frac{r^{nj+i} - s^{nj+i}}{r - s},$$

or

$$(r-s)u_{nj+i} = (ru_j + u_{j-1})^n r^i - (su_j + u_{j-1})^n s^i.$$

By expanding and recombining we obtain

$$u_{nj+i} = \sum_{t=0}^{n} \binom{n}{t} u_j^t \, u_{j-1}^{n-t} \, u_{i+t}$$

If we put $f(m)$ in place of j, we have

$$u_{nf(m)+i} \equiv u_{f(m)-1}^n \, u_i \pmod{m}.$$

Now since $u_{f(m)-1}^2 \equiv 1 \pmod{m}$ we have $u_{2f(m)+i} \equiv u_i \pmod{m}$. This gives $u_{2f(m)} \equiv u_0$ and $u_{2f(m)+1} \equiv u_1 \pmod{m}$, and so $k(m) \mid 2f(m)$. Also since $f(m) \mid k(m)$, we have either $k(m) = f(m)$ or $k(m) = 2f(m)$.

Now if $f(m)$ is odd, we have $u_{f(m)-1}^2 \equiv -1 \pmod{m}$. Since $m > 2$, $u_{f(m)-1}^2 \not\equiv 1 \pmod{m}$ and hence $u_{f(m)-1} \not\equiv \pm 1 \pmod{m}$. Also $u_{f(m)-1}^3 \equiv -u_{f(m)-1}$ and so $u_{f(m)-1}^3 \equiv \pm 1 \pmod{m}$. However, $u_{f(m)-1}^4 \equiv (-1)^2 \equiv 1 \pmod{m}$. Now since $u_{nf(m)+i} \equiv u_{f(m)-1}^n \, u_i \pmod{m}$, this gives $u_{4f(m)+i} \equiv u_i \pmod{m}$. Thus $u_{4f(m)} \equiv u_0$ and $u_{4f(m)+1} \equiv u_1 \pmod{m}$, but $u_{nf(m)+1} \not\equiv u_1 \pmod{m}$ for $n < 4$. Hence $k(m) \mid 4f(m)$ and

$f(m) \mid k(m)$ imply that $k(m) = 4f(m)$.

Since the theorem includes all possible cases, the converse follows.

Theorem 15: Let p be an odd prime and let e be any positive integer. Then

(1) if $2 \nmid f(p)$, then $k(p^e) = 4f(p^e)$;

(2) if $4 \mid f(p)$, then $k(p^e) = 2f(p^e)$;

(3) if $2 \mid f(p)$ but $4 \nmid f(p)$, then $k(p^e) = f(p^e)$;

(4) $k(2^2) = f(2^2)$ and for $e \geq 3$, $k(2^e) = 2f(2^e)$.

Conversely, if q represents any prime, then $k(q^e) = 4f(q^e)$ implies $f(q)$ is odd; $k(q^e) = 2f(q^e)$ implies $4 \mid f(q)$ or $q = 2$ and $e \geq 3$; and $k(q^e) = f(q^e)$ implies $2 \mid f(q)$ but $4 \nmid f(q)$ or $q^e = 2$ or 4.

Proof: If $p^{n+1} \mid u_{f(p^n)}$, then $f(p^{n+1}) = f(p^n)$. If $p^{n+1} \nmid u_{f(p^n)}$, then, as was shown in the proof of Theorem 4, $u_{pf(p^n)}$ is the first term which is divisible by p^{n+1} and $u_{pf(p^n)}$ is not divisible by p^{n+2}. Hence $f(p^{n+1}) = pf(p^n)$. It follows by induction that $f(p^e) = p^s f(p)$ where s is some non-negative integer. Hence since p is an odd prime, $f(p^e)$ and $f(p)$ are divisible by the same power of 2.

Thus in (1), $f(p)$ odd implies that $f(p^e)$ is odd, and so the result follows by Theorem 14.

In (2) and (3), $f(p^e)$ is even. Using the formula $u_{nf(m)+i} \equiv u^n_{f(m)-1}\, u_i \pmod m$ and putting p^e for m, 1 for n and $-\frac{1}{2}f(p^e)$ for i, we obtain $u_{(1/2)f(p^e)} \equiv u_{f(p^e)-1}\, u_{-(1/2)f(p^e)} \pmod{p^e}$. But $u_{-n} = (-1)^{n+1} u_n$ and so $u_{(-1/2)f(p^e)} = (-1)^{(1/2)f(p^e)+1}\, u_{(1/2)f(p^e)}$.

This gives $u_{f(p^e)-1}\, u_{(1/2)f(p^e)} \equiv (-1)^{(1/2)f(p^e)+1}\, u_{(1/2)f(p^e)} \pmod{p^e}$.

We have $\frac{1}{2}f(p^e) = \frac{1}{2}p^s f(p)$ where s is some non-negative integer. Since $\frac{1}{2}p^s$ is not an integer, $f(p) \neq \frac{1}{2}f(p^e)$. This implies that $u_{(1/2)f(p^e)} \not\equiv 0 \pmod{p}$. Therefore we may divide the congruence

$$u_{f(p^e)-1}\, u_{1/2f(p^e)} \equiv (-1)^{(1/2)f(p^e)+1}\, u_{(1/2)f(p^e)} \pmod{p^e}$$

by $u_{(1/2)f(p^e)}$. This gives $u_{f(p^e)-1} \equiv (-1)^{(1/2)f(p^e)+1} \pmod{p^e}$

Now in (2) since $4 \mid f(p)$, we have $4 \mid f(p^e)$ and so $\frac{1}{2}f(p^e)$ is even. Thus

$$u_{f(p^e)-1} \equiv -1 \pmod{p^e}$$

Hence

$$u^2_{f(p^e)-1} \equiv 1 \pmod{p^e}$$

and so $u_{2f(p^e)+i} \equiv u_i \pmod{p^e}$. This gives $u_{2f(p^e)} \equiv u_0$ and $u_{2f(p^e)+1} \equiv u_1 \pmod{p^e}$, and so $k(p^e) \mid 2f(p^e)$. But $f(p^e) \mid k(p^e)$ and $k(p^e) \neq f(p^e)$ because $u_{f(p^e)-1} \not\equiv 1 \pmod{p^e}$. Hence $k(p^e) = 2f(p^e)$.

Now in (3), $\frac{1}{2}f(p)$ is odd and so $\frac{1}{2}f(p^e)$ is odd. Thus we have $u_{f(p^e)-1} \equiv 1 \pmod{p^e}$. Thus $u_{f(p^e)+i} \equiv u_i \pmod{p^e}$, which gives $u_{f(p^e)} \equiv u_0$ and $u_{f(p^e)+1} \equiv u_1 \pmod{p^e}$. Hence $k(p^e) \mid f(p^e)$. But $f(p^e) \mid k(p^e)$, and so $k(p^e) = f(p^e)$.

To prove (4) we can easily verify that $f(2^2) = k(2^2) = 6$. Also we find $f(2) = 3$, $f(2^3) = 6$, $f(2^4) = 12$, and $f(2^5) = 24$. We shall prove by induction that $f(2^{2+a}) = 2^a f(2)$. We have already verified this for $a = 1$, 2, and 3. Now assume that it is true for all positive integers less than or equal to b where $b \geq 2$. Thus $f(2^{2+b-1}) = 2^{b-1} f(2)$ and $f(2^{2+b}) = 2^b f(2)$. Let $r = 2^{b-1} f(2)$; thus we have $f(2^{2+b-1}) = r$ and $f(2^{2+b}) = 2r$.

We have shown in Lemma 2 that any two consecutive terms in $\{u_n\}$ are relatively prime. Now since $2^{2+b-1} \mid u_r$, u_r is even and so both u_{r+1} and u_{r-1} are odd. Thus their sum, which by Lemma 9 is v_r, is even. Similarly, since $2^{2+b} \mid u_{2r}$, u_{2r} is even, and so both u_{2r+1} and u_{2r-1} are odd and v_{2r} is even. But in the proof of Theorem 4, it was shown that $(u_n, v_n) = 1$ or 2. Hence $2 \mid v_r$ but $2^2 \nmid v_r$, and $2 \mid v_{2r}$ but $2^2 \nmid v_{2r}$. Now, by Lemma 3, $u_{n+t} = u_{n+1}u_t + u_n u_{t-1}$. Putting r for both n and t, we obtain $u_{2r} = u_r(u_{r+1} + u_{r-1})$, or $u_{2r} = u_r v_r$. Since $2^{2+b-1} \mid u_r$ but $2^{2+b} \nmid u_r$, and $2 \mid v_r$ but $2^2 \nmid v_r$, we have $2^{2+b} \mid u_{2r}$ but $2^{2+b+1} \nmid u_{2r}$. Now, in the formula $u_{n+t} = u_{n+1} u_t + u_n u_{t-1}$, if we put $2r$ for both n and t, we obtain $u_{4r} = u_{2r} v_{2r}$. Hence, since $2 \mid v_r$ but $2^2 \nmid v_{2r}$ we obtain the result $2^{2+b+1} \mid u_{4r}$ and $2^{2+b+2} \nmid u_{4r}$. That is, we have shown that $f(2^{2+b+1}) \neq 2r$ and $f(2^{2+b+1}) \mid 4r$. Since $f(2^{2+b+1})$ must be a multiple of $f(2^{2+b}) = 2r$, we must have $f(2^{2+b+1}) = 4r = 2^{b+1} f(2)$. Thus we have established that for all positive integers, $f(2^{2+a}) = 2^a f(2)$, or $f(2^e) = 2^{e-2} f(2)$ for $e \geq 3$.

By Theorem 4, we have $k(2^e) = 2^{e-1} k(2)$. Hence for $e \geq 3$, $k(2^e) = 2f(2^e)$.

Since the cases in the direct statement of the theorem are all-inclusive, the converse follows.

Theorem 16: If $p \neq 2$ and $k(p^e) = 4t + 2$ then $k(p^e) = f(p^e)$ and $u_{2t+1} \not\equiv 0 \pmod{p}$.

Proof: Since $k(p^e) = 4t + 2$, $4 \nmid k(p^e)$. This implies that $f(p)$ must be even because if $f(p)$ is odd, then $k(p^e) = 4f(p^e)$ and so $4 \mid k(p^e)$. Also, $4 \nmid f(p)$ because otherwise $k(p^e) = 2f(p^e)$ and

again $4 \mid k(p^e)$. Thus $2 \mid f(p)$ but $4 \nmid f(p)$, and so $k(p^e) = f(p^e)$.

The result $u_{2t+1} \not\equiv 0 \pmod{p}$ follows from the fact that $f(p)$ is even because if $u_{2t+1} \equiv 0 \pmod{p}$, then $f(p) \mid 2t + 1$ which is impossible.

CHAPTER II

NUMBER OF SEQUENCES OF A GIVEN LENGTH

The Problem:

With a knowledge of the possible lengths h(a,b,m) of general Fibonacci sequences $\{f_n\}$ (mod m) we are now in a position to discuss the number of possible sequences of a given length with $0 \leq a < m$ and $0 \leq b < m$.

We first note that if we have an ordered pair (a,b) which gives a sequence of length h when reduced mod m, then there are h - 1 other pairs in this sequence which could have been used instead of (a,b) and would have produced the same length h. However these h periodic sequences are indistinguishable if we consider them as infinite sequences.

There may of course be other pairs, not found in the sequence containing (a,b), which also produce sequences of length h when reduced mod m. But it is clear that the total number of sequences of a given length h must be a multiple of h and the number of distinct sequences of length h can be found by dividing the total number of sequences of length h by the length h.

For a given modulus m, there are m possible non-negative residues. These can be paired among themselves in m^2 different ways. Therefore whatever the modulus, there will be m^2 sequences in all. The number of distinct sequences will depend on the possible values of h. But the following relation will always hold: If n_i represents

the number of distinct sequences of length h_i then $\sum n_i h_i = m^2$.

Throughout the discussion in Chapter I, it was assumed that $(a,b,m) = 1$. It was shown in Lemma 1, that for the purpose of studying possible lengths of periods of sequences this could be assumed. However we are now interested in the number of distinct sequences of a given length, and so we should also include sequences for which $(a,b,m) \neq 1$.

First consider the case when the modulus is a prime p. Since $0 \leq a < p$ and $0 \leq b < p$, there is just one sequence that gives $(a,b,p) \neq 1$, namely the pair (0,0). This will give one sequence of length 1.

Now suppose the modulus is p^2. In addition to all the sequences for which $(a,b,p^2) = 1$, we obtain all the sequences for mod p multiplied throughout by p. We have seen by Lemma 1 that this does not change the lengths of these sequences. The following example illustrates this.

For mod 3 we have

0, 0, ...

0, 1, 1, 2, 0, 2, 2, 1, 0, ...

Thus we have one sequence of length 1 and one distinct sequence of length 8.

Now for mod 3^2 we have

(1) 0, 0, ...

(2) 0, 1, 1, 2, 3, 5, 8, 4, 3, 7, 1, 8, 0, 8, 8, 7, 6, 4, 1, 5, 6, 2, 8, 1,0,...

(3) 0, 2, 2, 4, 6, 1, 7, 8, 6, 5, 2, 7, 0, 7, 7, 5, 3, 8, 2, 1, 3, 4, 7, 2,0,...

(4) 0, 3, 3, 6, 0, 6, 6, 3, 0, ...

(5) 0, 4, 4, 8, 3, 2, 5, 7, 3, 1, 4, 5, 0, 5, 5, 1, 6, 7, 4, 2, 6, 8, 5, 4,0,...

We observe that (2), (3), (5) are sequences for which $(a,b,3^2) = 1$; (1) and (4) are sequences for which $(a,b,3^2) \neq 1$. These correspond

to the sequences for mod 3; that is, the sequences for mod 3 multiplied throughout by 3 produce the sequences for mod 3^2 for which $(a,b,3^2) \neq 1$.

This can now be generalized. If the modulus is p^e, we obtain in addition to the sequences for which $(a,b,p^e) = 1$, all the sequences for mod p^{e-1} multiplied throughout by p. Thus if we know how to determine the number of distinct sequences of a given length when $(a,b,p^e) = 1$, we can find the total number of such sequences including the cases when $(a,b,p^e) \neq 1$.

The next three sections will be devoted to a discussion of the problem for prime power moduli for primes of different forms. We shall be assuming that $k(p^2) \neq k(p)$ and so $k(p^e) = p^{e-1} k(p)$. As was shown in Theorems 2 and 3, upper bounds have been found for k(p). There are many cases where k(p) has this maximum value. The following table lists p and k(p) for $5 < p < 3000$ where k(p) is smaller than the maximum value permitted by Theorems 2 and 3 [2,3] . Thus if a prime of the form $10x \pm 1$ is not listed its period is $p - 1$; and if a prime of the form $10x \pm 3$ is not listed its period is $2p + 2$.

Now, if the modulus is composite and of the form $m = \prod p_i^{e_i}$ we have seen by Theorem 13, that the lengths of the periods for mod $p_i^{e_i}$ for a given (a,b) determine the length of the period for mod $\prod p_i^{e_i}$ for that same (a,b) irrespective of whether $(a,b,m) = 1$ or not. We shall show later how this can be used to determine the number of distinct sequences of a given length.

Moduli of the Form p^e Where $p = 2$ or $p = 10x \pm 3$:

We have seen in Chapter I, that if $(a,b,p^e) = 1$, then $h(2^e) = k(2^e)$

Lengths of Periods Smaller Than The Upper Bounds for $5 < p < 3000$.

p	k(p)	p	k(p)	p	k(p)	p	k(p)
29	14	761	380	1291	430	2081	130
47	32	769	192	1307	872	2089	1044
89	44	797	228	1361	680	2161	80
101	50	809	202	1381	460	2179	198
107	72	811	270	1409	704	2207	64
113	76	829	276	1427	168	2221	148
139	46	859	78	1471	490	2237	1492
151	50	881	176	1483	424	2239	746
181	90	911	70	1511	302	2251	750
199	22	919	102	1523	1016	2267	1512
211	42	941	470	1549	774	2269	324
229	114	953	212	1553	1036	2281	760
233	52	967	176	1579	526	2333	1556
263	176	977	652	1597	68	2371	790
281	56	991	198	1601	160	2389	398
307	88	1009	126	1621	810	2417	124
331	110	1021	510	1669	834	2441	1220
347	232	1031	206	1699	566	2447	1632
349	174	1049	262	1709	854	2521	120
353	236	1061	530	1721	430	2591	518
401	200	1069	356	1733	1156	2621	1310
421	84	1087	128	1741	870	2659	886
461	46	1097	732	1789	894	2663	1776
509	254	1103	96	1823	1216	2687	1792
521	26	1109	554	1861	930	2689	896
541	90	1151	230	1871	374	2729	682
557	124	1217	812	1877	1252	2731	390
563	376	1223	816	1913	1276	2749	916
619	206	1229	614	1951	390	2753	1836
661	220	1231	410	1973	1316	2777	1852
677	452	1249	624	1999	666	2789	164
691	138	1277	852	2027	1352	2801	1400
709	118	1279	426	2029	1014	2861	1430
743	496	1289	322	2069	1034	2969	424

and $h(p^e) = k(p^e)$ for primes of the form $p = 10x \pm 3$. Now if $(a,b,p^e) \neq 1$, then we still have $h(a,b,p^e) \mid k(p^e)$. Since $k(p^e) = p^{e-1} k(p)$, $h(a,b,p^e)$ must always be a divisor of $p^{e-1}k(p)$. Hence its possible values are $1, k(p), pk(p), p^2k(p), \ldots, p^{e-1} k(p)$. We know that there is always one sequence of length 1, namely when $a = 0$ and $b = 0$.

Now for mod p^e let n_i be the number of distinct sequences of length $p^i k(p)$ where $i = 0, 1, \ldots, e - 1$. We will show that all of the n_{e-1} 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 length as the corresponding sequences for mod p^{e-1}. Since none of the sequences for mod p^{e-1} has a length greater than $k(p^{e-1}) = p^{e-2} k(p)$, no sequence for which $(a,b,p^e) \neq 1$ can have a length of $p^{e-1} k(p)$. Moreover all the sequences for which $(a,b,p^e) = 1$ have lengths of $p^{e-1} k(p)$ and so are included in n_{e-1}.

We have thus shown that for mod p^{e-1} the number of distinct sequences of length $p^i k(p)$ is given by n_i where $i = 0,1,\ldots,e-2$.

Since $\sum n_i h_i = m^2$ where h_i are the different possible lengths and n_i are the corresponding numbers of distinct sequences of each of these lengths, we must have

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

and

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

Subtracting we obtain

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

and so

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

Now since n_{e-2}, n_{e-3}, ..., n_0 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 $p^{e-2}\, k(p)$ are those for which $(a',b',p^{e-1}) = 1$ where $a = pa'$ and $b = pb'$. The number of these sequences gives n_{e-2}. Hence we may use the formula derived above and obtain $n_{e-2} = \frac{p^{e-2}(p^2 - 1)}{k(p)}$.

Thus in general for mod p^e we have $n_i = \frac{p^i\,(p^2 - 1)}{k(p)}$ distinct sequences of length $p^i\, k(p)$ for $i = 0, 1, \ldots, e - 1$. We can verify that this gives the total number of sequences equal to p^{2e}. We have

$$\sum n_i\, h_i = 1 + \sum_{i=0}^{e-1} \frac{p^i(p^2 - 1)}{k(p)}\, p^i\, k(p) = 1 + \sum_{i=0}^{e-1} p^{2i}(p^2 - 1).$$

This becomes

$$1 + (p^2 - 1) + (p^4 - p^2) + \ldots + (p^{2e} - p^{2e-2}) = p^{2e}.$$

Thus a knowledge of $k(p)$ enables us to find all possible lengths of sequences for mod p^e as well as the number of sequences corresponding to each of these lengths.

Example 1: Let $m = 2^5$. We have $k(2) = 3$. Therefore in addition to the sequence of length 1, there are $n_i = \frac{2^i(2^2 - 1)}{3} = 2^i$ distinct sequences of length $3 \cdot 2^i$ for $i = 0, 1, 2, 3, 4$. This gives a total of $1 + \sum_{i=0}^{4} 3 \cdot 2^{2i} = 1 + 3(1 + 4 + 16 + 64 + 256) = 1024 = 2^{10}$.

Example 2: Let $m = 7^2$. We have $k(7) = 16$. Therefore in addition to the sequence of length 1, there are $n_i = \frac{7^i\,(7^2 - 1)}{16} = 3 \cdot 7^5$

distinct sequences of length $16 \cdot 7^i$ for $i = 0, 1$. This gives 3 distinct sequences of length 16 and 21 distinct sequences of length 112.

Moduli of the Form 5^e:

With the assumption that $(a,b,5^e) = 1$ it was shown in Theorem 8 that if $(b^2 - ab - a^2, 5) = 1$, then $h(5^e) = k(5^e)$ and if $(b^2 - ab - a^2, 5) = 5$, then $h(5^e) = \frac{1}{5} k(5^e)$.

We can show that the assumption that $(a, b, 5^e) = 1$ is superfluous in the first case because if $(a, b, 5^e) \neq 1$, then $(a,b) = 5^r$ where $0 < r \leq e$ and so $5 \mid a$ and $5 \mid b$; hence $5 \mid b^2 - ab - a^2$ 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 $(a, b, p^e) = 1$. Here we have $5^{2e} - 5^{2e-2}$ pairs (a,b) with $(a, b, 5^e) = 1$. We shall determine how many of these 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

$$b \equiv 3a \pmod 5.$$

Now if $e = 1$, that is $m = 5$, it is clear that a can take values 1, 2, 3, 4 and b the corresponding values 3, 1, 4, 2. Thus there are 4 pairs (a,b) such that $(a,b,5) = 1$ and $(b^2 - ab - a^2, 5) = 5$.

If $e = 2$, that is $m = 25$, a can take the 20 values 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24 and corresponding to each value of a, 5 values of b can be found; e.g. when $a = 1$, b may be 3, 8, 13, 18, or 23; similarly when $a = 2$, b may be 1, 6, 11, 16, or 21; etc. Thus there are $20 \cdot 5 = 4 \cdot 5^2$ pairs (a,b) such that $(a,b,5^2) = 1$ and $(b^2 - ab - a^2, 5) = 5$.

Thus in general for mod 5^e, 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 $5^{e-1}(5^e - 5^{e-1}) = 5^{2e-2}(5 - 1) = 4 \cdot 5^{2e-2}$ pairs (a,b) such that $(a,b,5^e) = 1$ and $(b^2 - ab - a^2, 5) = 5$.

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

$$5^{2e} - 5^{2e-2} - 4 \cdot 5^{2e-2} = 5^{2e} - 5 \cdot 5^{2e-2}$$

$$= 5^{2e} - 5^{2e-1} = 4 \cdot 5^{2e-1} .$$

This is the number of sequences that have length $k(5^e)$. However, not all of these sequences are distinct. We know that the number of distinct sequences of a given length can be obtained by dividing the total number of sequences of the given length by that length.

We have $k(5) = 20$. Hence $k(5^e) = 5^{e-1} k(5) = 4 \cdot 5^e$. Since we have $4 \cdot 5^{2e-1}$ sequences of this length, $\frac{4 \cdot 5^{2e-1}}{4 \cdot 5^e} = 5^{e-1}$ is the number of distinct sequences of length $4 \cdot 5^e$.

We have also shown that there are $4 \cdot 5^{2e-2}$ sequences with $(a,b,5^e) = 1$ of length $\frac{1}{5} k(5^e) = 4 \cdot 5^{e-1}$. Hence $\frac{4 \cdot 5^{2e-2}}{4 \cdot 5^{e-1}} = 5^{e-1}$

distinct sequences of length $4 \cdot 5^{e-1}$.

Finally there are also the cases for which $(a,b,5^e) \neq 1$ in which case $h(a,b,5^e) \mid k(5^e)$. But we have explained that the sequences mod 5^e for which $(a,b,5^e) \neq 1$ are the same as the sequences mod 5^{e-1} multiplied throughout by 5. To see what the pattern is, let us look at a few simple cases:

For mod 5, there is only one sequence for which $(a,b,5^e) \neq 1$, namely when $a \equiv 0$ and $b \equiv 0$. This gives one sequence of length 1. We also have $5^{e-1} = 5^0 = 1$ distinct dequence of length $4 \cdot 5^{e-1} = 4 \cdot 5^0 = 4$ and $5^{e-1} = 5^0 = 1$ distinct sequence of length $4 \cdot 5^e = 4 \cdot 5 = 20$. These sequences are

0, 0, ...

1, 3, 4, 2, ...

0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, ...

Now for mod 25, the cases for which $(a,b,5^e) \neq 1$ are the following:

0, 0, ...

5, 15, 20, 10, ...

0, 5, 5, 10, 15, 0, 15, 15, 5, 20, 0, 20, 20, 15, 10, 0, 10, 10, 20, 5,...

These correspond to the sequences for mod 5. But if $(a,b,5^2) \equiv 1$ we have $5^{e-1} = 5$ distinct sequences of length $4 \cdot 5^{e-1} = 20$ and $5^{e-1} = 5$ distinct sequences of length $4 \cdot 5^e = 100$. Thus the total number of distinct sequences of each length is given by:

1	distinct	sequence(s)	of	length	1
$5^0 = 1$	"	"	"	"	4
$5 + 5^0 = 6$	"	"	"	"	20
5	"	"	"	"	100.

Now for mod 5^3, if $(a,b,5^3) = 1$ we have $5^{e-1} = 25$ distinct sequences of length $4 \cdot 5^{e-1} = 100$ and $5^{e-1} = 25$ distinct sequences of length $4 \cdot 5^e = 500$. The cases for which $(a,b,5^3) \neq 1$ are the same sequences for mod 5^2 multiplied throughout by 5. Therefore the total number of sequences for mod 5^3 is:

1	distinct	sequence(s)	of	length	1
$5^0 = 1$	"	"	"	"	4
$5 + 5^0 = 6$	"	"	"	"	20
$5^2 + 5 = 30$	"	"	"	"	100
$5^2 = 25$	"	"	"	"	500

Thus in general, for mod 5^e we get

1	distinct	sequence(s)	of	length	1
$5^0 = 1$	"	"	"	"	$4 \cdot 5^0$
$5 + 5^0 = 6 \cdot 5^0$	"	"	"	"	$4 \cdot 5$
$5^2 + 5 = 6 \cdot 5$	"	"	"	"	$4 \cdot 5^2$
.	.	.	.	.	.
$5^{e-1} + 5^{e-2} = 6 \cdot 5^{e-2}$	"	"	"	"	$4 \cdot 5^{e-1}$
5^{e-1}	"	"	"	"	$4 \cdot 5^e$

Example: For mod 5^6 we have e = 6. Hence

1	distinct	sequence(s)	of	length	1
$5^0 = 1$	"	"	"	"	$4.5^0 = 4$
$6\cdot5^0 = 6$	"	"	"	"	$4\cdot5 = 20$
$6\cdot5 = 30$	"	"	"	"	$4\cdot5^2 = 100$
$6\cdot5^2 = 150$	"	"	"	"	$4\cdot5^3 = 500$
$6\cdot5^3 = 750$	"	"	"	"	$4\cdot5^4 = 2500$
$6\cdot5^4 = 3750$	"	"	"	"	$4\cdot5^5 = 12500$
$5^5 = 3125$	"	"	"	"	$4\cdot5^6 = 62500$

Moduli of the Form p^e where $p = 10x \pm 1$

We know that $k(p^e)$ is even, and so it is either of the form $4t$ or of the form $4t + 2$.

We shall first consider the case for which $k(p^e) = 4t$. By Theorem 9, $k(p^e) = 4t$ implies that h cannot be odd; and if h is even then by Theorem 11, $h(p^e) = k(p^e)$. Thus on condition $(a,b,p^e) = 1$, $h(p^e) = k(p^e) = p^{e-1}\,k(p)$.

We know that for primes of the form $p = 10x \pm 1$, $k(p) \mid (p-1)$. Hence we may write $k(p) = \frac{p-1}{d}$ where d is some positive integer greater than or equal to 1. Now since $\sum n_i h_i = p^{2e}$, and for mod p all the sequences except the case a = 0, b = 0 give (a,b,p) = 1, we obtain.

1 sequence of length 1, and

$d(p + 1)$ distinct sequences of length $\frac{p-1}{d}$.

For mod p^2, the sequences for which $(a,b,p^2) \neq 1$ are those for mod p multiplied throughout by p. Since $\sum n_i h_i = p^4$ and $k(p^2) = pk(p) = \frac{p(p-1)}{d}$, we have

1 sequence of length 1,

$d(p+1)$ distinct sequences of length $\frac{p-1}{d}$, and

$d_\rho(p+1)$ distinct sequences of length $\frac{p(p-1)}{d}$.

For mod p^3, the sequences for which $(a,b,p^3) \neq 1$ are those for mod p^2 multiplied throughout by p. Since $\sum n_i h_i = p^6$ and $k(p^3) = \frac{p^2(p-1)}{d}$, we have in addition to the sequences obtained from those for mod p^2, $dp^2(p+1)$ distinct sequences of length $\frac{p^2(p-1)}{d}$.

Hence in general, for mod p^e, in addition to the sequences obtained from those for mod p^{e-1}, we have $dp^{e-1}(p+1)$ distinct sequences of length $\frac{p^{e-1}(p-1)}{d}$. Thus for mod p^e we have 1 sequence of length 1 and $dp^i(p+1)$ distinct sequences of length $\frac{p^i(p-1)}{d}$ with $i = 0, 1, \ldots, e-1$.

Example: For mod 89^3, we have $e = 3$ and $k(89) = 44$; that is $d = 2$. Hence we obtain 1 sequence of length 1 and $2 \cdot 89^i \cdot 90$ or $180 \cdot 89^i$ distinct sequences of length $\frac{89^i \cdot 88}{2}$ or $44 \cdot 89^i$ with $i = 0,1,2$. This gives 180 distinct sequences of length 44,

16020 distinct sequences of length 3916,

and

1425780 " " " " 348524

Next we consider the case when $k(p^e)$ is of the form $4t + 2$. By Theorem 10, we know that $h = 2t + 1$ for some (a,b). Therefore if $k(p^e) = 4t + 2 = \frac{p-1}{d}$ then $h = 2t + 1 = \frac{p-1}{2d}$ for some (a,b). It was

shown in Theorem 5, that if $(a,b,p^e) = 1$ and $(b^2 - ab - a^2, p^e) = 1$, then $h(p^e) = k(p^e)$. Now if $(b^2 - ab - a^2, p^e) \neq 1$ and $(a,b,p^e) = 1$, then $h(a,b,p^e) \mid k(p^e)$. We can show that in such cases the only possible values for $h(a,b,p^e)$ are $k(p^e)$ or $\frac{1}{2} k(p^e)$. If $h(a,b,p^e)$ is even, Theorem 11 shows that $h(a,b,p^e) = k(p^e)$; and if $h(a,b,p^e)$ is odd, Theorem 9 shows that $k(p^e) = 2h(a,b,p^e)$, and hence $h(a,b,p^e) = \frac{1}{2} k(p^e)$.

Let us first consider the case for mod p. We will determine the number of pairs (a,b) for which $(b^2 - ab - a^2, p) \neq 1$. This is equivalent to the condition $b^2 - ab - a^2 \equiv 0 \pmod{p}$, 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 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

$$b_1 \equiv ra \quad \text{and} \quad b_2 \equiv sa \pmod{p}$$

where

$$r \equiv \frac{1 + c}{2} \quad \text{and} \quad s \equiv \frac{1 - c}{2} \pmod{p}.$$

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 $p \mid a$; but $b \equiv \left(\frac{1 \pm c}{2}\right)a \pmod{p}$, and so $b \equiv 0 \pmod{p}$ and $p \mid b$; 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 $(b^2 - ab - a^2, p) \neq 1$; 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 $b_2 \equiv s$ (mod p)

If $a \equiv 2$, $b_1 \equiv 2r$ and $b_2 \equiv 2s$ (mod p)

If $a \equiv 3$, $b_1 \equiv 3r$ and $b_2 \equiv 3s$ (mod p)

. . . . .

If $a \equiv p - 1$, $b_1 \equiv (p-1)r$ and $b_2 \equiv (p-1)s$ (mod 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 pairs (a,b) with $h(a,b,p) = 2t+1$.

Without loss of generality we may assume a to be 1. This gives $b_1 \equiv r$ and $b_2 \equiv s$ (mod p). Now either (1,r) or (1,s) will produce a sequence of length $2t + 1$ when reduced mod p. We wish to show that not both of these can produce sequences of length $2t + 1$.

Now suppose that both (1, r) and (1,s) produce sequences of length $2t + 1$. We have

$$1, r, 1 + r, 1 + 2r, 2 + 3r, \ldots, u_{n-1} + u_n r, \ldots \quad \text{(mod p)}$$

$$1, s, 1 + s, 1 + 2s, 2 + 3s, \ldots, u_{n-1} + u_n s, \ldots \quad \text{(mod p)}.$$

Therefore we must have

$$u_{2t} + u_{2t+1} r \equiv 1 \pmod{p}$$

and

$$u_{2t} + u_{2t+1} s \equiv 1 \pmod{p}$$

Hence

$$u_{2t+1}(r - s) \equiv 0 \pmod{p}.$$

Since by Theorem 16, $u_{2t+1} \not\equiv 0 \pmod{p}$, 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 obtain

$$r + r^2 = r(1 + r) \equiv r^3, \pmod{p}$$

$$r^2 + r^3 = r(r + r^2) \equiv r^4, \pmod{p}, \text{ etc.}$$

Thus the sequence

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

may be written as

$$1, r, r^2, r^3, r^4, \ldots \pmod{p}$$

Similarly, the sequence

$$1, s, 1 + s, 1 + 2s, 2 + 3s, \ldots \pmod{p}$$

may be written as

$$1, s, s^2, s^3, s^4, \ldots \pmod{p}.$$

Therefore, the assumption that these two sequences have periods

of length $2t+1$ when reduced mod p, implies that

$$r^{2t+1} \equiv 1 \quad \text{and} \quad s^{2t+1} \equiv 1 \qquad (\text{mod } p).$$

Multiplying these two congruences we obtain

$$(rs)^{2t+1} \equiv 1 \quad (\text{mod } p)$$

But

$$rs \equiv \left(\frac{1+c}{2}\right)\left(\frac{1-c}{2}\right) = \frac{1-c^2}{4} \equiv -1 \quad (\text{mod } p)$$

because

$$c^2 \equiv 5 \ (\text{mod } p), \quad \text{and so} \quad (-1)^{2t+1} \equiv 1 \ (\text{mod } p)$$

which is impossible.

Hence again, if (1,r) produces a sequence of length $\frac{1}{2}k(p) = 2t+1$, then (1, s) cannot produce a sequence 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 $(a,b,p) = 1$, the $p-1$ pairs produce sequences of length $\frac{1}{2}k(p)$ and the other $p-1$ pairs produce sequences of length $k(p)$. However, not all of these are distinct. If $k(p) = \frac{p-1}{d}$, then there will be $\frac{p-1}{\frac{p-1}{d}} = d$ distinct sequences of length $\frac{p-1}{d}$ and $\frac{p-1}{\frac{p-1}{2d}} = 2d$ distinct sequences of length $\frac{p-1}{2d}$.

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 $(p^2-1) - 2(p-1) = p^2 - 2p + 1 = (p-1)^2$. All of these have periods of length $k(p) = \frac{p-1}{d}$. This gives $\frac{(p-1)^2}{\frac{p-1}{d}} = d(p-1)$ distinct sequences of length $\frac{p-1}{d}$.

Therefore for mod p we have

1	distinct	sequence(s)	of	length	1
2d	"	"	"	"	$\frac{p-1}{2d}$
$d + d(p-1) = dp$	"	"	"	"	$\frac{p-1}{d}$.

Example: For mod 151, we have $k(151) = 50$ which is $\frac{150}{3}$; that is, $d = 3$. We obtain

1	distinct	sequence(s)	of	length	1
6	"	"	"	"	25
453	"	"	"	"	50.

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

$$j = 0, 1, 2, \ldots, p^{e-1} - 1,$$

If

$$a \equiv 2,\ b_1 \equiv 2r + jp \quad \text{and} \quad b_2 \equiv 2s + jp \pmod{p^e}$$

where

$$j = 0, 1, \ldots, p^{e-1} - 1.$$

These are equivalent to

$$b_1 \equiv 2(r + jp) \quad \text{and} \quad b_2 \equiv 2(s + jp) \pmod{p^e}$$

where

$$j = 0, 1, 2, \ldots, p^{e-1} - 1.$$

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 $j = 0, 1, \ldots, p^{e-1} - 1$, it is sufficient to consider the sequences $(1, r + jp)$ and $(1, s + jp)$ for $j = 0, 1, \ldots, p^{e-1} - 1$.

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 $0, 1, 2, \ldots, p^{e-1}-1$, $h(1, s + ip, p^e) \neq 2t + 1$. Suppose for some i, $h = h(1, r + jp, p^e) = h(1, s + ip, p^e) = \frac{1}{2}k(p^e) = 2t + 1$. We have

$$1, r + jp, \ldots, u_{n-1} + u_n(r + jp), \ldots. \pmod{p^e}$$

$$1, s + ip, \ldots, u_{n-1} + u_n(s + ip), \ldots. \pmod{p^e};$$

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 Theorem 16, $u_h \not\equiv 0 \pmod{p}$, 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 $\frac{1}{2}k(p^e)$ or $2t + 1$.

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 $0, 1, \ldots, p^{e-1} - 1$. 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 Theorem 16, $u_h \not\equiv 0 \pmod{p}$, 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

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

Therefore, the number of distinct sequences of length $\frac{p^{e-1}(p-1)}{2d}$ is given by $\frac{p^{e-1}(p-1)}{p^{e-1}(p-1)/2d} = 2d$. 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 $k(p^e) = \frac{p^{e-1}(p-1)}{d}$ $= 4t + 2$. Therefore, the number of distinct such sequences of length

$\frac{p^{e-1}(p-1)}{d}$ is given by $\frac{p^{e-1}(p-1)(2p^{e-1}-1)}{p^{e-1}(p-1)/d} = d(2p^{e-1}-1)$.

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 $p^{2e-2}(p-1)(p+1) - 2p^{2e-2}(p-1)$, or $p^{2e-2}(p-1)^2$ pairs with $(b^2 - ab - a^2, p^e) = 1$. All of these produce sequences of length $k(p^e) = \frac{p^{e-1}(p-1)}{d}$. Hence there are $\frac{p^{2e-2}(p-1)^2}{p^{e-1}(p-1)/d}$ $= dp^{e-1}(p-1)$ distinct sequences of this kind.

In addition to these, there are the sequences for which $(a, b, p^e) \neq 1$. These are the sequences for mod p^{e-1} multiplied throughout by p. Thus for mod p^e we have 1 distinct sequence of length 1

2d	distinct	sequences	of	length	$\frac{p-1}{2d}$
dp	"	"	"	"	$\frac{p-1}{d}$
2d	"	"	"	"	$\frac{p(p-1)}{2d}$
$d(p^2+p-1)$	"	"	"	"	$\frac{p(p-1)}{d}$
2d	"	"	"	"	$\frac{p^2(p-1)}{2d}$
.	.	.	.	.	.
2d	"	"	"	"	$\frac{p^{e-1}(p-1)}{2d}$

$d(2p^{e-1}-1) + dp^{e-1}(p-1) = d(p^e + p^{e-1} - 1)$ distinct sequences of length $\frac{p^{e-1}(p-1)}{d}$

That is, we have 1 sequence of length 1, 2d distinct sequences of each of lengths $\frac{p^i(p-1)}{2d}$, and $d(p^{i+1} + p^i - 1)$ distinct sequences of length $\frac{p^i(p-1)}{d}$ for $i = 0, 1, \ldots, e-1$.

Example: For mod 139^3, $e = 3$ and $d = 3$.

We have

1	distinct	sequence(s)	of	length	1
6	"	"	"	"	23
417	"	"	"	"	46
6	"	"	"	"	3197
58377	"	"	"	"	6394
6	"	"	"	"	444383
8114817	"	"	"	"	888766

Composite Moduli of the Form $\prod p_i^{e_i}$

For any prime p, we have given rules for obtaining the number of distinct sequences (mod p^e) of each of the possible lengths. Thus, our problem is now reduced to a discussion of the case where the modulus is of the form $\prod p_i^{e_i}$. The notation involved will be considerably simpler if we consider the equivalent problem of the modulus being of the form $\prod m_i$ where the m_i are pairwise relatively prime.

Let us first discuss the case where $m = m_1 m_2$ and $(m_1, m_2) = 1$.

We have seen in Theorem 13, that if a pair (a,b) produces a sequence of length h_1 when reduced mod m_1 and produces a sequence of length h_2 when reduced mod m_2, then it will produce a sequence of length h when reduced mod $m_1 m_2$ where h is the least common multiple of h_1 and h_2.

Now suppose $h_1 = h(a, b, m_1)$ and $h_2 = h(c, d, m_2)$. By the Chinese Remainder Theorem, we know that each pair (a,b) (mod m_1)

and each pair (c,d) (mod m_2) gives rise to a unique pair (e,f) (mod $m_1 m_2$) such that $e \equiv a$, $f \equiv b \pmod{m_1}$, and $e \equiv c$, $f \equiv d \pmod{m_2}$. By Theorem 13, $h(e, f, m_1 m_2)$ 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 $h(e, f, m_1 m_2)$ is the least common multiple of h_1 and h_2.

Let $n(h, m)$ denote the number of distinct sequences of length $h \pmod{m}$, and let $N(h,m) = h \cdot n(h, m)$. Then $N(h, m)$ represents the number of pairs that produce sequences of length $h \pmod{m}$. The least common multiple of h_1 and h_2 will be denoted by $[h_1, h_2]$.

We have seen that each pair of pairs (a, b) (mod m_1) and (c,d) (mod m_2) gives a unique pair (e, f) (mod $m_1 m_2$) of length $h = [h_1, h_2]$; so there are $N(h_1, m_1) \cdot N(h_2, m_2)$ such pairs (e,f) with length h_1 (mod m_1) and length h_2 (mod m_2). Now any pair (e,f) (mod $m_1 m_2$) 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

$$N(h, m_1 m_2) = \sum_{[h_1, h_2] = h} N(h_1, m_1) \cdot N(h_2, m_2),$$

and the number of distinct sequences of length $h = [h_1, h_2] \pmod{m_1 m_2}$ is given by

$$n(h, m_1 m_2) = \sum_{[h_1, h_2] = h} \frac{N(h_1, m_1) \cdot N(h_2, m_2)}{[h_1, h_2]},$$

or

$$n(h, m_1 m_2) = \sum_{[h_1, h_2] = h} \frac{h_1 n(h_1, m_1) \cdot h_2 \cdot n(h_2, n_2)}{[h_1, h_2]},$$

or

$$n(h, m_1, m_2) = \sum_{[h_1, h_2] = h} n(h_1, m_1) \cdot n(h_2, m_2) \cdot (h_1, h_2)$$

where (h_1, h_2) denotes the greatest common divisor of h_1 and h_2.

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

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

and

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

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

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

and

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

Example: Let $m = 180 = 2^2 \cdot 3^2 \cdot 5$. We have $n(1, 2^2) = 1$, $n(3, 2^2) = 1$, $n(6, 2^2) = 2$, $n(1, 3^2) = 1$, $n(8, 3^2) = 1$, $n(24, 3^2) = 3$, $n(1,5) = 1$, $n(4,5) = 1$, and $n(20,5) = 1$. Therefore for mod 180, we have $n(1, 180) = 1$, $n(3, 180) = 1$, $n(4,180) = 1$, $n(6,180) = 2$, $n(8,180) = 1 + 4 = 5$, $n(12,180) = 1 + 4 = 5$, $n(20,180) = 1$, $n(24,180) = 3 + 12 + 1 + 4 + 9 + 36 + 4 + 16 + 36 + 144 = 265$, $n(40,180) = 4$, $n(60,180) = 1 + 4 = 5$, and $n(120,180) = 12 + 4 + 36 + 16 + 144 = 212$.

Summary:

We have shown that if $k(p^e)$ is known, it is possible to determine all possible values of $h(a, b, m)$ as well as the number of sequences corresponding to each h, no matter what the form of m may be.

The problem of determining the value of $k(p^e)$ is reduced to that of knowing the value of $k(p)$ if it can be proved that for all p, $k(p^2) \neq k(p)$, or if for every p the value of t is known where t is the largest integer for which $k(p^t) = k(p)$.

Using the notation of the previous section where $n(h,m)$ denotes the number of distinct sequences of length $h \pmod m$ and $N(h, m) = h \cdot n(h, m)$, the results we have found are summarized below. We will abbreviate $n(h, m)$ as $n(h)$ and $k(p)$ as k when necessary. We first give the formulas based on the assumption that $k(p^2) \neq k(p)$ and so $k(p^e) = p^{e-1} k(p)$. Note that for any h that is not mentioned below $n(h, m) = 0$.

I. $n(1, 2^e) = 1$ and $n(3 \cdot 2^i, 2^e) = 2^i$ for $i = 0,1,\ldots,e-1$.

II. $n(1, 5^e) = 1$, $n(4, 5^e) = 1$, $n(4 \cdot 5^i, 5^e) = 6 \cdot 5^{i-1}$

for $i = 1, \ldots, e-1$, and $n(4 \cdot 5^e, 5^e) = 5^{e-1}$.

III. If $m = p^e$ where $p \equiv \pm 3 \pmod{10}$, then $k(p) = \frac{2(p+1)}{d}$ for some $d \geq 1$. We have

$$n(1,p^e) = 1 \text{ and } n(p^i k) = \frac{p^i(p^2-1)}{k} \text{ for } i = 0,1,\ldots,e-1$$

or

$$n(1,p^e) = 1 \text{ and } n(2p^i(p+1)/d) = \frac{dp^i(p-1)}{2} \text{ for } i=0,1,\ldots,e-1.$$

IV. If $m = p^e$ where $p \equiv \pm 1 \pmod{10}$, then $k(p) = \frac{p-1}{d}$ for some $d \geq 1$.

A. If $4 \mid k(p)$,

$$n(1,p^e) = 1 \text{ and } n(p^i k) = \frac{p^i(p^2-1)}{k} \text{ for } i = 0,1,\ldots,e-1,$$

or

$$n(1,p^e) = 1 \text{ and } n(p^i(p-1)/d) = dp^i(p+1) \text{ for } i = 0,1,\ldots,e-1.$$

B. If $4 \nmid k(p)$,

$$n(1, p^e) = 1, \quad n(p^i k/2) = \frac{2(p-1)}{k}, \quad \text{and}$$

$$n(p^i k) = \frac{(p-1)(p^{i+1} + p^i - 1)}{k} \quad \text{for } i = 0, 1, \ldots, e-1.$$

Or

$$n(1, p^e) = 1, \quad n(p^i(p-1)/2d) = 2d, \quad \text{and}$$

$$n(p^i(p-1)/d) = d(p^{i+1} + p^i - 1) \quad \text{for } i = 0, 1, \ldots, e-1.$$

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

We will also give below the corresponding results for the case where t is the largest integer such that $k(p^t) = k(p)$ and $t > 1$, and so $k(p^e) = p^{e-t} k(p)$ for $e \geq t$. Since $k(2^2) \neq k(2)$ and $k(5^2) \neq k(5)$, this will only affect our results for $p \equiv \pm 3$ and $p \equiv \pm 1 \pmod{10}$.

I. For $m = p^e$, $p \equiv \pm 3 \pmod{10}$, $k(p) = \frac{2(p+2)}{d}$ for some $d \geq 1$:

$$n(1, p^e) = 1, \quad n(k) = \sum_{i=0}^{t-1} \frac{p^{2i}(p^2 - 1)}{k}, \quad \text{and}$$

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

Or

$$n(1, p^e) = 1, \quad n(2(p+1)/d) = \sum_{i=0}^{t-1} \frac{d p^{2i}(p-1)}{2}, \quad \text{and}$$

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

II. For $m = p^e$, $p \equiv \pm 1 \pmod{10}$, $k(p) = \frac{p-1}{d}$ for some $d \geq 1$:

A. If $4 \mid k(p)$,

$$n(1, p^e) = 1, \quad n(k) = \sum_{i=0}^{t-1} \frac{p^{2i}(p^2 - 1)}{k}, \quad \text{and}$$

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

Or

$$n(1,p^e) = 1,\ n((p-1)/d) = \sum_{i=0}^{t-1} dp^{2i}(p+1), \text{ and}$$

$$n(p^{i-t+1}(p-1)/d) = dp^{i+t-1}(p+1) \quad \text{for } i = t,\ldots,e-1.$$

B. If $4 \nmid k(p)$,

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

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

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

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

Or

$$n(1,p^e) = 1,\ n((p-1)/2d) = \sum_{i=0}^{t-1} 2dp^i,$$

$$n((p-1)/d) = \sum_{i=0}^{t-1} dp^i(p^{i+1}+p^i-1),$$

$$n(p^{i-t+1}(p-1)/2d) = 2dp^{t-1}, \text{ and}$$

$$n(p^{i-t+1}\,(p-1)/d) = dp^{t-1}(p^{i+1}+p^i-1) \quad \text{for } i = t,\ldots,e-1.$$

REFERENCES

1. N.N. Vorob'ev, Fibonacci Numbers, trans. H. Moss, New York; Blaisdell Publishing Company, 1961.

2. D.D. Wall, "Fibonacci Series Modulo m", Amer. Math. Monthly, 67 (1960) 525 - 532.

3. Brother U. Alfred, "Additional Factors of the Fibonacci and Lucas Series", The Fibonacci Quarterly, 1 (1963) 1:34 - 42.

4. D.W. Robinson, "The Fibonacci Matrix Modulo m", The Fibonacci Quarterly, 1 (1963) 2: 29 - 36.

5. J. Vinson, "The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence", The Fibonacci Quarterly, 1 (1963) 2: 37 - 45.

6. D. Jarden, "On the Periodicity of the Last Digits of the Fibonacci Numbers, " The Fibonacci Quarterly, 1 (1963) 4: 21 - 22.

7. Brother U. Alfred, "Primes Which Are Factors of All Fibonacci Sequences", The Fibonacci Quarterly, 2(1964) 1: 33 - 38.

8. R. L. Heimer, "Further Comments on the Periodicity of the Digits of the Fibonacci Sequence", The Fibonacci Quarterly, 2(1964) 3:211-214.

9. R.B. Ely, "Fibonaccious Factors", The Fibonacci Quarterly, 3(1965) 3: 187 - 198.

10. J.H. Halton, "On the Divisibility Properties of Fibonacci Numbers", The Fibonacci Quarterly, 4 (1966) 3: 217 - 240.

11. Brother U. Alfred, An Introduction to Fibonacci Discovery, California: The Fibonacci Association, 1965.

12. I. Niven and H.S. Zuckerman, An Introduction to the Theory of Numbers, New York: John Wiley and Sons, Inc., 1960.

13. W.J. LeVeque, Topics in Number Theory, vol. I, Reading, Mass: Addison Wesley Publishing Company, Inc., 1956.

APPENDIX

In answer to the letter sent to D.D. Wall regarding the proof of Theorem 11, we have received from him the outline of a proof using a different approach than the one he had used before. The following proof is suggested by his outline.

Theorem 11: If $m = p^e$, $p > 2$, $p \neq 5$, and h is even, then $h = k$.

Proof: As in Theorem 9, we must have

$$u_{h+1} + u_{h-1} \equiv 1 + (-1)^h \pmod{p^e}.$$

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

$$u_h \equiv 2(1 - u_{h-1}) \pmod{p^e}.$$

We have $f_h \equiv a$ and $f_{h+1} \equiv b \pmod{p^e}$ and $f_h = au_{h-1} + bu_h$, and so

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

and

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

Now, as it was shown in Theorem 5, 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 $h = k$. Next consider the cases for which $b^2 - ab - a^2 \equiv 0 \pmod{p}$. Since $u_h \equiv 2(1 - u_{h-1}) \pmod{p^e}$ we must have

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

or

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

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 aquivalent 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 $h = k$.