ON THE DIVISIBILITY PROPERTIES OF FIBONACCI NUMBERS

John H. Halton, University of Colorado, Boulder, Colorado

1. INTRODUCTION

The Fibonacci sequence is defined by the recurrence relation

$$F_{n+2} = F_{n+1} + F_n \qquad , \tag{1}$$

together with the particular values

$$(2)\quad \begin{cases} F_0 = 0, \quad F_1 = 1 \quad , \\ \text{whence} \\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8 = 2^3,\ F_7 = 13 \\ F_8 = 21 = 3 \cdot 7,\ F_9 = 34 = 2 \cdot 17,\ F_{10} = 55 = 5 \cdot 11, \cdots \quad ; \\ \text{and, in particular,} \\ F_{12} = 144 = 2^4 \cdot 3^2,\ F_{14} = 377 = 13 \cdot 29,\ F_{15} = 610 = 2 \cdot 5 \cdot 61, \\ F_{18} = 2584 = 2^3 \cdot 17 \cdot 19,\ F_{20} = 6765 = 3 \cdot 5 \cdot 11 \cdot 41, \\ F_{21} = 10946 = 2 \cdot 13 \cdot 421,\ F_{24} = 46368 = 2^5 \cdot 3^2 \cdot 7 \cdot 23 \ , \\ F_{25} = 75025 = 5^2 \cdot 3001,\ F_{28} = 317811 = 3 \cdot 13 \cdot 29 \cdot 281 \ , \\ F_{30} = 832040 = 2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61,\ F_{35} = 9227465 = 5 \cdot 13 \cdot 141961 \ , \\ F_{36} = 14930352 = 2^4 \cdot 3^3 \cdot 17 \cdot 19 \cdot 107,\ F_{42} = 267914296 = 2^3 \cdot 13 \cdot 29 \cdot 211 \cdot 421 \\ F_{70} = 190392490709135 = 5 \cdot 11 \cdot 13 \cdot 29 \cdot 71 \cdot 911 \cdot 141961 \quad . \end{cases}$$

In this paper, we shall be concerned with the sub-sequence of Fibonacci numbers which are divisible by powers of a given integer. We shall also be interested in the associated problem of the periodic nature of the sequence of remainders, when the Fibonacci numbers are divided by a given integer.

The Fibonacci sequence is defined for all integer values of the index n. However, the well-known identity

$$F_{-n} = (-1)^{n+1}F_n \tag{3}$$

shows that negative indices add nothing to the divisibility properties of the Fibonacci numbers. We shall consequently simplify our discussion, without loss of generality, by imposing the restriction that $n \geq 0$.

Of the many papers dealing with our problem, perhaps the most useful are those of Carmichael [1], Robinson [5], Vinson [6], and Wall [7]; and the reader can find many additional references in these. Most of the other papers in the field give either less complete results, or give them for more general sequences.

We shall make use, in what follows, of the well-known identities:*

$$F_n = \frac{1}{\sqrt{5}}\left\{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right\} \quad ; \tag{4}$$

$$F_n = \left(\frac{1}{2}\right)^{n-1} \sum_{s=0}^{[\frac{1}{2}(n-1)]} \binom{n}{2s+1} 5^s, \quad \text{if } n \geq 1 \quad ; \tag{5}$$

$$F_n^2 - F_{n-1}F_{n+1} = (-1)^{n-1} \quad ; \tag{6}$$

$$F_{kn+r} = \sum_{h=0}^{k} \binom{k}{n} F_n^h F_{n-1}^{k-h} F_{r+h}, \quad \text{if } k \geq 0 \; ; \tag{7}$$

and since $F_0 = 0$,

$$F_{kn} = F_n \sum_{h=1}^{k} \binom{k}{h} F_n^{h-1} F_{n-1}^{k-h} F_h \quad . \tag{8}$$

*See, for example, equations (6), (3), (5), (67), and (34), in my earlier paper [3]. Equation (5) above follows from (4) by the binomial theorem.

Also

$$\binom{k+1}{h} = \binom{k}{h} + \binom{k}{h-1} , \tag{9}$$

and

$$p \text{ divides } \binom{p}{s} \text{ if } p \text{ is prime and } 0 < s < p , \tag{10}$$

and Fermat's theorem, that

$$m^{p-1} \equiv 1 \pmod{p} \text{ if } p \text{ is prime and } (m,p) = 1 \tag{11}$$

As is customary, we use $(A, B, C, \cdots)$ to represent the greatest common factor of integers $A, B, C, \cdots$, and $[A, B, C, \cdots]$ to represent their least common multiple. We have

$$m^{\frac{1}{2}(p-1)} \equiv (m/p) \pmod{p} , \tag{12}$$

where p is an odd prime and (m/p) denotes the Legendre index, which is ± 1 if $(m,p) = 1$, and 0 otherwise.

Each writer seems to have invented his own notation. I shall adopt the following, which comes closest to that of Robinson in [5].

Definition 1. The least positive index α such that F_α is divisible by m^n (that is, $F_\alpha \equiv 0 \pmod{m^n}$) will be written

$$\alpha(m,n) = \alpha(m^n, 1) = \alpha(m^n) . \tag{13}$$

This is variously called the "rank of apparition" (why not "appearance"?) of m^n, or the "restricted period" of the Fibonacci sequence modulo m^n.

Definition 2. The least positive index μ such that both $F_\mu \equiv 0$ and $F_{\mu+1} \equiv 1 \pmod{m^n}$ will be written

(14) $$\mu(m,n) = \mu(m^n,1) = \mu(m^n) .$$

This notation follows Carmichael [2], who named μ the "characteristic number" of the Fibonacci sequence modulo m^n. It is also called the "period" of the sequence modulo m^n.

Definition 3. I shall write

(15) $$\mu(m,n)/\alpha(m,n) = \beta(m,n) = \beta(m^n,1) = \beta(m^n) .$$

Definition 4. The greatest integer ν such that $F_{\alpha(m,n)}$ is divisible by m^ν will be written

(16) $$\nu(m,n) = \nu(m^n,1) = \nu(m^n) .$$

It is then clear that

(17) $$\alpha(m,n) = \alpha(m,n+1) = \cdots = \alpha(m,\nu(m,n)) < \alpha(m,\nu(m,n)+1)$$

or, equivalently,

(18) $$\nu(m,\nu(m,n)) = \nu(m,n) .$$

Definition 5. I shall call the sequence

(19) $$F_{\alpha(m,1)},\ F_{\alpha(m,2)},\cdots,F_{\alpha(m,n)},\cdots ,$$

the divisibility sequence of m.

2. PRELIMINARIES

We shall need a number of preliminary results, whose proofs will be outlined for completeness.

Lemma 1. F_n, F_{n+1}, and F_{n+2} are always pairwise prime.
[If f divides two of the numbers, it must divide the third, by (1). Thus, , by

induction along the sequence, using (1), we see that f must divide every F_m. Thus, since $F_1 = 1$, $f = 1$.]

Lemma 2. If $n \geq 2$, F_n is a strictly increasing positive function of n. [By (1), if $F_{n-2} \geq 0$ and $F_{n-1} \geq 1$, $F_{n+1} > F_n \geq 1$. By (2), $F_0 = 0$ and $F_1 = 1$, whence the lemma follows by induction.]

Lemma 3. If $n \geq 3$

$$\alpha(F_n) = n \ . \tag{20}$$

[By Lemma 2, if $n \geq 3$, the least index m such that $F_m \geq F_n$ is n.]

Lemma 4.

$$(F_m, F_n) = F_{(m,n)} \ . \tag{21}$$

[Let $(m,n) = g$ and $(F_m, F_n) = G$. There are integers x and y (not both negative) such that $xm + yn = g$. Suppose $x \geq 0$; then, by (7),

$$F_g = \sum_{h=0}^{x} \binom{x}{h} F_m^h F_{m-1}^{x-h} F_{yn+h} \equiv 0 \pmod{G} ,$$

since G divides F_m and F_n, and by (8), F_n divides F_{yn}. Thus F_g is divisible by G. Again, by (8), $F_{kg} \equiv 0 \pmod{F_g}$. Thus, since g divides both m and n, F_g divides both F_m and F_n, and so G is divisible by F_g.]

Lemma 5. F_m is divisible by F_n, if and only if either m is divisible by n, or $n = 2$.
[By Lemma 4, $(F_m, F_n) = F_n$ if and only if $F_{(m,n)} = F_n$; that is, $(m,n) = n$ or $n = 2$.]

Definition 6. The remainder when F_n is divided by m will be written $F_n^{(m)}$ and will be called the residue of F_n modulo m. Clearly

$$F_n \equiv F_n^{(m)} \pmod{m}, \quad 0 \leq F_n^{(m)} < m \ . \tag{22}$$

Lemma 6. The sequence of residues $F_n^{(m)}$, modulo any integer $m \geq 2$, is periodic with period $\mu(m)$. That is

$$(23)\quad \left\{\begin{array}{l} F^{(m)}_{n+k\mu(m)} = F^{(m)}_n \\ \text{or} \\ F_{n+k\mu(m)} \equiv F_n \pmod{m}. \end{array}\right.$$

[The ordered pair of integers $F_n^{(m)}$, $F_{n+1}^{(m)}$ can take at most m^2 distinct values. Thus the $m^2 + 1$ such consecutive pairs in $F_0^{(m)}, F_1^{(m)}, \cdots, F_{m^2+1}^{(m)}$ must have a duplication. By backward induction on the indices of two equal pairs, using (1), we see that there must be a pair $F_k^{(m)}$, $F_{k+1}^{(m)}$ equal to $F_0^{(m)} = 0$, $F_1^{(m)} = 1$, with $2 \leq k \leq m^2$. By definition, the least such k is $\mu(m)$. The periodicity now follows from (1).]

Lemma 7. For any integer m, we can find an F_n divisible by m. [For example, $n = k\mu(m)$, for any integer k, by Lemma 6.]

Lemma 8. F_n is divisible by m if and only if n is divisible by $\alpha(m)$. [Since m is a factor of $F_{\alpha(m)}$; if n is divisible by $\alpha(m)$, F_n is divisible by m, by Lemma 5. Let $n = k\alpha(m) + r$, $0 \leq r < \alpha(m)$, and let m divide F_n. Then, by (7), $F^k_{\alpha(m)-1}F_r \equiv F_n \equiv 0 \pmod{m}$. Thus, since by Lemma 1, $(F_{\alpha(m)}, F_{\alpha(m)-1}) = 1$; $F_r \equiv 0 \pmod{m}$. Since $r < \alpha(m)$, which is minimal, $F_r = 0$; whence $r = 0$ and n is divisible by $\alpha(m)$.]

Lemma 9. For all integers m and $r \geq s > 0$, $\alpha(m,s)$ divides $\alpha(m,r)$. [$F_{\alpha(m,r)}$ is divisible by m^r and so by m^s. The result follows from Lemma 8.]

Lemma 10. $\mu(m)$ is divisible by $\alpha(m)$. That is, $\beta(m)$ is an integer. [Since $F^{(m)}_{\mu(m)} = F^{(m)}_0 = 0$, $F_{\mu(m)}$ is divisible by m. The lemma follows from Lemma 8.]

Lemma 11. If p is an odd prime, then p divides only one of F_{p-1}, F_p, and F_{p+1}; namely, F_m, where $m = p - (5/p)$. [$(p, 2) = 1$. Using (5), (10), and (11), we obtain that

$$(24)\qquad F_p \equiv 2^{p-1}F_p = \sum_{s=0}^{\frac{1}{2}(p-1)} \binom{p}{2s+1} 5^s \equiv 5^{\frac{1}{2}(p-1)} \pmod{p}$$

Thus p divides F_p if and only if $(5/p) = 0$, by (12); that is, when $p = 5$. By (5), (9), (10), and (11),

$$(25)\qquad 2F_{p+1} \equiv 2^p F_{p+1} = \sum_{s=0}^{\frac{1}{2}(p-1)} \left\{ \binom{p}{2s+1} + \binom{p}{2s} \right\} 5^s \equiv 1 + 5^{\frac{1}{2}(p-1)} \pmod p$$

and, by (1), (24), and (25),

$$(26)\qquad 2F_{p-1} \equiv 1 - 5^{\frac{1}{2}(p-1)} \pmod p \quad .$$

The lemma now follows. We may note that all but the dependence on $(5/p)$ follows directly from (6), which yields that, if $p \neq 5$, by (11) and (24),

$$F_{p-1}F_{p+1} = F_p^2 - 1 \equiv 0 \pmod p \quad ;$$

and from (1).]

Lemma 12. $\alpha(p)$ divides $p - (5/p)$, if p is an odd prime; and if $\alpha(p)$ is itself prime and $p \neq 5$, $\alpha(p) < p$.

[The first part follows from Lemmas 8 and 11. Thus $\alpha(p) < p + 1$. By Lemma 11, if $p \neq 5$ and $\alpha(p)$ is prime, since $p \pm 1$ is not prime, $\alpha(p) \leq p - 2$.]

Lemma 13. If

$$(27)\qquad m = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k} \quad ,$$

where the p_i are distinct primes and the λ_i are positive integers, then

$$(28)\qquad \alpha(m,n) = [\alpha(p_1, n\lambda_1), \alpha(p_2, n\lambda_2), \cdots, \alpha(p_k, n\lambda_k)]$$

and

$$(29)\qquad \mu(m,n) = [\mu(p_1, n\lambda_1), \mu(p_2, n\lambda_2), \cdots, \mu(p_k, n\lambda_k)]$$

[By Lemma 8, F_t is divisible by $p_i^{n\lambda_i}$ if and only if t is divisible by $\alpha(p_i, n\lambda_i)$. Thus F_t is divisible by m^n if and only if t is a multiple of all the $\alpha(p_i, n\lambda_i)$. Since $\alpha(m,n)$ is minimal, (28) follows. By Lemma 6, $F_{s+t} \equiv F_s \pmod{p_i^{n\lambda_i}}$ for every s if and only if t is a multiple of $\mu(p_i, n\lambda_i)$. Thus, by the Chinese remainder theorem, $F_{s+t} \equiv F_s \pmod{m^n}$ for every s if and only if t is a common multiple of the $\mu(p_i, n\lambda_i)$. Since $\mu(m,n)$ is the minimal such t, (29) follows.]

Lemma 14. For any integers m and n,

$$\text{(30)} \quad \left\{ \begin{array}{l} \alpha([m,n]) = [\alpha(m), \alpha(n)] \\ \text{and} \\ \mu([m,n]) = [\mu(m), \mu(n)] \end{array} \right. .$$

[This follows from Lemma 13, by expanding m and n in prime factors.]

Definition 7. The greatest integer n such that N is divisible by m^n will be written

$$\text{(31)} \qquad n = \mathrm{pot}_m N$$

and called the "potency" of N to base m, following H. Gupta. It is then clear that, in particular,

$$\text{(32)} \qquad \nu(m,n) = \mathrm{pot}_m F_{\alpha(m,n)} .$$

Lemma 15. $\mathrm{pot}_m F_N = n$ if and only if N is divisible by $\alpha(m,n)$ but not by $\alpha(m, n+1)$.

[This is an immediate consequence of Lemma 8.]

Lemma 16. If k and n are positive integers, then $(F_{kn}/F_n, F_n)$ is a factor of k.

[By (8), $F_{kn}/F_n \equiv kF_{n-1}^{k-1} \pmod{F_n}$. Thus, if $(F_{kn}/F_n, F_n) = g$, g divides kF_{n-1}^{k-1}. By Lemma 1, $(F_{n-1}, F_n) = 1$; so g divides k.]

Lemma 17. If k and n are both integers greater than one, then F_{kn}/F_n is a strictly increasing function of n and of k.
[By (8), $F_{kn}/F_n = \Sigma_{h=1}^{k}\binom{k}{h}F_n^{h-1}F_{n-1}^{k-h}F_h$. Every term in the sum is positive, and increases with F_n, F_{n-1}, and k. The result follows from Lemma 2.]

Of these results, those in Lemmas 1, 2, 4 — 7, 11, and 16 have been known for a long time. Lemmas 8 — 10 and 12 — 15 appear, or are implicit, in the papers of Robinson [5], Vinson [6], and Wall [7]. [My $\alpha(m)$, $\beta(m)$, $\mu(m)$ are written $\alpha(m)$, $\beta(m)$, $\delta(m)$ by Robinson, and f(m), t(m), s(m) by Vinson,, respectively; and Wall writes d(m), k(m) for my $\alpha(m)$, $\mu(m)$.]

3. THE DIVISIBILITY SEQUENCE

Theorem 1. If p is an odd prime and $n \geq \nu(p)$, then

$$\alpha(p,n) = p^{n-\nu(p)}\alpha(p) \quad , \tag{33}$$

$$\nu(p,n) = n \quad . \tag{34}$$

If $p \neq 5$, $(p,\alpha(p)) = 1$; while

$$\alpha(5,n) = 5^n \quad . \tag{35}$$

Further,

$$\alpha(2) = 3,\ \alpha(4) = 6 = \alpha(8) \quad , \tag{36}$$

and if $n \geq 3$,

$$\alpha(2,n) = 2^{n-2}\alpha(2) = 2^{n-2}\cdot 3 \quad . \tag{37}$$

Proof. By Lemma 9, $\alpha(p,n) = k\alpha(p,n-1)$, for some integer k. Write

$$F_{\alpha(p,n)} = p^nA,\ F_{\alpha(p,n-1)} = p^{n-1}B,\ F_{\alpha(p,n-1)-1} = C.$$

Then, by (8),

$$pA = \sum_{h=1}^{k} \binom{k}{h} p^{(n-1)(h-1)} B^h C^{k-h} F_h \quad . \tag{38}$$

Thus, if $n > \nu(p) \geq 1$, since $(p, C) = 1$, kB must be divisible by p. Hence, if $\nu(p, n-1) = n-1$, $(p, B) = 1$, whence p divides k. Since $\alpha(p, n)$ and so k, is minimal, $k = p$. Now, by (10), since $k > 2$, (38) yields that $A \equiv BC^{p-1} \pmod p$. Since the factors on the right are prime to p, so is A, whence $\nu(p,n) = n$. By (18), $\nu(p, \nu(p)) = \nu(p)$, so that, by induction, if $n \geq \nu(p)$, (34) holds and $\alpha(p,n) = p^{n-\nu(p)}\alpha(p, \nu(p))$. By (17), $\alpha(p, \nu(p)) = \alpha(p)$, yielding (33).

By Lemma 12, $\alpha(p)$ divides $p - (5/p)$. Thus, if $p \neq 5$, $(p, \alpha(p)) = 1$. If $p = 5$, then, by (2), $\alpha(5) = 5$, $\nu(5) = 1$, and, by (33), we get (35).

Finally, if $p = 2$, (38) still holds, and we see, as before, that $k = p = 2$ if $\nu(2, n-1) = n-1$. Thus $2A = 2^{n-1}B^2 + 2BC$, whence $(2, A) = 1$ and $\nu(2,n) = n$, as before, if $n \geq 3$. By (2), we have (36), whence we obtain (37) like (33).

Theorem 2. If $\text{pot}_p F_m = n \geq 1$, where p is prime and $p^n \neq 2$, and if $r \geq 0$ and $(p,t) = 1$; then $\text{pot}_p F_{p^r tm} = n + r$. If $p^n = 2$, tm is an odd multiple of 3 and F_{tm} is an odd multiple of 2, while, if $r \geq 1$, $\text{pot}_2 F_{2^r tm} = r + 2$.

Proof. We repeatedly use Lemma 15 and Theorem 1. If $n \geq 1$ and $p^n \neq 2$, either p is odd and $n \geq \nu(p)$, or $p = 2$ and $n \geq 3$; whence, by (33) or (37),

$$\alpha(p, n+r) = p^r \alpha(p, n) \quad . \tag{39}$$

Thus, $m = k\alpha(p,n)$ for some k prime to p. Hence $p^r tm = tk\alpha(p, n+r)$, so that $\text{pot}_p F_{p^r tm} = n + r$. By (36), if $p^n = 2$, m and tm are divisible by 3 but not by 6, so that $\text{pot}_2 F_{tm} = 1$, and similarly by (37), $\text{pot}_2 F_{2^r tm} = r + 2$, if $r \geq 1$.

Theorems 1 and 2 have a fairly long history. Lucas [4] (see pages 209 – 210) proved the simplest formula (39) with $r = 1$, but failed to notice the anomaly when $p^n = 2$. Carmichael [1] (see pages 40—42) proved Theorem 2 in full,* using the theory of cyclotomic polynomials. Both Lucas' and Carmichael's results apply to a more general sequence** than that defined by (1) and (2). Robinson [5] proves Theorem 1, for odd primes only, by a matrix method.

Theorem 3. If $\operatorname{pot}_p F_m = n \geq 1$, where p is prime and $p^n \neq 2$, and if $r \geq 0$; then there is a strictly increasing sequence of pairwise prime integers $\ell_s = \ell_s(m,p)(s = 0,1,2,\cdots)$, all prime to p, such that

$$F_{p^r m} = p^{n+r}\ell_0\ell_1\cdots\ell_r \quad . \tag{40}$$

Proof. When $r = 0$, we define $F_m = p^n\ell_0$, where $(p,\ell_0) = 1$. By Theorem 2, if $r \geq 1$, there are integers A, B, and C, such that

$$F_{p^r m} = p^{n+r}A,\ F_{p^{r-1}m} = p^{n+r-1}B,\ F_{p^{r-1}m-1} = C \quad ,$$

and $(p,A) = (p,B) = 1$, while, by Lemma 1, $(pB,C) = 1$. Thus, by (8),

$$A = B\sum_{h=1}^{p}\binom{p}{h}p^{(n+r-1)(h-1)-1}B^{h-1}C^{p-h}F_h \tag{41}$$

where, as in the proof of Theorem 1, the sum on the right is an integer, since $n \geq 1$. Thus A is divisible by B. If we write $A = \ell_r B$, it is clear that $A = \ell_0\ell_1\cdots\ell_r$, yielding (40). Further (41) gives us that

$$\ell_r = pB\sum_{h=2}^{p}\binom{p}{h}p^{(n+r-1)(h-1)-2}B^{h-2}C^{p-h}F_h + C^{p-1} \quad , \tag{42}$$

---

* He has a misprint, making the greatest power of 2 too small by one.

**The sequence is $D_n = (\alpha^n - \beta^n)/(\alpha - \beta)$, where $\alpha + \beta$ and $\alpha\beta$ are mutually prime integers. For F_n, by (4), $\alpha = (1/2)(1 + \sqrt{5})$ and $\beta = (1/2)(1 - \sqrt{5})$.

where the sum is again an integer, since either $p \geq 3$ and $n \geq 1$, or $p = 2$ and $n \geq 3$. Thus $\ell_r \equiv C^{p-1}$ (mod pB); so that, since C is prime to p, $\ell_0, \ell_1, \cdots, \ell_{r-1}$, so is ℓ_r. Again, since ℓ_r exceeds a positive integer multiple of pB, we have that

$$\ell_r > p\ell_0\ell_1 \cdots \ell_{r-1} > \ell_{r-1} \quad . \tag{43}$$

Corollary 1. If $\mathrm{pot}_p F_m = n \geq 1$ and $p^n \neq 2$, and if $r > s \geq 0$, then

$$\ell_{r-s}(p^s m,\ p) = \ell_r(m,p) \tag{44}$$

and

$$\ell_0(p^s m,\ p) = \ell_0(m,p)\,\ell_1(m,p) \cdots \ell_s(m,p) \quad . \tag{45}$$

Corollary 2. If $\mathrm{pot}_2 F_m = 1$ and $r \geq 1$, then

$$F_{2^r m} = 2^{r+2}\ell_0(2m,2)\,\ell_1(2m,2) \cdots \ell_{r-1}(2m,2) \quad . \tag{46}$$

Theorem 3, with its corollaries, contains a definition of $\ell_s(m,p)$ whenever $\mathrm{pot}_p F_m = n \geq 1$ and $p^n \neq 2$. By analogy with (40), (44), (45) and (46), we shall adopt the following definition for the remaining case.

Definition 8. If $m = 3t$ where t is odd (so that, by Theorem 2, $\mathrm{pot}_2 F_m = 1$), the sequence $\ell_s(m,2)$ is defined by

$$\ell_0(m,2) = \tfrac{1}{2} F_m \quad , \tag{47}$$

$$\ell_1(m,2) = 2\ell_0(2m,2)/\ell_0(m,2) \quad , \tag{48}$$

and

$$\ell_s(m,2) = \ell_{s-1}(2m,2) \text{ if } s \geq 2 \ . \tag{49}$$

Corollary 3. Adopting Definition 8, we obtain equation (40) for every prime p, and every positive integer m such that $\mathrm{pot}_p F_m = n \geq 1$. In every case, the numbers $\ell_s = \ell_s(m,p)(s = 0,1,2,\cdots)$ are integers, all pairwise prime, and all but $\ell_1(m,p)$ are always prime to p. If m is an odd multiple of $3, \ell_1(m,2)$ is an odd multiple of 2; in every other case, $\ell_1(m,p)$ is prime to p.

Proof. If $p^n \neq 2$, the corollary coincides with Theorem 3. If $p^n = 2$ (that is, m is an odd multiple of 3, by (36)) and $r \geq 1$, Corollary 2 and Definition 8 (equations (46), (48), and (49)) show that equation (40) holds, with $\frac{1}{2}\ell_0(m,2)\ell_1(m,2)$, $\ell_2(m,2), \ell_3(m,2), \cdots$ all pairwise prime odd integers, by Theorem 3. Finally, when $p^n = 2$ and $r = 0$, we get (40) from the definition (47), and, by Theorem 2, $\ell_0(m,2)$ is an odd integer.

Further, by (8), $F_{2m} = F_m(F_m + 2F_{m-1})$, which yields through (40) that $\ell_1(m,2) = \ell_0(m,2) + F_{m-1}$. Since $(\ell_0, F_{m-1}) = (\ell_1, F_{m-1}) = 1$ (by Lemma 4), and both ℓ_0 and F_{m-1} are odd, we see that $\ell_1(m,2)$ is even and prime to $\ell_0(m,2)$. Finally, since $\frac{1}{2}\ell_0\ell_1$ is odd, ℓ_1 must be an odd multiple of 2.

Theorem 4. Let $P = \{p_1, p_2, \cdots, p_k\}$ be a set of k distinct primes. Then P contains all the prime factors of $F_{p_1}, F_{p_2}, \cdots, F_{p_k}$ only if

$$(50)\qquad \left\{\begin{array}{l} k = 1 \text{ and } P = \{2\} \text{ or } \{5\} \quad , \\ k = 2 \text{ and } P = \{2,\ 3\} \text{ or } \{2,\ 5\} \quad , \\ \text{or} \\ k = 3 \text{ and } P = \{2,\ 3,\ 5\} \quad . \end{array}\right.$$

Proof. Let $k = 1$. Then F_{p_1} can have no prime factor other than p_1. By (2), Lemma 2, and Lemma 11, the only possible values of p_1 are 2 and 5.

Let $k \geq 2$, and first suppose that $2 \notin P$. By Lemma 4, if $i \neq j$, $(F_{p_i}, F_{p_j}) = 1$, so that no prime factor is common to two of the F_{p_i}; and by Lemma 2, since every $p_i \geq 3$, every F_{p_i} has at least one prime factor. Thus every F_{p_i} has exactly one prime factor. Let us now renumber the p_i, if necessary, so that p_1 is the least prime in P not equal to 5, and

$$(51)\qquad F_{p_1} = p_2^{r_2},\ F_{p_2} = p_3^{r_3},\ \cdots,\ F_{p_{i-1}} = p_i^{r_i},\ \cdots,$$

where each $r_i \geq 1$. This can always be done, and, since $p_1 \neq 5$, inductively $p_2, p_3, \cdots \neq 5$, and no $p_{i-1} = p_i$. Finally, by Lemma 8, each $p_{i-1} = \alpha(p_i)$ and so, by Lemma 12, $\alpha(p_i) = p_{i-1} < p_i$. Thus the sequence defined by (51) cannot terminate, and this contradicts the finiteness of P. Therefore $2 \in P$ and we may write $p_1 = 2$. If the F_{p_i} $(i = 2, 3, \cdots, k)$ are all odd, the $p_i (i = 2, 3, \cdots, k)$ from a set of $k - 1$ distinct odd primes containing all the prime factors of the corresponding set of F_{p_i}. We have just shown that this can only happen if $k - 1 = 1$ and $p_2 = 5$. Suppose now that one of the F_{p_i} is even. Then, by (2), we can write $p_2 = 3$, since $F_3 = 2$. If $k = 2$, this completes the enumeration of possible cases. If $k \geq 3$, then $p_3, p_4, \cdots, p_k$ form a set of $k - 2$ distinct odd primes containing all the prime factors of the corresponding set of F_{p_i}, because $\alpha(3) = 4$, which is not prime. Again, we know that this can only happen if $k - 2 = 1$ and $p_3 = 5$. This completes the proof.

Definition 9. If $\text{pot}_p F_N = n$, and if either $n \geq 1$ and $p = 5$, or $n > \nu(p)$, we shall call p a multiple prime factor (mpf) of F_N. If, on the contrary, $p \neq 5$ and $n = \nu(p)$, then p is a simple prime factor (spf) of F_N.

Lemma 18. p is a multiple prime factor of F_N if and only if it is a prime factor of both F_N and N. A prime factor of F_N which is not multiple is a simple prime factor.

[This follows from Definition 9, Lemma 8, and Theorem 1.]

Lemma 19. If k and n are positive integers and p is a multiple prime factor of F_n, it is also a multiple prime factor of F_{kn}. Conversely, if p is a simple prime factor of F_{kn}, it is also a simple prime factor of F_n.

[This follows from Lemmas 5 and 18.]

Theorem 5. F_N has at least one simple prime factor, unless $N = 1, 2, 5, 6$, or 12.

Proof. $F_1 = F_2 = 1$, so that these F_N have no prime factors at all, and so no spf, as stated. Let $N \geq 3$, and let $F_N = m$ satisfy (27). By Lemma 2, the set P of prime factors of F_N is not empty. If F_N has only mpfs, by Lemma 16, each p_i divides N; whence by Lemma 5, each F_{p_i} divides m. It follows that P contains all the prime factors of every F_{p_i}. This is the situation dealt with in Theorem 4, and it can only occur in the five cases listed in (50).

By (2), (50), Lemma 8, and Theorem 1, if F_N has only mpfs, we see that $F_N = 2^r \cdot 3^s \cdot 5^t$. Further, $r \leq 4; s \leq 2; t \leq 1; rt = 0; st = 0;$ if

$r = 0$ then $s = 0$ and $t = 1$; if $s = t = 0$ then $r = 3$; if $rs > 0$ then $r = 4$ and $s = 2$. Thus $F_N = 5, 8$, or 144; whence $N = 5, 6$, or 12; and all these cases are valid and stated in the theorem.

4. CARMICHAEL'S THEOREM

By using the theory of cyclotomic polynomials, Carmichael proved, for the general sequence* D_n, a theorem which, in our terminology, reads as follows [Compare [1], Theorem XXIII, pages 61—62.]

Carmichael's Theorem. If $N \neq 1, 2, 6$, or 12, then there is a prime p, such that $N = \alpha(p)$.

We shall proceed to derive this theorem, for the Fibonacci sequence, by the elementary considerations we have used so far. Let

$$N = q_1^{n_1} q_2^{n_2} \cdots q_k^{n_k} , \tag{52}$$

where the q_i are distinct primes and the $n_i \geq 1$. We shall write $N_{(1)}$ for any of the k integers $N_i = N/q_i$, and more generally $N_{(h)}$ for any of the $\binom{k}{h}$ integers $N/q_{i_1} q_{i_2} \cdots q_{i_h}$, with $\{i_1, i_2, \cdots, i_h\}$ a subset (without repetition) of $\{1, 2, \cdots, k\}$. We shall also write R_h for the product of the $\binom{k}{h}$ integers $F_{N_{(h)}}$.

Lemma 20. If N satisfies (52), then

$$\left[F_{N_1}, F_{N_2}, \cdots, F_{N_k}\right] = \frac{R_1 R_3 R_5 \cdots}{R_2 R_4 R_6 \cdots} = \prod_{h=1}^{h} R_h^{(-1)^{h-1}} . \tag{53}$$

[By repeated application of Lemma 4, we see that

$$\begin{aligned}(F_{N_{i_1}}, F_{N_{i_2}}, \cdots, F_{N_{i_h}}) &= F_{(N/q_{i_1}, N/q_{i_2}, \cdots, N/q_{i_h})} = \\ &\qquad F_{N/q_{i_1} q_{i_2} \cdots q_{i_h}} = F_{N_{(h)}} ;\end{aligned} \tag{54}$$

*See footnote on page 227 above.

so that R_h is the product of the greatest common factors of all sets of h numbers $F_{N_{(1)}}$. Let a prime factor p divide exactly s_1 of the $F_{N_{(1)}}$; and let $p^2, p^3, \cdots, p^m$ divide $s_2, s_3, \cdots, s_m$ of the $F_{N_{(1)}}$, respectively; but let no $F_{N_{(1)}}$ be divisible by p^{m+1}. Then $k \geq s_1 \geq s_2 \geq \cdots \geq s_m \geq 1$ and $\mathrm{pot}_p[F_{N_1}, F_{N_2}, \cdots, F_{N_k}] = m$. Of the $\binom{k}{h}$ factors in R_h, (54) shows that $\binom{s_1}{h}, \binom{s_2}{h}, \cdots, \binom{s_m}{h}$ are respectively divisible by $p, p^2, \cdots, p^m$. (Note that $\binom{s}{h} = 0$ if $s < h$, and that the set of factors divisible by p includes those divisible by p^2, which include those divisible by p^3, and so on). Thus

$$\mathrm{pot}_p R_h = \binom{s_1}{h} + \binom{s_2}{h} + \cdots + \binom{s_m}{h}, \text{ whence}$$

$$\mathrm{pot}_p\left(\frac{R_1\, R_3\, R_5 \cdots}{R_2\, R_4\, R_6 \cdots}\right) = \sum_{t=1}^{m}\sum_{h=1}^{k}(-1)^{h-1}\binom{s_t}{h} = \sum_{t=1}^{m}\{1 - (1-1)^{s_t}\} = m ,$$

which implies (53).]

It follows from Lemmas 5 and 20 that

$$Q_N = \frac{F_N\, R_2\, R_4 \cdots}{R_1\, R_3\, R_5 \cdots} = \frac{F_N}{[F_{N_1}, F_{N_2}, \cdots, F_{N_k}]} \tag{55}$$

is a positive integer. [Carmichael [1] writes D_N for my F_N, and $F_N(\alpha,\beta) = \beta^{\phi(N)}Q_N(\alpha/\beta)$ for my Q_N, where

$$\phi(N) = q_1^{n_1-1}(q_1 - 1)\, q_2^{n_2-1}(q_2 - 1) \cdots q_k^{n_k-1}(q_k - 1) \tag{56}$$

in the Euler ϕ-function.]

By (55) and Theorem 2, if a prime p divides Q_N, it is either a factor of F_N which is prime to every $F_{N_{(1)}}$, or it also divides some $F_{N_{(1)}}$. In the former case, by Lemma 8, since $\alpha(p)$ divides N, but no $N_{(1)}$, necessarily $N = \alpha(p)$, and if $N \neq 5$, $p \neq 5$ and p is a spf of F_N. In the latter case, by Theorem 2, p is a mpf of F_N, and $\mathrm{pot}_p Q_N = 1$, except if $N = 6$ (when $Q_N = Q_6 = F_6F_1/F_2F_3 = 4$.)

Lemma 21. If N satisfies (52) and

$$Q_N > q_1q_2 \cdots q_k \quad , \tag{57}$$

then there is a prime p such that $N = \alpha(p)$.
[As explained above, if $N = 6$, $Q_N = 4 < 2 \cdot 3$, so this case does not arise. Thus $\mathrm{pot}_p Q_N = 0$ or 1 and $Q_N/q_1q_2 \cdots q_k$ cannot be divisible by any q_i. Thus if this quotient exceeds one, Q_N must be divisible by some prime other than the q_i, and such a prime p has $N = \alpha(p)$.]

Lemma 22. If N satisfies (52) and $k \geq 4$, then (57) holds.
[Since R_h has $\binom{k}{h}$ Fibonacci-number factors, and since

$$\sum_{h=0}^{k}\binom{k}{h} = (1+1)^k = 2^k \quad \text{and} \quad \sum_{h=0}^{k}(-1)^h\binom{k}{h} = (1-1)^k = 0 \quad ,$$

we see that the numerator and denominator of Q_N, by (55), each has 2^{k-1} Fibonacci-number factors. Also, by (4), if $a = (1/2)(\sqrt{5}+1)$ and $b = (1/2)(\sqrt{5}-1)$ so that $a > 1 > b = 1/a$ [Carmichael writes α and $-\beta$ for my a and b],

$$a^n(1-b^2) \leq a^n(1-b^{2n}) \leq \sqrt{5}\,F_n \leq a^n(1+b^{2n}) \leq a^n(1+b^2) \quad . \tag{58}$$

Therefore, since $(1-b^2)/(1+b^2) = 1/\sqrt{5}$ and by (55) and (58), $Q_N \geq a^f(1/\sqrt{5})^{2^{k-1}}$, where, by (56),

$$f = N - \Sigma N_{(1)} + \Sigma N_{(2)} - \cdots = N\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_k}\right) = \phi(N);$$

so that

$$(59)\qquad Q_N \geq a^{\phi(N)}(1/\sqrt{5})^{2^{k-1}} \geq a^{(q_1-1)(q_2-1)\cdots(q_k-1)}(1/\sqrt{5})^{2^{k-1}} .$$

Clearly $(q_1 - 1)(q_2 - 1) \cdots (q_k - 1)$ exceeds the value when we put $q_1 = 2$ and $q_i = 2i - 1$ $(i \geq 2)$, namely $q^{k-1}(k - 1)!$. The function

$$2^k + \sum_{i=1}^{k}(q_i - 1)$$

increases more slowly with each q_i than does the product, and its value at the minimal point is $2^k + k^2 - k + 1$. If $k \geq 4$, this is seen to be less than $2^{k-1}(k - 1)!$. Thus, by (59),

$$(60)\qquad Q_N \geq \left\{\prod_{i=1}^{k} a^{q_i-1}\right\}(a^2/\sqrt{5})^8$$

The function a^{n-1}/n has a minimum for integer values of n when $n = 2$, and it exceeds one when $n \geq 4$. Thus, by (60),

$$(61)\quad Q_N/q_1q_2\cdots q_k \geq (a/2)(a^2/3)(a^4/5)(a^6/7)(a^2/\sqrt{5})^8 = a^{29}/131250 > 8 ,$$

and the lemma follows.]

Lemma 23. If N satisfies (52) and $k = 3$, then (57) holds if at least one $q_i \geq 11$, or if no $q_i = 2$, or if any $n_i \geq 2$.

[As in the proof of Lemma 21, (59) still holds. Now, if we suppose that $q_1 < q_2 < q_3$, we see that $q_1 \geq 2$, $q_2 \geq 3$, and, by the first supposition of the lemma, $q_3 \geq 11$. Thus

(62)

$$(q_1 - 1)(q_2 - 1)(q_3 - 1) = (q_1 - 1)(q_2 - 1)(q_3 - 2) + (q_1 - 1)(q_2 - 2) + (q_1 - 1)$$

$$\geq 2(q_3 - 2) + (q_2 - 2) + (q_1 - 1) \geq (q_1 - 1) + (q_2 - 1) + (q_3 - 1) + 7 ;$$

and so, by (59) and (62), as before,

$$(63) \qquad Q_N/q_1q_2q_3 \geq (a/2)(a^2/3)(a^{10}/11)(a^7/5^2) = a^{20}/1650 > 9 \quad ,$$

and (57) follows.

Adopting the second supposition, we have $q_1 \geq 3$, $q_2 \geq 5$, and $q_3 \geq 7$ Then (62) is replaced by

$$(64) \quad (q_1 - 1)(q_2 - 1)(q_3 - 1) \geq 8(q_3 - 2) + 2(q_2 - 2) + q_1 - 1 \geq (q_1 - 1) + (q_2 - 1) + (q_3 - 1) + 36 ,$$

and (63) by

$$(65) \qquad Q_N/q_1q_2q_3 \geq (a^2/3)(a^4/5)(a^6/7)(a^{36}/5^2) = a^{48}/2625 > 10^6 \quad ,$$

and (57) follows again.

Finally, if any $n_i \geq 2, \phi(n) \geq 2(q_1 - 1)(q_2 - 2)(q_3 - 1)$. Thus, as before, $q_1 \geq 2$, $q_2 \geq 3$, $q_3 \geq 5$, and $2(q_1 - 1)(q_2 - 1)(q_3 - 1) \geq (q_1 - 1) + (q_2 - 1) + (q_3 - 1) + 9$; whence

$$(66) \qquad Q_N/q_1q_2q_3 \geq (a/2)(a^2/3)(a^4/5)(a^9/5^2) = a^{16}/750 \approx 2.9$$

and we get (57).]

Lemma 24. If N satisfies (52) and $k = 2$, then (57) holds if $N/q_1q_2 \geq 3$, or if at least one $q_i \geq 11$.

[Let $N/q_1q_2 = r$. Then by (55), $Q_N = F_{q_1q_2r}F_r/F_{q_2r}F_{q_1r}$, and by (8),

$$(67) \qquad Q_N = \sum_{h=1}^{q_1} \binom{q_1}{h} F_{q_2r}^{h-1} F_{q_2r-1}^{q_1-h} F_h \Bigg/ \sum_{h=1}^{q_1} \binom{q_1}{h} F_r^{h-1} F_{r-1}^{q_1-h} F_h \quad ,$$

whence, by Lemma 2, $Q_N \geq (F_{q_2r-1}/F_r)^{q_1-1}$. Thus, by (58)

$$(68) \qquad Q_N/q_1q_2 \geq \left\{a^{(q_2-1)r-1}(1 - b^{2(q_2r-1)})/(1 + b^{2r})\right\}^{q_1-1} \Big/ q_1q_2 \quad .$$

First we assume that $r \geq 3$. Then, by the kind of argument used above, if $q_1 \geq 3$ and $q_2 \geq 2$, and by (68),

$$(69)\quad Q_N/q_1q_2 \geq (a^{q_1-3}/q_1)(a^{3q_2-4}/q_2)\{a(1-b^{10})/(1+b^6)\}^{q_1-1} > a^4(0.94)^2/6 > 1 .$$

Next, we assume that $q_1 \geq 2$, $q_2 \geq 11$, $r \geq 1$. Then, by (68),

$$(70)\quad Q_N/q_1q_2 \geq (a^{8q_1-17}/q_1)(a^{q_2-2}/q_2)\{a(1-b^{20})/(1+b^2)\}^{q_1-1} > a^9(0.72)/22 > 2.$$

The results (69) and (70) establish the lemma.]

Lemma 25. If q is prime and $q \geq 3$, then there is a prime p such that $q = \alpha(p)$.

[If $q \geq 3$, $F_q \geq 2$, by Lemma 2, and so F_q has a prime factor p. By Lemma 8, $\alpha(p)$ divides q, whence, since q is prime, $\alpha(p) = q$.]

Lemma 26. If q is prime and $\lambda \geq 2$, then there is a prime $p \neq 5$, such that $q^\lambda = \alpha(p)$.

[By Lemma 16 and Theorem 1, if $q^{\lambda-1} = m$, $(F_{qm}/F_m, F_m) = 1$ if $q \neq 5$; and if $5^{\lambda-1} = m$, $(F_{5m}/F_m, F_m) = 5$. If $q \neq 5$, by Lemma 17, $F_{qm}/F_m \geq F_4/F_2 = 3$; so that F_{qm} must have a prime factor $p \neq 5$, prime to F_m. If $q = 5$, since $F_{25}/5F_5 = 3001$, by (2), Lemma 17 shows that again F_{qm} has a prime factor $p \neq 5$, prime to F_m. Thus, by Lemma 8, for any $q, \alpha(p)$ divides $qm = q^\lambda$ but not $m = q^{\lambda-1}$. Therefore $q^\lambda = \alpha(p)$.]

We now have sufficient information to prove Carmichael's theorem.

Theorem 6. If $N \neq 1, 2, 6$, or 12, then there is a prime p such that $N = \alpha(p)$.

Proof. Let the (unique) prime-power expansion of N be given by (52). By Lemma 21, Lemmas 22, 23, and 24 show that the theorem holds in the following cases: (i) if $k \geq 4$, all N; (ii) if $k = 3$ and either (a) one $q_i \geq 11$, (b) no $q_i = 2$, or (c) one $n_i \geq 2$; and (iii) if $k = 2$ and either (a) $N/q_1q_2 \geq 3$ or (b) one $q_1 \geq 11$. In addition, Lemmas 25 and 26 show that the theorem holds (iv) if $k = 1$ and $N \neq 2$. We see from (2) that, indeed, when $N = 1, 2,$

6, or 12, there is no prime p such that $N = \alpha(p)$. It therefore remains to show that such a p exists, (v) when $k = 3$, no $q_i \geq 11$, one $q_i = 2$, and no $n_i \geq 2$, and (vi) when $k = 2$, $N \neq 6$ or 12, $N/q_1q_2 = 1$ or 2, and no $q_i \geq 11$. We look for primes p which divide F_N but no corresponding $F_{N_{(1)}}$, for then $N = \alpha(p)$, as explained earlier.

Case (v). We have $N = 2 \cdot 3 \cdot 5 = 30$, $2 \cdot 3 \cdot 7 = 42$, and $2 \cdot 5 \cdot 7 = 70$. We see from (2) that $30 = \alpha(31)$, $42 = \alpha(211)$, and $70 = \alpha(71) = \alpha(911)$; so that the theorem holds.

Case (vi). We have $N = 2 \cdot 5 = 10$, $2^2 \cdot 5 = 20$, $2 \cdot 7 = 14$, $2^2 \cdot 7 = 28$, $3 \cdot 5 = 15$, $3 \cdot 7 = 21$, and $5 \cdot 7 = 35$. We see from (2) that $10 = \alpha(11)$, $20 = \alpha(41)$, $14 = \alpha(29)$, $28 = \alpha(281)$, $15 = \alpha(61)$, $21 = \alpha(421)$, and $35 = \alpha(141961)$. This completes the theorem.

Lemma 27. If $N = \alpha(p)$ and $N \neq 5$ whence $p \neq 5$), p is a simple prime factor of F_N.

[By Lemma 18, if p is a mpf of F_N, p divides both N and F_N. Thus, since, by Theorem 1, if $p \neq 5$, $(p, \alpha(p)) = 1$; N must be divisible by $p\alpha(p)$, so that $N \neq \alpha(p)$. The lemma follows.]

By Lemma 27, Theorem 5 is seen to follow from Theorem 6. We also see that Theorem 3 and its corollaries follow from Theorems 1, 2, and 6 (with the exception of the fact that the $\ell_s(m,p)$ increase with s).

For completeness, we also state the following result.

Lemma 28. If $f_1 = 1, f_2, f_3, \cdots, f_m = N$ are all the divisors of N, then

$$F_N = \prod_{r=1}^{m} Q_{f_r} \quad . \tag{71}$$

[If N satisfies (52), its divisors are the $(n_1 + 1)(n_2 + 1) \cdots (n_k + 1) = m$ integers

$$f = q_1^{s_1} q_2^{s_2} \cdots q_k^{s_k} \quad ,$$

where $0 \leq s_i \leq n_i$, $i = 1, 2, \cdots, k$. By (55), a particular factor F_g can appear only once in Q_f; and this, when

$$g = q_1^{t_1} q_2^{t_2} \cdots q_k^{t_k}$$

and $t_i = n_i$ except when $i = i_1, i_2, \cdots, i_h$ (when $t_i < n_i$), only if $f = g$ or gq_{i_1} or $gq_{i_1}q_{i_2}$ or $\cdots$ or $gq_{i_1}q_{i_2} \cdots q_{i_h}$. It follows by (55) that F_g appears in

$$\prod_{r=1}^{m} Q_{f_r}$$

to the total power

$$1 - \binom{h}{1} + \binom{h}{2} - \cdots + (-1)^h \binom{h}{h} = (1 - 1)^h = 0 \text{ if } h \ge 1 \quad ,$$

and 1 if $h = 0$. This proves that the product is simply F_N.]

5. PERIODICITY OF RESIDUES

We shall complete this discussion of divisibility properties with a survey of results pertaining to the characteristic number $\mu(m,n)$ defined in Section 1.

Lemmas 13 and 14 show that we may limit the study of the functions $\alpha(m,n)$ and $\mu(m,n)$ to that of $\alpha(p,n)$ and $\mu(p,n)$, where p is prime. We have established the essential properties of $\alpha(p,n)$ in Theorem 1. Thus, by (15), the corresponding behaviour of $\mu(p,n)$ is known if we know that of $\beta(p,n)$. So far, we have only stated, in Lemma 10, that $\beta(m)$ (and, in particular, $\beta(p,n)$) is always an integer. The papers of Robinson [5], Vinson [6], and Wall [7] have answered almost every question that may be asked about $\beta(p,n)$, and it is their work which will be outlined here. Proofs of all the results quoted below may be found in Vinson's paper [6], and so will be omitted here.

Theorem 7. If p is an odd prime and n a positive integer, then

$$\beta(p,n) = \begin{Bmatrix} 4 \text{ if } \operatorname{pot}_2 \alpha(p) = 0 \\ 1 \text{ if } \operatorname{pot}_2 \alpha(p) = 1 \\ 2 \text{ if } \operatorname{pot}_2 \alpha(p) \ge 2 \end{Bmatrix} \quad ; \tag{72}$$

but

$$\beta(2,1) = \beta(2,2) = 1, \quad \text{and} \quad \beta(2,n) = 2 \text{ if } n \geq 3 \quad . \tag{73}$$

We note that, with the two exceptions given in (73), $\beta(p,n)$ is independent of n. Also, $\beta(p,n)$ always takes one of the three values 1, 2, or 4 — a remarkably simple result.

Theorem 8. If m is a positive integer satisfying (27), then (i) $\beta(m) = 4$, if $m \geq 3$ and $\alpha(m)$ is odd; (ii) $\beta(m) = 1$, if $\mathrm{pot}_2\alpha(p_i) = 1$ for every $p_i \neq 2$ $(i = 1, 2, \cdots, k)$ and if $\mathrm{pot}_2 m \leq 2$; and (iii) $\beta(m) = 2$ for all other m.

We note that Theorem 8 contains Theorem 7, as a special case, when $m = p^n$, where p is prime. (The connection is through Lemma 13.)

Theorem 9. If p is an odd prime, not equal to 5, and n a positive integer, then

$$\beta(p,n) = \left\{ \begin{array}{l} 1 \text{ if } p \equiv 11 \text{ or } 19 \pmod{20} \\ 2 \text{ if } p \equiv 3 \text{ or } 7 \pmod{20} \\ 4 \text{ if } p \equiv 13 \text{ or } 17 \pmod{20} \end{array} \right\} \quad ; \tag{74}$$

and (of the remaining values of $p \equiv 1$ or $9 \pmod{20}$) $\beta(p,n) \neq 2$ if $p \equiv 21$ or $29 \pmod{40}$.

These results are connected with the foregoing by way of Lemma 12. Vinson points out that the theorem is "complete" in the sense that every remaining possibility occurs; he lists the examples:

$$\left\{ \begin{array}{llll} \beta(521) = 1, & \beta(41) = 2, & \beta(761) = 4, & [p \equiv 1 \pmod{40}] ; \\ \beta(809) = 1, & \beta(409) = 2, & \beta(89) = 4, & [p \equiv 9 \pmod{40}] ; \\ \beta(101) = 1, & \beta(61) = 4, & & [p \equiv 21 \pmod{40}] ; \\ \beta(29) = 1, & \beta(109) = 4, & & [p \equiv 29 \pmod{40}] . \end{array} \right. \tag{75}$$

REFERENCES

1. R. D. Carmichael, "On the Numerical Factors of the Arithmetic Form $\alpha^n \pm \beta^n$, Ann. Math., 15 (1913–14) 30–70.

2. R. D. Carmichael, "A Simple Principle of Unification in the Elementary Theory of Numbers," Amer. Math. Monthly 36 (1929) 132 – 143.

3. J. H. Halton, "On a General Fibonacci Identity," Fibonacci Quarterly, 3 (1965) 1: 31 – 43.

4. E. Lucas, "Théorie des Fonctions Numériques Simplement Périodiques," Amer. J. Math, 1 (1878) 184 – 240, 289 – 321.

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

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

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

* * * * *

All subscription correspondence should be addressed to Brother U. Alfred, St. Mary's College, Calif. All checks ($4.00 per year) should be made out to the Fibonacci Association or the Fibonacci Quarterly. Manuscripts intended for publication in the Quarterly should be sent to Verner E. Hoggatt, Jr., Mathematics Department, San Jose State College, San Jose, Calif. All manuscripts should be typed, double-spaced. Drawings should be made the same size as they will appear in the Quarterly, and should be done in India ink on either vellum or bond paper. Authors should keep a copy of the manuscripts sent to the editors.

* * * * *

NOTICE TO ALL SUBSCRIBERS!!!

Please notify the Managing Editor AT ONCE of any address change. The Post Office Department, rather than forwarding magazines mailed third class, sends them directly to the dead-letter office. Unless the addressee specifically requests the Fibonacci Quarterly to be forwarded at first class rates to the new address, he will not receive it. (This will usually cost about 30 cents for first-class postage.) If possible, please notify us AT LEAST THREE WEEKS PRIOR to publication dates: February 15, April 15, October 15, and December 15.

* * * * *