DUCCI-PROCESSES OF 5-TUPLES

Anne Ludington-Young
Dept. of Mathematical Sciences, Loyola College in Maryland, Baltimore, MD 21210
(Submitted January 1997-Final Revision May 1997)

Ducci-sequences are successive iterations of the function

$$f(x_1, x_2, \ldots, x_n) = (|x_1 - x_2|, |x_2 - x_3|, \ldots, |x_n - x_1|).$$

Note that $f: Z^n \to Z^n$, where Z^n is the set of n-tuples with integer entries. Since they were introduced in 1937, Ducci-sequences, also known as the n-number game, have been studied extensively (e.g., [1], [3], [5], [6], [7], [8]). In 1982, Wong suggested a generalization which he called Ducci-processes [12]. Ducci-processes are successive iterations of a function $g: Z^n \to Z^n$ which satisfies the following three conditions:

(i) there exists a function $h: Z^2 \to Z$;

(ii) $g(x_1, x_2, \ldots, x_n) = (h(x_1, x_2), h(x_2, x_3), \ldots, h(x_n, x_1))$

(iii) the n entries of $g^k(x_1, x_2, \ldots, x_n)$ are bounded for all k.

Note that Ducci-sequences are an example of a Ducci-process with $h(x, y) = |x - y|$.

In [4], Engel introduced the Ducci-process D_m, where $h(x, y) = (x + y) \pmod m$:

$$D_m(x_1, x_2, \ldots, x_n) = (x_1 + x_2 \pmod m, x_2 + x_3 \pmod m, \ldots, x_n + x_1 \pmod m).$$

Since numbers are reduced modulo m, we can view the domain and range of D_m as Z_m^n, the set of n-tuples with entries from Z_m. Because Z_m^n is a finite set, the iterations $\{D_m^j(X)\}$ will eventually repeat, resulting in a cycle. As with Ducci-sequences, the goal is to characterize cycles in terms of n and m. This is done in [9] for $n = 4$.

We will begin with some general observations about D_m. Then we will focus on 5-tuples, where the Fibonacci numbers play a prominent role.

GENERAL OBSERVATIONS

To simplify notation, we define two functions on Z^n. For $X = (x_1, x_2, \ldots, x_n) \in Z^n$,

$$D(X) = D(x_1, x_2, \ldots, x_n) = (x_1 + x_2, x_2 + x_3, \ldots, x_n + x_1),$$
$$H(X) = H(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, x_1).$$

We write $D(X) \equiv (x_1 + x_2, x_2 + x_3, \ldots, x_n + x_1) \pmod m$ in lieu of $D_m(X)$. Note that D and H are commutative, linear operators; moreover, $D(X) = X + H(X)$. Iterations of D and H are defined as $D^j(X) = D(D^{j-1}(X))$ and $H^j(X) = H(H^{j-1}(X))$, respectively. Thus, $H^n(X) = X$ and $H^j(X) = H^{j \pmod n}(X)$.

A further simplification occurs with the introduction of the special n-tuple $A = (1, 0, \ldots, 0)$. Using the function H, we can write $X = (x_1, x_2, \ldots, x_n)$ in terms of A:

$$\begin{aligned} X &= x_1 \cdot (1, 0, \ldots, 0) + x_2 \cdot (0, 1, \ldots, 0) + \cdots + x_n \cdot (0, 0, \ldots, 1) \\ &= x_1 \cdot A + x_2 \cdot H^{n-1}(A) + x_3 \cdot H^{n-2}(A) + \cdots + x_{n-1} \cdot H^2(A) + x_n \cdot H(A) \\ &= \Sigma_{1 \le i \le n} x_i H^{n+1-i}(A). \end{aligned}$$

Hence,

$$D(X) = \sum_{1\le i\le n} x_i H^{n+1-i}(D(A)).$$

Similarly, $D^j(X)$ can be written in terms of $D^j(A)$.

As we noted above, the iterations of X will eventually lead to a cycle. That is, there exist nonnegative integers l and s for which $D^{l+s}(X) \equiv D^s(X) \pmod m$. If l and s are as small as possible, then we will write $\mathfrak{l}_m(X) = l$ and $\mathfrak{s}_m(X) = s$. When the context is clear, we will omit the subscript m. Thus, $\mathfrak{l}(X)$ is the length of the cycle generated by X, while $\mathfrak{s}(X)$ is the number of iterations necessary to reach that cycle. Considering all members of Z_m^n, let Y and W be the tuples for which $\mathfrak{l}(Y)$ and $\mathfrak{s}(W)$ are maximum, respectively. We denote these maximum lengths by $\mathfrak{l}(m)$ and $\mathfrak{s}(m)$. Our goal is to characterize $\mathfrak{l}(m)$ and $\mathfrak{s}(m)$.

Theorem 1: For all n, $\mathfrak{l}(m) = \mathfrak{l}(A)$ and $\mathfrak{s}(m) = \mathfrak{s}(A)$. Further, if $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_j^{k_j}$, where the p_i's are distinct primes, then $\mathfrak{l}(m) = \operatorname{lcm}\{\mathfrak{l}(p_1^{k_1}), \ldots, \mathfrak{l}(p_j^{k_j})\}$ and $\mathfrak{s}(m) = \max\{\mathfrak{s}(p_1^{k_1}), \ldots, \mathfrak{s}(p_j^{k_j})\}$.

Proof: Let $X = (x_1, x_2, \ldots, x_n) \in Z_m^n$. As we noted above, $D^j(X) = \sum_{1\le i\le n} x_i H^{n+1-i}(D^j(A))$. Thus,

$$\begin{aligned} D^{\mathfrak{l}(A)+\mathfrak{s}(A)}(X) &\equiv \sum_{1\le i\le n} x_i H^{n+1-i}(D^{\mathfrak{l}(A)+\mathfrak{s}(A)}(A)) \pmod m \\ &\equiv \sum_{1\le i\le n} x_i H^{n+1-i}(D^{\mathfrak{s}(A)}(A)) \pmod m \\ &\equiv D^{\mathfrak{s}(A)}(X). \end{aligned}$$

Hence, for all X, $\mathfrak{s}(X) \le \mathfrak{s}(A)$ and $l(X) | l(A)$. We conclude that $\mathfrak{l}(m) = \mathfrak{l}(A)$ and $\mathfrak{s}(m) = \mathfrak{s}(A)$.

Using the prime decomposition of m, we know that

$$Z_m \cong Z_{p_1^{k_1}} \oplus Z_{p_2^{k_2}} \oplus \cdots \oplus Z_{p_j^{k_j}},$$

where $\oplus$ denotes the direct sum. For an n-tuple

$$\begin{array}{ccccc} (x_1, x_2, \ldots, x_n) & \cong & ((x_1, x_2, \ldots, x_n), \ldots, (x_1, x_2, \ldots, x_n)). \\ \in Z_m^n & & \in Z_{p_1^{k_1}}^n & & \in Z_{p_j^{k_j}}^n \end{array}$$

Thus, $D^{l+s}(X) \equiv D^s(X) \pmod m$ if and only if $D^{l+s}(X) \equiv D^s(X) \pmod{p_i^{k_i}}$ for $1 \le i \le j$. Consequently, $\mathfrak{l}(m) = \operatorname{lcm}\{\mathfrak{l}(p_1^{k_1}), \ldots, \mathfrak{l}(p_j^{k_j})\}$ and $\mathfrak{s}(m) = \max\{\mathfrak{s}(p_1^{k_1}), \ldots, \mathfrak{s}(p_j^{k_j})\}$. □

Theorem 1 greatly simplifies our work. To determine $\mathfrak{l}(m)$ and $\mathfrak{s}(m)$, it suffices to calculate $\mathfrak{l}_u(A)$ and $\mathfrak{s}_u(A)$ for $u = p^k$ with p a prime. Since our ultimate goal is to characterize $\mathfrak{l}(m)$ and $\mathfrak{s}(m)$ for 5-tuples, we narrow our focus to n-tuples with n odd.

Lemma 1: Let n be odd. If m is odd, then for each n-tuple X there exists a unique n-tuple Y such that $D(Y) \equiv X \pmod m$.

Proof: Let $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$ be n-tuples. In order for $D(Y) \equiv X \pmod m$, we must have

$$(y_1 + y_2, y_2 + y_3, \ldots, y_n + y_1) \equiv (x_1, x_2, \ldots, x_n) \pmod m. \tag{1}$$

Hence,

$$(y_1 + y_2) - (y_2 + y_3) + \cdots + (-1)^{i+1}(y_i + y_{i+1}) + \cdots + (y_n + y_1) \equiv \sum_{1\le i\le n}(-1)^{i+1} x_i \pmod m,$$

which simplifies to

$$2y_1 \equiv \Sigma_{1\le i\le n}(-1)^{i+1}x_i \pmod m. \tag{2}$$

Since m is odd, 2 has an inverse in Z_m, so (2) has a solution for y_1. We solve, in turn, for the other entries of Y using (1):

$$y_2 \equiv x_1 - y_1 \pmod m,\ y_3 \equiv x_2 - y_2 \pmod m, \ldots, y_n \equiv x_{n-1} - y_{n-1} \pmod m. \tag{3}$$

Since the solutions in (2) and (3) are unique, Y is unique. □

Theorem 2: Let n be odd. Then $\mathcal{S}(m) = 0$ if and only if m is odd.

Proof: We begin with the case in which m is even. Suppose there exists an n-tuple $Y = (y_1, y_2, \ldots, y_n)$ such that $D(Y) \equiv A \pmod m$. Then

$$(y_1 + y_2, y_2 + y_3, \ldots, y_n + y_1) \equiv (1, 0, \ldots, 0) \pmod m. \tag{4}$$

As in Lemma 1, (4) implies $2y_1 \equiv 1 \pmod m$. But this is impossible since m is even. Thus A is not in a cycle and $\mathcal{S}(A) > 0$. Hence, when m is even, $\mathcal{S}(m) \neq 0$.

When m is odd, we know from Lemma 1 that every n-tuple has a predecessor. For $X \in Z_m^n$, we can find a sequence of n-tuples such that

$$D(Y_1) \equiv X,\ D(Y_2) \equiv Y_1,\ D(Y_3) \equiv Y_2,\ D(Y_4) \equiv Y_3,\ D(Y_5) \equiv Y_4, \ldots \pmod m \tag{5}$$

or, equivalently,

$$D(Y_1) \equiv X,\ D^2(Y_2) \equiv X,\ D^3(Y_3) \equiv X,\ D^4(Y_4) \equiv X,\ D^5(Y_5) \equiv X, \ldots \pmod m.$$

Since there are only a finite number of n-tuples, eventually the sequence in (5) must repeat. That is, $Y_i \equiv Y_j \pmod m$ for some $i > j$. This implies $D^j(Y_i) \equiv D^j(Y_j) \equiv X \pmod m$. Hence, X is in a cycle and $\mathcal{S}(X) = 0$. We conclude that $\mathcal{S}(m) = 0$. □

Using Theorems 1 and 2, we see that, when n is odd,

$$\mathcal{S}(m) = \max\{\mathcal{S}(2^k), \mathcal{S}(p_2^{k_2}), \ldots, \mathcal{S}(p_j^{k_j})\} = s(2^k),$$

where the p_i's are distinct primes and $m = 2^k \cdot p_2^{k_2} \cdot \cdots \cdot p_j^{k_j}$. Thus, finding $\mathcal{S}(m)$ requires only calculating $\mathcal{S}(2^k)$.

As for $\mathfrak{l}(m)$, since A is in a cycle if and only if m is odd, there are two cases: $\mathfrak{l}(p^k)$, where p is an odd prime and $\mathfrak{l}(2^k)$, In much of what follows, we will consider the first case, leaving the second, special case for the end.

Theorem 3: Let n be odd and p be an odd prime. Suppose that $D^t(A) \equiv A \pmod{p^k}$. Then $D^{pt}(A) \equiv A \pmod{p^{k+1}}$. Thus, $\mathfrak{l}(p^{k+1})$ equals either $\mathfrak{l}(p^k)$ or $p \cdot \mathfrak{l}(p^k)$.

Proof: We begin by noting that Theorem 2 guarantees the existence of $t > 0$ for which $D^t(A) \equiv A \pmod{p^k}$. Rewriting the congruence as an equation gives

$$D^t(A) = A + (b_1 p^k,\ b_2 p^k, \ldots, b_n p^k) = A + \Sigma_{1\le i\le n} b_i p^k H^{n+1-i}(A).$$

Thus

$$\begin{aligned} D^{2t}(A) &= D^t\left(A + \Sigma_{1\le i\le n} b_i p^k H^{n+1-i}(A)\right) \\ &= D^t(A) + \Sigma_{1\le i\le n} b_i p^k H^{n+1-i}(D^t(A)) \\ &= A + \Sigma_{1\le i\le n} b_i p^k H^{n+1-i}(A) + \Sigma_{1\le i\le n} b_i p^k H^{n+1-i}\left(A + \Sigma_{1\le j\le n} b_j p^k H^{n+1-j}(A)\right) \\ &= A + \Sigma_{1\le i\le n} 2b_i p^k H^{n+1-i}(A) + p^{2k} \Sigma_{1\le i\le n} \Sigma_{1\le j\le n} b_i b_j H^{2n+2-i-j}(A) \\ &= A + \Sigma_{1\le i\le n} 2b_i p^k H^{n+1-i}(A) + p^{2k} X_2, \end{aligned}$$

where $X_2 = \Sigma_{1\le i\le n} \Sigma_{1\le j\le n} b_i b_j H^{2n+2-i-j}(A)$. By induction,

$$D^{ht}(A) = A + \Sigma_{1\le i\le n} h b_i p^k H^{n+1-i}(A) + p^{hk} X_h$$

for some n-tuple X_h. Hence,

$$\begin{aligned} D^{pt}(A) &= A + \Sigma_{1\le i\le n} p b_i p^k H^{n+1-i}(A) + p^{pk} X_p \\ &= A + \Sigma_{1\le i\le n} b_i p^{k+1} H^{n+1-i}(A) + p^{pk} X_p \\ &\equiv A \pmod{p^{k+1}}. \end{aligned}$$

Now let $t = \mathfrak{l}(p^k)$. If $p | b_i$ for all i, then $D^t(A) \equiv A \pmod{p^{k+1}}$. In this case, $\mathfrak{l}(p^{k+1}) = \mathfrak{l}(p^k)$. On the other hand, if $p \nmid b_i$ for some i, then $\mathfrak{l}(p^{k+1}) = p \cdot \mathfrak{l}(p^k)$. □

Corollary 1: Let n be odd and p be an odd prime.

(i) If $\mathfrak{l}(p^2) \neq \mathfrak{l}(p)$, then $\mathfrak{l}(p^k) = p^{k-1} \cdot \mathfrak{l}(p)$ for all $k \ge 2$.

(ii) If $\mathfrak{l}(p^2) = \mathfrak{l}(p)$, then there exists $u \ge 2$ such that $\mathfrak{l}(p^k) = \mathfrak{l}(p)$ for all $k \le u$ and $\mathfrak{l}(p^k) = p^{k-u} \cdot \mathfrak{l}(p)$ for all $k > u$.

Proof: The proof of Theorem 3 shows that, if $D^t(A) \equiv A \pmod{p^k}$ and $D^t(A) \not\equiv A \pmod{p^{k+1}}$, then $D^{pt}(A) \equiv A \pmod{p^{k+1}}$ and $D^{pt}(A) \not\equiv A \pmod{p^{k+2}}$. Hence, if $\mathfrak{l}(p^{k+1}) = p \cdot \mathfrak{l}(p^k)$, then $\mathfrak{l}(p^{k+2}) = p^2 \cdot \mathfrak{l}(p^k)$. Results (i) and (ii) follow immediately from this observation. □

Corollary 1 greatly reduces our work since $\mathfrak{l}(p^k) = p^s \cdot \mathfrak{l}(p)$ for some $s \le k-1$. This allows us to focus on $\mathfrak{l}(p)$

5-TUPLES AND FIBONACCI NUMBERS

We now restrict our attention to 5-tuples. We begin by considering $D^j(A)$. Surprisingly, $D^j(A)$ can be expressed in terms of the Fibonacci numbers. We will use the standard notation: $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, and $F_{j+1} = F_{j-1} + F_j$.

Theorem 4: For $i \ge 1$,

$$\begin{aligned} D^{2i}(A) = (&2^{2i-4}F_2 + 2^{2i-6}F_4 + \cdots + 2^2 F_{2i-4} + F_{2i-2}) \cdot (1, 1, 1, 1, 1) \\ &+ H^i(F_{2i+1}, F_{2i}, 0, 0, F_{2i}). \end{aligned} \tag{6}$$

Proof: We proceed by induction. First, note that

$A = (1, 0, 0, 0, 0)$,

$D(A) = (1, 0, 0, 0, 1)$,

$D^2(A) = (1, 0, 0, 1, 2) = H^1(F_3, F_2, 0, 0, F_2)$.

Thus (6) holds for $i = 1$. Now assume (6) holds for i. Then

$$\begin{aligned} D^{2i+1}(A) &= (2^{2i-4}F_2 + 2^{2i-6}F_4 + \cdots + 2^2F_{2i-4} + F_{2i-2})\cdot(2,2,2,2,2) \\ &\quad + H^i(F_{2k+2}, F_{2i}, 0, F_{2i}, F_{2k+2}) \end{aligned} \tag{7}$$

and

$$\begin{aligned} D^{2i+2}(A) &= (2^{2i-4}F_2 + 2^{2i-6}F_4 + \cdots + 2^2F_{2i-4} + F_{2i-2})\cdot(4,4,4,4,4) \\ &\quad + H^i(F_{2i+2} + F_{2i}, F_{2i}, F_{2i}, F_{2i} + F_{2i+2}, F_{2i+2} + F_{2i+1} + F_{2i}) \\ &= (2^{2i-2}F_2 + 2^{2i-4}F_4 + \cdots + 2^4F_{2i-4} + 2^2F_{2i-2})\cdot(1,1,1,1,1) \\ &\quad + (F_{2i}, F_{2i}, F_{2i}, F_{2i}, F_{2i}) + H^i(F_{2i+2}, 0, 0, F_{2i+2}, F_{2i+3}) \\ &= (2^{2i-2}F_2 + 2^{2i-4}F_4 + \cdots + 2^4F_{2i-4} + 2^2F_{2i-2} + F_{2i})\cdot(1,1,1,1,1) \\ &\quad + H^{i+1}(F_{2i+3}, F_{2i+2}, 0, 0, F_{2i+2}). \quad \square \end{aligned}$$

Since the sum in (6) will occur frequently, we will adopt the following notation:

$$\mathrm{SUM}(2i) = 2^{2i-4}F_2 + 2^{2i-6}F_4 + \cdots + 2^2F_{2k-4} + F_{2i-2}.$$

Note that SUM is defined only for even integers. We use this notation to rewrite (6) and (7) for $i \geq 1$:

$$D^{2i}(A) = \mathrm{SUM}(2i)\cdot(1,1,1,1,1) + H^i(F_{2i+1}, F_{2i}, 0, 0, F_{2i}); \tag{8}$$

$$D^{2i+1}(A) = 2\cdot\mathrm{SUM}(2i)\cdot(1,1,1,1,1) + H^i(F_{2i+2}, F_{2i}, 0, F_{2i}, F_{2i+2}). \tag{9}$$

Theorem 5: Let m be odd. Suppose $D^{\mathfrak{l}}(A) \equiv A \pmod{m}$.

If $\mathfrak{l}$ is even, then $F_{\mathfrak{l}} \equiv 0 \pmod{m}$, $F_{\mathfrak{l}+1} \equiv 1 \pmod{m}$, $\mathrm{SUM}(\mathfrak{l}) \equiv 0 \pmod{m}$, and $5 \mid \mathfrak{l}$.

If $\mathfrak{l}$ is odd, then $F_{\mathfrak{l}} \equiv 0 \pmod{m}$, $F_{\mathfrak{l}+1} \equiv -1 \pmod{m}$.

Proof: If $\mathfrak{l}$ is even, then (8) applies with $2i = \mathfrak{l}$. To simplify notation, let $s = \mathrm{SUM}(\mathfrak{l})$. Then

$$\begin{aligned} D^{\mathfrak{l}}(A) &= (s,s,s,s,s) + H^{\mathfrak{l}/2}(F_{\mathfrak{l}+1}, F_{\mathfrak{l}}, 0, 0, F_{\mathfrak{l}}) \\ &= H^{\mathfrak{l}/2}(s + F_{\mathfrak{l}+1}, s + F_{\mathfrak{l}}, s, s, s + F_{\mathfrak{l}}) \\ &\equiv (1,0,0,0,0) \pmod{m}. \end{aligned}$$

Hence, $5 \mid \mathfrak{l}$, $s \equiv 0 \pmod{m}$, $F_{\mathfrak{l}} \equiv 0 \pmod{m}$, and $F_{\mathfrak{l}+1} \equiv 1 \pmod{m}$.

If $\mathfrak{l}$ is odd, then (9) applies with $2i + 1 = \mathfrak{l}$. Let $s = \mathrm{SUM}(\mathfrak{l} - 1)$. Then

$$\begin{aligned} D^{\mathfrak{l}}(A) &= s\cdot(2,2,2,2,2) + H^{(\mathfrak{l}-1)/2}(F_{\mathfrak{l}+1}, F_{\mathfrak{l}-1}, 0, F_{\mathfrak{l}-1}, F_{\mathfrak{l}+1}) \\ &= H^{(\mathfrak{l}-1)/2}(2\cdot s + F_{\mathfrak{l}+1}, 2\cdot s + F_{\mathfrak{l}-1}, 2\cdot s, 2\cdot s + F_{\mathfrak{l}-1}, 2\cdot s + F_{\mathfrak{l}+1}) \\ &= H^{(\mathfrak{l}-1)/2+2}(2\cdot s, 2\cdot s + F_{\mathfrak{l}-1}, 2\cdot s + F_{\mathfrak{l}+1}, 2\cdot s + F_{\mathfrak{l}+1}, 2\cdot s + F_{\mathfrak{l}-1}) \\ &\equiv (1,0,0,0,0) \pmod{m}. \end{aligned}$$

Hence, $2\cdot s \equiv 1 \pmod{m}$, $F_{\mathfrak{l}-1} \equiv -1 \pmod{m}$, and $F_{\mathfrak{l}+1} \equiv -1 \pmod{m}$. The last two congruences imply that $F_{\mathfrak{l}} \equiv 0 \pmod{m}$. $\square$

PROPERTIES OF $F_K \equiv 0 \pmod{m}$

For m odd, $\mathfrak{l}(m)$ equals the smallest positive integer $\mathfrak{l}$ for which $D^{\mathfrak{l}}(A) \equiv A \pmod{m}$. From Theorem 5, we know that $F_{\mathfrak{l}} \equiv 0 \pmod{m}$ and either $F_{\mathfrak{l}+1} \equiv 1 \pmod{m}$ or $F_{\mathfrak{l}+1} \equiv -1 \pmod{m}$, depending on whether $\mathfrak{l}$ is even or odd, respectively. Thus, we now consider numbers K for which $F_K \equiv 0 \pmod{m}$. We begin by observing that there does exist a $K > 0$ such that $F_K \equiv 0 \pmod{m}$. Since Z_m is finite, there exist $i > j$ such that $F_i \equiv F_j \pmod{m}$ and $F_{i+1} \equiv F_{j+1} \pmod{m}$. These congruences together imply that $F_{i-1} \equiv F_{j-1} \pmod{m}$ which, in turn, implies $F_{i-2} \equiv F_{j-2} \pmod{m}$. Continuing, we see that $F_{i-j} \equiv F_0 \equiv 0 \pmod{m}$.

Numbers K for which $F_K \equiv 0 \pmod{m}$ have been studied in [2], [10], and [11]. The lemmas that follow, as well as the observations in the previous paragraph, are well known. Their proofs are included because they involve techniques that we will use when we derive results about $\mathfrak{l}(m)$.

Lemma 2: Suppose $F_K \equiv 0 \pmod{m}$ and $F_{K+1} \equiv a \pmod{m}$ with $K > 0$. Then

$$F_{K-j} \equiv (-1)^{j+1} a \cdot F_j \pmod{m} \tag{10}$$

and

$$F_{iK+j} \equiv a^i \cdot F_j \pmod{m} \tag{11}$$

for all $i \geq 1$ and $j = 0, 1, \ldots, K-1$.

Proof: To prove (10), we first note that $F_K \equiv 0 \equiv -a \cdot F_0 \pmod{m}$ and $F_{K-1} = F_{K+1} - F_K \equiv a - 0 \equiv a \cdot F_1 \pmod{m}$. Thus, (10) holds for $j = 0$ and $j = 1$. Now assume (10) holds for $j-1$ and j; then

$$\begin{aligned} F_{K-(j+1)} &= F_{K-(j-1)} - F_{K-j} \\ &\equiv (-1)^j a \cdot F_{j-1} - (-1)^{j+1} a \cdot F_j \pmod{m} \\ &\equiv (-1)^j a \cdot (F_{j-1} + F_j) \pmod{m} \\ &\equiv (-1)^{j+2} a \cdot F_{j+1} \pmod{m}. \end{aligned}$$

To prove (11), we make use of the well-known identity: $F_{i+j} = F_{i-1}F_j + F_iF_{j+1}$. Now

$$F_{K+j} = F_{j+1+K-1} = F_jF_{K-1} + F_{j+1}F_K \equiv F_j \cdot a + F_{j+1} \cdot 0 \equiv a \cdot F_j \pmod{m}.$$

Thus (11) holds for $i = 1$. Now assume (11) holds for i. Then

$$F_{(i+1)K+j} = F_{iK+j+1+K-1} = F_{iK+j}F_{K-1} + F_{iK+j+1}F_K \equiv a^i \cdot F_j \cdot a \equiv a^{i+1} \cdot F_j \pmod{m}. \quad \square$$

Lemma 3: Suppose $F_K \equiv 0 \pmod{m}$ and $F_{K+1} \equiv a \pmod{m}$ with $K > 0$. Then $a^2 \equiv (-1)^K \pmod{m}$. Thus, when $m > 2$, $a^2 \equiv 1 \pmod{m}$ if and only if K is even.

Proof: By (10),

$$1 = F_1 = F_{K-(K-1)} \equiv (-1)^K \cdot a \cdot F_{K-1} \equiv (-1)^K \cdot a \cdot a \equiv (-1)^K \cdot a^2 \pmod{m}.$$

Thus $a^2 \equiv (-1)^K \pmod{m}$. As for the second statement, when $m > 2$, $(-1)^K \equiv 1 \pmod{m}$ if and only if K is even. $\square$

In Theorem 5 we consider $\mathfrak{l}$ for which $D^{\mathfrak{l}}(A) \equiv A \pmod{m}$ where, of course, m is odd. We showed that $F_{\mathfrak{l}} \equiv 0 \pmod{m}$ and either $F_{\mathfrak{l}+1} \equiv 1 \pmod{m}$ or $F_{\mathfrak{l}+1} \equiv -1 \pmod{m}$ depending on

whether ℓ is even or odd, respectively. Lemma 3 shows that the second case with ℓ odd is impossible. Thus, when $D^{\ell}(A) \equiv A \pmod{m}$, ℓ is even with $F_{\ell} \equiv 0 \pmod{m}$ and $F_{\ell+1} \equiv 1 \pmod{m}$. We now show that there is always a $K > 0$ for which $F_K \equiv 0 \pmod{m}$ and $F_{K+1} \equiv 1 \pmod{m}$.

Lemma 4: Suppose $F_K \equiv 0 \pmod{m}$ and $F_{K+1} \equiv a \pmod{m}$ with $K > 0$. Then:

$$F_{2K} \equiv 0 \pmod{m} \text{ and } F_{2K+1} \equiv (-1)^K \pmod{m};$$
$$F_{4K} \equiv 0 \pmod{m} \text{ and } F_{4K+1} \equiv 1 \pmod{m}.$$

Proof: Using Lemmas 2 and 3, we find:

$$F_{2K} \equiv a^2 F_0 \equiv 0 \pmod{m} \text{ and } F_{2K+1} \equiv a^2 F_1 \equiv (-1)^K \pmod{m};$$
$$F_{4k} \equiv a^4 F_0 \equiv 0 \pmod{m} \text{ and } F_{4k+1} \equiv a^4 F_1 \equiv (-1)^{2K} \equiv 1 \pmod{m}. \ \square$$

Thus that there is always a $K > 0$ for which $F_K \equiv 0 \pmod{m}$ and $F_{K+1} \equiv 1 \pmod{m}$. We denote the smallest such integer by $K(m)$. That is,

$$K(m) = \min\{K > 0 | F_K \equiv 0 \pmod{m} \text{ and } F_{K+1} \equiv 1 \pmod{m}\}.$$

By Lemma 3, $K(m)$ is even when $m > 2$. We note that $K(2) = 3$. The next lemma contains a useful property of $K(m)$.

Lemma 5: Let $K > 0$. Then $F_K \equiv 0 \pmod{m}$ and $F_{K+1} \equiv 1 \pmod{m}$ if and only if $K(m) | K$.

Proof: Suppose $F_K \equiv 0 \pmod{m}$ and $F_{K+1} \equiv 1 \pmod{m}$. By definition, $K(m)$ is the smallest number satisfying these conditions. Thus $K(m) \le K$. Let $K = q \cdot K(m) + r$, where $0 \le r < K(m)$. Then by Lemma 2, $F_K = F_{qK(m)+r} \equiv F_r \pmod{m}$. Since $F_K \equiv 0 \pmod{m}$, $F_r \equiv 0 \pmod{m}$. Hence $r = 0$. The converse follows immediately from Lemma 2. $\square$

Corollary 2: Let m be odd. Then $\ell(m) = \text{lcm}\{5, j \cdot K(m)\}$, where j is the smallest integer for which $\text{SUM}(j \cdot K(m)) \equiv 0 \pmod{m}$.

Proof: We know that $\ell(m)$ is the smallest ℓ for which $D^{\ell}(A) \equiv A \pmod{m}$. As we observed above, ℓ is even, $F_{\ell} \equiv 0 \pmod{m}$ and $F_{\ell+1} \equiv 1 \pmod{m}$. By Lemma 5, ℓ is a multiple of $K(m)$. The conclusion now follows immediately from Theorem 5. $\square$

By Corollary 2, when p is an odd prime, $\ell(p^k)$ is a multiple $K(p^k)$. The following lemma connects $K(p^k)$ and $K(p)$. This relationship will greatly aid in the calculation of $\ell(p^k)$.

Lemma 6: Let p be a prime. Then

(i) For $k \ge 1$, $K(p^{k+1})$ equals either $K(p^k)$ or $p \cdot K(p^k)$.

(ii) If $K(p^2) \ne K(p)$, then $K(p^k) = p^{k-1} \cdot K(p)$ for $k \ge 2$.

(iii) If $K(p^2) = K(p)$, then there exists $u \ge 2$ such that $K(p^k) = K(p)$ for $k \le u$ and $K(p^k) = p^{k-u} \cdot K(p)$ for $k > u$.

Proof: This is a well-known result; its proof is given in [1]. Note the similarities between the properties of K in this lemma and the properties of ℓ in Theorem 3 and Corollary 1. $\square$

We know that $\ell(p^k)$ is a multiple of $K(p^k)$, while the latter is a multiple of $K(p)$. Thus, $\ell(p^k)$ is a multiple of $K(p)$. We conclude this section with a lemma that gives bounds on $K(p)$.

Although the result is well known [10], the proof is included because it shows the way in which the different cases arise. As we will see, $K(p)$ depends on the value of $5^{(p-1)/2}$ modulo p. When $p=5$, $5^{(p-1)/2}$ is, of course, congruent to 0. Hence $p=5$ is a special case. For all other odd primes, $5^{(p-1)/2}$ is congruent to 1 or -1 depending on whether 5 is a quadratic residue or non-residue of p, respectively. If p is congruent to 1 or 9 modulo 10, then

$$(5/p)=(p/5)=([10q\pm1]/5)=(\pm1/5)=1,$$

where $(\cdot)$ is the Legendre symbol. Hence 5 is a quadratic residue and $5^{(p-1)/2}\equiv 1 \pmod{p}$. On the other hand, if p is congruent to 3 or 7 modulo 10, then

$$(5/p)=(p/5)=([10q\pm3]/5)=(\pm3/5)=-1.$$

In this case, 5 is a nonresidue and $5^{(p-1)/2}\equiv -1 \pmod{p}$.

Lemma 7: Let p be an odd prime. Then

$$\begin{aligned} &K(p)\,|\,(p-1) && p\equiv 1 \text{ or } 9 \pmod{10},\\ &K(p)\,|\,(2p+2) && p\equiv 3 \text{ or } 7 \pmod{10},\\ &K(5)=20. \end{aligned}$$

Proof: By Binet's formula,

$$\begin{aligned} F_p &= \frac{(1+\sqrt{5})^p-(1-\sqrt{5})^p}{\sqrt{5}\,2^p}\\ &= \frac{1}{2^{p-1}}\left[\binom{p}{1}+\binom{p}{3}5+\cdots+\binom{p}{p-2}5^{(p-3)/2}+\binom{p}{p}5^{(p-1)/2}\right]\\ &\equiv 5^{(p-1)/2} \pmod{p} \end{aligned}$$

and

$$\begin{aligned} F_{p+1} &= \frac{(1+\sqrt{5})^{p+1}-(1-\sqrt{5})^{p+1}}{\sqrt{5}\,2^{p+1}}\\ &= \frac{1}{2^p}\left[\binom{p+1}{1}+\binom{p+1}{3}5+\cdots+\binom{p+1}{p-2}5^{(p-3)/2}+\binom{p+1}{p}5^{(p-1)/2}\right]\\ &\equiv 2^{-1}[1+5^{(p-1)/2}] \pmod{p}. \end{aligned}$$

When $p\equiv 1$ or 9 (mod 10), $F_p\equiv 1 \pmod{p}$ and $F_{p+1}\equiv 1 \pmod{p}$. These imply $F_{p-1}\equiv 0 \pmod{p}$. Hence by Lemma 5, $K(p)\,|\,(p-1)$.

When $p\equiv 3$ or 7 (mod 10), $F_p\equiv -1 \pmod{p}$ and $F_{p+1}\equiv 0 \pmod{p}$. These imply $F_{p+2}\equiv -1 \pmod{p}$. By Lemma 4, $F_{2p+2}\equiv 0 \pmod{p}$ and $F_{2p+3}\equiv 1 \pmod{p}$. Hence $K(p)\,|\,(2p+2)$.

By direct calculation we find that $K(5)=20$. □

PROPERTIES OF SUM (mod m)

By Corollary 2, for odd m, $\mathfrak{l}(m)=\operatorname{lcm}\{5, j\cdot K(m)\}$, where j is the smallest integer for which $\operatorname{SUM}(j\cdot K(m))\equiv 0 \pmod{m}$. We now consider such sums.

Lemma 8: Suppose $F_K \equiv 0 \pmod{m}$ and $F_{K+1} \equiv 1 \pmod{m}$, where K is an even positive integer. Then

$$\mathrm{SUM}(jK) \equiv (2^{(j-1)K} + \cdots + 2^K + 1) \cdot \mathrm{SUM}(K) \pmod{m}.$$

Proof: The congruence certainly holds for $j = 1$. Assume it holds for j and consider $j+1$:

$$\begin{aligned}\mathrm{SUM}((j+1)\cdot K) &= 2^{(j+1)K-4}F_2 + 2^{(j+1)K-6}F_4 + \cdots + 2^{jK}F_{K-2} + 2^{jK-2}F_K \\ &\quad + 2^{jK-4}F_{K+2} + \cdots + 2^2 F_{(j+1)K-4} + F_{(j+1)K-2} \\ &= 2^{jK}\cdot(2^{K-4}F_2 + 2^{K-6}F_4 + \cdots + F_{K-2}) + 2^{jK-2}F_K \\ &\quad + 2^{jK-4}F_{K+2} + \cdots + 2^2 F_{(j+1)K-4} + F_{(j+1)K-2}.\end{aligned}$$

Now by Lemma 2, $F_{K+2} \equiv F_2 \pmod{m}, \ldots, F_{(j+1)K-2} \equiv F_{K-2} \equiv F_{jK-2} \pmod{m}$. Thus

$$\begin{aligned}\mathrm{SUM}((j+1)\cdot K) &\equiv 2^{jK}\cdot(2^{K-4}F_2 + 2^{K-6}F_4 + \cdots + F_{K-2}) + 2^{jK-2}F_K \\ &\quad + 2^{jK-4}F_2 + \cdots + 2^2 F_{jK-4} + F_{jK-2} \pmod{m} \\ &\equiv 2^{jK}\cdot\mathrm{SUM}(K) + 0 + \mathrm{SUM}(jK) \pmod{m} \\ &\equiv 2^{jK}\cdot\mathrm{SUM}(K) + (2^{(j-1)K} + \cdots + 2^K + 1)\cdot\mathrm{SUM}(K) \pmod{m} \\ &\equiv (2^{jK} + 2^{(j-1)K} + \cdots + 2^K + 1)\cdot\mathrm{SUM}(K) \pmod{m}. \ \square\end{aligned}$$

For odd m, $\mathfrak{l}(m)$ is a multiple of $j \cdot K(m)$. Lemma 8 tells us how to find j. First, we calculate $\mathrm{SUM}(K(m))$. If $\mathrm{SUM}(K(m)) \equiv 0 \pmod{m}$, $\mathfrak{l}(m) = \mathrm{lcm}\{5, K(m)\}$. On the other hand, if $\mathrm{SUM}(K(m)) \not\equiv 0 \pmod{m}$, then we must select j so that

$$(2^{(j-1)K(m)} + \cdots + 2^{K(m)} + 1)\cdot\mathrm{SUM}(K(m)) \equiv 0 \pmod{m}.$$

The next lemma will aid in calculating $\mathrm{SUM}(K(m))$ modulo m.

Lemma 9: Suppose $F_K \equiv 0 \pmod{m}$ and $F_{K+1} \equiv 1 \pmod{m}$, where K is an even positive integer. Then

$$\mathrm{SUM}(K) \equiv \sum_{j=1}^{K/2} \binom{K}{2j} 5^{j-1} \pmod{m}.$$

Proof: By Lemma 2, $F_{K-j} \equiv (-1)^{j+1}F_j \pmod{m}$. Thus

$$\begin{aligned}\mathrm{SUM}(K) &= 2^{K-4}F_2 + 2^{K-6}F_4 + \cdots + 2^2 F_{K-4} + F_{K-2} \\ &\equiv -2^{K-4}F_{K-2} - 2^{K-6}F_{K-4} - \cdots - 2^2 F_4 - F_2 \pmod{m}.\end{aligned} \tag{12}$$

In preparation for using Binet's formula, let $a = (1+\sqrt{5})$ and $b = (1-\sqrt{5})$. Note that

$$a^2 - 1 = 5 + 2\sqrt{5},\ b^2 - 1 = 5 - 2\sqrt{5}, \text{ and } (a^2-1)\cdot(b^2-1) = 5.$$

Now, by Binet's formula, $F_j = [a^j - b^j]/(2^j\sqrt{5})$. Thus $2^{j-2}F_j = [a^j - b^j]/(2^2\sqrt{5})$. Hence

$$\begin{aligned}&2^{K-4}F_{K-2} + 2^{K-6}F_{K-4} + \cdots + 2^2 F_4 + F_2 \\ &= [a^{K-2} - b^{K-2} + a^{K-4} - b^{K-4} + \cdots + a^2 - b^2]/(2^2\sqrt{5}) \\ &= [(a^{K-2} + a^{K-4} + \cdots + a^2 + 1) - (b^{K-2} + b^{K-4} + \cdots + b^2 + 1)]/(2^2\sqrt{5}) \\ &= [(a^K - 1)/(a^2 - 1) - (b^K - 1)/(b^2 - 1)]/(2^2\sqrt{5})\end{aligned}$$

$$= [(a^K - 1)\cdot(5 - 2\sqrt{5}) - (b^K - 1)\cdot(5 + 2\sqrt{5})] / (2^2 \cdot 5\sqrt{5})$$
$$= [5a^K - 2\sqrt{5}\,a^K - 5 + 2\sqrt{5} - 5b^K - 2\sqrt{5}\,b^K + 5 + 2\sqrt{5}] / (2^2 \cdot 5\sqrt{5})$$
$$= (a^K - b^K) / (2^2\sqrt{5}) - (a^K + b^K) / (2 \cdot 5) + 1/5$$
$$= 2^{K-2} F_K - 5^{-1}[(a^K + b^K)/2 - 1]. \tag{13}$$

We use the Binomial Theorem to rewrite $5^{-1}[(a^K + b^K)/2 - 1]$ as

$$5^{-1}\left[\frac{(1+\sqrt{5})^K + (1-\sqrt{5})^K}{2} - 1\right] = \sum_{j=1}^{K/2} \binom{K}{2j} 5^{j-1}. \tag{14}$$

We now combine (12), (13), and (14) and reduce modulo m:

$$\begin{aligned} \text{SUM}(K) &\equiv -2^{K-4} F_{K-2} - 2^{K-6} F_{K-4} - \cdots - 2^2 F_4 - F_2 \pmod{m} \\ &\equiv -2^{K-2} F_K + 5^{-1}[(a^K + b^K)/2 - 1] \pmod{m} \\ &\equiv \sum_{j=1}^{K/2} \binom{K}{2j} 5^{j-1} \pmod{m}. \quad \square \end{aligned} \tag{15}$$

Note that Lemmas 8 and 9 hold for all m so long as K is an even positive integer.

DETERMINING $\mathfrak{l}(p)$ FOR ODD PRIMES

We are now going to determine $\mathfrak{l}(p)$ for odd primes. We will consider four cases: $p = 3$, $p = 5$, $p \equiv 1$ or 9 (mod 10), and $p \equiv 3$ or 7 (mod 10). Although the derivations will be different, the final result will be the same. In order to state the result, we need some additional notation. For $a \in Z_m$ with $\gcd(a, m) = 1$, we will denote the order of a in Z_m by $o_m(a)$. Thus, if $s > 0$ is the smallest positive integer for which $a^s \equiv 1 \pmod{m}$, we will write $o_m(a) = s$. Of course, if $a \equiv 1 \pmod{m}$, $o_m(a) = 1$. What we will show is that for odd p,

$$\mathfrak{l}(p) = \text{lcm}\{5, o_p(2^{K(p)}) \cdot K(p)\}. \tag{16}$$

We showed in Corollary 2 that $\mathfrak{l}(p)$ is the least common multiple of 5 and $j \cdot K(p)$, where j is the smallest integer for which $\text{SUM}(j \cdot K(p)) \equiv 0 \pmod{p}$. As we observed above, to find j we first calculate $\text{SUM}(K(m))$. If $\text{SUM}(K(m)) \equiv 0 \pmod{m}$, $\mathfrak{l}(m) = \text{lcm}\{5, K(m)\}$. On the other hand, if $\text{SUM}(K(m)) \not\equiv 0 \pmod{m}$, then we must select j so that

$$(2^{(j-1)K(m)} + \cdots + 2^{K(m)} + 1) \cdot \text{SUM}(K(m)) \equiv 0 \pmod{m}.$$

We begin with the two special cases, $p = 3$ and $p = 5$.

Theorem 6: $\mathfrak{l}(3) = 40$ and $\mathfrak{l}(5) = 20$.

Proof: By direct calculation, it is easy to verify that $K(3) = 8$. Now, by Lemma 9,

$$\begin{aligned} \text{SUM}(8) &\equiv \sum_{j=1}^{4} \binom{8}{2j} 5^{j-1} \pmod{3} \equiv \binom{8}{2} + \binom{8}{4} 5 + \binom{8}{6} 5^2 + \binom{8}{8} 5^3 \pmod{3} \\ &\equiv 1 + 2 + 1 + 2 \pmod{3} \equiv 0 \pmod{3}. \end{aligned}$$

Hence $\mathfrak{l}(3) = \text{lcm}\{5, 8\} = 40$.

It is also easy to verify that $K(5) = 20$. Now, by Lemma 9,

$$\text{SUM}(20) \equiv \sum_{j=1}^{10} \binom{20}{2j} 5^{j-1} \pmod 5 \equiv \binom{20}{2} \pmod 5 \equiv 0 \pmod 5.$$

Hence $\mathfrak{l}(5) = \text{lcm}\{5, 20\} = 20$. □

We note that (16) holds for $p = 3$ and $p = 5$. In both cases, $K(p)$ is a multiple of $\phi(p) = p - 1$; hence, $2^{K(p)} \equiv 1 \pmod p$. Therefore, for $p = 3$ and $p = 5$, $o_p(2^{K(p)}) = 1$ and $\mathfrak{l}(p) = \text{lcm}\{5, o_p(2^{K(p)}) \cdot K(p)\}$.

Next we consider primes for which $p \equiv 1$ or $9 \pmod{10}$. We begin with a lemma which deals with $\text{SUM}(K(p^j))$ modulo p^j for $j \geq 1$. At the moment we are concerned only when $j = 1$. However, we state and prove the more general case since we will need it later.

Lemma 10: Let p be a prime such that $p \equiv 1$ or $9 \pmod{10}$. Let $q = p^j$ for $j \geq 1$. Then

$$\text{SUM}(K(q)) \equiv 5^{-1}[2^{K(q)} - 1] \pmod q.$$

Proof: To simplify notation, let $K = K(q)$. Since 5 is quadratic residue, the congruence $x^2 \equiv 5 \pmod q$ has a solution in Z_q. Let r be such a solution. Then Binet's formula holds in Z_p:

$$F_K \equiv [(1+r)^K - (1-r)^K]/(2^K r) \equiv 0 \pmod q \tag{17}$$

and

$$F_{K+1} \equiv [(1+r)^{K+1} - (1-r)^{K+1}]/(2^{K+1} r) \equiv 1 \pmod q. \tag{18}$$

From (17), we see that $(1+r)^K \equiv (1-r)^K \pmod p$. Thus, we can rewrite (18) as

$$1 \equiv (1+r)^K \cdot [(1+r) - (1-r)]/(2^{K+1} r) \equiv (1+r)^K / 2^K \pmod q.$$

Hence $(1+r)^K \equiv 2^K \pmod p$. Now, by (15) of Lemma 9,

$$\begin{aligned} \text{SUM}(K) &\equiv 5^{-1}[((1+r)^K + (1-r)^K)/2 - 1] \pmod q \\ &\equiv 5^{-1}[2^K - 1] \pmod q. \quad \square \end{aligned}$$

Theorem 7: Let p be a prime such that $p \equiv 1$ or $9 \pmod{10}$. Then

$$\mathfrak{l}(p) = \text{lcm}\{5, o_p(2^{K(p)}) \cdot K(p)\}.$$

Proof: Again, to simplify notation, we let $K = K(p)$. Using Lemmas 8 and 10, we have

$$\begin{aligned} \text{SUM}(j \cdot K) &\equiv (2^{(j-1)K} + \cdots + 2^K + 1) \cdot \text{SUM}(K) \pmod p \\ &\equiv (2^{(j-1)K} + \cdots + 2^K + 1) \cdot 5^{-1}[2^K - 1] \pmod p \\ &\equiv \{[2^{jK} - 1]/[2^K - 1]\} \cdot 5^{-1}[2^K - 1] \pmod p \\ &\equiv 5^{-1}[2^{jK} - 1] \pmod p. \end{aligned}$$

We want the smallest j for which $\text{SUM}(j \cdot K) \equiv 0 \pmod p$. Clearly, $j = o_p(2^K)$ and hence $\mathfrak{l}(p) = \text{lcm}\{5, o_p(2^K) \cdot K\}$. □

We now consider the case in which $p \equiv 3$ or $7 \pmod{10}$. Since 5 is a nonresidue in this case, Binet's theorem cannot be used as above.

Lemma 11: Let p be a prime such that $p \equiv 3$ or 7 (mod 10) with $p > 3$. Then $\text{SUM}(2p+2) \equiv 3 \pmod{p}$ and $\text{SUM}(K(p)) \not\equiv 0 \pmod{p}$.

Proof: By Lemma 9,

$$\text{SUM}(2p+2) \equiv \sum_{j=1}^{p+1} \binom{2p+2}{2j} 5^{j-1} \pmod{p}.$$

For $1 < j < (p+1)/2$,

$$\binom{2p+2}{2j} \equiv 0 \pmod{p} \quad \text{and} \quad \binom{2p+2}{2p+2-2j} \equiv 0 \pmod{p}.$$

Also

$$\binom{2p+2}{2} \equiv 1 \pmod{p}, \quad \binom{2p+2}{2p} \equiv 1 \pmod{p},$$

and

$$\binom{2p+2}{p+1} = \frac{(2p+2)(2p+1)2p(p+p-1)\cdots(p+2)}{(p+1)p(p-1)\cdots 2} \equiv \frac{2\cdot 1\cdot 2\cdot (p-1)!}{1\cdot (p-1)!} \equiv 4 \pmod{p}.$$

Since 5 is nonresidue, $5^{(p-1)/2} \equiv -1 \pmod{p}$. Hence

$$\begin{aligned}\text{SUM}(2p+2) &\equiv \binom{2p+2}{2} + \binom{2p+2}{p+1} 5^{(p-1)/2} + \binom{2p+2}{2p} 5^{p-1} + \binom{2p+2}{2p+2} 5^{p} \pmod{p} \\ &\equiv 1 + 4\cdot(-1) + 1 + 5 \pmod{p} \equiv 3 \pmod{p}.\end{aligned}$$

By Lemma 7, $K(p) | (2p+2)$. If $K(p) \neq (2p+2)$, let $j = (2p+2)/K(p)$. Then by Lemma 8,

$$\text{SUM}(2p+2) \equiv \text{SUM}(j \cdot K(p)) \equiv (2^{(j-1)K(p)} + \cdots + 2^{K(p)} + 1) \cdot \text{SUM}(K(p)) \pmod{p}.$$

Since $\text{SUM}(2p+2) \not\equiv 0 \pmod{p}$ when $p > 3$, $\text{SUM}(K(p)) \not\equiv 0 \pmod{p}$. □

Lemma 12: Let p be a prime such that $p \equiv 3$ or 7 (mod 10) with $p > 3$. Then $2^{K(p)} \not\equiv 1 \pmod{p}$.

Proof: Assume to the contrary that $2^{K(p)} \equiv 1 \pmod{p}$. This means $o_p(2) | K(p)$ which, in turn, implies that $o_p(2) | (2p+2)$. But we know $o_p(2) | (p-1)$. Since $\gcd(p-1, p+1) = 2$, $o_p(2)$ must equal 2 or 4. For $p > 3$, $2^2 \not\equiv 1 \pmod{p}$ and so $o_p(2) \neq 2$. Now $2^4 \equiv 2 \pmod{7}$, $2^4 \equiv 3 \pmod{13}$ and, for all other p, $2^4 < p$. Thus, for $p > 3$, $2^4 \not\equiv 1 \pmod{p}$, so $o_p(2) \neq 4$. We conclude that $2^{K(p)} \not\equiv 1 \pmod{p}$. □

Theorem 8: Let p be a prime such that $p \equiv 3$ or 7 (mod 10) with $p > 3$. Then we have $\mathfrak{l}(p) = \text{lcm}\{5, o_p(2^K) \cdot K\}$

Proof: To simplify notation, we let $K = K(p)$. Using Lemma 8, we have $\text{SUM}(j \cdot K) \equiv (2^{(j-1)K} + \cdots + 2^K + 1) \cdot \text{SUM}(K) \pmod{p}$. By Lemma 11, $\text{SUM}(K) \not\equiv 0 \pmod{p}$, so we want the smallest j for which

$$2^{(j-1)K} + \cdots + 2^K + 1 \equiv 0 \pmod{p}. \tag{19}$$

Now $2^K \not\equiv 1 \pmod{p^k}$ by Lemma 12. Thus, the smallest j for which (19) holds is $o_p(2^K)$. □

DETERMINING $\mathfrak{l}(p^k)$ FOR ODD PRIMES

We know that $\mathfrak{l}(p^k) = p^s \cdot \mathfrak{l}(p)$ for some $s \le k-1$. We now show that for most, if not all, primes, $\mathfrak{l}(p^k) = p^{k-1} \cdot \mathfrak{l}(p)$. There are several cases.

Corollary 3: Let p be an odd prime with $p \neq 5$. If $K(p^2) \neq K(p)$, then $\mathfrak{l}(p^k) = p^{k-1} \cdot \mathfrak{l}(p)$.

Proof: By the theorems above, we know that $\mathfrak{l}(p) = \text{lcm}\{5, o_p(2^{K(p)}) \cdot K(p)\}$. Of course, $o_p(2^{K(p)})$ is relatively prime to p. Further, for $p \neq 5$, by Lemma 7, $K(p)$ is also relatively prime to p. Hence, $\gcd(\mathfrak{l}(p), p) = 1$.

By Lemma 6(ii), $K(p^k) = p^{k-1} \cdot K(p)$ for $k \ge 2$. We know from Corollary 2 that $\mathfrak{l}(p^2)$ is a multiple of $K(p^2) = p \cdot K(p)$; hence, $p | \mathfrak{l}(p^2)$. On the other hand, Corollary 1 tells us that $\mathfrak{l}(p^2)$ equals either $\mathfrak{l}(p)$ or $p \cdot \mathfrak{l}(p)$. Since $\gcd(\mathfrak{l}(p), p) = 1$, $\mathfrak{l}(p^2) = p \cdot \mathfrak{l}(p)$. This, in turn, implies by Corollary 1 that $\mathfrak{l}(p^k) = p^{k-1} \cdot \mathfrak{l}(p)$ for $k \ge 2$. □

When $p = 5$, the proof of Corollary 3 does not apply since $K(5) = 20$, hence $\gcd(\mathfrak{l}(5), 5) \neq 1$. However, direct calculation shows that $\mathfrak{l}(5^2) \neq \mathfrak{l}(5)$. Thus $\mathfrak{l}(5^k) = 5^{k-1} \cdot \mathfrak{l}(5)$ for $k \ge 2$.

Even if $K(p^2) = K(p)$, it may still be the case that $\mathfrak{l}(p^2) = p \cdot \mathfrak{l}(p)$. We now consider this possibility.

Corollary 4: Let p be an odd prime with $p \neq 5$. Suppose that $K(p^2) = K(p)$. If $o_{p^2}(2^{K(p)}) \neq o_p(2^{K(p)})$, then $\mathfrak{l}(p^k) = p^{k-1} \cdot \mathfrak{l}(p)$.

Proof: Let $K = K(p)$. By Corollary 2 and Lemma 8, $\mathfrak{l}(p^2) = \text{lcm}\{5, j \cdot K\}$, where j is the smallest integer for which

$$\text{SUM}(j \cdot K) \equiv (2^{(j-1)K} + \cdots + 2^K + 1) \cdot \text{SUM}(K) \equiv 0 \pmod{p^2}. \tag{20}$$

First, suppose that $\text{SUM}(K) \equiv 0 \pmod{p^2}$; this implies $\text{SUM}(K) \equiv 0 \pmod{p}$. By Lemmas 10 and 11, this can occur only when $p \equiv 1$ or $9 \pmod{10}$, $o_p(2^K) = 1$ and $o_{p^2}(2^K) = 1$. But this contradicts the hypothesis. Thus, $\text{SUM}(K) \not\equiv 0 \pmod{p^2}$ and $2^K \not\equiv 1 \pmod{p}$. Hence, the smallest j for which (20) holds is $o_{p^2}(2^K) = p \cdot o_p(2^K)$. The proof now proceeds in the same manner as the proof of Corollary 3. We conclude that $\mathfrak{l}(p^2) \neq \mathfrak{l}(p)$ and hence $\mathfrak{l}(p^k) = p^{k-1} \cdot \mathfrak{l}(p)$. □

As Wall points out, it is not known whether there exists a prime p for which $K(p^2) = K(p)$ [11]. It has been verified that $K(p^2) \neq K(p)$ for $p < 10{,}000$. Even if there is a prime for which $K(p^2) \neq K(p)$, it may still be the case that $\mathfrak{l}(p^2) = p \cdot \mathfrak{l}(p)$. In order for $\mathfrak{l}(p^2) \neq p \cdot \mathfrak{l}(p)$, two conditions must hold: $K(p^2) = K(p)$ and $o_{p^2}(2^K) = o_p(2^K)$. Of course, although rare, it is possible for an element to have the same order modulo p and p^2.

BOUNDS ON $\mathfrak{l}(p)$

We now use the results from the previous sections to find bounds on $\mathfrak{l}(p)$. First, we note an alternate way to calculate $\mathfrak{l}(p)$.

Corollary 5: Let p be prime with $p > 5$. Then $\mathfrak{l}(p) = \text{lcm}\{5, o_p(2), K(p)\}$.

Proof: By Theorems 7 and 8, it suffices to show that $o_p(2^{K(p)}) \cdot K(p) = \text{lcm}\{o_p(2), K(p)\}$. Now $o_p(2^{K(p)}) = o_p(2) / \gcd(K(p), o_p(2))$. Hence

$$o_p(2^{K(p)}) \cdot K(p) = o_p(2) / \gcd(K(p), o_p(2)) \cdot K(p) = \text{lcm}\{o_p(2), K(p)\}. \quad \square$$

Corollary 6: Let p be prime with $p > 5$. Define $B(p)$ as follows:

$$\begin{aligned} B(p) &= (p-1) && p \equiv 1 \pmod{10}; \\ B(p) &= 5 \cdot (p-1) && p \equiv 9 \pmod{10}; \\ B(p) &= 5 \cdot (p^2-1)/2 && p \equiv 3 \text{ or } 7 \pmod{10} \text{ and } p \equiv 1 \pmod{4}; \\ B(p) &= 5 \cdot (p^2-1) && p \equiv 3 \text{ or } 7 \pmod{10} \text{ and } p \equiv 3 \pmod{4} \end{aligned}$$

Then $\mathfrak{l}(p) | B(p)$.

Proof: We know by Lemma 7 that $o_p(2) | (p-1)$. Now, for $p \equiv 1$ or 9 (mod 10), we have $K(p) | (p-1)$. Hence, for these primes, $\text{lcm}\{o_p(2), K(p)\} | (p-1)$. Thus $\mathfrak{l}(p) | B(p)$.

For $p \equiv 3$ or 7 (mod 10), $K(p) | 2 \cdot (p+1)$. Therefore, for these primes,

$$\text{lcm}\{o_p(2), K(p)\} | \text{lcm}\{p-1, 2 \cdot (p+1)\}.$$

Since

$$\begin{aligned} \text{lcm}\{p-1, 2 \cdot (p+1)\} &= (p^2-1)/2 && p \equiv 1 \pmod{4}, \\ \text{lcm}\{p-1, 2 \cdot (p+1)\} &= (p^2-1) && p \equiv 3 \pmod{4}, \end{aligned}$$

$\mathfrak{l}(p) = B(p)$. $\square$

For the bounds given in Corollary 6, the most common situation is that $\mathfrak{l}(p) = B(p)$. This is certainly the case when $o_p(2)$ equals $p-1$ and $K(p)$ equals $p-1$ or $2p+2$, depending on whether p is congruent to ± 1 or ± 3 modulo 10, respectively.

For $p \equiv 1$ or 9 (mod 10), $\mathfrak{l}(p)$ can equal $B(p)$ even when $K(p) < (p-1)$. The smallest examples are

$$\begin{aligned} p = 101: &\quad K(101) = 50, o_{101}(2) = 100, \text{ so } \mathfrak{l}(101) = 100 = B(101), \\ p = 29: &\quad K(29) = 14, o_{29}(2) = 28, \text{ so } \mathfrak{l}(29) = 5 \cdot 28 = B(29). \end{aligned}$$

However, $\mathfrak{l}(p) < B(p)$ if and only if both $K(p)$ and $o_p(2)$ are less than $p-1$. The smallest examples are

$$\begin{aligned} p = 401: &\quad K(401) = 200, o_{401}(2) = 200, \text{ so } \mathfrak{l}(401) = 200 < 400 = B(401), \\ p = 89: &\quad K(89) = 44, o_{89}(2) = 11, \text{ so } \mathfrak{l}(89) = 5 \cdot 44 < 5 \cdot 88 = B(89). \end{aligned}$$

On the other hand, for $p \equiv 3$ or 7 (mod 10), $\mathfrak{l}(p) \neq B(p)$ if $K(p) < (2p+2)$. The proof of Lemma 7 shows that $K(p) \neq p+1$. Hence, if $K(p) \neq (2p+2)$, then $K(p) < (p+1)$. However, $\mathfrak{l}(p)$ can be less than $B(p)$ in a variety of ways. As we have already noted, this is the case when $K(p) < (2p+2)$. It can also occur even when $K(p) = (2p+2)$. There are 8 possibilities: $p \equiv 3$ or 7 (mod 10), $p \equiv 1$ or 3 (mod 4), $K(p)$ less than or equal to $(2p+2)$. Here are examples of each:

$$\begin{aligned} p = 113: &\quad K(113) = 76, o_{113}(2) = 28, \text{ so } \mathfrak{l}(113) = 5 \cdot 532 < 5 \cdot 6384 = B(113), \\ p = 73: &\quad K(73) = 148, o_{73}(2) = 8, \text{ so } \mathfrak{l}(73) = 5 \cdot 296 < 5 \cdot 2664 = B(73), \\ p = 43: &\quad K(43) = 88, o_{43}(2) = 14, \text{ so } \mathfrak{l}(43) = 5 \cdot 616 < 5 \cdot 1848 = B(43), \\ p = 263: &\quad K(263) = 176, o_{263}(2) = 131, \text{ so } \mathfrak{l}(263) = 5 \cdot 23056 < 5 \cdot 69168 = B(263), \end{aligned}$$

$p = 557$: $K(557) = 124$, $o_{557}(2) = 556$, so $\mathfrak{l}(557) = 5 \cdot 17236 < 5 \cdot 155124 = B(557)$,
$p = 17$: $K(17) = 36$, $o_{17}(2) = 8$, so $\mathfrak{l}(17) = 5 \cdot 72 < 5 \cdot 144 = B(17)$,
$p = 47$: $K(47) = 32$, $o_{47}(2) = 23$, so $\mathfrak{l}(47) = 5 \cdot 736 < 5 \cdot 2208 = B(47)$,
$p = 127$: $K(127) = 256$, $o_{127}(2) = 7$, so $\mathfrak{l}(127) = 5 \cdot 1792 < 5 \cdot 16128 = B(127)$.

DETERMINING $\mathfrak{s}(2^k)$ AND $\mathfrak{l}(2^k)$

Finally, we consider powers of 2.

Lemma 13: For $k > 1$, $K(2^k) = 3 \cdot 2^{k-1}$. Further, $\gcd(\mathrm{SUM}(5 \cdot \mathrm{K}(2^k)), 2) = 1$.

Proof: It is easy to verify that $K(2) = 3$ and $K(2^2) \neq 3$. Thus, for $k > 1$, $K(2^k) = 3 \cdot 2^{k-1}$.

To simplify notation, let $K = K(2^k)$, where $k > 1$. Since $\phi(2^k) = 2^{k-1}$, $K = 3 \cdot \phi(2^k)$. Thus $2^K \equiv 1 \pmod{2^k}$. Combining this observation with Lemma 8 gives us

$$\begin{aligned}\mathrm{SUM}(5K) &\equiv (2^{4K} + 2^{3K} + 2^{2K} + 2^K + 1) \cdot \mathrm{SUM}(K) \pmod{2^k} \\ &\equiv 5 \cdot \mathrm{SUM}(K) \pmod{2^k}.\end{aligned}$$

Thus, to show $\gcd(\mathrm{SUM}(5K), 2) = 1$, it suffices to show that $\gcd(\mathrm{SUM}(K), 2) = 1$. By Lemma 9,

$$\begin{aligned}\mathrm{SUM}(K) &\equiv \sum_{j=1}^{3 \cdot 2^{k-2}} \binom{3 \cdot 2^{k-1}}{2j} 5^{j-1} \pmod{2^k} \\ &\equiv \sum_{j=1}^{3 \cdot 2^{k-2}-1} \binom{3 \cdot 2^{k-1}}{2j} 5^{j-1} + 5^{3 \cdot 2^{k-2}-1} \pmod{2^k} \\ &\equiv 0 + 1 \pmod{2}.\end{aligned}$$

Hence $\gcd(\mathrm{SUM}(K), 2) = 1$. □

Theorem 9: $\mathfrak{s}(2^k) = k$ and $\mathfrak{l}(2^k) = 15 \cdot 2^{k-1}$.

Proof: As can easily be verified, $D^{16}(A) \equiv D(A) \pmod{2}$. Thus $\mathfrak{s}(2) = 1$ and $\mathfrak{l}(2) = 15$.

For $k > 1$, set $K = K(2^k) = 3 \cdot 2^{k-1}$. Note that K is even and $\gcd(K, 5) = 1$. Now, by Theorem 5,

$$\begin{aligned}D^{k-1+5K}(A) &= D^{k-1}(D^{5K}(A)) \\ &\equiv D^{k-1}(\mathrm{SUM}(5K) \cdot (1, 1, 1, 1, 1) + H^{5K/2}(A)) \pmod{2^k} \\ &\equiv 2^{k-1} \cdot \mathrm{SUM}(5K) \cdot (1, 1, 1, 1, 1) + D^{k-1}(A) \pmod{2^k}.\end{aligned}$$

Since $\gcd(\mathrm{SUM}(5K), 2) = 1$, $2^{k-1} \cdot \mathrm{SUM}(5K) \not\equiv 0 \pmod{2^k}$. Hence, $D^{k-1+5K}(A) \not\equiv D^{k-1}(A) \pmod{2^k}$. On the other hand,

$$\begin{aligned}D^{k+5K}(A) &= D^k(D^{5k}(A)) \\ &\equiv D^k(\mathrm{SUM}(5K) \cdot (1, 1, 1, 1, 1) + H^{5K/2}(A)) \pmod{2^k} \\ &\equiv 2^k \cdot \mathrm{SUM}(5K) \cdot (1, 1, 1, 1, 1) + D^k(A) \pmod{2^k} \\ &\equiv D^k(A) \pmod{2^k}.\end{aligned}$$

Thus $\mathfrak{s}(2^k) = k$ and $\mathfrak{l}(2^k) = 15 \cdot 2^{k-1}$. □

REFERENCES

1. C. Ciamberlini & A. Marengoni. "Su una interessante curiosità numerica." *Periodiche di Matematiche* **17** (1937):25-30.
2. A. Ehrlich. "On the Periods of the Fibonacci Sequence Modulo *M*." *The Fibonacci Quarterly* **27.1** (1989):11-13.
3. A. Ehrlich. "Periods in Ducci's *N*-Number Game of Differences." *The Fibonacci Quarterly* **28.4** (1990):302-05.
4. A. Engel. *Mathematisches Experimentieren mit dem Computer.* Sutttgart, 1991.
5. H. Glaser & G. Schöffl. "Ducci-Sequences and Pascal's Triangle." *The Fibonacci Quarterly* **33.4** (1995):313-24.
6. A. Ludington-Young. "Length of the *n*-Number Game." *The Fibonacci Quarterly* **28.3** (1990):259-65.
7. A. Ludington-Young. "Length of the 7-Number Game." *The Fibonacci Quarterly* **26.3** (1988):195-204.
8. L. Meyers. "Ducci's Four-Number Problem: A Short Bibliography." *Crux Mathematicorum* **8** (1982):262-66.
9. G. Schöffl. "Ducci Processes of 4-Tuples." *The Fibonacci Quarterly* (to appear).
10. J. Vinson. "The Relation of the Period Modulo to the Rank of Apparition of *m* in the Fibonacci Sequence." *The Fibonacci Quarterly* **1.1** (1963):37-46.
11. D. D. Wall. "Fibonacci Series Modulo *m*." *Amer. Math. Monthly* **67** (1960):525-32.
12. F. B. Wong. "Ducci Processes." *The Fibonacci Quarterly* **20.2** (1982):97-105.

AMS Classification Number: 11B65

❖❖❖

CORRIGENDUM TO THE PAPER "ON MULTIPLICITY SEQUENCES"

***The Fibonacci Quarterly*, Vol. 35, no. 1, pp. 9-10**

Piotr Zarzycki
Department of Mathematics, University of Gdańsk

It was pointed out by Professor Harvey L. Abbott that the statement in the Theorem from the paper is not true. The counterexample given by Professor Abbot is as follows:

If $g(1) = 1$ *and* $g(n) = 2n$ *for* $n > 1$, *then* $L.C.M.(g(m), g(n)) = g(L.C.M.(m, n))$ *for any* m, n *and* $G.C.D.(g(m), g(n)) \neq g(G.C.D.(m, n))$ *for some* m, n.

The Theorem is true in a weaker form:

If g *is a multiplicity sequence and* g *is also quasi-multiplicative which means that* $g(m)g(n) = cg(mn)$ *for any relatively prime* m, n, *then* g *is a strong divisibility sequence.*