PALINDROMES

Clifford S. Queen
Department of Mathematics, Lehigh University, Bethlehem PA 18015
(Submitted August 1991)

INTRODUCTION

A *palindrome* is a finite sequence of positive integers which is unchanged when written in reverse order. Sometimes such sequences are referred to as *symmetric* (see [3] and [5]). The objective of this paper is to show how some simple properties of palindromes can be used to obtain results in elementary number theory. We give new elementary proofs of known results and what appear to be some new results.

In §1 we prove some elementary properties of palindromes and their associated finite continued fractions. In §2 we apply the properties established in §1. The reader will note that the application of Proposition 4 of §1 constitutes a method for obtaining the results of §2.

1. ELEMENTARY PROPERTIES OF PALINDROMES

Let n be a nonnegative integer. We call a sequence of positive integers $\alpha = \{\alpha(0), \alpha(1), \cdots, \alpha(n)\}$ of length $n+1$ a palindrome if $\alpha(i) = \alpha(n-i)$ for $0 \le i \le n$.

Example: Let n be a nonnegative integer and define the sequence α by

$$\alpha(i) = \binom{n}{i} = \frac{n!}{(n-i)!i!},$$

for $0 \le i \le n$. The condition for α to be a palindrome is the well-known binomial coefficient identity $\binom{n}{i} = \binom{n}{n-i}$.

We are especially interested in sequences of positive integers generated by the division algorithm (see [1]). Explicitly, if P and Q are relatively prime integers such that $1 < Q < P$. Then (see [1], p.325) P and Q uniquely determine two sequences of positive integers α and r as follows:

$$\begin{aligned}
P &= \alpha(0)Q + r(0), && 0 < r(0) < Q;\\
Q &= \alpha(1)r(0) + r(1), && 0 < r(1) < r(0);\\
&\vdots\\
r(i-2) &= \alpha(i)r(i-1) + r(i), && 0 < r(i) < r(i-1);\\
&\vdots\\
r(n-3) &= \alpha(n-1)r(n-2) + r(n-1), && 1 = r(n-1) < r(n-2);\\
r(n-2) &= \alpha(n)r(n-1) = \alpha(n).
\end{aligned} \tag{1}$$

Since $\alpha(n) = r(n-2) > 1$, we have $\alpha(n) \ge 2$. We call α the sequence of quotients and r the sequence of remainders determined by the pair (P, Q). For any integer c we define

$$A_c = \begin{pmatrix} c & 1 \\ 1 & 0 \end{pmatrix}.$$

The equations in (1) are equivalent to

$$A_{\alpha(i)}\begin{pmatrix} r(i-1) \\ r(i) \end{pmatrix} = \begin{pmatrix} r(i-2) \\ r(i-1) \end{pmatrix}, \text{ for } 0 \le i \le n,$$

where $r(-2) = P, r(-1) = Q$, and $r(n) = 0$. Hence

$$A_{\alpha(0)}A_{\alpha(1)} \cdots A_{\alpha(n)}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} P \\ Q \end{pmatrix}. \tag{2}$$

Let α be any sequence of positive integers of length $n+1$. If we define

$$\begin{pmatrix} P_i & Q_i \\ P_{i-1} & Q_{i-1} \end{pmatrix} = A_{\alpha(i)}A_{\alpha(i-1)} \cdots A_{\alpha(0)}, \tag{3}$$

then it is known (see [6]) that

$$P_i / Q_i = [\alpha(0), \alpha(1), \ldots, \alpha(n)] = \alpha(0) + \cfrac{1}{\alpha(1) + \cfrac{1}{\alpha(2) + \ddots \cfrac{1}{\alpha(i-1) + \cfrac{1}{\alpha(i)}}}} \tag{4}$$

a finite simple continued fraction. The elementary properties of continued fractions that we need can be found in [1]. In what follows we denote the greatest integer function by $[\![\ ]\!]$.

Lemma 1: Let $\alpha = \{\alpha(0), \alpha(1), \ldots, \alpha(n)\}$ be a sequence of positive integers of length $n+1 > 2$. If

$$A_{\alpha(n)}A_{\alpha(n-1)} \cdots A_{\alpha(0)} = \begin{pmatrix} P_n & Q_n \\ P_{n-1} & Q_{n-1} \end{pmatrix},$$

then P_n / Q_n is not an integer and $[\![P_n / Q_n]\!] = \alpha(0)$

Proof: Using (3) and (4), we have $P_n / Q_n = \alpha(0) + 1/[\alpha(1), \alpha(2), \ldots, \alpha(n)]$. So we need only show that $[\alpha(1), \alpha(2), \ldots, \alpha(n)] > 1$ to obtain the result. To that end, we note that because $n+1 > 2$, $[\alpha(1), \alpha(2), \ldots, \alpha(n)] \ge \alpha(2) \ge 1$. Thus,

$$[\alpha(1), \alpha(2), \ldots, \alpha(n)] = \alpha(1) + 1/[\alpha(2), \alpha(3), \ldots, \alpha(n)] > \alpha(1).$$

Now, since $\alpha(1) \ge 1$, the conclusion follows. □

The following Lemma, accounting for a difference in notation, can be found as an exercise in [6, p. 251]. Since we use it in an essential way, we provide a proof for the sake of completeness.

Lemma 2: If α and β are two sequences of positive integers of lengths $n+1$ and $m+1$, respectively, then

$$A_{\alpha(n)}A_{\alpha(n-1)} \cdots A_{\alpha(0)} = A_{\beta(m)}A_{\beta(m-1)} \cdots A_{\beta(0)} \tag{5}$$

if and only if $n = m$ and $\alpha = \beta$.

Proof: We will proceed by induction on the length of the sequence α. If $n+1 = 1$, then $n = 0$ and

$$\begin{pmatrix} \alpha(0) & 1 \\ 1 & 0 \end{pmatrix} = A_{\beta(m)} A_{\beta(m-1)} \cdots A_{\beta(0)} = \begin{pmatrix} P_m & Q_m \\ P_{m-1} & Q_{m-1} \end{pmatrix}.$$

Thus, $\alpha(0) = P_m / Q_m$ is an integer. So, by Lemma 1, $m \le 1$. Now $\det\left(\begin{pmatrix} c & 1 \\ 1 & 0 \end{pmatrix}\right) = -1$, for any integer c, where det( ) is the determinant. So, if $m = 1$, we would have $-1 = \det(A_{\alpha(0)}) = \det(A_{\beta(1)} A_{\beta(0)}) = 1$. Thus, $m = 0$ and $\alpha(0) = \beta(0)$

Now assume our result is true when the length of α is less than $n+1$, with $n \ge 1$. We first note that $m \ge 1$. Because, if $m = 0$, we argue as above, with the roles of α and β interchanged, and conclude that $n = 0$. Multiplying both sides of (5) on the left by A_1, we have

$$A_1 A_{\alpha(n)} \cdots A_{\alpha(0)} = A_1 A_{\beta(m)} \cdots A_{\beta(0)} = \begin{pmatrix} P_{m+1} & Q_{m+1} \\ P_m & Q_m \end{pmatrix}.$$

Because $\{\alpha(0), \alpha(1), \ldots, \alpha(n), 1\}$ and $\{\beta(0), \beta(1), \ldots, \beta(m), 1\}$ both have length bigger than 2, we have by Lemma 1 that $\alpha(0) = [\![P_{m+2} / Q_{m+2}]\!] = \beta(0)$. Finally, multiplying both sides of (5) on the right by the inverse of $A_{\alpha(0)}$, we have

$$A_{\alpha(n)} A_{\alpha(n-1)} \cdots A_{\alpha(1)} = A_{\beta(m)} A_{\beta(m-1)} \cdots A_{\beta(1)}.$$

Hence, by the induction hypothesis, $\{\alpha(1), \alpha(2), \ldots, \alpha(n)\} = \{\beta(1), \beta(2), \ldots, \beta(m)\}$ and, thus, $n = m$ and $\alpha = \beta$. □

Proposition 1: If α is a sequence of positive integers of length $n+1$, then α is a palindrome if and only if the matrix

$$A_{\alpha(n)} A_{\alpha(n-1)} \cdots A_{\alpha(0)} \tag{6}$$

is symmetric.

Proof: Since each $A_{\alpha(i)}$ is symmetric, the transpose of (6) is

$$A_{\alpha(0)} A_{\alpha(1)} \cdots A_{\alpha(n)}.$$

So by Lemma 2 the result follows. □

Proposition 2: If α is a palindrome of length $n+1$ and

$$A_{\alpha(n)} A_{\alpha(n-1)} \cdots A_{\alpha(0)} = \begin{pmatrix} P_n & Q_n \\ P_{n-1} & Q_{n-1} \end{pmatrix}. \tag{7}$$

Then

$$Q_n^2 \equiv (-1)^n \pmod{P_n}.$$

Proof: By Proposition 1, $P_{n-1} = Q_n$. Since the determinant of $A_{\alpha(i)}$ is -1 for all i, we have, by taking determinants in (7), $(-1)^{n+1} = P_n Q_{n-1} - Q_n^2$ and, thus, $Q_n^2 = (-1)^n + P_n Q_{n-1}$. □

Now we give an elementary proof of an easy extension of a result which can be found in [3].

Proposition 3: Let P and Q be integers such that $1 < Q < P$ and $Q^2 \equiv \pm 1 \pmod{P}$. Then there exists a palindrome α of length $n+1$ with

$$A_{\alpha(n)} A_{\alpha(n-1)} \cdots A_{\alpha(0)} = \begin{pmatrix} P & Q \\ Q & Q_{n-1} \end{pmatrix}$$

where $Q^2 \equiv (-1)^n \pmod{P}$. Further, α is uniquely determined by P and Q.

Proof: Let α be the sequence of quotients in the division algorithm determined by the pair (P, Q). Set

$$A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(0)} = \begin{pmatrix} P_n & Q_n \\ P_{n-1} & Q_{n-1} \end{pmatrix}. \tag{8}$$

Taking the transpose in (2) we have $\begin{pmatrix} 1 & 0 \end{pmatrix} A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(0)} = \begin{pmatrix} P & Q \end{pmatrix}$. Thus, $P_n = P$ and $Q_n = Q$.

Taking determinants in (8), we have $(-1)^{n+1} = P_nQ_{n-1} - Q^2$ and, thus, $P_{n-1}Q = (-1)^n + PQ_{n-1}$. Further, because $Q^2 \equiv \pm 1 \pmod{P}$, we have

$$P_{n-1} \equiv -(\pm 1)(-1)^n Q \pmod{P}. \tag{9}$$

Next, because

$$A_{\alpha(0)}A_{\alpha(1)}\cdots A_{\alpha(n)} = \begin{pmatrix} P & P_{n-1} \\ Q & Q_{n-1} \end{pmatrix},$$

we have $P/P_{n-1} = [\alpha(n), \alpha(n-1), \ldots, \alpha(0)] \geq \alpha(n)$. We know, from (1), that $\alpha(n) \geq 2$ and, thus, $P_{n-1} \leq P/2$. Now, if $Q < P/2$, then (9) implies that $Q = P_{n-1}$. So, by Proposition 1, α is a palindrome.

Suppose $P/2 < Q < P$. Then $1 < P/Q < 2$ and $\alpha(0) = [\![P/Q]\!] = 1$. Next, if we multiply both sides of (8) on the left by

$$A_1A_{\alpha(n)-1}A_{\alpha(n)}^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$$

we have

$$A_1A_{\alpha(n)-1}A_{\alpha(n-1)}\cdots A_{\alpha(0)} = \begin{pmatrix} P & Q \\ P - P_{n-1} & Q - Q_{n-1} \end{pmatrix}.$$

Taking the determinant, we have $P(Q - Q_{n-1}) - (P - P_{n-1})Q = (-1)^n$ and, so,

$$(P - Q)P_{n-1} - P(P_{n-1} - q_{n-1}) = (-1)^{n+1}.$$

Hence, $(P - Q)P_{n-1} \equiv (-1)^{n+1} \pmod{P}$. Because $P - Q \equiv -Q \pmod{P}$, we have $(P - Q)^2 \equiv \pm 1 \pmod{P}$ and, thus,

$$P_{n-1} \equiv -(\pm 1)(-1)^{n+1}(P - Q) \pmod{P}. \tag{10}$$

Since $P - Q < P/2$ and $P_{n-1} < P/2$, (10) implies that $P - Q = P_{n-1}$. That is, $Q = P - P_{n-1}$ and, so, by Proposition 1, $\{\alpha(0), \alpha(1), \ldots, \alpha(n-1), \alpha(n) - 1, 1\}$ is a palindrome.

Now we prove uniqueness. Let α be the palindrome constructed above and β another of length $m+1$ with

$$A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(0)} = \begin{pmatrix} P & Q \\ Q & Q_{n-1} \end{pmatrix} \text{ and } A_{\beta(m)}A_{\beta(m-1)}\cdots A_{\beta(0)} = \begin{pmatrix} P & Q \\ Q & R \end{pmatrix}.$$

Taking determinants, we have $PQ_{n-1} - Q^2 = (-1)^{n+1}$ and $PR - Q^2 = (-1)^{m+1}$. Thus, $Q^2 \equiv (-1)^n \pmod{P}$ where, because $P > 2$, we must have $(-1)^n = (-1)^m$. Hence, $P(Q_{n-1} - R) = 0$ and, thus, $R = Q_{n-1}$. Finally, by Lemma 2, $\alpha = \beta$. □

Corollary 1: Let P and Q be integers such that $1<Q<P$ and $Q^2 \equiv \pm 1 \pmod{P}$. If α is the sequence of quotients in the division algorithm determined by the pair (P, Q), then α or $\{\alpha(0), \alpha(1), \ldots, \alpha(n-1), \alpha(n)-1, 1\}$ is a palindrome.

Proof: It follows from (1) that $\alpha(n) \geq 2$. Further, the palindrome referred to in Propositioin 3 was shown to be either α or $\{\alpha(0), \alpha(1), \ldots, \alpha(n-1), \alpha(n)-1, 1\}$. □

Proposition 4: Let α be a sequence of positive integers of length $n+1$ and n a nonnegative integer such that

$$A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(0)} = \begin{pmatrix} P & Q \\ P_{n-1} & Q_{n-1} \end{pmatrix}, \tag{11}$$

where $Q^2 \equiv \pm 1 \pmod{P}$ and $1 \leq Q < P$, with $P > 2$. Then we have exactly one of the following possibilities:

(a) α is a palindrome and $Q^2 \equiv (-1)^n \pmod{P}$.

(b) $\alpha(n) = 1$, $\{\alpha(0), \alpha(1), \ldots, \alpha(n-2), \alpha(n-1)+1\}$ is a palindrome, and $Q^2 \equiv (-1)^{n+1} \pmod{P}$.

(c) $\alpha(n) > 1$, $\{\alpha(0), \alpha(1), \ldots, \alpha(n-1), \alpha(n)-1, 1\}$ is a palindrome, and $Q^2 \equiv (-1)^{n+1} \pmod{P}$.

Proof: If $\alpha(n) > 1$, then α is clearly the sequence of quotients in the division algorithm for the pair (P, Q). Hence, by Corollary 1, either α or $\{\alpha(0), \alpha(1), \ldots, \alpha(n-1), \alpha(n)-1, 1\}$ is a palindrome. Now, if α is a palindrome, then by Proposition 2, $Q^2 \equiv (-1)^n \pmod{P}$. Next, if $\{\alpha(0), \alpha(1), \ldots, \alpha(n-1), \alpha(n)-1, 1\}$ is a palindrome, then multiplying both sides of (11) by

$$A_1 A_{\alpha(n)-1} - 1A_{\alpha(n)}^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix},$$

we have

$$A_1 A_{\alpha(n)-1} A_{\alpha(n-1)} \cdots A_{\alpha(0)} = \begin{pmatrix} P & Q \\ P - P_{n-1} & Q - Q_{n-1} \end{pmatrix}.$$

So, by Propositions 1 and 2, $P - P_{n-1} = Q$ and $Q^2 \equiv (-1)^{n+1} \pmod{P}$.

If $\alpha(n) = 1$, then multiplying both sides of (11) on the left by

$$A_{\alpha(n-1)+1}A_{\alpha(n-1)}^{-1}A_1^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$$

we have

$$A_{\alpha(n-1)+1}A_{\alpha(n-2)} \cdots A_{\alpha(0)} = \begin{pmatrix} P & Q \\ P - P_{n-1} & Q - Q_{n-1} \end{pmatrix}. \tag{12}$$

So, again, $\{\alpha(0), \alpha(1), \ldots, \alpha(n-2), \alpha(n-1)+1\}$ is the sequence of quotients in the division algorithm for the pair (P, Q). Hence, by Corollary 1, $\{\alpha(0), \alpha(1), \ldots, \alpha(n-2), \alpha(n-1)+1\}$ or α is a palindrome. If $n = 1$, we understand $\{\alpha(0), \alpha(1), \ldots, \alpha(n-2), \alpha(n-1)+1\}$ to be $\{\alpha(0)+1\}$. Now, if $\{\alpha(0), \alpha(1), \ldots, \alpha(n-2), \alpha(n-1)+1\}$ is a palindrome, then (12) and Proposition 2 give $Q^2 \equiv (-1)^{n+1} \pmod{P}$.

Next, we show that two of these possibilities cannot hold at the same time. Clearly (b) and (c) cannot both be true. If (a) and (b) or (a) and (c) hold, then $Q^2 \equiv (-1)^n \pmod{P}$ and $Q^2 \equiv (-1)^{n+1} \pmod{P}$. That is $1 \equiv -1 \pmod{P}$, which is impossible since $P > 2$. □

If α is a sequence of positive integers of length $n+1$, we obtain a sequence α_* of length n by deleting $\alpha(0)$. Specifically, $\alpha_*(i) = \alpha(i+1)$ for $0 \le i \le n-1$. That is, $\alpha_* = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$. Further, if $\alpha(n) > 1$, we form a sequence α^* of length $n+1$ by deleting $\alpha(0)$ and replacing $\alpha(n)$ by $\{\alpha(n)-1, 1\}$. That is, $\alpha^* = \{\alpha(1), \ldots, \alpha(n-1), \alpha(n)-1, 1\}$, where $\alpha^*(i) = \alpha(i+1)$ for $0 \le i \le n-2$, $\alpha^*(n-1) = \alpha(n)-1$ and $\alpha^*(n) = 1$.

Proposition 5: If α and α_* are both palindromes, then $\alpha(i) = \alpha(0)$ for $0 \le i \le n$.

Proof: If $0 \le i \le n-1$, then $\alpha(i+1) = \alpha_*(i) = \alpha_*(n-1-i) = \alpha(i)$. □

Proposition 6: If $\alpha(n) > 1$ and both α and α^* are palindromes, then we have two possibilities:

(a) If n is odd, then $\alpha(0) = \alpha(n) = 2$ and $\alpha(i) = 1$ for $1 \le i \le n-1$.

(b) If n is even, then $\alpha(0) = \alpha(n) = c > 1$. Further, $\alpha(2k-1) = 1$ for $1 \le k \le n/2$ and $\alpha(2k) = c-1$ for $1 \le k < n/2$.

Proof: If $0 < i < n-2$, then $\alpha^*(i-1) = \alpha(i) = \alpha(n-i) = \alpha^*(n-i-1) = \alpha^*(i+1) = \alpha(i+2)$. Hence, $1 = \alpha^*(n) = \alpha^*(0) = \alpha(1) = \alpha(2k-1)$ for $1 \le k \le [\![n/2]\!]$. Further, $\alpha(2) = \alpha(2k)$ for $1 \le k \le [\![n/2]\!]$, where $\alpha(2) = \alpha^*(1) = \alpha^*(n-1) = \alpha(n)-1 = \alpha(0)-1$.

So, if n is even, we have proved (b). If n is odd, then $\alpha((n-1)/2) = \alpha(n-(n-1)/2) = \alpha((n+1)/2)$. Since one of $(n-1)/2$ and $(n+1)/2$ is even and the other odd, we must have $\alpha(i) = 1$ for $1 \le i < n-1$. Further, since $1 = \alpha(2) = \alpha(0)-1$, we also have $\alpha(0) = \alpha(n) = 2$. □

2. APPLICATIONS

In what follows, we sill prove four propositions. Propositions 7 and 10 are known results and we give new elementary proofs. Propositions 8 and 9 are of the same general type as Proposition 7 and are apparently new.

We define a sequence of polynomials as follows: $J_1(X) = 0, J_0(X) = 1$ and $J_{k+1}(X) = XJ_k(X) + J_{k-1}(X)$ for $k \ge 0$ or, equivalently, for $k \ge 1$,

$$\begin{pmatrix} J_k(X) & J_{k-1}(X) \\ J_{k-1}(X) & J_{k-2}(X) \end{pmatrix} = \begin{pmatrix} X & 1 \\ 1 & 0 \end{pmatrix}^k. \tag{13}$$

Remark 2: It is easy to see that $\{F_k = J_{k-1}(1) \mid k \ge 0\}$ is the sequence of Fibonacci numbers.

The following is an elementary proof of a result of Owings (see [2]).

Proposition 7: If P and Q are integers with $1 \le Q < P$, $Q^2 \equiv -1 \pmod{P}$ and $P^2 \equiv -1 \pmod{Q}$, then there exists an odd integer k such that

$$Q = F_k \quad \text{and} \quad P = F_{k+2},$$

where F_k is the k^{th} Fibonacci number.

Proof: If $Q = 1$, then $Q^2 \equiv -1 \pmod{P}$ and $P > Q$ implies that $P = 2$. Hence, $Q = F_1$ and $P = F_3$. Next, if $Q = 2$, then $Q^2 \equiv -1 \pmod{P}$ implies that $P = 5$. So $Q = F_3$ and $P = F_5$.

From now on, we will assume that $Q > 2$. By Proposition 3 there is a palindrome α of even length $n+1$ such that

$$A_{\alpha(n)}A_{\alpha(n-1)} \cdots A_{\alpha(0)} = \begin{pmatrix} P & Q \\ Q & Q_{n-1} \end{pmatrix}$$

and $Q^2 \equiv (-1)^n \pmod{P}$. We will prove that α^* is a palindrome. To that end, we note that

$$A_{\alpha(n)}A_{\alpha(n-1)} \cdots A_{\alpha(1)} = \begin{pmatrix} Q & P - \alpha(0)Q \\ Q_{n-1} & Q - \alpha(0)Q_{n-1} \end{pmatrix}.$$

Since $P - \alpha(0)Q \equiv P \pmod{Q}$ and $P^2 \equiv -1 \pmod{Q}$, we have that $(P - \alpha(0)Q)^2 \equiv -1 \pmod{Q}$. Now, because $Q > 2$, we have by Proposition 4 exactly one of the following possibilities:

(a) $\{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ is a palindrome with $(P - \alpha(0)Q)^2 \equiv (-1)^{n-1} \pmod{Q}$;

(b) $\alpha(n) = 1$ and $\{\alpha(1), \ldots, \alpha(n-2), \alpha(n-1)+1\}$ is a palindrome with $(P - \alpha(0)Q)^2 \equiv (-1)^n \pmod{Q}$;

(c) $\alpha(n) > 1$ and $\alpha^* = \{\alpha(1), \ldots, \alpha(n-1), \alpha(n)-1, 1\}$ is a palindrome with $(P - \alpha(0)Q)^2 \equiv (-1)^n \pmod{Q}$.

The case (a) cannot hold since $n-1$ is even, and the two congruences, $P - \alpha(0)Q \equiv P \pmod{Q}$ and $P^2 \equiv -1 \pmod{Q}$, imply that $1 \equiv -1 \pmod{Q}$. Contradicting that $Q > 2$. Now, suppose $\alpha(n) = 1$ and $\{\alpha(1), \ldots, \alpha(n-2), \alpha(n-1)+1\}$ is a palindrome. Since n is odd, it follows that $n > 2$ and, thus, $\alpha(n-1) = \alpha(1) = \alpha(n-1)+1$ yields a contradiction. Hence, we have shown that $\alpha(n) > 1$ and $\alpha^* = \{\alpha(1), \ldots, \alpha(n-1), \alpha(n)-1, 1\}$ is a palindrome.

Because α and α^* are both palindromes and n is odd, we have, by Proposition 5, that $\alpha(0) = \alpha(n) = 2$ and $\alpha(i) = 1$ for $1 \le i \le n-1$. Hence,

$$A_{\alpha(n)}A_{\alpha(n-1)} \cdots A_{\alpha(1)} = A_2 A_1^{n-1} A_2.$$

But, from (13) we have

$$A_1^{n-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} = \begin{pmatrix} J_{n-1}(1) & J_{n-2}(1) \\ J_{n-2}(1) & J_{n-3}(1) \end{pmatrix}.$$

Hence,

$$A_2 A_1^{n-1} A_2 = A_2 \begin{pmatrix} J_{n-1}(1) & J_{n-2}(1) \\ J_{n-2}(1) & J_{n-3}(1) \end{pmatrix} A_2 = \begin{pmatrix} J_{n+3}(1) & J_{n+1}(1) \\ J_{n+1}(1) & J_{n-1}(1) \end{pmatrix}.$$

We have already observed that $F_{i+1} = J_i(1)$ for $i \ge 0$. Thus, the result is established. □

Proposition 8: If P and Q are integers with $1 \le Q < P$, $P^2 \equiv \pm 1 \pmod{Q}$ and $Q^2 \equiv -(\pm 1) \pmod{P}$, then there exist integers $k \ge 0$ and $c \ge 1$ such that $J_k(c) = Q$ and $J_{k+1}(c) = P$.

Proof: If $Q = 1$ then, for any $P > 1$, we have $J_0(P) = Q$ and $J_1(P) = P$. Next, if $Q = 2$, then $Q^2 \equiv -(\pm 1) \pmod{P}$ implies that $P = 3$ or $P = 5$. If $P = 3$, we have $J_2(1) = 2$ and $J_3(1) = 3$. For the case $P = 5$, we have $J_1(2) = 2$ and $J_2(2) = 5$.

From now on, we will assume that $Q > 2$. By Proposition 3, there is a palindrome α of length $n+1$ such that

$$A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(0)} = \begin{pmatrix} P & Q \\ Q & Q_{n-1} \end{pmatrix}$$

where $Q^2 \equiv (-1)^n \pmod{P}$. We will show that α^* is a palindrome. To that end, we note that

$$A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(1)} = \begin{pmatrix} Q & P-\alpha(0)Q \\ Q_{n-1} & Q-\alpha(0)Q_{n-1} \end{pmatrix}.$$

Now, since $P - \alpha(0)Q \equiv P \pmod{Q}$, it follows that $(P-\alpha(0)Q)^2 \equiv -(-1)^n \pmod{Q}$. Therefore, because $Q > 2$, we have, by Proposition 4, exactly one of the following possibilities:

(a) $\alpha_* = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ is a palindrome with $(P-\alpha(0)Q)^2 \equiv (-1)^{n-1} \pmod{Q}$;

(b) $\alpha(n) = 1$ and $\{\alpha(1), \ldots, \alpha(n-2), \alpha(n-1)+1\}$ is a palindrome with $(P-\alpha(0)Q)^2 \equiv (-1)^n \pmod{Q}$;

(c) $\alpha(n) > 1$ and $\{\alpha(1), \ldots, \alpha(n-1), \alpha(n)-1, 1\}$ is a palindrome with $(P-\alpha(0)Q)^2 \equiv (-1)^n \pmod{Q}$.

If either (b) or (c) holds, it follows, by Proposition 3, that $(P-\alpha(0)Q)^2 \equiv (-1)^n \pmod{Q}$. Since $P - a(0)Q \equiv P \pmod{Q}$ and $P^2 \equiv -(-1)^n \pmod{Q}$, we have $(-1)^n \equiv -(-1)^n \pmod{Q}$, but $Q > 2$ makes this impossible. So α_* is indeed a palindrome.

By Proposition 5, $\alpha(i) = \alpha(0) = c$ for $0 \le i \le n$. That is, $\alpha = \{c, c, \ldots, c\}$. Thus,

$$A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(0)} = \begin{pmatrix} c & 1 \\ 1 & 0 \end{pmatrix}^{n+1} = \begin{pmatrix} J_{n+1}(c) & J_n(c) \\ J_n(c) & J_{n-1}(c) \end{pmatrix},$$

and hence our result. □

We need another sequence of polynomials as follows: $H_{-1}(X) = 0$, $H_0(X) = 1$ and, for $k \ge 0$, $H_{k+1}(X) = (X+1)H_k(X) - H_{k-1}(X)$. Equivalently, for $k \ge 1$,

$$\begin{pmatrix} X+1 & -1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} H_k(X) & -H_{k-1}(X) \\ H_{k-1}(X) & -H_{k-2}(X) \end{pmatrix}.$$

Proposition 9: Suppose P and Q are integers with $1 < Q < P$, $Q^2 \equiv 1 \pmod{P}$, $P^2 \equiv 1 \pmod{Q}$, and $P \ne Q+1$. Then there exist integers k and c such that $H_k(c) = Q$ and $H_{k+1}(c) = P$.

Proof: By Proposition 3, there exists a Palindrome α of odd length $n+1$ such that

$$A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(0)} = \begin{pmatrix} P & Q \\ Q & Q_{n-1} \end{pmatrix}.$$

We will prove first that α^* is also a palindrome. To that end, we observe that

$$A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(1)} = \begin{pmatrix} Q & P-\alpha(0)Q \\ Q_{n-1} & Q-\alpha(0)Q_{n-1} \end{pmatrix}.$$

Now $Q>2$ since, otherwise, $Q^2 \equiv 1 \pmod{P}$ implies that $P=3$. That is, $P=Q+1$, a case we have excluded. Next, $P-\alpha(0)Q \equiv P \pmod{Q}$ gives $(P-\alpha(0)Q)^2 \equiv 1 \pmod{Q}$. Now, since $Q>2$ and $(P-\alpha(0)Q)^2 \equiv 1 \pmod{Q}$ we have, by Proposition 4, exactly one of the following possibilities:

(a) $\{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ is a palindrome and $(P-\alpha(0)Q)^2 \equiv (-1)^{n-1} \pmod{Q}$;

(b) $\alpha(n)=1, \{\alpha(1), \ldots, \alpha(n-2), \alpha(n-1)+1\}$ is a palindrome and $(P-\alpha(0)Q)^2 \equiv (-1)^n \pmod{Q}$;

(c) $\alpha(n)>1, \alpha^* = \{\alpha(1), \ldots, \alpha(n-1), \alpha(n)-1, 1\}$ is a palindrome and $(P-\alpha(0)Q)^2 \equiv (-1)^n \pmod{Q}$.

If (a) were true, we would have $(P-\alpha(0)Q)^2 \equiv -1 \pmod{Q}$, since $n-1$ is odd. However, $(P-\alpha(0)Q) \equiv P \pmod{Q}$ and $P^2 \equiv 1 \pmod{Q}$ give $1 \equiv -1 \pmod{Q}$, contradicting the conclusion that $Q>2$.

Next, if (b) is true and $n>2$, with α and $\{\alpha(1), \ldots, \alpha(n-2), \alpha(n-1)+1\}$ both palindromes, implies that $\alpha(n-1)=\alpha(1)=\alpha(n-1)+1$, which is clearly impossible. So, if (b) is true, we have $n=2$ and, thus, $\alpha=\{1, \alpha(1), 1\}$. However, in this case, $Q=\alpha(1)+1$ and $P=\alpha(1)+2$, a case we have excluded. Hence, $\alpha(n)>1$ and α^* is a palindrome.

Since α and α^* are both palindromes and n is even, we have, by Proposition 6, that $\alpha(0)=\alpha(n)=c>1, 1=\alpha(1)=\alpha(2k-1)$ for $1 \le k \le n/2$ and $\alpha(2k)=c-1$ for $1 \le k < n/2$. If $n=2$, then

$$A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(0)} = A_cA_1A_c = \begin{pmatrix} c+1 & -1 \\ 1 & 0 \end{pmatrix}^2 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

An easy induction on n gives, in general, that

$$A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(0)} = \begin{pmatrix} c+1 & -1 \\ 1 & 0 \end{pmatrix}^{(n+2)/2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Now, recalling that $\begin{pmatrix} X+1 & -1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} H_k(X) & -H_{k-1}(X) \\ H_{k-1}(X) & -H_{k-2}(X) \end{pmatrix}$ we have

$$A_{\alpha(n)}A_{\alpha(n-1)}\cdots A_{\alpha(0)} = \begin{pmatrix} H_{n/2+1}(X) & -H_{n/2}(X) \\ H_{n/2}(X) & -H_{n/2-1}(X) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} H_{n/2+1}(c) & H_{n/2}(c) \\ H_{n/2}(c) & H_{n/2-1}(c) \end{pmatrix}$$

and thus our result. □

Remark 3: In the above result $c=[\![P/Q]\!]$. Furthermore, by Leme's Theorem (see [4]), $n<5\log_{10}(Q)$, and so $k=n/2<(5/2)\log_{10}(Q)<(5/2)\log_{10}(P/2)$.

If D is a nonsquare, positive integer, then it is known (see [1]) that $\theta = \lfloor\sqrt{D}\rfloor + \sqrt{D}$ has an infinite purely periodic continued fraction expansion. Let p be the smallest period of θ. Our notation is $\theta = [\overline{a_0, a_1, \ldots, a_{p-1}}]$. We now give an elementary proof of a known result (see [5]).

Proposition 10: We claim that $\{a_1, a_2, \ldots, a_{p-1}\}$ is a palindrome.

Proof: Set $\alpha = \{\alpha(0), \alpha(1), \ldots, \alpha(p)\}$, where $\alpha(i) = a_1$ for $0 \le i \le p-1$ and $\alpha(p) = a_0$. Setting

$$A_{\alpha(p-1)}A_{\alpha(p-2)}\cdots A_{\alpha(0)} = \begin{pmatrix} P_{p-1} & Q_{p-1} \\ P_{p-2} & Q_{p-2} \end{pmatrix}$$

we have (see [1], p. 329)

$$\theta = [\alpha(0), \alpha(1), \ldots, \alpha(p-1), \theta] = \frac{\theta P_{p-1} + P_{p-2}}{\theta Q_{p-1} + Q_{p-2}}.$$

Thus, θ is a root of the quadratic polynomial equation

$$f(X) = Q_{p-1}X^2 + (Q_{p-2} - P_{p-1})X - P_{p-2} = 0.$$

However, the minimal polynomial of θ over the rational numbers is

$$m(X) = X^2 - \alpha(0)X + (\alpha(0)^2 - 4D)^2 - 4D)/4.$$

Because $m(X)$ divides the polynomial $f(X)$, we have $Q_{p-2} - P_{p-1} = -\alpha(0)Q_{p-1}$. That is,

$$P_{p-1} = \alpha(0)q_{p-1} + Q_{p-2} = Q_p,$$

where

$$A_{\alpha(p)}A_{\alpha(p-1)}\cdots A_{\alpha(0)} = \begin{pmatrix} P_p & Q_p \\ P_{p-1} & Q_{p-1} \end{pmatrix}.$$

So, by Proposition 1, $\alpha = \{a_0, a_1, \ldots, a_{p-1}, a_0\}$ is a palindrome. Thus, it follows that $\{a_1, \ldots, a_{p-1}\}$ is a palindrome. □

Remark 4: If P is a positive integer such that $P > 1$ and P is a product of primes congruent to 1 modulo 4 or twice such a product, then there exists an integer Q with $1 \le Q \le P/2$ and $Q^2 \equiv -1 \pmod{P}$. By Proposition 3, there is a palindrome $\alpha_Q = \{\alpha(0), \alpha(1), \ldots, \alpha(n)\}$ of even length $L_Q = n+1$ such that $P/Q = [\alpha(0), \alpha(1), \ldots, \alpha(n)]$. We define the index of P by

$$I(P) = \min\{L_Q | Q\}.$$

It is clear that for any integer of our type, $I(P) = 2$ if and only if there is a positive integer m such that $P = m^2 + 1$. The following seem to be natural questions:

(1) Are there infinitely many integers P of index i, for i an even integer bigger than 4?

(2) Let M be a positive integer such that $M \ge 2$. Are there infinitely many primes P, with $P \equiv 1 \pmod{4}$ and $I(P) \le M$?

In (1) we have restricted ourselves to $I(P) > 4$, because the curious reader will find it easy to produce an infinite number of P with $I(P) = 4$. Further, (2) simply generalizes the question: "Are there infinitely many primes of the form $m^2 + 1$?

Remark 5: In Proposition 7 we describe all pairs of positive integers P and Q with $P^2 \equiv 1 \pmod{Q}$ and $Q^2 \equiv 1 \pmod{P}$. This problem was posed by Tom Cusick of the University of Buffalo at a meeting of the Seaway Number Theory Conference in May 1991. We understand that he also has a description by a different method.

REFERENCES

1. I. Niven, H. S. Zuckerman, & H. L. Montgomery. *An Introduction to the Theory of Numbers.* 5th ed. New York: Wiley, 1991.
2. J. C. Owings. "Solution of the System $a^2 \equiv -1 \pmod{b}$, $b^2 \equiv -1 \pmod{a}$." *Fibonacci Quarterly* **25.3** (1987):245-49.
3. O. Perron. "Die lehre von den Kettenbruchen." In *Mathematischen Wissenschaften.* Leipzig and Berlin: Druck und Verlag Von B. G. Teubner, 1913.
4. K. Rosen. *Elementary Number Theory.* 2nd ed. New York: Addison-Wesley, 1988.
5. W. Sierpinski. "Elementary Theory of Numbers." *Monografie Mathematgezne* **42** (Polska Ajademia Nauk; 1964).
6. H. Stark. *An Introduction to Number Theory.* Boston: MIT Press, 1978.
7. S. Vojda. *Fibonacci and Lucas Numbers, and the Golden Section.* New York: Wiley, 1989.

AMS numbers: 11A05, 11A55, 11B39

❖❖❖