Journal of Integer Sequences, Vol. 25 (2022),
Article 22.7.2

Generalization of Jarden's Theorem

E. L. Roettger
Department of General Education
Mount Royal University
4825 Mount Royal Gate SW
Calgary, AB T3E 6K6
Canada
eroettger@mtroyal.ca

H. C. Williams
Department of Mathematics and Statistics
University of Calgary
2500 University Drive NW
Calgary, AB T2N 1N4
Canada
hwilliam@ucalgary.ca

Abstract

Let $(F_n)_{n\geq 0}$ and $(L_n)_{n\geq 0}$ denote the sequences of Fibonacci numbers and Lucas numbers, respectively. In 1950 Dov Jarden showed that if $m = 5$ and n is odd and positive, then

$$L_{mn}/L_n = A_n B_n,$$

where

$$A_n = 5F_n^2 - 5F_n + 1, \quad B_n = 5F_n^2 + 5F_n + 1.$$

He went on to show that if n and k are both odd and positive and η is the value of the Legendre symbol $(k|5)$, then $A_n \mid A_{kn}$, $B_n \mid B_{kn}$ when $\eta = 1$ and $A_n \mid B_{kn}$, $B_n \mid A_{kn}$ when $\eta = -1$. In this paper we show how to generalize these results for values of m which are odd and square-free to the Lucas sequence $(V_n)_{n\geq 0}$.

1 Introduction

Let P, Q be integers and α, β denote the zeros of $f(x) = x^2 - Px + Q$. We will use D $(= P^2 - 4Q)$ to represent the discriminant $(\alpha - \beta)^2$ of $f(x)$. Let

$$U_n = (\alpha^n - \beta^n)/(\alpha - \beta) \quad \text{and} \quad V_n = \alpha^n + \beta^n. \tag{1}$$

For $n \geq 0$, it is easy to see that both U_n and V_n are integers. The sequences (U_n) and (V_n) are called the Lucas sequences. For example, if we put $P = 1$, $Q = -1$, then $U_n = F_n$ and $V_n = L_n$, where (F_n) is the sequence of Fibonacci numbers and (L_n) is the sequence of Lucas numbers. In the sequel we will use n to denote a positive integer.

In a short paper originally published in Hebrew in 1950, Dov Jarden (see [8, §8] for an English version) verified by using (1) the identity

$$L_{5n}/L_n = A_n B_n, \tag{2}$$

where n is odd and

$$A_n = 5F_n^2 - 5F_n + 1, \quad B_n = 5F_n^2 + 5F_n + 1.$$

This rather pretty identity does not seem to be very well known. Since

$$L_n^2 - 5F_n^2 = 4(-1)^n,$$

we can write

$$A_n = L_n^2 - 5F_n + 5, \quad B_n = L_n^2 + 5F_n + 5.$$

Let k be any odd positive integer. Most of Jarden's paper is devoted to proving the following result.

Theorem 1. *Let n, k denote odd positive integers. We have*

$$A_n \mid A_{kn} \quad \textit{and} \quad B_n \mid B_{kn} \quad \textit{when } k \equiv 1, 4 \pmod 5.$$

Also,

$$A_n \mid B_{kn} \quad \textit{and} \quad B_n \mid A_{kn} \quad \textit{when } k \equiv 2, 3 \pmod 5.$$

This result was called a crossover theorem by Brillhart, Montgomery, and Silverman [2] and was enlisted by them to assist in compiling a table of integer factorizations of the Lucas numbers.

The purpose of this paper is to generalize Jarden's crossover theorem. In order to do this we will require some results from the theory of what today are called Aurifeuillians. We begin by defining the cyclotomic polynomial $\Phi_m(x) \in \mathbb{Z}[x]$ to be

$$\Phi_m(x) = \prod (x - \zeta_m^s),$$

where ζ_m is a primitive m^{th} root of unity and the product is taken over all values s between 0 and m and relatively prime to m. It is well known that we can write $\Phi_m(x)$ as

$$\Phi_m(x) = \prod_{d|m} (x^d - 1)^{\mu(m/d)}, \tag{3}$$

where μ is the Möbius function. Lucas [5, 6], observed that certain formulas for $\Phi_m(x)$, which he attributed to Aurifeuille and Le Lasseur, could be used to derive identities involving the Lucas sequences and for factoring some of these expressions. For example, in [6, p. 172] he gave the identity

$$V_{10n}/V_{2n} = (V_{4n} + 5Q^n V_{2n} + 7Q^{2n})^2 - 10Q^n(V_{2n} + 2Q^n V_n)^2.$$

He derived this from the Aurifeuillian formula

$$\Phi_{20}(x) = \frac{x^{10}+1}{x^2+1} = (x^4 + 5x^3 + 7x^2 + 5x + 1)^2 - 10x(x^3 + 2x^2 + 2x + 1)^2,$$

by putting $x = \alpha^n/\beta^n$. Notice that this expression for V_{10n}/V_{2n} will factor as a difference of squares when $10Q^n$ is a perfect integral square. This means that $Q = 10L^2$, where L is an integer.

Other results, apparently unknown to Lucas, can be obtained by substituting other expressions involving α^n/β^n for x in Aurifeuillian formulas. As an example, consider

$$\Phi_5(x) = \frac{x^5 - 1}{x - 1} = (x^2 + 3x + 1)^2 - 5x(x + 1)^2,$$

a formula known to Lucas [6, p. 168]. If we put $x = (-\alpha^n/\beta^n)^{1/2}$, we get

$$V_{5n}/V_n = (V_n^2 - 5Q^n)^2 + 5Q^n DU_n^2 = (DU_n^2 - Q^n)^2 + 5Q^n DU_n^2.$$

If $-5Q^n D$ is a perfect integral square we can find a factorization of V_{5n}/V_n. When we consider the special case of $P = 1$, $Q = -1$, we have $-5Q^n D = 25$ when n is odd and we get (2).

For recent information concerning Aurifeuillians and additional references the reader is advised to consult Granville and Pleasants [7] and Wagstaff [12, §4.1]. For some historical commentary, see Williams [13, pp. 126–127, pp. 318–319].

2 Preliminary results

Let m (> 3) be a fixed square-free positive odd integer. Put $\sigma = (-1)^{\frac{m-1}{2}}$ and $m^* = \sigma m \equiv 1 \pmod 4$. For a real number r, we will use $\sqrt{r}$ to denote the positive square root of r when $r \geq 0$ or $i\sqrt{|r|}$ when $r < 0$. Next, set

$$S_m = \{s : 1 \leq s < m; \gcd(m, s) = 1\}.$$

By the definition of $\phi(m)$, we have

$$\#S_m = \phi(m).$$

Now let $\epsilon \in \{1, -1\}$ and put $S_m^{(\epsilon)} = \{s : 1 \leq s < m; (s|m) = \epsilon\}$ for a fixed ϵ. As there are just as many values of $s \in S_m$ such that $(s|m) = 1$ and that $(s|m) = -1$, we see that

$$\#S_m^{(\epsilon)} = \#S_m^{(-\epsilon)} = \phi(m)/2.$$

Also, note that for any $s \in S_m$, we also have $m - s \in S_m$. Thus, S_m consists of $\phi(m)/2$ pairs $(s, m - s)$. It follows that since $s + m - s = m$, we get

$$\sum_{s \in S_m} s = m\phi(m)/2.$$

If we put

$$\Sigma_m^{(\epsilon)} = \sum_{s \in S_m^{(\epsilon)}} s,$$

we have

$$\Sigma_m^{(\epsilon)} + \Sigma_m^{(-\epsilon)} = m\phi(m)/2.$$

Since $m > 3$, there must exist some integer r such that the Jacobi symbol $(r|m) = -1$ and $\gcd(r + 1, m) = 1$. Thus, we get

$$r\Sigma_m^{(\epsilon)} \equiv \sum_{s \in S_m^{(\epsilon)}} rs \equiv \sum_{s \in S_m^{(-\epsilon)}} s = \Sigma_m^{(-\epsilon)} \pmod{m}.$$

Since $m \mid \Sigma_m^{(\epsilon)} + \Sigma_m^{(-\epsilon)}$, we get

$$(r + 1)\Sigma_m^{(\epsilon)} \equiv 0 \pmod{m}$$

which means that

$$\Sigma_m^{(\epsilon)} \equiv \Sigma_m^{(-\epsilon)} \equiv 0 \pmod{m}. \tag{4}$$

Also, since $(rs|m) = -(s|m)$, we find that

$$\sum_{s \in S_m} (s|m) = -\sum_{s \in S_m} (s|m);$$

hence,

$$\sum_{s \in S_m} (s|m) = 0. \tag{5}$$

Let I be a given integral domain and let $p(x) \in I[x]$ be the polynomial

$$p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,$$

where $a_j \in I$ $(j = 0, 1, \ldots, n)$. If $p(x) = p(-x)$, then $a_j = 0$ whenever $2 \nmid j$; also, if $p(x) = -p(-x)$, then $a_j = 0$ whenever $2 \mid j$. We say that $p(x)$ is *palindromic of order n* over I if

$$a_j = a_{n-j} \quad (j = 0, 1, 2, \ldots, n),$$

and that $p(x)$ is *antipalindromic of order n* if

$$a_j = -a_{n-j} \quad (j = 0, 1, 2, \ldots, n).$$

When $I = \mathbb{Z}$, we will omit including I and simply say that $p(x)$ is palindromic or antipalindromic. Notice that under this definition the polynomial $x = (0x^2 + x + 0)$ is palindromic of order 2 over I. Also, if $p(x)$ is antipalindromic of degree n, where $2 \mid n$, then $a_{n/2} = 0$.

The next results follow easily from the above observations and definitions. We first let $p(x)$ denote a polynomial over I which is either palindromic or antipalindromic of order n and define $q(x) = p(-x)$.

i) If $2 \mid n$, then $q(x)$ is either palindromic or antipalindromic of order n over I, according to whether $p(x)$ is palindromic or antipalindromic.

ii) If $2 \nmid n$, then $q(x)$ is antipalindromic or palindromic of order n over I, according to whether $p(x)$ is palindromic or antipalindromic.

iii) If $2 \mid n$ and $p(x) = q(x)$, then $p(x) = r(x^2)$, where $r(x)$ is a palindromic or antipalindromic polynomial over I of order $n/2$, according to whether $p(x)$ is palindromic or antipalindromic.

iv) If $2 \mid n$ and $p(x) = -q(x)$, then $p(x)/x = r(x^2)$, where $r(x)$ is a palindromic or antipalindromic polynomial over I of order $n/2 - 1$, according to whether $p(x)$ is palindromic or antipalindromic.

Proposition 2. *$p(x)$ is palindromic of order n over I if and only if*

$$p(x) = x^n p(1/x)$$

and $p(x)$ is antipalindromic of order n over I if and only if

$$p(x) = -x^n p(1/x).$$

From this result, we can easily derive the following:

v) If c_1, $c_2 \in I$ and $p_1(x)$, $p_2(x)$ are both either palindromic or antipalindromic polynomials of order n over I, then

$$c_1 p_1(x) + c_2 p_2(x)$$

is a palindromic or antipalindromic polynomial of order n over I according to whether $p_1(x)$ and $p_2(x)$ are palindromic or antipalindromic.

vi) If $p_1(x)$ and $p_2(x)$ are both palindromic or antipalindromic polynomials of order n_1 and n_2, respectively, over I, then

$$p_1(x)p_2(x)$$

is a palindromic polynomial of order $n_1 + n_2$ over I.

vii) If p_1 is a palindromic polynomial of degree n_1 and p_2 is an antipalindromic polynomial of degree n_2, then

$$p_1(x)p_2(x)$$

is an antipalindromic polynomial of order $n_1 + n_2$ over I.

3 Some Aurifeuillian identities

We now let ζ_h denote any fixed primitive h^{th} root of unity. Define for m above

$$A_m^{(\epsilon)}(x) = \prod_{s \in S_m^{(\epsilon)}} (x - \zeta_m^s). \tag{6}$$

Set $e = \phi(m)/2$ and observe that if $\sigma = 1$, then $2 \mid e$. By results of Gauss and Dirichlet (see [3]), we know that $A_m^{(\epsilon)}(x)$ is a polynomial of degree e over $\mathcal{O}$, the maximal order of the quadratic field $\mathbb{Q}(\sqrt{m^*})$. Indeed

$$A_m^{(\epsilon)}(x) = \frac{1}{2}(Y_m(x) - \epsilon\sqrt{m^*}Z_m(x)),$$

where $Y_m(x)$, $Z_m(x) \in \mathbb{Z}[x]$ and $Y_m(x) \equiv Z_m(x) \pmod 2$. Also, by using (4) we can show that we have

$$A_m^{(\epsilon)}(x) = x^e A_m^{(\epsilon)}(1/x)$$

when $m \equiv 1 \pmod 4$ and

$$A_m^{(\epsilon)}(x) = (-x)^e A_m^{(-\epsilon)}(1/x)$$

when $m \equiv -1 \pmod 4$. Hence,

$$Y_m(x) = x^e Y_m(1/x), \quad Z_m(x) = x^e Z_m(1/x)$$

when $m \equiv 1 \pmod 4$ and

$$Y_m(x) = (-x)^e Y_m(1/x), \quad -Z_m(x) = (-x)^e Z_m(1/x)$$

when $m \equiv -1 \pmod 4$. By using Proposition 2 we can summarize the palindromic-antipalindromic properties of $Y_m(x)$, $Z_m(x)$ in Table 1.

$m \pmod 4$	$e \pmod 2$	$Y_m(x)$	$Z_m(x)$
1	0	palindromic of order e	palindromic of order e
-1	0	palindromic of order e	antipalindromic of order e
-1	1	antipalindromic of order e	palindromic of order e

Table 1: Palindromic-antipalindromic properties of $Y_m(x)$, $Z_m(x)$.

Put

$$\begin{aligned} L_m^{(\epsilon)}(x) &= A_m^{(\epsilon)}(x)A_m^{(-\epsilon)}(-x), \\ &= G_m(x) - \epsilon x\sqrt{m^*}H_m(x), \end{aligned} \tag{7}$$

where

$$\begin{aligned} G_m(x) &= \frac{1}{4}(Y_m(x)Y_m(-x) - m^*Z_m(x)Z_m(-x)), \\ H_m(x) &= \frac{1}{4}(Y_m(-x)Z_m(x) - Y_m(x)Z_m(-x)). \end{aligned}$$

Notice that because $Y_m(x) \equiv Z_m(x) \pmod 2$, we have $G_m(x)$, $H_m(x)$ both polynomials over $\mathbb{Z}$. By appealing to Table 1 and Properties v), vi), vii) of Section 2, we can produce Table 2.

$m \pmod 4$	$e \pmod 2$	$G_m(x)$	$H_m(x)$
1	0	palindromic of order $2e$	palindromic of order $2e$
-1	0	palindromic of order $2e$	antipalindromic of order $2e$
-1	1	antipalindromic of order $2e$	palindromic of order $2e$

Table 2: Palindromic-antipalindromic properties of $G_m(x)$, $H_m(x)$.

We note that $G_m(-x) = G_m(x)$ and $H_m(-x) = -H_m(x)$; thus, by Properties iii) and iv) of Section 2, we have $G_m(x) = P_m(x^2)$, $\frac{H_m(x)}{x} = Q_m(x^2)$, where the palindromic/antipalindromic properties of $P_m(x)$, $Q_m(x)$ are presented in Table 3.

σ	$e \pmod 2$	$P_m(x)$	$Q_m(x)$
1	0	palindromic of order e	palindromic of order $e-1$
-1	0	palindromic of order e	antipalindromic of order $e-1$
-1	1	antipalindromic of order e	palindromic of order $e-1$

Table 3: Palindromic-antipalindromic properties of $P_m(x)$, $Q_m(x)$.

Notice that if $\sigma = -1$ ($m \equiv -1 \pmod 4$), then by Properties i) and ii) both $P_m(-x)$ and $Q_m(-x)$ are palindromic of order e, $e-1$, respectively. We now have

$$L_m^{(\epsilon)}(x) = P_m(x^2) - \epsilon x\sqrt{m^*}Q_m(x^2), \tag{8}$$

an identity proved in greater generality by Schinzel [10]. If we put $C_m(x) = P_m(x)$, $D_m(x) = Q_m(x)$ when $\sigma = 1$ and $C_m(x) = P_m(-x)$, $D_m(x) = Q_m(-x)$ when $\sigma = -1$. We see that both $C_m(x)$ and $D_m(x)$ are palindromic of order e and $e-1$, respectively. We write

$$C_m(x) = \sum_{j=0}^{e} c_j x^{e-j} \quad (c_j \in \mathbb{Z}, j = 0, 1, \ldots, e)$$

and

$$D_m(x) = \sum_{j=0}^{e-1} d_j x^{e-1-j} \quad (d_j \in \mathbb{Z}, j = 0, 1, \ldots, e-1).$$

For small values of m, a table of coefficients c_j and d_j can be found in Riesel [9, Table 34]. Also, Brent [1], has given an efficient algorithm for computing these coefficients.

Note also that

$$A_m^{(\epsilon)}(x)A_m^{(-\epsilon)}(x) = \Phi_m(x).$$

Since

$$A_m^{(\epsilon)}(-x)A_m^{(-\epsilon)}(-x) = \Phi_m(-x),$$

we get

$$L_m^{(\epsilon)}(x)L_m^{(-\epsilon)}(x) = \Phi_m(x)\Phi_m(-x) = \Phi_m(x^2). \tag{9}$$

Suppose $\sigma = -1$. In this case we must have $m^* = -m$. If we replace x by ix, where $i^2 = -1$, in (8), we get

$$\begin{aligned} L_m^{(\epsilon)}(ix) &= P_m(-x^2) - \epsilon ix\sqrt{m^*}Q_m(-x^2) \\ &= P_m(-x^2) - \epsilon x\sqrt{m}Q_m(-x^2) \\ &= C_m(x^2) - \epsilon x\sqrt{m}D_m(x^2) \end{aligned} \tag{10}$$

and

$$L_m^{(\epsilon)}(ix)L_m^{(-\epsilon)}(ix) = \Phi_m(-x^2) = \Phi_{2m}(x^2). \tag{11}$$

Thus, if $\sigma = 1$, we have $m^* = m$ and

$$L_m^{(\epsilon)}(x) = C_m(x^2) - \epsilon x\sqrt{m}D_m(x^2)$$

and if $\sigma = -1$, we have $m^* = -m$ and

$$L_m^{(\epsilon)}(ix) = C_m(x^2) - \epsilon x\sqrt{m}D_m(x^2).$$

4 Aurifeuillian factorizations

For a fixed m, put

$$F_n^{(\epsilon)} = \beta^{ne} L_m^{(\epsilon)}((-\alpha^n/\beta^n)^{1/2}).$$

Notice by (9) and (3)

$$\begin{aligned} F_n^{(\epsilon)} F_n^{(-\epsilon)} &= \beta^{2ne} \Phi_m(-\alpha^n/\beta^n) \\ &= \beta^{n\phi(m)} \Phi_m(-\alpha^n/\beta^n) \\ &= \prod_{d|m} V_{nd}^{\mu(m/d)}. \end{aligned}$$

This is the Aurifeuillian factorization of the integer $\prod_{d|m} V_{nd}^{\mu(m/d)}$.

Let $R(x)$, $S(x) \in \mathbb{Z}[x]$, where $R(x)$, $S(x)$ are palindromic of order d, $d-1$ respectively. If $2 \mid d$, we can write

$$R(x) = \sum_{j=0}^{d} r_j x^j = \sum_{j=0}^{d/2-1} r_j(x^j + x^{d-j}) + r_{d/2} x^{d/2} \tag{12}$$

and

$$S(x) = \sum_{j=0}^{d-1} s_j x^j = \sum_{j=0}^{d/2-1} s_j(x^j + x^{d-1-j}), \tag{13}$$

where $r_j \in \mathbb{Z} (j = 0, 1, \ldots, d/2-1)$ and $s_j \in \mathbb{Z} (j = 0, 1, \ldots, d/2-1)$. When $2 \nmid d$, we can write

$$R(x) = \sum_{j=0}^{(d-1)/2} r_j(x^j + x^{d-j}), \tag{14}$$

$$S(x) = \sum_{j=0}^{(d-1)/2} s_j(x^j + x^{d-1-j}) + s_{(d-1)/2} x^{(d-1)/2}, \tag{15}$$

$$\tag{16}$$

where $r_j \in \mathbb{Z}$ $(j = 0, 1, \ldots, (d-1)/2)$ and $s_j \in \mathbb{Z}$ $(j = 0, 1, \ldots, (d-1)/2)$. We can now establish the following simple theorem.

Theorem 3. *Suppose* $2 \mid d$, $\sigma = 1$ *and*

$$K^{(\epsilon)}(x) = R(x^2) - \epsilon x \sqrt{m} S(x^2),$$

then

$$\beta^{dn} K^{(\epsilon)}((-\alpha^n/\beta^n)^{1/2}) = I_{d,n} + \epsilon \sqrt{m} \sqrt{-Q^n} (\alpha - \beta) J_{d,n},$$

where

$$I_{d,n} = \sum_{j=0}^{d/2-1} r_j(-1)^j Q^{nj} V_{(d-2j)n} + (-1)^{d/2} r_{d/2} Q^{nd/2},$$
$$J_{d,n} = \sum_{j=0}^{d/2-1} s_j(-1)^j Q^{nj} U_{(d-2j-1)n}.$$

Proof. This follows easily from (12) and (13) by putting $x = (-\alpha^n/\beta^n)^{1/2}$ and noting that

$$\alpha^{jn}\beta^{(d-j)n} + \alpha^{(d-j)n}\beta^{jn} = \alpha^{jn}\beta^{jn}(\alpha^{(d-2j)n} + \beta^{(d-2j)n}) = Q^{jn}V_{(d-2j)n}$$

and

$$\alpha^{jn}\beta^{(d-1-j)n} - \alpha^{(d-1-j)n}\beta^{jn} = \alpha^{jn}\beta^{jn}(\beta^{(d-2j-1)n} - \alpha^{(d-2j-1)n}) = -Q^{jn}(\alpha-\beta)U_{(d-2j-1)n}.$$

Hence,

$$I_{d,n} = \beta^{dn} R(-\alpha^n/\beta^n), \quad J_{d,n} = \beta^{(d-1)n} S(-\alpha^n/\beta^n).$$

□

We also have.

Theorem 4. *Suppose* $2 \mid d$, $\sigma = -1$ *and*

$$K^{(\epsilon)}(ix) = R(x^2) - \epsilon x\sqrt{m} S(x^2),$$

then

$$\beta^{dn} K^{(\epsilon)}((-\alpha^n/\beta^n)^{1/2}) = I_{d,n} - \epsilon\sqrt{m}\sqrt{Q^n} J_{d,n},$$

where

$$I_{d,n} = \sum_{j=0}^{d/2-1} r_j Q^{nj} V_{(d-2j)n} + r_{d/2} Q^{nd/2},$$
$$J_{d,n} = \sum_{j=0}^{d/2-1} s_j Q^{nj} V_{(d-2j-1)n}.$$

Proof. This follows on putting $x = (\alpha^n/\beta^n)^{1/2}$ and making use of (12) and (13). □

Theorem 5. *Suppose* $2 \nmid d$ *and*

$$K^{(\epsilon)}(ix) = R(x^2) - \epsilon x\sqrt{m} S(x^2),$$

then

$$\beta^{dn} K^{(\epsilon)}((-\alpha^n/\beta^n)^{1/2}) = I_{d,n} - \epsilon\sqrt{m}\sqrt{Q^n} J_{d,n},$$

where

$$I_{d,n} = \sum_{j=0}^{(d-1)/2} r_j Q^{nj} V_{(d-2j)n},$$
$$J_{d,n} = \sum_{j=0}^{(d-1)/2} s_j Q^{nj} V_{(d-2j-1)n} + s_{(d-1)/2} Q^{n(d-1)/2}.$$

Proof. Putting $x = (\alpha^n/\beta^n)^{1/2}$ we get

$$I_{d,n} = \beta^{dn} R(\alpha^n/\beta^n), \quad J_{d,n} = \beta^{(d-1)n} S(\alpha^n/\beta^n)$$

from (14) and (15). □

It follows from Theorem 3 that if $\sigma = 1$, then

$$F_n^{(\epsilon)} = I_{e,n} + \epsilon\sqrt{m}\sqrt{-Q^n}(\alpha - \beta)J_{e,n};$$

if $\sigma = -1$, then by Theorems 4 ($2 \mid e$) and 5 ($2 \nmid e$)

$$F_n^{(\epsilon)} = I_{e,n} + \epsilon\sqrt{m}\sqrt{Q^n}J_{e,n}.$$

In the former case, we see that $F_n^{(\epsilon)} \in \mathbb{Z}$ if and only if $\sqrt{m}\sqrt{-Q^n}(\alpha - \beta) \in \mathbb{Z}$; in the latter case we have $F_n^{(\epsilon)} \in \mathbb{Z}$ if and only if $\sqrt{m}\sqrt{Q^n} \in \mathbb{Z}$.

Remark 6. If $2 \mid e$, by Theorem 3 we have for $x = (-\alpha^n/\beta^n)^{1/2}$

$$F_n^{(\epsilon)} = I_n + \epsilon\sqrt{m^*}\sqrt{-Q^n}(\alpha - \beta)J_n,$$

where in this case

$$I_n = \sum_{j=0}^{e/2-1} c_j(-1)^j Q^{nj} V_{(e-2j)n} + (-1)^{e/2} c_{e/2} Q^{ne/2},$$
$$J_n = \sum_{j=0}^{e/2-1} d_j(-1)^j Q^{nj} U_{(e-2j-1)n}.$$

If $2 \nmid e$, by Theorem 5, we get for $x = (\alpha^n/\beta^n)^{1/2}$,

$$F_n^{(\epsilon)} = I_n + \epsilon\sqrt{m}\sqrt{Q^n}J_n,$$

where

$$I_n = \sum_{j=0}^{(e-1)/2} c_j Q^{nj} V_{(e-2j)n},$$
$$J_n = \sum_{j=0}^{(e-3)/2} d_j Q^{nj} V_{(e-2j-1)n} + d_{(e-1)/2} Q^{n(e-1)/2}.$$

We conclude this section with two simple examples.

Example 1: $m = 5$**.**

Suppose $m = 5$; in this case we have $e = \phi(5)/2 = 2$ and from [9] we find that $c_0 = 1$ and $c_1 = 3$ and $d_0 = 1$. Thus, by (7) and Theorem 3, we have

$$F_n^{(\epsilon)} = I_{e,n} + \epsilon\sqrt{5}\sqrt{-Q^n}(\alpha - \beta)J_{e,n},$$

where

$$\begin{aligned} I_{e,n} &= c_0 V_{2n} - c_1 Q^n = V_{2n} - 3Q^n = V_n^2 - 5Q^n, \\ J_{e,n} &= d_0 U_n = U_n. \end{aligned}$$

Thus,

$$V_{5n}/V_n = (V_n^2 - 5Q^n + \sqrt{5}\sqrt{-Q^n}(\alpha - \beta)U_n)(V_n^2 - 5Q^n - \sqrt{5}\sqrt{-Q^n}(\alpha - \beta)U_n)$$

when n is odd we need $(\alpha - \beta) \in \mathbb{Z}$ in order that $F_n^{(\epsilon)} \in \mathbb{Z}$. This will be the case when $Q = -1$ and $P = 1$, and we get

$$V_{5n}/V_n = L_{5n}/L_n = (L_n^2 + 5 + 5F_n)(L_n^2 + 5 - 5F_n),$$

which is Jarden's identity.

Example 2: $m = 7$**.**

Suppose $m = 7$. We get $e = \phi(7)/2 = 3$ and $c_0 = 1$, $c_1 = 3$, $d_0 = 1$, $d_1 = 1$. By Theorem 5, we get

$$F_n^{(\epsilon)} = I_{e,n} + \epsilon\sqrt{7}\sqrt{Q^n}J_{e,n},$$

where

$$\begin{aligned} I_{e,n} &= c_0 V_{3n} + c_1 Q^n V_n = V_{3n} + 3Q^n V_n = V_n^3, \\ J_{e,n} &= d_0 V_{2n} + d_1 Q^n = V_{2n} + Q^n = V_n^2 - Q^n. \end{aligned}$$

Thus,

$$F_n^{(\epsilon)} = V_n^3 + \epsilon\sqrt{7Q^n}(V_n^2 - Q^n)$$

and

$$V_{7n}/V_n = F_n^{(\epsilon)} F_n^{(-\epsilon)}.$$

We see that $F_n^{(\epsilon)} \in \mathbb{Z}$ when n is odd and $Q = 7L^2$. In this case

$$F_n^{(\epsilon)} = V_n^3 + \epsilon 7^{\frac{n+1}{2}} L^n (V_n^2 - Q^n),$$

and

$$V_{7n}/V_n = (V_n^3 + 7^{\frac{n+1}{2}} L^n (V_n^2 - Q^n))(V_n^3 - 7^{\frac{n+1}{2}} L^n (V_n^2 - Q^n)).$$

5 The main result

Let k be an odd integer such that $\gcd(k,m)=1$ and we let η denote the Jacobi symbol $(k|m)$. Consider

$$A_m^{(\epsilon)}(x^k)=\prod_{s\in S_m^{(\epsilon)}}(x^k-\zeta_m^s).$$

We then have

$$A_m^{(\epsilon\eta)}(x^k)=\prod_{s\in S_m^{(\epsilon)}}(x^k-\zeta_m^{sk}).$$

This is because

$$\{\zeta_m^s : s\in S_m^{(\epsilon\eta)}\}=\{\zeta_m^{ks} : s\in S_m^{(\epsilon)}\},$$

which follows from

$$\begin{aligned}S_m^{(\epsilon\eta)}&=\{s' : (s'|m)=\epsilon\eta, s'\in S_m\}\\&=\{s' : s'\equiv ks \pmod m, s\in S_m^{(\epsilon)}\}\\&\equiv kS_m^{(\epsilon)} \pmod m.\end{aligned}$$

Put

$$\begin{aligned}T_{m,k}^{(\epsilon)}(x)&=\frac{A_m^{(\epsilon\eta)}(x^k)}{A_m^{(\epsilon)}(x)}\\&=\prod_{s\in S_m^{(\epsilon)}}\frac{x^k-\zeta_m^{sk}}{x-\zeta_m^s}\\&=\prod_{s\in S_m^{(\epsilon)}}\zeta_m^{(k-1)s}\frac{(x/\zeta_m^s)^k-1}{(x/\zeta_m^s)-1}.\end{aligned}$$

Let $C_k(x)$ denote the polynomial $\frac{x^k-1}{x-1}\in\mathbb{Z}[x]$, which is of degree $k-1$ and symmetric over $\mathbb{Z}$. From

$$\frac{x^k-1}{x-1}=\prod_{j=1}^{k-1}(x-\zeta_k^j),$$

we find that

$$\begin{aligned}T_{m,k}^{(\epsilon)}(x)&=\prod_{s\in S_m^{(\epsilon)}}\zeta_m^{(k-1)s}\prod_{j=1}^{k-1}(x/\zeta_m^s-\zeta_k^j)\\&=\prod_{s\in S_m^{(\epsilon)}}\prod_{j=1}^{k-1}(x-\zeta_m^s\zeta_k^j).\end{aligned}$$

By standard arguments in algebraic number theory, we know that

$$\zeta_m^s \zeta_k^j \quad \text{where} \quad s \in S_m^{(\epsilon)}, \quad j = 1, 2, \ldots, k-1$$

are the $(k-1)e$ eigenvalues of a square matrix M of size $(k-1)e$ with entries from $\mathcal{O}$. Indeed, $M = \mathcal{C}_1 \otimes \mathcal{C}_2$, where $\mathcal{C}_1$ is the companion matrix of $C_k(x)$, $\mathcal{C}_2$ is the companion matrix of $A_m^{(\epsilon)}(x)$ and $\otimes$ denotes the Kronecker product. Thus, $T_{m,k}^{(\epsilon)}(x)$ is a monic polynomial of degree $(k-1)e$ in $\mathcal{O}[x]$. It follows that

$$T_{m,k}^{(\epsilon)}(x) = \frac{1}{2}[X_{m,k}(x) - \epsilon\sqrt{m^*}W_{m,k}(x)],$$

where $X_{m,k}(x)$, $W_{m,k}(x) \in \mathbb{Z}[x]$ and $X_{m,k}(x) \equiv W_{m,k}(x) \pmod 2$. From the definition of $T_{m,k}^{(\epsilon)}(x)$, it is easy to show that

$$T_{m,k}^{(\epsilon)}(x) = \begin{cases} x^{(k-1)e} T_{m,k}^{(\epsilon)}(1/x), & \text{if } m \equiv 1 \pmod 4; \\ x^{(k-1)e} T_{m,k}^{(-\epsilon)}(1/x), & \text{if } m \equiv -1 \pmod 4. \end{cases}$$

Thus, when $m \equiv 1 \pmod 4$, both $X_{m,k}(x)$ and $W_{m,k}(x)$ are palindromic of order $(k-1)e$ and when $m \equiv -1 \pmod 4$, $X_{m,k}(x)$ is palindromic and $W_{m,k}(x)$ is antipalindromic of order $(k-1)e$.

By using the arguments in Section 4, we find from (7) that if we define

$$K_{m,k}^{(\epsilon)}(x) = L_m^{(\epsilon\eta)}(x^k)/L_m^{(\epsilon)}(x),$$

then

$$K_{m,k}^{(\epsilon)}(x) = T_{m,k}^{(\epsilon)}(x) T_{m,k}^{(-\epsilon)}(-x) = R_{m,k}(x^2) - \epsilon x\sqrt{m^*} S_{m,k}(x^2), \tag{17}$$

where $R_{m,k}(x)$, $S_{m,k}(x) \in \mathbb{Z}[x]$ with palindromic-antipalindromic properties given in Table 4.

σ	$R_{m,k}(x)$	$S_{m,k}(x)$
1	palindromic of order $d(k-1)$	palindromic of order $d(k-1)-1$
-1	palindromic of order $d(k-1)$	antipalindromic of order $d(k-1)-1$

Table 4: Palindromic-antipalindromic properties of $R_{m,k}(x)$, $S_{m,k}(x)$.

We are now able to prove a more general version of Jarden's theorem.

Theorem 7. *If $\sigma = 1$, n is odd and $\sqrt{m}\sqrt{-Q}(\alpha - \beta) \in \mathbb{Z}$, then $F_n^{(\epsilon)}$, $F_{nk}^{(\epsilon\eta)} \in \mathbb{Z}$ and $F_n^{(\epsilon)} \mid F_{nk}^{(\epsilon\eta)}$ when k is odd and $\eta = (k|m)$.*

Proof. By (17) and Theorem 3, we see that $\beta^{dn}K_{m,k}^{(\epsilon)}(x) \in \mathbb{Z}$ when k is odd, $x = (-\alpha^n/\beta^n)^{1/2}$ and $d = (k-1)e$. Since

$$F_n^{(\epsilon)} = \beta^{ne}L_m((-\alpha^n/\beta^n)^{1/2}) \quad \text{and} \quad F_{nk}^{(\epsilon\eta)} = \beta^{nke}L_m((-\alpha^{nk}/\beta^{nk})^{1/2}),$$

we see that if $\sigma = 1$ and $\sqrt{m}\sqrt{-Q}(\alpha-\beta) \in \mathbb{Z}$, then $F_n^{(\epsilon)}$, $F_{nk}^{(\epsilon\eta)} \in \mathbb{Z}$. Also, by (17) we see that $F_{nk}^{(\epsilon\eta)}/F_n^{(\epsilon)} \in \mathbb{Z}$. □

If we have integers L, M, S such that

$$M^2 + 4(-1)^{\frac{m-1}{2}}L^2 = mS^2 \tag{18}$$

and put $P = M$, $Q = (-1)^{\frac{m+1}{2}}L^2$, we get

$$D = (\alpha-\beta)^2 = mS^2 \Rightarrow (\alpha-\beta) = \sqrt{m}S \Rightarrow \sqrt{m^*}\sqrt{-Q}(\alpha-\beta) = \sqrt{m}L\sqrt{m}S = mLS \in \mathbb{Z}.$$

When $\sigma = -1$, we define $\kappa = (-1)^{(k-1)/2}$. We have

$$ix^k = \begin{cases} (ix)^k, & \text{when } \kappa = 1; \\ -(ix)^k, & \text{when } \kappa = -1. \end{cases}$$

It follows from (6) that when $\kappa = 1$, we have

$$A_m^{(\epsilon)}(ix^k) = \prod_{s \in S_m^{(\epsilon)}} ((ix)^k - \zeta_m^s)$$

and

$$A_m^{(\epsilon\eta)}(ix^k) = \prod_{s \in S_m^{(\epsilon)}} ((ix)^k - \zeta_m^{ks}).$$

As done earlier in this section we find that

$$A_m^{(\epsilon\eta)}(ix^k)/A_m^{(\epsilon)}(ix) = \prod_{s \in S_m^{(\epsilon)}} \frac{(ix)^k - \zeta_m^{ks}}{ix - \zeta_m^s} = T_{m,k}^{(\epsilon)}(ix).$$

We are now able to deduce from (7) that

$$K_{m,k}^{(\epsilon)}(ix) = L_m^{(\epsilon\eta)}(ix^k)/L_m^{(\epsilon)}(ix) = T_{m,k}^{(\epsilon)}(ix)T_{m,k}^{(-\epsilon)}(-ix). \tag{19}$$

When $\kappa = -1$, we get

$$A_m^{(\epsilon)}(ix^k) = \prod_{s \in S_m^{(\epsilon)}} (-(ix)^k - \zeta_m^s)$$

and

$$A_m^{(\epsilon\eta)}(ix^k) = \prod_{s \in S_m^{(\epsilon)}} (-(ix)^k - \zeta_m^{ks}).$$

Thus, since k is odd, we have

$$A_m^{(\epsilon\eta)}(-ix^k) = \prod_{s\in S_m^{(\epsilon)}} ((ix)^k - \zeta_m^{ks}).$$

Also, since

$$A_m^{(-\epsilon)}(ix^k) = \prod_{s\in S_m^{(-\epsilon)}} (-(ix)^k - \zeta_m^s) = \prod_{s\in S_m^{(-\epsilon)}} ((-ix)^k - \zeta_m^s),$$

we get

$$A_m^{(-\epsilon\eta)}(ix^k) = \prod_{s\in S_m^{(-\epsilon)}} ((-ix)^k - \zeta_m^{ks}).$$

Now from (7), we have

$$\begin{aligned} L_m^{(-\epsilon\eta)}(ix^k) &= A_m^{(-\epsilon\eta)}(ix^k)A_m^{(\epsilon\eta)}(-ix^k) \\ &= \prod_{s\in S_m^{(-\epsilon)}} ((-ix)^k - \zeta_m^{ks}) \prod_{s\in S_m^{(\epsilon)}} ((ix)^k - \zeta_m^{ks}); \end{aligned}$$

Thus,

$$\frac{L_m^{(-\epsilon\eta)}(ix^k)}{L_m^{(\epsilon)}(ix)} = \prod_{s\in S_m^{(-\epsilon)}} \frac{(-ix)^k - \zeta_m^{ks}}{-ix - \zeta_m^s} \prod_{s\in S_m^{(\epsilon)}} \frac{(ix)^k - \zeta_m^{ks}}{ix - \zeta_m^s} = T_{m,k}^{(-\epsilon)}(-ix)T_{m,k}^{(\epsilon)}(ix).$$

By combining this formula with (19) and (17), we get

$$\frac{L_m^{(\kappa\eta\epsilon)}(ix^k)}{L_m^{(\epsilon)}(ix)} = T_{m,k}^{(\epsilon)}(ix)T_{m,k}^{(-\epsilon)}(-ix) = K_{m,k}^{(\epsilon)}(ix). \tag{20}$$

We are now able to prove a version of Theorem 7 when $\sigma = -1$.

Theorem 8. *If $\sigma = -1$, n is odd and $\sqrt{mQ} \in \mathbb{Z}$, then $F_n^{(\epsilon)}$, $F_{nk}^{(\kappa\eta\epsilon)} \in \mathbb{Z}$ and $F_n^{(\epsilon)} \mid F_{nk}^{(\kappa\eta\epsilon)}$ when k is odd and $\eta = (k|m)$.*

Proof. By (17), we have

$$K_{m,k}^{(\epsilon)}(ix) = R_{m,k}(-x^2) - \epsilon i\sqrt{m^*}S_{m,k}(-x^2),$$

where both $R_{m,k}(-x)$, $S_{m,k}(-x)$ are palindromic of order d and $d-1$, respectively. Thus, by Theorem 4, we see that

$$\beta^{dn}K_{m,k}^{(\epsilon)}(ix) \in \mathbb{Z}$$

when k is odd, $x = (-\alpha^n/\beta^n)^{1/2}$ and $\sqrt{mQ} \in \mathbb{Z}$. The remainder of the proof follows in the same way as the proof of Theorem 7. □

In the case of $\sigma = -1$, we must have $\sqrt{mQ} \in \mathbb{Z}$, which means that $Q = mL^2$, where L is an integer. Thus, Theorems 7 and 8 are the generalized Jarden crossover theorems for odd, square-free $m > 3$.

6 Some further remarks

Although we have constrained $m > 3$, it is possible to prove the crossover theorem in the case that $m = 3$. Here, we get

$$F_n^{(\epsilon)} = V_n + \epsilon\sqrt{3}Q^{\frac{n}{2}} = V_n + \epsilon 3^{\frac{n+1}{2}}L^n,$$

for $Q = 3L^2$. It is a simple matter to verify that

$$F_n^{(\epsilon)} \mid F_n^{(-\epsilon\eta)}$$

for odd n, k and

$$\eta = (k|m) = \begin{cases} 1, & \text{if } k \equiv 1 \pmod 3; \\ -1, & \text{if } k \equiv 2 \pmod 3. \end{cases}$$

Hence, the crossover theorem can also be generalized for $m = 3$.

We also note that in the case of $m \equiv 1 \pmod 4$, we can write $I_{e,n}$ (and consequently $F_n^{(\epsilon)}$) in terms of the (U_n) sequence only by making use of the simple identity

$$V_{2n} = DU_n^2 + 2Q^n.$$

We find that

$$\begin{aligned} I_{e,n} &= \sum_{j=0}^{e/2-1} (-1)^j c_j Q^{nj} V_{(e-2j)n} + (-1)^{e/2} c_{e/2} Q^{ne/2} \\ &= D \sum_{j=0}^{e/2-1} (-1)^j c_j Q^{nj} U_{(e/2-j)n}^2 + Q^{ne/2} \left(2 \sum_{j=0}^{e/2-1} (-1)^j c_j + (-1)^{e/2} c_{e/2} \right). \end{aligned}$$

Note that

$$2 \sum_{j=0}^{e/2-1} (-1)^j c_j + (-1)^{e/2} c_{e/2} = \sum_{j=0}^{e} (-1)^j c_j = C_m(-1).$$

Thus,

$$I_{e,n} = D \sum_{j=0}^{e/2-1} (-1)^j c_j Q^{nj} U_{(e/2-j)n}^2 + Q^{ne/2} C_m(-1).$$

By (7) and (8), we have

$$L_m^{(\epsilon)}(i) = C_m(-1) - \epsilon i\sqrt{m} D_m(-1)$$

and

$$L_m^{(\epsilon)}(i) L_m^{(-\epsilon)}(i) = \Phi_m(-1) = 1;$$

hence,

$$C_m^2(-1) + mD_m^2(-1) = 1,$$

which, since $C_m(-1)$ and $D_m(-1) \in \mathbb{Z}$, means that $C_m^2(-1) = 1$ and $D_m(-1) = 0$. By a result in Wagstaff [11, Theorem 2], we have

$$C_m(x^2) - \sqrt{m}xD_m(x^2) = \prod_{s \in S'_m} (x^2 - 2(s|m)\cos\left(\frac{2\pi s}{m}\right)x + 1), \tag{21}$$

where $S'_m = \{s : s \in S_m, s \le (m-1)/2\}$. Here we have $2\cos\left(\frac{2\pi s}{m}\right) = \zeta_m^s + \zeta_m^{-s}$. Since $m - s \in S_m$ whenever $s \in S_m$, we see that $\#S'_m = \phi(m)/2$. If we put $x = i$ in (21), we get

$$\begin{aligned} C_m(-1) &= \prod_{s \in S'_m} -i(s|m)2\cos\left(\frac{2\pi s}{m}\right) \\ &= (-1)^{\frac{\phi(m)}{4}} \prod_{s \in S'_m} (s|m) \prod_{s \in S'_m} 2\cos\left(\frac{2\pi s}{m}\right). \end{aligned}$$

Since $(m - s|m) = (-s|m) = (s|m)$, we see from (5) that

$$2\sum_{s \in S'_m} (s|m) = \sum_{s \in S_m} (s|m) = 0.$$

Thus, for each $s \in S'_m$, there must exist some $s^* \in S'_m$ ($s^* \ne s$) such that $(s^*|m) = -(s|m)$ or $(s^*s|m) = -1$. It follows that

$$\prod_{s \in S'_m} (s|m) = (-1)^{\phi(m)/4}.$$

Thus,

$$C(-1) = \prod_{s \in S'_m} 2\cos\left(\frac{2\pi s}{m}\right).$$

When m is prime, we know by an old result of Gauss (see [4, (4)]) that

$$\prod_{s \in S'_m} 2\cos\left(\frac{2\pi s}{m}\right) = \prod_{s \in S'_m} \zeta_m^s + \zeta_m^{-s} = (-1)^{(m-1)/4}.$$

If m is composite, there is a very simple proof in Gurak [4, pp. 255–256] that

$$\prod_{s \in S'_m} 2\cos\left(\frac{2\pi s}{m}\right) = 1.$$

It follows that

$$C(-1) = \begin{cases} (-1)^{(m-1)/4}, & \text{if } m \text{ is prime;} \\ 1, & \text{if } m \text{ is composite.} \end{cases}$$

References

[1] Richard P. Brent, On computing factors of cyclotomic polynomials, *Math. Comput.* **61** (1993), 131–149.

[2] John Brillhart, Peter L. Montgomery and Robert D. Silverman, Tables of Fibonacci and Lucas factorizations, *Math. Comput.* **50** (1988), 251–260.

[3] P. G. Lejeune Dirichlet, *Vorlesungen über Zahlentheorie*, 4^{th} edition, Supplement VII, Chelsea, 1968.

[4] S. Gurak, Minimal polynomials for Gauss periods with $f = 2$, *Acta Arith.* **121** (2007), 233–257.

[5] E. Lucas, Théorèmes d'arithmétique, *Atti della Reale Accademia delle scienze di Torino* **13** (1878), 271–278.

[6] E. Lucas, Sur les formules de Cauchy et de Lejeune-Dirichlet, *Assoc. Française pour l'Avancement des Sciences, Comptes Rendus* **7** (1878), 164–173.

[7] Andrew Granville and Peter Pleasants, Aurifeuillian factorization, *Math. Comput.* **75** (2005), 489–508.

[8] Dov Jarden, *Recurring Sequences*, 2^{nd} edition, Riveon Lematematika, 1966.

[9] Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhaüser, 1985.

[10] A. Schinzel, On primitive prime factors of $a^n - b^n$, *Math. Proc. Cambridge Philos. Soc.* **58** (1962), 555–562.

[11] S. S. Wagstaff, Jr., Aurifeuillian factorizations and the period of the Bell numbers modulo a prime, *Math. Comput.* **65** (1996), 383–391.

[12] S. S. Wagstaff, Jr., *The Joy of Factoring*, Volume **68**, Student Mathematical Library, American Mathematical Society, 2013.

[13] H. C. Williams, *Édouard Lucas and Primality Testing*, CMS series of Monographs and Advanced Texts, Volume **22**, Wiley-Interscience, John Wiley & Sons, 1998.

2010 *Mathematics Subject Classification*: Primary 11B37; Secondary 11Y11, 11B50.
Keywords: linear recurrence, Lucas function.

Received May 30 2022; revised version received August 8 2022. Published in *Journal of Integer Sequences*, August 8 2022.

Return to Journal of Integer Sequences home page.