SHORT PERIODS OF CONTINUED FRACTION CONVERGENTS MODULO M: A GENERALIZATION OF THE FIBONACCI CASE

Sandy D. Balkin
10 Dorothy Avenue, Livingston, NJ 07039

Deborah S. Cousins
72 Cambridge Road, Glenmont, NY 12077

Christopher K. Orr
Route 1, Box 429, West Union, SC 29696

Clifford A. Reiter
Department of Mathematics, Lafayette College, Easton, PA 18042
(Submitted September 1993)

1. INTRODUCTION

The period length of the continued fraction convergents modulo m of reduced quadratic irrationals α was studied in [1]. Of course, for $\alpha=(1+\sqrt{5})/2$, this is just the period length of the Fibonacci sequence modulo m, a well studied problem (see [2] and [6]). The period of the convergents of α modulo m is bounded above by linear expressions in m. These linear bounds on the period are achieved with some frequency, yet there are many moduli m with much smaller periods. However, all the periods are at least $c\log(m)$, where c is a constant depending on α [1]. Work classifying some of the short periods in the special case of the Fibonacci sequence has been done (see [3] and [5]). This paper classifies many m having short periods for the convergents of general reduced quadratic irrationals. They are specified in parametric form by particular polynomials whose values generate moduli giving rise to short periods. The periods are short in the sense that the period lengths grow linearly while the moduli grow exponentially in the families generated by these polynomials.

Consider the following example. Continued fraction convergents are computed via the recursions $p_{-1}=0$, $p_0=1$, $p_n=a_np_{n-1}+p_{n-2}$, and $q_{-1}=1$, $q_0=0$, $q_n=a_nq_{n-1}+q_{n-2}$. Consider the convergents of $\alpha=[\overline{1,1,2}]=(2+\sqrt{10})/3$ modulo 13 shown below.

			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
n			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a_n			1	1	2	1	1	2	1	1	2	1	1	2	1	1	2	1	1	2
$p_n \pmod{13}$	0	1	1	2	5	7	12	5	4	9	9	5	1	7	8	2	12	1	0	1
$q_n \pmod{13}$	1	0	1	1	3	4	7	5	12	4	7	11	5	8	0	5	3	11	1	0

The block $\binom{0\ 1}{1\ 0}$ is repeated after 18 steps and hence the continued fraction convergents are repeated thereafter. We designate the period length of the convergents of α modulo m by $k(\alpha, m)$ or just $k(m)$. In this example, $k(\alpha, 13)=18$. The period is always well defined for α with purely periodic continued fraction expansions.

Many properties of these periods are known [1]. In particular, if we let t denote the period length of α and d be the discriminant associated with α defined in Section 2, then it is known that, for odd primes p, the period $k(p)$ divides $(p-1)t, 4pt$, or $2(p+1)t$ depending on whether the Legendre symbol $(\frac{d}{p})$ is 1, 0, or -1, respectively. Moreover, a factor of 2 can be removed from the second two bounds if t is even. In Table 1, the period of $\alpha = [\overline{1, 1, 2}]$ is given for the primes less than or equal to 1000, and the quotient of that period with the bounds mentioned above are given by $Q(p)$. Notice that the quotient is 1 for 111 of the 167 primes given; however, the quotient is sometimes quite large. For example, $Q(859) = 43$. While there is not an obvious pattern, we can explain, up to a factor of 2, all of the quotients over 1 appearing in Table 1. The explanation will be given in terms of the families of moduli with short periods that we will construct in Section 4.

2. FUNDAMENTAL MATRICES AND THE $\mathscr{L}_n$-SEQUENCE

The first four theorems below give a matrix reformulation of the process used to find the periods of the convergents, following [1]. Let $\alpha = [\overline{a_1, a_2, \ldots, a_t}]$. **Note:** We will use "t" throughout this paper to designate the length of the period of the purely periodic continued fraction. The convergents at the end of one t-period can be used to compute the convergents at the end of the subsequent t-periods and this information can be used to find the period of the continued fraction sequence modulo m.

Theorem 1: Let $W = \begin{pmatrix} q_{t-1} & q_t \\ p_{t-1} & p_t \end{pmatrix}$. Then $W^n = \begin{pmatrix} q_{nt-1} & q_{nt} \\ p_{nt-1} & p_{nt} \end{pmatrix}$.

The matrix W is called the *fundamental matrix* for α.

The period of α is preserved mod m means that the period of α does not change when the partial quotients are reduced mod m. For example, the convergents of $\alpha = [\overline{1, 2, 3, 4}]$ are the same as those for $[\overline{1, 2}]$ mod 2; hence, the period of α is not preserved mod 2.

Theorem 2:

(i) If $W^n \equiv I \bmod m$, then $k(m) | nt$.

(ii) If the period of α is preserved mod m, then c is the smallest integer such that $W^c \equiv I \bmod m$ if and only if $k(m) = ct$.

As an example of Theorem 2, consider the fundamental matrix for $\alpha = [\overline{1, 1, 2}]$ and its powers modulo 13.

$$W = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}, \qquad W^2 \equiv \begin{pmatrix} 7 & 5 \\ 12 & 5 \end{pmatrix}, \qquad \text{and } W^3 \equiv \begin{pmatrix} 4 & 7 \\ 9 & 9 \end{pmatrix},$$

$$W^4 \equiv \begin{pmatrix} 5 & 8 \\ 1 & 7 \end{pmatrix}, \qquad W^5 \equiv \begin{pmatrix} 8 & 3 \\ 2 & 12 \end{pmatrix}, \qquad \text{and } W^6 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Notice that the sixth power is the first power congruent to the identity; by Theorem 2, $k(13) = 3 \cdot 6 = 18$, as we saw previously.

TABLE 1

The Periods of the Convergents of $\alpha = [\overline{1, 1, 2}]$ Modulo Small Primes

p	$k(p)$	$Q(p)$	p	$k(p)$	$Q(p)$	p	$k(p)$	$Q(p)$
3	6	1	271	90	9	619	3720	1
5	60	1	277	276	3	631	630	3
7	48	1	281	60	14	641	960	2
11	72	1	283	282	3	643	1926	1
13	18	2	293	876	1	647	432	9
17	108	1	307	918	1	653	978	2
19	24	5	311	930	1	659	1320	3
23	144	1	313	1884	1	661	3972	1
29	180	1	317	474	2	673	4044	1
31	90	1	331	1992	1	677	1014	2
37	36	3	337	2028	1	683	2046	1
41	120	1	347	1038	1	691	4152	1
43	126	1	349	2100	1	701	4212	1
47	288	1	353	2124	1	709	4260	1
53	78	2	359	1074	1	719	2154	1
59	120	3	367	2208	1	727	4368	1
61	372	1	373	1116	1	733	732	3
67	66	3	379	2280	1	739	4440	1
71	210	1	383	2304	1	743	4464	1
73	444	1	389	2340	1	751	2250	1
79	234	1	397	594	2	757	2268	1
83	246	1	401	1200	1	761	1140	2
89	264	1	409	1224	1	769	2304	1
97	588	1	419	360	7	773	1158	2
101	612	1	421	2532	1	787	2358	1
103	48	13	431	258	5	797	1194	2
107	318	1	433	2604	1	809	1212	2
109	660	1	439	438	3	811	4872	1
113	684	1	443	1326	1	821	1644	3
127	768	1	449	168	8	823	4944	1
131	72	11	457	2748	1	827	354	7
137	276	3	461	924	3	829	996	5
139	840	1	463	2784	1	839	2514	1
149	900	1	467	1398	1	853	1278	2
151	450	1	479	1434	1	857	156	33
157	468	1	487	2928	1	859	120	43
163	486	1	491	984	3	863	5184	1
167	336	3	499	3000	1	877	2628	1
173	516	1	503	432	7	881	528	5
179	360	3	509	3060	1	883	294	9
181	1092	1	521	390	4	887	5328	1
191	114	5	523	1566	1	907	2718	1
193	1164	1	541	3252	1	911	546	5
197	294	2	547	1638	1	919	2754	1
199	594	1	557	1668	1	929	1392	2
211	1272	1	563	1686	1	937	804	7
223	1344	1	569	1704	1	941	5652	1
227	678	1	571	312	11	947	2838	1
229	1380	1	577	3468	1	953	5724	1
233	468	3	587	1758	1	967	5808	1
239	714	1	593	3564	1	971	5832	1
241	90	8	599	1794	1	977	5868	1
251	1512	1	601	900	2	983	5904	1
257	1548	1	607	3648	1	991	2970	1
263	528	3	613	918	2	997	1494	2
269	1620	1	617	3708	1			

Define

$$C_j = \begin{pmatrix} q_{j-1} & q_j \\ p_{j-1} & p_j \end{pmatrix}.$$

Note that $C_j \equiv I \pmod{m}$ for $j < k(m)$ is possible if j is not a multiple of t. It is not difficult to show that the set of j for which $C_j \equiv I \pmod{m}$ is a union of $\le t$ arithmetic progressions with the difference between consecutive terms in each arithmetic progression equal to $k(m)$.

Next, the general fundamental matrix W has eigenvalues

$$\lambda_1 = \frac{1}{2}((p_t + q_{t-1}) + \sqrt{d}) \quad \text{and} \quad \lambda_2 = \frac{1}{2}((p_t + q_{t-1}) - \sqrt{d})$$

where

$$d = (p_t + q_{t-1})^2 + 4(-1)^{t-1}.$$

It follows immediately that the norm and trace of W are given by

$$\lambda_1\lambda_2 = (-1)^t \quad \text{and} \quad \lambda_1 + \lambda_2 = p_t + q_{t-1}.$$

Theorem 3: Define

$$\mathscr{L}_n = \frac{\lambda_1^n - \lambda_2^n}{\sqrt{d}}.$$

Then $\mathscr{L}_0 = 0$, $\mathscr{L}_1 = 1$, and $\mathscr{L}_{n+1} = (p_t + q_{t-1})\mathscr{L}_n + (-1)^{t-1}\mathscr{L}_{n-1}$.

One consequence of this theorem is that $\mathscr{L}_n$ is an integer.

Theorem 4: Let W be the fundamental matrix for α. Then

$$W^n = \begin{pmatrix} q_{t-1}\mathscr{L}_n + (-1)^{t-1}\mathscr{L}_{n-1} & q_t\mathscr{L}_n \\ p_{t-1}\mathscr{L}_n & p_t\mathscr{L}_n + (-1)^{t-1}\mathscr{L}_{n-1} \end{pmatrix} = \mathscr{L}_n W + (-1)^{t-1}\mathscr{L}_{n-1} I.$$

Proof: This theorem is proved in [1] except that there the (2, 2) entry of the right-hand side is $\mathscr{L}_{n+1} - q_{t-1}\mathscr{L}_n$. Applying Theorem 3 gives the desired result. □

Theorem 5:

(i) Suppose m is a modulus so that $\mathscr{L}_{n-1} \equiv 1$ and $\mathscr{L}_n \equiv 0 \bmod m$. Then $k(m)|2nt$ if t is even and $k(m)|nt$ is *t is odd.*

(ii) Suppose the period of α is preserved modulo m, $\gcd(q_t, m) = 1$, and that c is the smallest integer so that $\mathscr{L}_{c-1} \equiv 1$ and $\mathscr{L}_c \equiv 0$. Then $k(m) = ct$ if t is odd and $k(m) = 2ct$ if t is even.

Proof:

(i) Applying the congruences to Theorem 4 gives $W^n \equiv (-1)^{t-1}I$ modulo m. If t is odd, $W^n \equiv I$ and Theorem 2 gives the desired result; otherwise, square both sides to get $W^{2n} \equiv I$ mod m and the case for even t follows.

(ii) Suppose α, m, and c are as described. Again we see $W^c \equiv (-1)^{t-1}I$ and we claim c is the smallest such integer. If not, there is an n with $n < c$ and such that $W^n \equiv (-1)^{t-1}I$. Then, looking at $W_{1,2}^n$ in Theorem 4, we see $q_t\mathscr{L}_n \equiv 0$ so $\mathscr{L}_n \equiv 0$ since $\gcd(q_t, m) = 1$. Then, looking at $W_{1,1}^n$, we see $(-1)^{t-1}\mathscr{L}_{n-1} + q_{t-1}\mathscr{L}_n \equiv (-1)^{t-1}$, which implies $\mathscr{L}_{n-1} \equiv 1$, and these contradict the minimal choice of c. Thus, c is the smallest integer such that $W^c \equiv (-1)^{t-1}I$. If t is odd, Theorem 2(ii) gives $k(m) = ct$. If t is even, we know that $W^{2c} \equiv I$. We claim $2c$ is the smallest power of W giving the identity matrix mod m. If not, say $W^n \equiv I$ with $n < 2c$ is the smallest such power. Consider two cases: $n \geq c$ and $n < c$. If $n \geq c$, we use the Euclidian algorithm to write $n = qc + r$ with $0 \leq r < c$. So $I \equiv W^n = (W^c)^q W^r$. If q is even, this means $W^r \equiv I$, contradicting the minimality of n unless $r = 0$ or $q = 0$. However, $q = 0$ is impossible since $n \geq c$. In the case with $r = 0$, we get $n = cq \geq 2c$, contradicting $n < 2c$. If q is odd, $W^r \equiv -I$, contradicting the minimal choice of c. Next, consider the case $n < c$. The Euclidean algorithm gives $c = qn + r$ with $0 \leq r < n$. So $-I \equiv W^c = (W^n)^q W^r \equiv W^r$. But $r < n < c$, contradicting the minimality of c unless $r = 0$, which is impossible. Thus, $2c$ is the smallest power of W giving the identity, by Theorem 2, $k(m) = 2ct$. □

For example, consider $\alpha = [\overline{1, 1, 2}]$; the trace is 6, so $\mathcal{L}_0 = 0$, $\mathcal{L}_1 = 1$, and $\mathcal{L}_n = 6\mathcal{L}_{n-1} + \mathcal{L}_{n-2}$. Modulo 13, we get

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$\mathcal{L}_n \pmod{13}$	0	1	6	11	7	1	0	1	6	11	7	1	0

Notice that $\mathcal{L}_{n-1} \equiv 1$, $\mathcal{L}_n \equiv 0$ for $n = 6$, and this is the smallest such n. Also gcd(3, 13) = 1 and the period of α is preserved mod 13, so $k(13) = 6 \cdot 3 = 18$ as we have seen.

We now turn to a matrix formulation that can be used to compute the $\mathcal{L}_n$-sequence. In particular, it will allow us to compute reduction formulas for $\mathcal{L}_{in}$ and $\mathcal{L}_{in-1}$ in terms of $\mathcal{L}_n$ and $\mathcal{L}_{n-1}$.

Theorem 6: Let

$$T = \begin{pmatrix} 0 & 1 \\ (-1)^{t-1} & p_t + q_{t-1} \end{pmatrix} = \begin{pmatrix} (-1)^{t-1}\mathcal{L}_0 & \mathcal{L}_1 \\ (-1)^{t-1}\mathcal{L}_1 & \mathcal{L}_2 \end{pmatrix}.$$

Then

$$T^n = \begin{pmatrix} (-1)^{t-1}\mathcal{L}_{n-1} & \mathcal{L}_n \\ (-1)^{t-1}\mathcal{L}_n & \mathcal{L}_{n+1} \end{pmatrix}.$$

Proof: For $n = 1$, T has the desired form. Now suppose the theorem is true for n. Then

$$T^{n+1} = TT^n = \begin{pmatrix} 0 & 1 \\ (-1)^{t-1} & p_t + q_{t-1} \end{pmatrix}\begin{pmatrix} (-1)^{t-1}\mathcal{L}_{n-1} & \mathcal{L}_n \\ (-1)^{t-1}\mathcal{L}_n & \mathcal{L}_{n+1} \end{pmatrix}$$

$$= \begin{pmatrix} (-1)^{t-1}\mathcal{L}_n & \mathcal{L}_{n+1} \\ (-1)^{2(t-1)}\mathcal{L}_{n-1} + (-1)^{t-1}(p_t + q_{t-1})\mathcal{L}_n & (-1)^{t-1}\mathcal{L}_n + (p_t + q_{t-1})\mathcal{L}_{n+1} \end{pmatrix}$$

$$= \begin{pmatrix} (-1)^{t-1}\mathcal{L}_n & \mathcal{L}_{n+1} \\ (-1)^{t-1}\mathcal{L}_{n+1} & \mathcal{L}_{n+2} \end{pmatrix}$$

as desired. □

Corollary 7: Successive entries in the $\mathcal{L}_n$-sequence satisfy a quadratic identity:

$$\mathcal{L}_{n-1}^2 = -(-1)^{-(t-1)}(p_t + q_{t-1})\mathcal{L}_{n-1}\mathcal{L}_n + (-1)^{-(t-1)}\mathcal{L}_n^2 + (-1)^{tn-2(t-1)}.$$

Proof: Taking the determinant of T^n in Theorem 6 and using the recursion for $\mathcal{L}_{n+1}$ yields

$$(-1)^{tn} = (-1)^{t-1}\mathcal{L}_{n-1}((p_t+q_{t-1})\mathcal{L}_n + (-1)^{t-1}\mathcal{L}_{n-1}) - (-1)^{t-1}\mathcal{L}_n^2.$$

The desired formula results from distributing and solving for $\mathcal{L}_{n-1}^2$. □

One can use Theorem 6 to compute reduction formulas for the $\mathcal{L}_n$-sequence. For example,

$$T^{2n} = \begin{pmatrix} (-1)^{t-1}\mathcal{L}_{2n-1} & \mathcal{L}_{2n} \\ (-1)^{t-1}\mathcal{L}_{2n} & \mathcal{L}_{2n+1} \end{pmatrix}$$

$$= (T^n)^2 = \begin{pmatrix} (-1)^{2(t-1)}\mathcal{L}_{n-1}^2 + (-1)^{t-1}\mathcal{L}_n^2 & (-1)^{t-1}\mathcal{L}_{n-1}\mathcal{L}_n + \mathcal{L}_n\mathcal{L}_{n+1} \\ (-1)^{2(t-1)}\mathcal{L}_{n-1}\mathcal{L}_n + (-1)^{t-1}\mathcal{L}_n\mathcal{L}_{n+1} & (-1)^{t-1}\mathcal{L}_n^2 + \mathcal{L}_{n+1}^2 \end{pmatrix}$$

Now considering the (1, 1) entries of those, we see that

$$\mathcal{L}_{2n-1} = (-1)^{t-1}\mathcal{L}_{n-1}^2 + \mathcal{L}_n^2 = -(p_t+q_{t-1})\mathcal{L}_{n-1}\mathcal{L}_n + 2\mathcal{L}_n^2 + (-1)^{tn-(t-1)}$$

using Corollary 7 for the second equality. Notice that using Corollary 7 removes the appearances of $\mathcal{L}_{n-1}^2$. Likewise,

$$\mathcal{L}_{2n} = -2(-1)^t\mathcal{L}_{n-1}\mathcal{L}_n + (p_t+q_{t-1})\mathcal{L}_n^2.$$

In general, $\mathcal{L}_{in-1}$ and $\mathcal{L}_{in}$ can be described in terms of $\mathcal{L}_{n-1}$ and $\mathcal{L}_n$ in that way. We formalize the idea of eliminating square powers of $\mathcal{L}_{n-1}$ as follows. We define the matrix:

$$U = \begin{pmatrix} (-1)^{t-1}a & b \\ (-1)^{t-1}b & (-1)^{t-1}a + (p_t+q_{t-1})b \end{pmatrix}.$$

U captures the symmetry of T^n. In fact, if $a = \mathcal{L}_{n-1}$ and $b = \mathcal{L}_n$, then U is T^n. We will call a polynomial in a and b a-simplified when the identity

$$a^2 = -(-1)^{-(t-1)}(p_t+q_{t-1})ab + (-1)^{-(t-1)}b^2 + (-1)^{tn-2(t-1)}$$

has been used to eliminate all appearances of a^2 and other powers of a higher than 1. Our definition generalizes the definition used in [4] and [5]. The next section gives a canonical form for the a-simplified powers of U. This canonical form allows us to identify moduli, m, which generate very short periods for the convergents of continued fractions modulo m; see Section 4.

3. PARAMETRIZING THE a-SIMPLIFIED REDUCTION FORMULAS

We define polynomials R_{2j} and S_{2j}, generalizing polynomials defined in [5], using intertwined recursions. These will be used to parametrize the reduction formulas for the $\mathcal{L}_n$-sequence. Let

$$\begin{cases} R_0 = 0,\ R_2 = 1, \text{ and } R_{2j} = S_{2j-2} + (-1)^{tn}R_{2j-4}, \\ S_0 = 2,\ S_2 = 1, \text{ and } S_{2j} = b^2dR_{2j-2} + (-1)^{tn}S_{2j-4}. \end{cases}$$

Table 2 below gives the values of R_{2j} for small j when n is even. Notice that the power of b is always twice the power of d and that the degree increases at every other term.

The table also suggests the conjecture that if $i\,|\,j$ then $R_{2i}\,|\,R_{2j}$.

TABLE 2. R_{2j} for Small j and Even n

$R_0 = 0$
$R_2 = 1$
$R_4 = 1$
$R_6 = 3 + b^2d$
$R_8 = 2 + b^2d$
$R_{10} = 5 + 5b^2d + b^4d^2$
$R_{12} = 3 + 4b^2d + b^4d^2 = (1+b^2d)(3+b^2d)$
$R_{14} = 7 + 14b^2d + 7b^4d^2 + b^6d^3$
$R_{16} = 4 + 10b^2d + 6b^4d^2 + b^6d^3 = (2+b^2d)(2+4b^2d+b^4d^2)$
$R_{18} = 9 + 30b^2d + 27b^4d^2 + 9b^6d^3 + b^8d^4 = (3+b^2d)(3+9b^2d+6b^4d^2+b^6d^3)$
$R_{20} = 5 + 20b^2d + 21b^4d^2 + 8b^6d^3 + b^8d^4 = (1+3b^2d+b^4d^2)(5+5b^2d+b^4d^2)$
$R_{22} = 11 + 55b^2d + 77b^4d^2 + 44b^6d^3 + 11b^8d^4 + b^{10}d^5$
$R_{24} = 6 + 35b^2d + 56b^4d^2 + 36b^6d^3 + 10b^8d^4 + b^{10}d^5 = (1+b^2d)(2+b^2d)(3+b^2d)(1+4b^2d+b^4d^2)$

Lemma 8:
(i) The polynomials R_{2j} and S_{2j}, with variable b, only include even degree terms.
(ii) $\deg(R_{4j-2}) = \deg(S_{4j-2}) = 2j-2$, $\deg(R_{4j}) = 2j-2$, $\deg(S_{4j}) = 2j$.
(iii) The polynomials R_{2j} and S_{2j} have positive coefficients when tn is even and is identical when tn is odd except that every other coefficient, beginning with the second highest, is the opposite of the corresponding coefficient of R_{2j} or S_{2j}.

Proof:

(i) This follows because the base cases are constants and the general recursions only involve b as b^2.

(ii) $\deg(R_{4j+2}) = \deg(S_{4j} + (-1)^{tn}R_{4j-2}) = \max(2j, 2j-2) = 2j$. Notice that the highest order term is not $(-1)^{tn}$ so there is no possibility of cancellation. The other polynomials can be checked in a similar manner.

(iii) First, we claim that R_{2j} and S_{2j} are homogeneous in the expressions b^2 and $(-1)^{tn}$. The claim is true when $j = 0$ and $j = 1$. Since $\deg(R_{2j}) = \deg(S_{2j-2})$ and $\deg(S_{2j}) = 2 + \deg(R_{2j-2})$, this homogeneity is preserved by the recursive definitions. Hence, the claim is true. Since the highest terms of R_{2j} and S_{2j} do not involve $(-1)^{tn}$, each term with lower powers of b^2 will have complementary powers of $(-1)^{tn}$. Hence, there is an alternation of sign. □

Next, we give a result which shows that certain combinations of these polynomials are 1.

Lemma 9: For $j \geq 1$,
(i) $R_{2j+2}S_{2j-2} - R_{2j}S_{2j} = (-1)^{(j-1)tn}$,
(ii) $R_{2j-2}S_{2j+2} - R_{2j}S_{2j} = -(-1)^{(j-1)tn}$.

Proof: We prove both parts simultaneously by induction. For $j = 1$,

$$R_4S_0 - R_2S_2 = 2\cdot 1 - 1\cdot 1 = 1 = (-1)^{0tn},$$
$$R_0S_4 - R_2S_2 = 0\cdot S_4 - 1\cdot 1 = -1 = -(-1)^{0tn}.$$

Assuming now that parts (i) and (ii) hold for j, consider $j+1$ in part (i):

$$\begin{aligned}R_{2j+4}S_{2j} - R_{2j+2}S_{2j+2} &= (S_{2j+2} + (-1)^{tn}R_{2j})S_{2j} - (S_{2j} + (-1)^{tn}R_{2j-2})S_{2j+2}\\ &= (-1)^{tn}(R_{2j}S_{2j} - R_{2j-2}S_{2j+2})\\ &= (-1)^{tn}(-1)^{(j-1)tn} \text{ using the induction hypothesis from (ii)}\\ &= (-1)^{jtn}.\end{aligned}$$

The induction step for part (ii) is similar. □

Theorem 10: The first row of U^{2j} after a-simplification is given by

$$\begin{aligned}v(j) = ((-1)^{tjn} + bR_{2j}((-1)^t a(p_t + q_{t-1})S_{2j} + b(-1)^{tn}dR_{2j-2}\\ + 2b(-1)^{t-1}S_{2j}),\ b(b(p_t + q_{t-1}) + 2(-1)^{t-1}a)R_{2j}S_{2j}).\end{aligned}$$

Proof: By induction on j. The first row of U^2 after a-simplification is

$$((-1)^{nt} - 2(-1)^t b^2 + (-1)^t ab(p_t + q_{t-1}),\ -2(-1)^t ab + b^2(p_t + q_{t-1})),$$

which is the same as $v(1)$. Next, we need to show that $v(j+1)$ equals the a-simplified form of $v(j)U^2$. We begin with the second components. The a-simplified form of $v(j)$ times the second column of U^2 is

$$\begin{aligned}&v(j)(2(-1)^{2t}ab - (-1)^t b^2(p_t + q_{t-1}),\ (-1)^t a(p_t + q_{t-1}) + b^2(p_t + q_{t-1})^2)\\ &= b(2(-1)^{t-1}a + b(p_t + q_{t-1}))\cdot((-1)^{jnt} + (-1)^{nt}b^2dR_{2j}R_{2j-2} + (-1)^{nt}R_{2j}S_{2j} + b^2dR_{2j}S_{2j}),\end{aligned}$$

where we have used the definition of d to simplify. Using Lemma 9(i), we can replace $(-1)^{jnt}$ by R and S polynomials. Thus, the third factor of the above is

$$\begin{aligned}&(-1)^{nt}R_{2j+2}S_{2j-2} - (-1)^{nt}R_{2j}S_{2j} + (-1)^{nt}b^2dR_{2j}R_{2j-2} + (-1)^{nt}R_{2j}S_{2j} + b^2dR_{2j}S_{2j}\\ &= b^2dR_{2j}(S_{2j} + (-1)^{nt}R_{2j-2}) + (-1)^{nt}R_{2j+2}S_{2j-2}\\ &= b^2dR_{2j}R_{2j+2} + (-1)^{nt}R_{2j+2}S_{2j-2} = R_{2j+2}S_{2j+2}.\end{aligned}$$

Thus, the second component of $v(j)$ times the second column of U^2 is

$$b(2(-1)^{t-1}a + b(p_t + q_{t-1}))R_{2j+2}S_{2j+2}.$$

On the other hand, the second component of $v(j+1)$ is the same thing, which checks the induction step for the second component.

The first component can be checked in a similar, but more tedious, manner. □

Consider when $j = 3$ and $\alpha = [\overline{1, 1, 2}]$, for example. Then, by Theorem 10, the first row of U^6 after a-simplification is

$$((-1)^{9n}+bR_6((-1)^3a(p_3+q_2)S_6+b((-1)^{3n}dR_4+2(-1)^2S_6)),\ b(b(p_3+q_2)+2(-1)^2a)R_6S_6),$$

where $R_6=3+b^2d$, $R_4=1$, and $S_6=1+b^2d$. Now, letting $a=\mathcal{L}_{n-1}$, $b=\mathcal{L}_n$, $d=40$, and $p_3+q_2=6$, we get reduction formulas for $\mathcal{L}_{6n-1}$ and $\mathcal{L}_{6n}$ in terms of $\mathcal{L}_{n-1}$ and $\mathcal{L}_n$:

$$\mathcal{L}_{6n-1}=(-1)^{9n}+\mathcal{L}_n(3+40\,\mathcal{L}_n^2)((-1)6\,\mathcal{L}_{n-1}(1+40\,\mathcal{L}_n^2)+\mathcal{L}_n(40(-1)^{3n}+2(1+40\,\mathcal{L}_n^2)))$$

and

$$\mathcal{L}_{6n}=\mathcal{L}_n(6\,\mathcal{L}_n+2\,\mathcal{L}_{n-1})(3+40\,\mathcal{L}_n^2)(1+40\,\mathcal{L}_n^2).$$

In particular, let $n=4$, then $\mathcal{L}_3=37$, $\mathcal{L}_4=288$, so

$$\begin{aligned}\mathcal{L}_{23}&=1+228(3+40(228)2)((-6)(37)(1+40(228)^2)+228(40+2(1+40(228)^2)))\\&=230684837784645817\end{aligned}$$

and

$$\begin{aligned}\mathcal{L}_{24}&=228(6(228)+2(37))(3+40(228)^2)(1+40(228)^2)\\&=1421544022419889368,\end{aligned}$$

which are straightforward and unpleasant to check.

Corollary 11: Let $j\ge 1$. The first row of U^{2j+1} after a-simplification is given by

$$\begin{aligned}&((-1)^t(-(-1)^{jnt}a-bR_{2j}(abdR_{2j+2}+S_{2j}(-1)^{(n-1)t}(p_t+q_{t-1}))),\\&\qquad b((-1)^{jnt}+R_{2j}(b^2dR_{2j+2}+2S_{2j}(-1)^{nt}))).\end{aligned}$$

Proof: Multiplying out $v(j)U$ and a-simplifying yields

$$\begin{aligned}&((-1)^t(-(-1)^{jnt}a+bR_{2j}(-(-1)^{tn}abdR_{2j-2}+S_{2j}(4(-1)^tab-(-1)^{(n-1)t}(p_t+q_{t-1})-ab(p_t+q_{t-1})^2))),\\&\qquad b((-1)^{jnt}+R_{2j}((-1)^{nt}b^2dR_{2j-2}+S_{2j}(2(-1)^{nt}-4(-1)^tb^2+b^2(p_t+q_{t-1})^2)))).\end{aligned}$$

The recursive definition for R_{2j+2} and the definition for d simplifies this into the desired result. $\square$

Consider when $j=4$ and $\alpha=[\overline{1,1,2}]$, for example. Then, by Corollary 11, the first row of U^9 after a-simplification is

$$((-1)^3(-(-1)^{12n}a-bR_8(abdR_{10}+S_8(-1)^{3(n-1)}(p_3+q_2))),\ b((-1)^{12n}+R_8(b^2dR_{10}+2S_8(-1)^{3n}))),$$

where $R_8=2+b^2d$, $S_8=2+4b^2d+b^4d^2$ and $R_{10}=5+5b^2d+b^4d^2$, as seen in Table 2 and from the recursive definition of S_{2j}. Letting $a=\mathcal{L}_n$, $b=\mathcal{L}_n$, $d=40$, and $p_3+q_2=6$, we get reduction formulas for $\mathcal{L}_{9n-1}$ and $\mathcal{L}_{9n}$ in terms of $\mathcal{L}_{n-1}$ and $\mathcal{L}_n$:

$$\begin{aligned}\mathcal{L}_{9n-1}=&-(-\mathcal{L}_{n-1}-\mathcal{L}_n(2+40\,\mathcal{L}_n^2)(40\,\mathcal{L}_{n-1}\mathcal{L}_n(5+200\,\mathcal{L}_n^2+40^2\,\mathcal{L}_n^4)\\&+6(-1)^{3(n-1)}(2+160\,\mathcal{L}_n^2+40^2\,\mathcal{L}_n^2)))\end{aligned}$$

and

$$\mathcal{L}_{9n}=\mathcal{L}_n(1+(2+40\,\mathcal{L}_n^2)((40\,\mathcal{L}_n^2)(5+200\,\mathcal{L}_n^2+40^2\,\mathcal{L}_n^2)+2(-1)^{nt}(2+160\,\mathcal{L}_n^2+40^2\,\mathcal{L}_n^4))).$$

Let $n=4$, then $\mathscr{L}_3 = 37, \mathscr{L}_4 = 228$, so

$$\begin{aligned}\mathscr{L}_{35} &= -(-37-228(2+40(228)^2)(40(37)(228)(5+200(228)^2+(40)^2(228)^4)\\ &\quad -6(2+160(228)^2+(40)^2(228)^4)))\\ &= 6916943132821966691278601\,65\end{aligned}$$

and

$$\begin{aligned}\mathscr{L}_{36} &= 228(1+(2+40(228)^2)(40(228)^2(5+200(228)^2+(40)^2(228)^4)\\ &\quad +2(2+160(228)^2+(40)^2(228)^4)))\\ &= 42624124144043888363109140\,52,\end{aligned}$$

which are correct.

4. SHORT PERIODS

The following theorem is our main result. It gives families of moduli with short periods. These families are given by divisors of the polynomials $bR_{2j}(b)$ evaluated at numbers in the $\mathscr{L}_n$-sequence.

Theorem 12: Let m divide $\mathscr{L}_n R_{2j}(\mathscr{L}_n)$.

(i) If t is even, then $k(m)|4jnt$.

(ii) If t is odd but jnt is even, then $k(m)|2jnt$.

(iii) If jnt is odd, then $k(m)|4jnt$.

Proof: First, consider (i) and (ii), where we have jnt is even. Let $a=\mathscr{L}_{n-1}$ and $b=\mathscr{L}_n$ in Theorem 10 and note that all the terms of $v(j)$ are divisible by m except the $(-1)^{jnt}$. With this substitution, $v(j)$ gives the a-simplification of the first row of T^{2jn}. Also using Theorem 6, we see that $v(j)\equiv(1,0)\equiv((-1)^{t-1}\mathscr{L}_{2jn-1},\mathscr{L}_{2jn})$. Thus, $\mathscr{L}_{2jn-1}\equiv(-1)^{t-1} \bmod m$ and $\mathscr{L}_{2jn}\equiv 0 \bmod m$. Hence, by Theorem 5, $k(m)|4jnt$ if t is even and $k(m)|2jnt$ if t is odd.

Now, in part (iii), jnt is odd. The same idea as above works except that $v(j)\equiv(-1,0)\equiv((-1)^{t-1}\mathscr{L}_{2jn-1},\mathscr{L}_{2jn})$. Thus, $\mathscr{L}_{2jn-1}\equiv -1 \bmod m$ and $\mathscr{L}_{2jn}\equiv 0 \bmod m$. Now the identities for $\mathscr{L}_{2n-1}$ and $\mathscr{L}_{2n}$ given after Corollary 7 allow us to see that $\mathscr{L}_{4jn-1}\equiv 1$ (remember t is odd), and $\mathscr{L}_{4jn}\equiv 0$. Now Theorem 5 gives $k(m)|4jnt$ as desired. □

Notice that the bounds for k in all cases are linear in n, while $\mathscr{L}_n$, and hence the modulus, is exponential in n. Thus, we can construct families of moduli having periods logarithmic in the modulus. In Table 3, the example of $\alpha=[\overline{1,1,2}]$ with $m=R_6(\mathscr{L}_n)$ is considered. Notice the large m.

Now we can explain, up to a factor of 2, all of the periods less than the linear upper bounds given for the primes in Table 1. Table 4 gives a list of $R_{2j}(\mathscr{L}_n)$ that are divisible by those primes. The upper bounds for the periods given in Theorem 12 fully explain the periods that actually occur in this table, except those marked with an asterisk where the upper bound is twice the actual period.

TABLE 3

Logarithmic Bounds on Periods for a Family of Moduli for $\alpha = [\overline{1, 1, 2}]$

n	$\mathcal{L}_n$	$m = R_6(\mathcal{L}_n)$	$2jnt$
2	6	1443	36
4	228	2079363	72
6	8658	2998438563	108
8	328776	4323746327043	144
10	12484830	6234839205156003	180
12	474094764	8990633810088627843	216
14	18003116202	12964487719308596192163	252
n	$\mathcal{L}_n$	$m = R_6(\mathcal{L}_n)$	$4jnt$
1	1	37	36
3	37	54757	108
5	1405	78960997	180
7	53353	113861704357	252
9	2026009	164188498723237	324
11	76934989	236759701297204837	396
13	2921503573	341407325082070653157	468
15	110940200785	492309126008644584648997	540

TABLE 4

Values of $R_{2j}(\mathcal{L}_n)$ Explaining Short Periods

*13	$R_6(\mathcal{L}_2)$	281	$R_{10}(\mathcal{L}_2)$	*677	$R_{26}(\mathcal{L}_{26})$
19	$R_8(\mathcal{L}_1)$	*317	$R_{158}(\mathcal{L}_2)$	733	$R_{122}(\mathcal{L}_2)$
37	$R_6(\mathcal{L}_1)$	*397	$R_{18}(\mathcal{L}_{22})$	761	$R_{10}(\mathcal{L}_{38})$
*53	$R_{26}(\mathcal{L}_2)$	419	$R_6(\mathcal{L}_{20})$	*773	$R_{386}(\mathcal{L}_2)$
59	$R_8(\mathcal{L}_5)$	*431	$R_{86}(\mathcal{L}_2)$	*797	$R_{398}(\mathcal{L}_2)$
*67	$R_{22}(\mathcal{L}_2)$	*439	$R_{146}(\mathcal{L}_2)$	809	$R_{202}(\mathcal{L}_2)$
103	$R_8(\mathcal{L}_2)$	449	$R_8(\mathcal{L}_7)$	821	$R_{274}(\mathcal{L}_2)$
131	$R_6(\mathcal{L}_4)$	461	$R_{14}(\mathcal{L}_{11})$	*827	$R_{118}(\mathcal{L}_2)$
137	$R_{46}(\mathcal{L}_2)$	491	$R_{82}(\mathcal{L}_4)$	829	$R_{166}(\mathcal{L}_2)$
167	$R_8(\mathcal{L}_{14})$	503	$R_6(\mathcal{L}_{24})$	*853	$R_{142}(\mathcal{L}_6)$
179	$R_6(\mathcal{L}_{20})$	*521	$R_{26}(\mathcal{L}_{10})$	857	$R_{26}(\mathcal{L}_2)$
*191	$R_{38}(\mathcal{L}_2)$	571	$R_8(\mathcal{L}_{13})$	859	$R_8(\mathcal{L}_5)$
*197	$R_{14}(\mathcal{L}_{14})$	601	$R_{10}(\mathcal{L}_{15})$	881	$R_8(\mathcal{L}_{22})$
233	$R_6(\mathcal{L}_{26})$	*613	$R_{14}(\mathcal{L}_{18})$	*883	$R_{14}(\mathcal{L}_{14})$
*241	$R_6(\mathcal{L}_{10})$	*631	$R_{28}(\mathcal{L}_{15})$	*911	$R_{26}(\mathcal{L}_{14})$
*263	$R_{16}(\mathcal{L}_{22})$	647	$R_6(\mathcal{L}_{24})$	929	$R_{16}(\mathcal{L}_{29})$
*271	$R_6(\mathcal{L}_{10})$	*653	$R_{326}(\mathcal{L}_2)$	937	$R_{134}(\mathcal{L}_2)$
277	$R_{46}(\mathcal{L}_2)$	659	$R_{22}(\mathcal{L}_{20})$	*997	$R_{166}(\mathcal{L}_6)$

ACKNOWLEDGMENTS

This work was supported in part by the NSF REU grant DMS-9300555 and by Lafayette College. The authors appreciate the help of the referee and J. C. Lagarias. Their suggestions led to many improvements in the paper.

REFERENCES

1. R. Bateman, E. Clark, M. Hancock, & C. Reiter. "The Period of Convergents Modulo *M* of Reduced Quadratic Irrationals." *The Fibonacci Quarterly* **29.3** (1991):220-29.
2. L. Dickson. *History of the Theory of Numbers*, Vol. 1, Ch. 17. New York: Chelsea, 1923; rpt. 1971.
3. Amos Ehrlich. "On the Periods of the Fibonacci Sequence Modulo *m*." *The Fibonacci Quarterly* **27.1** (1989):11-13.
4. C. Reiter. "Fast Fibonacci Numbers." *The Mathematica Journal* **2.3** (1992):58-60.
5. C. Reiter. "Fibonacci Numbers: Reduction Formulas and Short Periods." *The Fibonacci Quarterly* **31.4** (1993):315-24.
6. D. D. Wall. "Fibonacci Series Modulo *m*." *Amer. Math. Monthly* **67** (1960):525-32.

AMS Classification Numbers: 11B50, 11A55