THE PERIOD OF CONVERGENTS MODULO M OF REDUCED QUADRATIC IRRATIONALS*

Roger A. Bateman
Student, Albright College, Reading, PA 19612

Elizabeth A. Clark
Student, Messiah College, Grantham, PA 17027

Michael L. Hancock
Student, Shippensburg University, Shippensburg, PA 17257

Clifford A. Reiter
Lafayette College, Easton, PA 18042
(Submitted August 1989)

Introduction

The properties of the period lengths of the continued fraction convergents modulo m of reduced quadratic irrationals are studied in this paper. These period lengths vary wildly, yet will be shown to satisfy strong divisibility properties. Wall [6] studied these period lengths for the Fibonacci numbers that arise as convergents of the simple continued fraction with all partial quotients equal to 1. Many other papers, including [1], [3], [4], and [5], extend and complement those results. Some of the theorems in Wall extend in a direct manner to the continued fraction investigation given here; however, a key theorem of Wall about occurrences of zeros does not generalize so that new approaches are required. In some cases, known properties of continued fractions, for a reference see Rosen [2], yield simpler proofs for the analogs of theorems from Wall. Two theorems presented here give properties of the periods for reversals and rotations of the continued fractions which have no analogs from the Fibonacci numbers. Matrix computation of the convergents is developed and analyzed to produce further results including remarkably good bounds on the period lengths.

Definition of the Period

Reduced quadratic irrationals, denoted α in this paper, are those real numbers that have purely periodic simple continued fraction expansions. Consider such an α:

$$\alpha = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; a_t + \cfrac{1}{\alpha}}}$$

where $a_i \in \mathbb{Z}^+$ and t is chosen as small as possible. This is abbreviated by $\alpha = [\overline{a_1, a_2, \ldots, a_t}]$, where t is said to be the *period* of α. Associated with each continued fraction are the p,q sequences defined in the following manner:

$$p_{-1} = 0,\ p_0 = 1,\ p_n = a_n p_{n-1} + p_{n-2},$$
$$q_{-1} = 1,\ q_0 = 0,\ q_n = a_n q_{n-1} + q_{n-2}.$$

*This work was done at Moravian College during an NSF REU program which was supported by grant DMS-8900839.

We illustrate the calculation of these sequences with $\alpha = (1 + \sqrt{3})/2 = [\overline{1, 2}]$.

a_n:			1	2	1	2	1	2	1	2	1	2
p_n:	0	1	1	3	4	11	15	41	56	153	209	571
q_n:	1	0	1	2	3	8	11	30	41	112	153	418

Below are the values in this table modulo 2. One can see that the sequence p_n, the sequence q_n, and both sequences taken together are all periodic.

a_n:			1	0	1	0	1	0	1	0	1	0
p_n:	0	1	1	1	0	1	1	1	0	1	1	1
q_n:	1	0	1	0	1	0	1	0	1	0	1	0

Theorem 1: The p,q sequence modulo m is purely periodic.

Proof: Consider the 2×2 block of p's and q's (mod m) at $st - 1$ and st, where $s = 0, 1, 2, \ldots$ and t is the period of α. Since there are only m^4 possibilities for this block, it eventually repeats so that, for some i, j, say with $i < j$,

$$p_{it-1} \equiv p_{jt-1},\ p_{it} \equiv p_{jt},$$
$$q_{it-1} \equiv q_{jt-1},\ q_{it} \equiv q_{jt} \pmod{m}.$$

Since $a_{it+n} = a_{jt+n}$, the defining relations give that the p,q sequence repeats. Also, from the defining relations, we see that

$$p_{it-2} = p_{it} - a_{it}p_{it-1} \equiv p_{jt} - a_{jt}p_{jt-1} = p_{jt-2}$$
$$p_{it-3} = p_{it-1} - a_{it-1}p_{it-2} \equiv p_{jt-1} - a_{jt-1}p_{jt-2} = p_{jt-3}$$
$$\vdots$$
$$p_{it-(it-1)} = p_1 \equiv p_{jt-(it-1)} = p_{(j-i)t+1}.$$

The same argument holds for the q sequence. Therefore, the p,q sequence is purely periodic. □

The *period of the p,q sequence modulo m* is denoted $k(\alpha, m)$, or $k(m)$, or k if no ambiguity occurs. It is evident from the proof of this theorem that $k(\alpha, m) \leq m^4 t$. The remainder of this paper will explore the properties of $k(\alpha, m)$.

Elementary Properties

In light of the initial conditions for the p,q sequences and the definition of k, we get an immediate corollary.

Corollary 2: When $k = k(m)$, then $p_{k-1} \equiv 0$, $p_k \equiv 1$, $q_{k-1} \equiv 1$, and $q_k \equiv 0$ modulo m.

Next is a theorem which establishes that k is even for all moduli greater than 2.

Theorem 3: If $m > 2$, then $k(m)$ is even.

Proof: Suppose that $k = k(m)$ is odd. Then, by using the continued fraction identity $p_k q_{k-1} - p_{k-1}q_k = (-1)^k$ and substituting the values of the p,q sequence from the corollary into this equation, we have $(1)(1) - (0)(0) = -1 \bmod m$. Therefore, $2 \equiv 0 \bmod m$, which implies a modulus of 2. □

Theorem 4: If $m_1 | m_2$, then $k(m_1) | k(m_2)$.

Proof: Let $k = k(m_2)$ and $m_1 | m_2$, then $m_2 | p_{k-1}$ implies $m_1 | p_{k-1}$, and $m_2 | q_{k-1} - 1$ implies $m_1 | q_{k-1} - 1$. Likewise, for $p_k - 1$ and q_k. Hence, $k(m_1) | k(m_2)$. □

The following theorem shows that, if the periods of the prime power factors of a modulus are known, then the period of the modulus can readily be calculated.

Theorem 5: If m has the prime factorization $m = \prod p_i^{e_i}$ and if k_i denotes the length of the period of the p,q sequence mod $p_i^{e_i}$, then $k(m) = \text{lcm}[k_i]$.

Proof: Since $k_i | k$ for all i, $\text{lcm}[k_i] | k$. On the other hand, since $p_k \equiv 1 \bmod p_i^{e_i}$ for all i, $p_k \equiv 1 \bmod \text{lcm}[p_i^{e_i}]$. Similarly, $p_{k-1} \equiv 0$, $q_{k-1} \equiv 1$, $q_k \equiv 0$. Therefore, $k | \text{lcm}[k_i]$. □

For the sequence of Fibonacci numbers modulo m, the zeros are known to be in arithmetic progression. The placement of zeros is not simple for continued fractions in general. Consider an example with $m = 3$:

a_n:		3 5 2	3 5 2	3 5 2	3 5 2	3 5 2	3 5 2	3 5 2	3 5 2
p_n: 0 1		0 1 2	1 1 0	1 2 2	2 0 2	0 2 1	2 2 0	2 1 1	1 0 1
q_n: 1 0		1 2 1	2 0 2	0 2 1	2 2 0	2 1 1	1 0 1	0 1 2	1 1 0

The theorem below begins giving insight into the structure of the convergents without controlling the zeros.

Notice that, for some α's and moduli m, the period of α reduces mod m. For example, $\alpha = [1, 2, 3, 4] \bmod 2$ is "the same as" $[1, 2] \bmod 2$. We say the period of α is *preserved* modulo m when this does not occur. It is frequently convenient to restrict consideration of $k(\alpha, m)$ to the case where the period of α is preserved modulo m. Of course, one can get information about $k(\alpha, m)$ when the period of α is not preserved. For example, one can consider $[1, 2]$ instead of $[1, 2, 3, 4]$ when the modulus is 2.

The next theorem states that $k(\alpha, m)$ is always a multiple of the period of α. This is useful information about the structure of the periods and also gives a trivial lower bound.

Theorem 6: If $\alpha = [\overline{a_1, a_2, \ldots, a_t}]$ and the period of α is preserved mod m, then $t | k(m)$.

Proof: Suppose that $k = k(m)$, then $p_n \equiv p_{n+k}$ for $n = 1, 2, \ldots$. So,

$$a_n p_{n-1} + p_{n-2} \equiv a_{n+k} p_{n+k-1} + p_{n+k-2} \bmod m.$$

Thus,

$$a_n p_{n-1} \equiv a_{n+k} p_{n+k-1} \equiv a_{n+k} p_{n-1}.$$

Similarly,

$$a_n q_{n-1} \equiv a_{n+k} q_{n-1} \bmod m.$$

Multiplying the congruences by q_n and p_n, respectively, and subtracting gives

$$\begin{aligned} a_n(-1)^{n-1} &= a_n(q_n p_{n-1} - p_n q_{n-1}) \equiv a_{n+k}(q_n p_{n-1} - p_n q_{n-1}) \\ &= a_{n+k}(-1)^{n-1}. \end{aligned}$$

It follows that $a_n \equiv a_{n+k} \bmod m$ and, therefore, $t | k(m)$. □

The hypothesis that the period of α is preserved mod m is indeed necessary, since for $\alpha = [1, 2, 3, 4, 5, 6]$, $t = 6 \nmid 4 = k(\alpha, 2)$ and α reduced mod 2 is "the same as" $[1, 2]$.

It is now known that in order to determine $k(m)$ one need only look at the $nt - 1$ and nt places in the p,q sequence, where $n = 1, 2, \ldots$.

Corollary 7: If the period of α is preserved mod m, the period length k is of the form $k = ct$, where c is the smallest positive integer with

$$p_{ct-1} \equiv 0, \quad p_{ct} \equiv 1, \quad q_{ct-1} \equiv 1, \quad q_{ct} \equiv 0.$$

Matrix Formulation

The following theorems allow us to look at only these blocks of integers without going through the intermediate calculations. First, we establish the following lemma.

Lemma 8: Define $r_n = a_n r_{n-1} + r_{n-2}$ with initial conditions $r_{-1} = a$, $r_0 = b$, where $a, b \in \mathbb{Z}^+$. Then $r_n = bp_n + aq_n$.

Proof: For $n = -1$ and $n = 0$, the relation holds trivially. Now suppose that $r_n = bp_n + aq_n$ and $r_{n+1} = bp_{n+1} + aq_{n+1}$. Then,

$$r_{n+2} = a_{n+2}(bp_{n+1} + aq_{n+1}) + bp_n + aq_n = bp_{n+2} + aq_{n+2}. \quad \square$$

We now define a matrix W called the *fundamental matrix* which depends only on α and that can be used to compute the blocks of convergents at the end of blocks of length t.

Theorem 9: Let

$$W = \begin{pmatrix} q_{t-1} & q_t \\ p_{t-1} & p_t \end{pmatrix}; \quad \text{then} \quad W^n = \begin{pmatrix} q_{nt-1} & q_{nt} \\ p_{nt-1} & p_{nt} \end{pmatrix}.$$

Proof: Consider the function F_α: $\mathbb{Z}^2 \to \mathbb{Z}^2$ which takes an initial condition pair (a, b) to the pair (r_{t-1}, r_t) giving the last two terms resulting from applying one period of recursions $r_j = a_j r_{j-1} + r_{j-2}$, $j = 1, \ldots, t$, to initial conditions $r_{-1} = a$, $r_0 = b$. In light of the lemma, F_α can be written in matrix form:

$$F_\alpha(a, b) = (a, b)W.$$

On the other hand, applying n periods of the recursions is just n iterations of F_α and (p_{nt-1}, p_{nt}) is the result of applying n periods of the recursion to $(0, 1)$. Hence,

$$(p_{nt-1}, p_{nt}) = F_\alpha^n(0, 1) = (0, 1)W^n.$$

Likewise,

$$(q_{nt-1}, q_{nt}) = (1, 0)W^n$$

and the conclusion follows. $\square$

Notice in the example below that W, W^2, and W^3 appear upside down in the list of convergents of $\alpha = [\overline{3, 5, 2}]$.

$$W = \begin{pmatrix} 5 & 11 \\ 16 & 35 \end{pmatrix}, \quad W^2 = \begin{pmatrix} 201 & 440 \\ 640 & 1401 \end{pmatrix}, \quad W^3 = \begin{pmatrix} 8045 & 17611 \\ 25616 & 56075 \end{pmatrix},$$

a_k:		3	5	2	3	5	2	3	5	2
p_k:	0 1	3	16	35	121	640	1401	4843	25616	56075
q_k:	1 0	1	5	11	38	201	440	1521	8045	17611

The following corollary is a direct consequence of Theorem 9 and Corollary 7.

Corollary 10:

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

(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 $k(m) = ct$.

Remark: If p is an odd prime, the order of the multiplicative group of matrices $\{A \in M_2(\mathbb{Z}_p) \mid \det(A) = \pm 1\}$ is $2(p + 1)p(p - 1)$ and it follows that

$$k(p) \mid 2(p + 1)p(p - 1)t.$$

This establishes a slightly better upper bound for $k(p)$ than the p^4t observed earlier. Furthermore, this remark limits the factors appearing in $k(p)$.

Reversals and Rotations

Given an $\alpha = [\overline{a_1, a_2, \ldots, a_t}]$, we construct other quadratic irrationals related to α: the *reversal* of α, $\alpha^\phi = [a_t, a_{t-1}, \ldots, a_1]$ and the *rotation* of by one position, $\alpha^* = [a_t, a_1, a_2, \ldots, a_{t-1}]$. The rotation of α by j positions to the right is indicated by α^{*j}. The following theorems show that $k(\alpha, m)$ is not changed when α is reversed or rotated. Thus, if we know $k(\alpha, m)$, then we really know $k(m)$ for up to $2t$ different quadratic irrationals.

Theorem 11: $k(\alpha, m) = k(\alpha^*, m) = k(\alpha^{*2}, m) = \ldots = k(\alpha^{*t-1}, m)$.

Proof: First, notice that if the period of α is not preserved mod m, then the period of α^{*j} is not preserved mod m for all j. If $\alpha = [\overline{a_1, a_2, \ldots, a_t}]$ degenerates into $\alpha' = [\overline{a_1, a_2, \ldots, a_{t'}}]$ mod m. That is, t' is the smallest positive integer so that for all j, $a_j \equiv a_{j+t'} \bmod m$. Then for all j, $k(\alpha^{*j}, m) = k(\alpha'^{*j}, m)$, but the period of α' is preserved mod m. Thus, without loss of generality, we will assume the period of α is preserved mod m.

Let W be the fundamental matrix for α, let c be the smallest positive integer with $W^c \equiv I \bmod m$, let F_α be the function as in the proof of Theorem 8 which gives the last two terms resulting from applying one α period of recursions to given initial conditions, and let p_n^*, q_n^* denote the p,q sequence for α^*.

Note that $\alpha^* = [a_t, \overline{a_1, a_2, \ldots, a_t}]$. Thus, (p_t^*, p_{t+1}^*) arise from applying one period of the α recursion relations to initial condition (p_0^*, p_1^*). That is,

$$(p_t^*, p_{t+1}^*) = F_\alpha(p_0^*, p_1^*) = (p_0^*, p_1^*)W$$

and applying "c" periods of the α recursions gives

$$(p_{ct}^*, p_{ct+1}^*) = F_\alpha^c(p_0^*, p_1^*) = (p_0^*, p_1^*)W^c.$$

Likewise for the q sequence. Thus, $k(\alpha^*, m) \mid k(\alpha, m)$. Applying this fact to further rotations gives

$$k(\alpha, m) = k(\alpha^{*t}, m) \mid k(\alpha^{*t-1}, m) \mid \ldots \mid k(\alpha^*, m) \mid k(\alpha, m)$$

and, hence, the required equalities must hold. □

Theorem 12: $k(\alpha, m) = k(\alpha^\phi, m)$.

Proof: If $k = k(\alpha, m)$, then, from well-known identities (see Rosen [2, p. 363]) of continued fractions $p_k^\phi/q_k^\phi = p_k/p_{k-1}$ and $p_{k-1}^\phi/q_{k-1}^\phi = q_k/q_{k-1}$. Therefore,

$$p_{k-1}^\phi = q_k \equiv 0, \quad p_k^\phi = p_k \equiv 1,$$
$$q_{k-1}^\phi = q_{k-1} \equiv 1, \quad q_k^\phi = p_{k-1} \equiv 0,$$

which implies $k(\alpha^\phi, m) \mid k(\alpha, m)$. It is evident that $k(\alpha^\phi, m) = k(\alpha, m)$ since, by applying the process on α^ϕ, we obtain $k(\alpha, m) \mid k(\alpha^\phi, m)$. □

Periods of Powers of Primes

The relation between $k(\alpha, p)$ and $k(\alpha, p^e)$ is explored next. Consider the periods of $\alpha = [\overline{1, 1, 1, 1, 1, 2}]$ for several prime power moduli.

p	$k(\alpha, p)$	$k(\alpha, p^2)$	$k(\alpha, p^3)$	$k(\alpha, p^4)$
2	12	24	48	96
3	18	18	18	54
5	36	36	180	900
7	84	588	4116	28812

Notice when the exponent of p in the modulus is increased by one the period seems to "increase" by a factor of p or 1. Indeed, the following theorems show that as the exponent of p increases the period $k(p^e)$ will increase by a factor of p after some initial constant sequence. An exception is $p = 2$, which is slightly more complicated.

It is interesting to note that for the analogous theorem of Wall [6] about the Fibonacci numbers there are no known examples with $k(p) = k(p^2)$. For the α given above, $k(p) = k(p^e)$ for some $e > 1$ does occur. Identifying when this occurs remains an open problem.

We now turn to proving the above properties. Let A be a matrix with integer entries. If p^e divides each element of A but p^{e+1} does not divide some element of A, we say p^e *exactly divides* A, and write $p^e \| A$. This means that A can be written $A = p^e S$ for some matrix S with integer entries where S contains an element which is not divisible by p.

Lemma 13: Let U be a matix with integer entries, I be the identity matrix, and p be an odd prime number. If $p^e \| U - I$ for some $e \geq 1$, then $p^{e+1} \| U^p - I$. Moreover, for $p = 2$, if $e \geq 2$ and $2^e \| U - I$, then $2^{e+1} \| U^2 - I$.

Proof: Suppose first that p is an odd prime with $p^e \| U - I$, so $U = I + p^e S$ where S is a matrix with integer entries and p does not divide some entry in S. The binomial theorem is not true for matrices in general, but it is true when one of the matrices is the identity. The third and higher terms of the binomial expansion below have at least two factors of p^e plus another factor of p coming from the binomial coefficient or from an additional factor of p^e. Thus, for some matrix T, we have

$$U^p = (I + p^e S)^p = \sum_{j=0}^{p} \binom{p}{j} p^{je} S^j = \binom{p}{0} I + \binom{p}{1} p^e S + p^{2e+1} T.$$

Thus, $U^p - I = p^{e+1} S + p^{2e+1} T$. Notice that $p^{e+1} \mid U^p - I$ and that if p^{e+2} did, then p would divide all the elements of S, which contradicts the hypothesis. Therefore, $p^{e+1} \| U^p - I$ as required.

Similarly, if $p = 2$ and $2^e \| U - I$, U has the same form as above and

$$U^2 = I + 2^{e+1} S + 2^{2e} S^2.$$

Thus, $2^{e+1} \mid U^2 - I$. Now, for $e \geq 2$, $2e \geq e + 2$ so that if $2^{e+2} \mid U^2 - I$ then $2 \mid S$, which is not so. Thus, $2^{e+1} \| U^2 - I$. □

Theorem 14: Let p be an odd prime which preserves the period of α. There is a positive integer e so that

$$k(p) = k(p^2) = \cdots = k(p^e) \quad \text{and} \quad k(p^{e+j}) = p^j k(p) \text{ for all } j \geq 1.$$

Moreover, for $p = 2$ there is an integer $e \geq 2$ such that

$$k(2^2) = k(2^3) = \cdots = k(2^e) \quad \text{and} \quad k(2^{e+j}) = 2^j k(2) \text{ for all } j \geq 1.$$

Also, $k(2) = k(4)$ or $k(2) = \frac{1}{2} k(4)$.

Proof: Let p be an odd prime and W be the fundamental matrix for α. Notice that p^n preserves the period of α for all n. So, by Corollary 10, $k(p^e) = nt$ if and only if n is the smallest positive integer with $W^n \equiv I \bmod p^e$. Select c to be the smallest exponent for which $W^c \equiv I \bmod p$. Then let e be the largest exponent (possibly 1) for which $k(p) = k(p^2) = \cdots = k(p^e)$. Notice that e must be finite, since for large enough e, p^e will be larger than the entries in W^c and, hence, $W^c \not\equiv I \bmod p^e$. Now $p^e \| W^c - I$ so that, by the lemma, $p^{e+1} \| W^{pc} - I$. Thus, $ct = k(p^e) \mid k(p^{e+1}) \mid pct$. So, $k(p^{e+1}) = ct$ or pct. If $k(p^{e+1}) = ct$, then $p^{e+1} \mid W^c - I$, which is impossible since $p^e \| W^c - I$. Therefore, $k(p^{e+1}) = pk(p^e)$. Continuing inductively gives $k(p^{e+j}) = p^j k(p^e)$.

Moreover, for $p = 2$, the same argument works beginning with $k(2^2)$, since the lemma used requires $e \geq 2$ in this case. Also, if $W^e \equiv I \bmod 2$, then for some matrix T, $W^e = I + 2T$; hence, $W^{2e} \equiv I \bmod 4$ and the ratio $k(4)/k(2)$ is 1 or 2. □

The special possibilities mentioned in the theorem for $p = 2$ do occur as indicated by the examples:

α	$k(2)$	$k(4)$	$k(8)$	$k(16)$	$k(32)$
$[\overline{1, 2}]$	4	8	8	16	32
$[\overline{1, 1, 2}]$	6	12	24	48	96
$[\overline{1, 2, 3}]$	6	6	12	24	48

Bounds for Prime Periods

It was shown in Corollary 10 that e is the smallest positive integer such that $W^e \equiv I \bmod m$ if $k(m) = et$. To facilitate the analysis of W^e, we diagonalize the fundamental matrix. The eigenvalues of this matrix are

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

where

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

It is evident from the definitions of λ_1 and λ_2 that

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

These identities are used in the following lemmas and theorems. Computing the eigenvectors and completing the diagonalization, we find the following form for W^n.

Theorem 15: Let W be the fundamental matrix for α and let $\mathscr{L}_n = (\lambda_1^n - \lambda_2^n)/\sqrt{d}$. Then,

$$W^n = \begin{bmatrix} (-1)^{t-1}\mathscr{L}_{n-1} + q_{t-1}\mathscr{L}_n & q_t\mathscr{L}_n \\ p_{t-1}\mathscr{L}_n & \mathscr{L}_{n+1} - q_{t-1}\mathscr{L}_n \end{bmatrix} \quad \text{for } n = 1, 2, \ldots .$$

Proof: The fundamental matrix can be diagonalized by the matrix P, where

$$P = \begin{bmatrix} q_t & q_t \\ \lambda_1 - q_{t-1} & \lambda_2 - q_{t-1} \end{bmatrix} \quad \text{and} \quad P^{-1} = \frac{-1}{q_t\sqrt{d}} \begin{bmatrix} \lambda_2 - q_{t-1} & -q_t \\ -(\lambda_1 - q_{t-1}) & q_t \end{bmatrix}.$$

Computing $W^n = PD^nP^{-1}$, where D is the diagonal matrix with λ_1 and λ_2 on the diagonal, we get

$$W^n = \frac{1}{q_t\sqrt{d}} \begin{bmatrix} q_t((\lambda_1 - q_{t-1})\lambda_2^n - (\lambda_2 - q_{t-1})\lambda_1^n) & q_t^2(\lambda_1^n - \lambda_2^n) \\ -(\lambda_1 - q_{t-1})(\lambda_2 - q_{t-1})(\lambda_1^n - \lambda_2^n) & q_t(\lambda_1^n(\lambda_1 - q_{t-1}) - \lambda_2^n(\lambda_2 - q_{t-1})) \end{bmatrix}.$$

This simplifies into the required matrix using the properties of the eigenvalues. □

Remark: An interesting consequence of this diagonalization is that

$$p_{nt-1}q_t = q_{nt}p_{t-1} \text{ for all } n = 1, 2, \ldots .$$

Lemma 16:

$$\mathscr{L}_{n-1} = (-1)^t[(p_t + q_{t-1})\mathscr{L}_n - \mathscr{L}_{n+1}] \quad \text{for } n = 1, 2, \ldots .$$

Proof: The eigenvalues λ_1 and λ_2 satisfy the characteristic equation of W. Thus, $\lambda_1^2 - (p_t + q_{t-1})\lambda_1 + (-1)^t = 0$ and, likewise, for λ_2. Multiplying these equations by λ_1^{n-1} and λ_2^{n-1}, respectively, and subtracting yields

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

Solving for $\mathscr{L}_{n-1}$ gives the conclusion. □

Notice that $\mathscr{L}_0$ and $\mathscr{L}_1$ are integers and that $\mathscr{L}_{n+1}$ is an integer combination of $\mathscr{L}_n$ and $\mathscr{L}_{n-1}$. Therefore, $\mathscr{L}_n$ is an integer for $n = 1, 2, \ldots$.

Lemma 17: If p is an odd prime and $\left(\frac{d}{p}\right)$ is the Legendre symbol, then

(i) $\mathscr{L}_p \equiv \left(\frac{d}{p}\right) \bmod p$, and

(ii) $\mathscr{L}_{p+1} \equiv 2^{-1}(p_t + q_{t-1})\left[\left(\frac{d}{p}\right) + 1\right] \bmod p$.

Proof: By writing out λ_1^p and λ_2^p in their respective binomial expansions, cancalling the even terms, reducing modulo p, and applying Euler's criterion, we get that

$$\text{(i)}\quad \mathscr{L}_p = \frac{1}{\sqrt{d}}(\lambda_1^p - \lambda_2^p) = 2^{1-p}\sum_{\substack{1 \le j \le p \\ j \text{ odd}}}\binom{p}{j}(p_t + q_{t-1})^{p-j}d^{(j-1)/2}$$

$$\equiv \binom{p}{p}d^{(p-1)/2} \equiv \left(\frac{d}{p}\right) \bmod p, \text{ and}$$

$$\text{(ii)}\quad \mathscr{L}_{p+1} = \frac{1}{\sqrt{d}}(\lambda_1^{p+1} - \lambda_2^{p+1}) = 2^{-p}\sum_{\substack{1 \le j \le p \\ j \text{ odd}}}\binom{p+1}{j}(p_t + q_{t-1})^{p+1-j}d^{(j-1)/2}$$

$$\equiv 2^{-1}\left[\binom{p+1}{1}(p_t + q_{t-1}) + \binom{p+1}{p}(p_t + q_{t-1})d^{(p-1)/2}\right] \bmod p$$

$$\equiv 2^{-1}(p_t + q_{t-1})[(p_t + q_{t-1})^{p-1} + d^{(p-1)/2}] \bmod p$$

$$\equiv 2^{-1}(p_t + q_{t-1})\left[\left(\frac{d}{p}\right) + 1\right] \bmod p. \quad \square$$

The following three corollaries are direct consequences of the previous two lemmas. They provide information about the entries in W^n when $n = p - \left(\frac{d}{p}\right)$.

Corollary 18: If $\left(\frac{d}{p}\right) = 1$, then

(i) $\mathscr{L}_{p-2} \equiv (-1)^{t-1} \bmod p$,
(ii) $\mathscr{L}_{p-1} \equiv 0 \bmod p$, and
(iii) $\mathscr{L}_p \equiv 1 \bmod p$.

Corollary 19: If $\left(\frac{d}{p}\right) = 0$, then

(i) $\mathscr{L}_{p-1} \equiv 2^{-1}(-1)^{t-1}(p_t + q_{t-1}) \bmod p$,
(ii) $\mathscr{L}_p \equiv 0 \bmod p$, and
(iii) $\mathscr{L}_{p+1} \equiv 2^{-1}(p_t + q_{t-1}) \bmod p$.

Corollary 20: If $\left(\frac{d}{p}\right) = -1$, then

(i) $\mathscr{L}_p \equiv -1 \bmod p$,
(ii) $\mathscr{L}_{p+1} \equiv 0 \bmod p$, and
(iii) $\mathscr{L}_{p+2} \equiv (-1)^t \bmod p$.

Corollary 10 describes the relation of $k(p)$ to c such that $W^c \equiv I$ and Theorem 15 gives a form for W^n. These are combined to obtain divisibility properties for $k(p)$. These multiples of $k(p)$ also give upper bounds on $k(p)$.

Theorem 21: If p is an odd prime, then $k(p)$ divides $\begin{cases}(p-1)t & \text{if } \left(\frac{d}{p}\right) = 1, \\ 4pt & \text{if } \left(\frac{d}{p}\right) = 0, \\ 2(p+1)t & \text{if } \left(\frac{d}{p}\right) = -1.\end{cases}$

Proof:

Case 1. Suppose that $\left(\frac{d}{p}\right) = 1$, and then apply Corollary 18 to W^{p-1}:

$$W^{p-1} = \begin{bmatrix} (-1)^{t-1}\mathcal{L}_{p-2} + q_{t-1}\mathcal{L}_{p-1} & q_t\mathcal{L}_{p-1} \\ p_{t-1}\mathcal{L}_{p-1} & \mathcal{L}_p - q_{t-1}\mathcal{L}_{p-1} \end{bmatrix}$$

$$\equiv \begin{bmatrix} (-1)^{t-1}(-1)^{t-1} & 0 \\ 0 & 1 \end{bmatrix} = I \bmod p.$$

Therefore, $k(p) \mid (p-1)t$ for $\left(\frac{d}{p}\right) = 1$.

Case 2. Suppose that $\left(\frac{d}{p}\right) = 0$, and then apply Corollary 19 to W^p:

$$W^p = \begin{bmatrix} (-1)^{t-1}\mathcal{L}_{p-1} + q_{t-1}\mathcal{L}_p & q_t\mathcal{L}_p \\ p_{t-1}\mathcal{L}_p & \mathcal{L}_{p+1} - q_{t-1}\mathcal{L}_p \end{bmatrix}$$

$$\equiv \begin{bmatrix} 2^{-1}(p_t + q_{t-1}) & 0 \\ 0 & 2^{-1}(p_t + q_{t-1}) \end{bmatrix} \bmod p.$$

Thus, $W^{2p} \equiv 4^{-1}(p_t + q_{t-1})^2 I$, but since $(p_t + q_{t-1})^2 = d + 4(-1)^t \equiv 4(-1)^t \bmod p$ we have $W^{2p} \equiv (-1)^t I$. Therefore, $W^{4p} \equiv I$ and $k(p) \mid 4pt$ in this case.

Case 3. Suppose that $\left(\frac{d}{p}\right) = -1$, and then apply Corollary 20 to W^{p+1}:

$$W^{p+1} = \begin{bmatrix} (-1)^{t-1}\mathcal{L}_p + q_{t-1}\mathcal{L}_{p+1} & q_t\mathcal{L}_{p+1} \\ p_{t-1}\mathcal{L}_{p+1} & \mathcal{L}_{p+2} - q_{t-1}\mathcal{L}_{p+1} \end{bmatrix} \equiv \begin{bmatrix} (-1)^t & 0 \\ 0 & (-1)^t \end{bmatrix} \bmod p.$$

Thus, $W^{2(p+1)} \equiv I$ and $k(p) \mid 2(p+1)t$ in this case. □

The proof of the previous theorem allows tightening of the bound when the period of α is even.

Theorem 22: If t is even, then $k(p)$ divides $\begin{cases} (p-1)t & \text{if } \left(\frac{d}{p}\right) = 1, \\ 2pt & \text{if } \left(\frac{d}{p}\right) = 0, \\ (p+1)t & \text{if } \left(\frac{d}{p}\right) = -1. \end{cases}$

The bounds given by Theorems 21 and 22 are met with some frequency. For example, considering the primes less than 1000 for the modulus, the bounds are met about 66 percent of the time for $\alpha = [\overline{2, 1, 4, 3, 5}]$ and 35 percent of the time for $\alpha = [\overline{4, 5, 1, 3, 2, 5}]$.

Questions

We leave the reader with some questions. First, when does $k(p) = k(p^e)$? Wall stated that, for $\alpha = [\overline{1}]$, no examples for $k(p) = k(p^2)$ occur for $p < 10{,}000$ and we have checked this for $p < 100{,}000$. Does $k(p) = k(p^2)$ ever happen in that case? Given $\alpha = [\overline{a_1, a_2, \ldots, a_t}]$, can bounds be given on the p's for which $k(p) = k(p^2)$? Does t play a role in such bounds? Can anything be said for $k(p) = k(p^e)$ for $e = 3, 4, \ldots$?

Wall gives considerable discussion of the period length of the sequence of r_n's defined in Lemma 8 for the case in which $a_n = 1$ for all n. There, the period is often independent of the initial conditions a and b. To what extent does that theory work for periodic sequences of a_n's?

The next question concerns the upper bounds for $k(p)$ given by Theorems 21 and 22. We would like to know when $k(p)$ equals its upper bound. We conjecture that $k(p)$ is the upper bound with some frequency; perhaps two-thirds of the $k(p)$ equal their upper bound when t is a prime. Can the bounds be improved when t is composite?

Addendum on Lower Bounds

Theorem 6 gives a trivial lower bound on $k(p)$. It seems reasonable to expect $k(m) > c \log(m)$ for some constant c depending on α. Are such bounds possible? The referee offered the following solution. Let $a_1, a_2, \ldots, a_n$ be the complete list of the partial quotients for a given quadratic irrational α. Set $A = \max\{a_1, \ldots, a_n\} + 1$. Then

$$p_t \le (A - 1)p_{t-1} + p_{t-2} \le Ap_{t-1} \text{ for all } t \ge 2$$

and $p_1 = a_1 < A$ so that

$$p_t < A^t \text{ for all } t \ge 1.$$

For $A^t \le m < A^{t+1}$, this means that $k(m) \ge t$. It follows that

$$k(m) > \frac{\log m}{\log A} - 1 \text{ for all } m \ge 1.$$

References

1. Derek K. Chang. "Higher Order Fibonacci Sequences Modulo m." *Fibonacci Quarterly* *24.2* (1986):138-39.
2. Kenneth H. Rosen. *Elementary Number Theory and Its Applications*, 2nd ed. New York: Addison Wesley, 1988.
3. A. P. Shah. "Fibonacci Sequence Modulo m." *Fibonacci Quarterly* *6.2* (1968): 139-41.
4. T. E. Stanley. "Powers of the Period Function for the Sequence of Fibonacci Numbers" and "Some Remarks on the Periodicity of the Sequence of Fibonacci Numbers II." *Fibonacci Quarterly* *18.1* (1980):44-47.
5. John Vinson. "The Relation of the Period Modulo to the Rank of Apparition of m in the Fibonacci Sequence." *Fibonacci Quarterly* *1.1* (1963):37-46.
6. D. D. Wall. "Fibonacci Series Modulo m." *Amer. Math. Monthly* *67* (1960): 525-32.

*****