PERIODS OF (q, r)-FIBONACCI SEQUENCES AND ELLIPTIC CURVES

Deidra A. Coleman
Student, Shaw University, Raleigh, NC 27601

Christopher J. Dugan
Student, St. Joseph's University, Philadelphia, PA 19131

Robert A. McEwen
Student, Lafayette College, Easton, PA 18042

Clifford A. Reiter
Lafayette College, Easton, PA 18042

Tran T. Tang
Student, California State University Long Beach, Long Beach, CA 90840
(Submitted September 2003-Final Revision January 2004)

ABSTRACT

The periods of the Fibonacci Sequence modulo m have long been studied and remain intriguing. Generalizations of the sequence suitable for application to elliptic curve groups are investigated. This leads to the study of general initial conditions including the establishment of a criterion for periods to be possible. A class equation for the set of all initial conditions is given. There is a close relationship between the order of elements in the elliptic curve group and the lengths of the periods of the Fibonacci sequences and most of the properties of generalized Fibonacci sequences extend to elliptic curve groups. However, Fibonacci sequences on elliptic curve groups do exhibit some periodicity not seen modulo m.

1. INTRODUCTION

The Fibonacci numbers have been studied both for their applications and the mathematical beauty of the rich and varied identities that they satisfy. Since many of the identities involve both addition and multiplication, many of the properties require the full ring structure of the integers. However, generalizations to groups have been considered [8,13].

The arithmetic of elliptic curves has recently become important for its relevance to factorization algorithms and hence to computer security [2]. In particular, finding points of relatively small order on elliptic curves over finite fields is often of interest. We were motivated to study what features of the Fibonacci sequence remain true when generalized to elliptic curves. Since the analogous sequences must allow more general initial conditions, we first study that situation modulo m. Possible periods are investigated and connections with circulant matrices are obtained. We study equivalence classes and obtain a partition theorem for the set of all possible initial conditions. We will see that the period length of a Fibonacci sequence on an elliptic curve is closely related to the order of elements on the elliptic curve and to the period of the ordinary Fibonacci sequence.

As it turns out, most of what we say for elliptic curve groups is true for any abelian group. However, we will discuss the analogous properties in the context of elliptic curves since that motivated our work and our examples will be from those groups.

2. THE FIBONACCI SEQUENCE

It is known that the Fibonacci sequence is finite and periodic if the sequence is computed modulo m. Let the period of that sequence be denoted $k(m)$. For instance, the Fibonacci sequence computed modulo 11 is 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, ..., which implies $k(11) = 10$.

The following theorem contains some of the fundamental properties known about the periods of the Fibonacci sequence modulo m.

Theorem 1:
(a) If p is prime and $p \equiv \pm 1 \bmod 10$, then $k(p) \mid p - 1$.
(b) If p is prime and $p \equiv \pm 3 \bmod 10$, then $k(p) \mid 2(p + 1)$.
(c) If m has prime factorization $\prod {p_i}^{e_i}$, then $k(m) = lcm(k({p_i}^{e_i}))$.
(d) If $n \mid m$, then $k(n) \mid k(m)$.
(e) If $m > 2$ and n is the smallest positive integer that is either even and $m \mid F_n$ or else n is odd and $m \mid F_{n-1} + F_{n+1}$, then $k(m) = 2n$.

Proof: See [12] for (a) - (d) and [13] for (e). □

Returning to the example above, since 11 is a prime number that is congruent to 1 modulo 10, it can be seen that 11 satisfies (a). The Fibonacci sequence modulo 22 is 0, 1, 1, 2, 3, 5, 8, 13, 21, 12, 11, 1, 12, 13, 3, 16, 19, 13, 10, 1, 11, 12, 1, 13, 14, 5, 19, 2, 21, 1, 0, 1, ... and thus $k(22) = 30$. Modulo 2 the sequence is 0, 1, 1, 0, 1, ... and thus $k(2) = 3$. Since $k(11) = 10$, part (c) gives $k(22) = lcm(k(2), k(11)) = lcm(3, 10) = 30$ as we have seen. An illustration of (d) is that $11 \mid 22$ implies $k(11) \mid k(22)$ as the above examples also demonstrate. Also $11 \mid 3 + 8 = F_4 + F_6$ illustrates (e).

Figure 1: $k(p)$ versus p for primes less than 5000.

Figure 1 shows the length of the Fibonacci sequence for prime moduli less than 5000. Notice the two prominant lines. The highest one corresponds to primes with $k(p) = 2(p + 1)$ which is the maximal length from Theorem 1(b). The second highest corresponds to maximal Theorem 1(a) where $k(p) = p - 1$ and also the half-maximal period $k(p) = p + 1$ from (b). Despite the fact that Theorem 1 provides a great deal of information about $k(m)$, there remain unresolved issues. In particular, while much is known about $k(p^e)$, it is conjectured that $k(p^2) = pk(p)$ for all primes p, but this remains unproven.

3. THE (q, r)-FIBONACCI SEQUENCE

We next consider Fibonacci sequences with generalized initial conditions, which were considered as early as Tagiuri in 1901 [4]. Fully generalized, nondegenerate second order constant coefficient recursions with general initial conditions have been much studied and are often called Horadam sequences [7].

We refer to the (q, r)-Fibonacci sequence as the sequence defined by $G_0 = q$ and $G_1 = r$ for integers q and r, such that $G_n = G_{n-1} + G_{n-2}$. Notice that G_n depends on q and r, but that fact is suppressed in the notation for the sequence. If $q = 3$, $r = 2$, and $m = 3$, then ten values of the (q, r)-Fibonacci sequence and its residues modulo m are given below.

n	0	1	2	3	4	5	6	7	8	9
G_n	3	2	5	7	12	19	31	50	81	131
$G_n \ mod \ 3$	0	2	2	1	0	1	1	2	0	2

Note that $G_8 \equiv 0$ and $G_9 \equiv 2$, which repeats the two initial conditions and hence the sequence modulo 3 is periodic. Also note that if $q = 2$ and $r = 1$, then the resulting $(q, r)-$Fibonacci sequence is the classical Lucas sequence.

Proposition 2: Let q, r, m be integers with $m \geq 2$.
(a) The (q, r)-Fibonacci sequence G_n satisfies $G_n = F_{n-1}q + F_n r$.
(b) The (q, r)-Fibonacci sequence modulo m is purely periodic.

Proof: (a). This follows from a straightforward induction. (b). There are only m^2 possibilities for two successive terms in the (q, r)-Fibonacci sequence modulo m and two successive terms are enough to determine the entire sequence forward and backward. Hence, there will eventually be repetitions and no preperiod; hence the sequence is purely periodic. □

The period of a (q, r)-Fibonacci sequence reduced modulo m will be denoted as $k(q, r, m)$. Thus, it was shown in the previous example that $k(3, 2, 3) = 8$. Next is a proposition about the properties of the periods of a (q, r)-Fibonacci sequence and its relation to the periods of the $(0, q)$ and $(0, r)$-Fibonacci sequences.

Proposition 3: Let G_n be the terms of a (q, r)-Fibonacci sequence where q, r, and m are any integers with $m \geq 2$.
(a) $c = k(q, r, m)$ if and only if c is the smallest positive integer such that $G_c \equiv G_0$ and $G_{c+1} \equiv G_1$ modulo m.
(b) If $G_n \equiv G_0$ and $G_{n+1} \equiv G_1$ modulo m, then $k(q, r, m) \mid n$.
(c) $k(0, r, m) = k(r, 0, m)$ and $k(0, r, m) \mid k(m)$.
(d) If $gcd(r, m) = 1$, then $k(0, r, m) = k(m)$.
(e) $k(q, r, m) \mid lcm(k(0, q, m), k(0, r, m))$.

Proof: (a) and (b) follow from the definition of periodicity and Proposition 2(b). (c). Since the $(r, 0)$-sequence begins r, 0, r, the $(r, 0)$ sequence is the same as the $(0, r)$ sequence except for the starting point. Thus $k(0, r, m) = k(r, 0, m)$. Note that the $(0, r)-$Fibonacci sequence G_i has terms $F_i r$ and that $F_i \equiv F_j$ implies $F_i r \equiv F_j r$. Therefore, if $c = k(m)$, then $F_0 r \equiv F_c r$ and $F_1 r \equiv F_{c+1} r$. By (b), $k(0, r, m)|c = k(m)$. (d). We have noted that $k(0, r, m)$ depends on the sequence $F_i r$ modulo m. When $gcd(r, m) = 1$, the invertibility of r modulo m implies $F_i \equiv F_j \bmod m$ if and only if $F_i r \equiv F_j r$. Thus, $k(0, r, m) = k(m)$. (e). Let $c = k(0, q, m)$ and $d = k(0, r, m)$. Using Proposition 2(a), this implies $F_{c-1} q \equiv q$, $F_c q \equiv 0$ and $F_d r \equiv 0$, $F_{d+1} r \equiv r$. Let $t = lcm(c, d)$. Since $c \mid t$ and $d \mid t$, then $F_{t-1} q \equiv q$, $F_t q \equiv 0$ and $F_t r \equiv 0$, $F_{t+1} r \equiv r$. These facts and Proposition 2(a) give $G_t \equiv q+0 \equiv q$ and $G_{t+1} \equiv 0+r \equiv r$. Hence, $k(q, r, m) \mid t = lcm(c, d)$. □

Having explored basic properties of periodicity modulo m of the (q, r)-sequences, we next consider equivalence classes for these sequences.

4. THE (q, r)-EQUIVALENCE CLASSES

Recall that the Fibonacci sequence computed modulo 11 is 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, ...; thus, if we look at the $(8, 2)$-Fibonacci sequence modulo 11, we have the same terms in a different order. We say (a, b) is *equivalent* to (q, r) if a and b (modulo m) appear as successive terms in the (q, r)-sequence modulo m. Since successive terms completely determine the sequence modulo m, this is an equivalence relation on $Z_m \times Z_m$, the pairs of integers modulo m. Table 1 gives all the equivalence classes modulo 11.

$k(q, r, 11)$	(q, r)
1	$(0, 0)$
10	$(0, 1), (1, 1), (1, 2), (2, 3), (3, 5), (5, 8), (8, 2), (2, 10), (10, 1), (1, 0)$
10	$(0, 2), (2, 2), (2, 4), (4, 6), (6, 10), (10, 5), (5, 4), (4, 9), (9, 2), (2, 0)$
10	$(0, 3), (3, 3), (3, 6), (6, 9), (9, 4), (4, 2), (2, 6), (6, 8), (8, 3), (3, 0)$
10	$(0, 4), (4, 4), (4, 8), (8, 1), (1, 9), (9, 10), (10, 8), (8, 7), (7, 4), (4, 0)$
10	$(0, 5), (5, 5), (5, 10), (10, 4), (4, 3), (3, 7), (7, 10), (10, 6), (6, 5), (5, 0)$
10	$(0, 6), (6, 6), (6, 1), (1, 7), (7, 8), (8, 4), (4, 1), (1, 5), (5, 6), (6, 0)$
10	$(0, 7), (7, 7), (7, 3), (3, 10), (10, 2), (2, 1), (1, 3), (3, 4), (4, 7), (7, 0)$
10	$(0, 8), (8, 8), (8, 5), (5, 2), (2, 7), (7, 9), (9, 5), (5, 3), (3, 8), (8, 0)$
10	$(0, 9), (9, 9), (9, 7), (7, 5), (5, 1), (1, 6), (6, 7), (7, 2), (2, 9), (9, 0)$
10	$(0, 10), (10, 10), (10, 9), (9, 8), (8, 6), (6, 3), (3, 9), (9, 1), (1, 10), (10, 0)$
5	$(1, 4), (4, 5), (5, 9), (9, 3), (3, 1)$
10	$(1, 8), (8, 9), (9, 6), (6, 4), (4, 10), (10, 3), (3, 2), (2, 5), (5, 7), (7, 1)$
5	$(2, 8), (8, 10), (10, 7), (7, 6), (6, 2)$

Table 1. The (q, r)-equivalence classes modulo 11.

The size of the equivalence class containing (q, r) is $k(q, r, m)$. Given a fixed modulus m, we define $c_d(m)$ as the number of distinct equivalence classes of size d. Thus, in Table 1 we see $c_1(11) = 1$, $c_5(11) = 2$, $c_{10}(11) = 11$, and all other $c_d(11) = 0$ for all other d. The small equivalence classes are described by the following Proposition.

Proposition 4: Let $m \geq 2$ be an integer.

(a) $c_1(m) = 1$.
(b) $c_2(m) = 0$.
(c) If m is even, then $c_3(m) = 1$ and otherwise $c_3(m) = 0$.
(d) If $5 \nmid m$, then $c_4(m) = 0$ while if $5 \mid m$, then $c_4(m) = 1$ and 0 does not appear as a term in the period.

Proof: (a) A sequence for $c_1(m)$ has the form a, a, a, ... modulo m. Thus, $a + a \equiv a$, so $a \equiv 0 \bmod m$. Hence, we have that the sequence is in fact $0, 0, 0, ...$ and since that sequence always occurs, $c_1(m) = 1$.

(b) A sequence for $c_2(m)$ has the form a, b, a, b, ... We know that $a + b \equiv a \bmod m$, so $b \equiv 0$. Likewise, $b + a \equiv b \bmod m$, so $a \equiv 0$. This yields the sequence 0, 0, 0, 0, ..., which is in fact the sequence for the $c_1(m)$ class. Thus, $c_2(m) = 0$.

(c) A sequence for $c_3(m)$ has the form a, b, c, a, b, c, ... Thus we have $a+b \equiv c$, $b+c \equiv a$, $c + a \equiv b$ modulo m. These congruences imply $2b \equiv 2c \equiv 2a \equiv 0$. If m is odd, congruences (4)-(6) imply that $a \equiv b \equiv c \equiv 0$, yielding a class of length 1. Hence, $c_3(m) = 0$ when m is odd. If m is even, then congruences (4)-(6) imply that a, b, and c must each be congruent to 0 or $\frac{m}{2}$. The only valid period (up to order) is 0, $\frac{m}{2}$, $\frac{m}{2}$, hence $c_3(m) = 1$ in this case.

(d) A sequence for $c_4(m)$ may be written as a, b, $a + b$, $a + 2b$, a, ... From this we have that $2a + 3b \equiv a$ and that $2a + 2b \equiv b$. These imply that $b \equiv -2a$ and $5a \equiv 0$, so either we have a trivial sequence or $a \equiv j \cdot \frac{m}{5}$ and $b \equiv \frac{12ja}{5} \equiv \frac{3ja}{5}$ where $j = 1, 2, 3$, or 4. The period (up to order) is then $\frac{m}{5}$, $\frac{3m}{5}$, $\frac{4m}{5}$, $\frac{2m}{5}$ where no term is a 0. So if $5 \nmid m$, then $c_4(m) = 0$, otherwise $c_4(m) = 1$ and no term is a 0. □

While Proposition 4 gives information about $c_d(m)$ for small d, we consider further cases in a general manner. First, observe that if x_1, x_2,...x_d is a period of the (x_1, x_2)-Fibonacci Sequence modulo m, then $x_1 + x_2 \equiv x_3$, $x_2 + x_3 \equiv x_4$, and $x_n + x_1 \equiv x_2$. Thus,

$$\begin{pmatrix} 1 & 1 & -1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 1 & -1 & \dots & 0 & 0 \\ \vdots & & \vdots & & & \ddots & & \vdots \\ -1 & 0 & 0 & 0 & 0 & \dots & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{d-1} \\ x_d \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \bmod m$$

We define the *Fibonacci circulant matrix*, W_n, and the *standard circulant matrix*, π_n, to be the n by n matrices of the following form.

$$W_n = \begin{pmatrix} 1 & 1 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & -1 & \dots & 0 & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 & 0 \\ \vdots & & \vdots & & \ddots & & \vdots \\ -1 & 0 & 0 & 0 & \dots & 1 & 1 \\ 1 & -1 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \quad \pi_n = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

The matrix π_n is also known as the *forward permutation matrix*. Also, we denote $w_n = |\det(W_n)|$ for the magnitude of the determinant of the Fibonacci circulant matrix.

Circulants arise in Physics, image processing, probability, numerical analysis, number theory, knot theory and geometry [3]. Our particular sequence, w_n, arises in the study of

quasicrystals [1,5]. For our application to the periods of the Fibonacci sequence, we are most interested in an explicit form for w_n. Some related explicit formulas appear in [9] which were motivated by problems in knot theory. We will develop the relevant explicit forms directly.

Proposition 5: Let w_n be defined as above.
(a) $w_n = (-1)^{n-1} \prod_{j=0}^{n-1} \left(1 + e^{\frac{2\pi ij}{n}} - e^{\frac{4\pi ij}{n}}\right)$
(b) $w_n = (-1)^{n-1} - 1 + F_{n+1} + F_{n-1}$
(c) If n is odd, then $w_n = F_{n+1} + F_{n-1} = L_n$ where L_n is the n^{th} Lucas number. Moreover, if n is divisible by 4, then $w_n = 5F_{\frac{n}{2}}^2$ and if $n \equiv 2 \bmod 4$, then $w_n = L_{\frac{n}{2}}^2$.

Proof: (a). The matrix π_n has distinct eigenvalues that are the n^{th} roots of unity $e^{\frac{2\pi ij}{n}}$; see [3]. Since $W_n = I + \pi_n - \pi_n^2$, where I is the identity matrix, the eigenvalues of W_n are $1 + e^{\frac{2\pi ij}{n}} - e^{\frac{4\pi ij}{n}}$. The determinant is the product of the eigenvalues which is negative iff n is even, hence the conditional minus sign in (a).

In order to see (b), we can check $n = 3$ directly. For larger n we apply direct row reduction on W_n until the three nonzero entries in the lower left have been moved to the last four columns. To move the nonzero entries to the right, we use the diagonal pivots with appropriate weights, which turn out to be Fibonacci numbers with alternating signs. In order to deal with row $n-1$ we add to row $n-1$ one times row one and then -1 times row two and 2 times row three and so on up to $(-1)^{n-5}F_{n-4}$ times row $n-4$. The weights are shifted by one to deal with the n^{th} row. After those operations, the lower right 4 by 4 submatrix is the following.

$$\begin{pmatrix} 1 & 1 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ (-1)^{n-1}F_{n-3} & (-1)^n F_{n-4} & 1 & 1 \\ (-1)^n F_{n-2} & (-1)^{n-1}F_{n-3} & 0 & 1 \end{pmatrix}$$

Since the entries to the left are zeros and the first $n-4$ pivots remain 1, w_n is the same as the absolute value of the determinant of the 4 by 4 matrix. Computing that determinant, simplifying with Simpson's formula, $F_{n-1}^2 + F_{n-1}F_n - F_n^2 = (-1)^n$, and the Fibonacci recursion, and multiplying by $(-1)^{n-1}$ as previously noted, results in the desired formula. Part (c) follows by considering even and odd cases in part (b) and using standard facts about the Lucas numbers [6, p. 59]. □

Now we can state the relevance of the w_n sequence to the period of the Fibonacci sequence modulo m.

Theorem 6: Let q and r be integers, not both 0, and let m be an integer such that $m \geq 2$. If $c = k(q, r, m)$, then $\gcd(w_c, m) > 1$.

Proof: Suppose not. Suppose $\gcd(w_c, m) = 1$ and let G_n denote the (q, r)-Fibonacci sequence modulo m. Then $X = (G_0, G_1, \ldots, G_{c-1})$ is a nontrivial solution to the system $W_c X \equiv 0 \bmod m$. On the other hand, $\gcd(w_c, m) = 1$ implies W_c is invertible modulo m, so that $W_c X \equiv 0$ has only $X \equiv 0$ as a solution, yielding the desired contradiction. □

In Table 2 we see some values for the w_n sequence. Notice the many square factors for even terms, as expected, in light of Proposition 5(c). We interpret the theorem by considering the entry $w_5 = 11$. If any (q, r)-sequence has period length 5 modulo m, then $11 \mid m$. In general, period length n can only occur for moduli with a nontrivial factor in common with

w_n. Thus, the prime factors of w_n gives a finite list of primes, at least one of which must divide m in order for $k(q, r, m)$ to be n.

n	w_n	n	w_n	n	w_n	n	w_n
3	$4 = 2^2$	10	$121 = 11^2$	17	$3571 = 3571$	24	$103680 = 2^8 3^4 5$
4	$5 = 5$	11	$199 = 199$	18	$5776 = 2^4 19^2$	25	$167761 = 11\ 101\ 151$
5	$11 = 11$	12	$320 = 2^6 5$	19	$9349 = 9349$	26	$271441 = 521^2$
6	$16 = 2^4$	13	$521 = 521$	20	$15125 = 5^3 11^2$	27	$439204 = 2^2 19\ 5779$
7	$29 = 29$	14	$841 = 29^2$	21	$24476 = 2^2 29\ 211$	28	$710645 = 5\ 13^2 29^2$
8	$45 = 3^2 5$	15	$1364 = 2^2 11\ 31$	22	$39601 = 199^2$	29	$1149851 = 59\ 19489$
9	$76 = 2^2 19$	16	$2205 = 3^2 5\ 7^2$	23	$64079 = 139\ 461$	30	$1860496 = 2^4 11^2 31^2$

Table 2. The w_n Numbers and Their Prime Factorizations.

Compare the values of w_n in Proposition 5(c) with those in Theorem 1(e). The appearance of Lucas and Fibonacci numbers is as expected. However, Proposition 5 and Theorem 6 deal with general (q, r)-sequences which are less restrictive. In particular, we can not demand divisibility of the w_n. For example, $0, 3, 3$ is a period length 3 sequence modulo 6, but 6 only has a factor in common with $w_3 = 4$.

The following Theorem counts the elements of $Z_m \times Z_m$ corresponding to the partition of that set into equivalence classes.

Theorem 7: Let $m > 1$ and $c_d(m)$ be defined as above, then

$$m^2 = \sum_{d|k(m)} c_d(m) d$$

Proof: The (q, r)-equivalence classes form a partition of $Z_m \times Z_m$ and each class will have a size that divides $k(m)$. By summing the number of elements in each class of length d for all $d \mid k(m)$, we get the number of possible pairs, which is m^2. □

There can be considerably less or more regularity than we saw modulo 11 in Table 1. In Table 3, looking at $m = 10$ with $k(10) = 60$, we find there is the breakdown of partitions so no two classes have the same size.

Divisor d	1	2	3	4	5	6	10	12	15	20	30	60
$c_d(10)$	1	0	1	1	0	0	0	1	0	1	0	1

Table 3. Lengths and Number of Equivalence Classes modulo 11.

However, except for the $(0, 0)$-class which always has length 1, we may have every class have length $k(m)$, as exhibited in Table 4 by the case when $m = 7$, with $k(m) = 16$.

Divisor d	1	2	4	8	16
$c_d(7)$	1	0	0	0	3

Table 4. Lengths and Number of Equivalence Classes modulo 7.

We might hope to rewrite the class equation in Theorem 7 in a form suitable for Möbius inversion. This would require having $d \mid m$ instead of $d \mid k(m)$. However, as Table 3 indicates,

10 has classes of 6 different sizes, but only 4 divisors. Thus we can't hope to accomplish such rewriting in general.

There are cases where Theorem 7 can be used to determine all $c_d(m)$. First, we need a theorem which gives information about the number of zeroes, denoted $t(p)$, in the standard $(0, 1)$-Fibonacci sequence reduced modulo a prime p.

Theorem 8: Let p be a prime.
(a) If $p \equiv 11$ or 19 mod 20, then $t(p) = 1$.
(b) If $p \equiv 3$ or 7 mod 20, then $t(p) = 2$.
(c) If $p \equiv 13$ or 17 mod 20, then $t(p) = 4$.
(d) If $p \equiv 21$ or 29 mod 40, then $t(p) \neq 2$.

Proof: See [11]. □

We see in Figure 1 that k(p) = 2(p+1) appears to occur with some frequency. When $p \equiv 3$ or 7 modulo 20, we know that $t(p) = 2$. In the following proposition we see those conditions together allow us to determine all the $c_d(p)$ values.

Proposition 9: If p is a prime such that $p \equiv 3$ or 7 modulo 20 and $k(p) = 2(p + 1)$, then $c_0(p) = 1$, $c_{2(p+1)} = \frac{p-1}{2}$, and $c_d(p) = 0$ for all other d.

Proof: There are $p-1$ pairs of form $(0, q)$ containing a zero and a non-zero value and the $(0, 1)$-sequence reduced modulo m can be multiplied by any $q < m$ to get the $(0, q)$-sequence modulo m. By Theorem 8(b), each such sequence will contain exactly two of those pairs $(0, q)$. We find that the number of sequences of length $2(p+1)$ generated this way is equal to $\frac{p-1}{2}$. Along with the $(0, 0)$-sequence, this accounts for $(\frac{p-1}{2})2(p + 1) + 1 = p^2$ pairs, hence all other $c_d(p) = 0$ and there are no additional sequences of size $2(p + 1)$. □

The classes modulo 7 illustrate Proposition 9 and were shown in Table 4.

Next we discuss elliptic curve arithmetic in preparation for discussion of analogous sequences on elliptic curves.

5. ELLIPTIC CURVES

A non-singular elliptic curve can be defined by an equation of the form $y^2 = x^3 + ax + b$, with the cubic having distinct roots. These curves can be considered over any field, such as the reals, although we assume that the field is not characteristic 2 in order to avoid complications. The points on such a non-singular elliptic curve, which are the pairs (x, y) that are solutions to the cubic, and the point at infinity, denoted O, form an abelian group under chord-and-tangent addition with O as the identity element.

Geometrically, the chord-and-tangent addition is performed as follows over the reals. Any line on the curve will intersect it at either one or three points counting multiplicities. Therefore, if a line is drawn through two points Q and R on the curve, then the line will intersect at a third point, called $Q * R$. By drawing a vertical line through $Q * R$, another point will be obtained, which is the negation of $Q * R$ and is denoted $Q + R$. The point $Q + R$ can also be algebraically computed using the equations, given below, as found in [10]. These formulas are convenient for computations over finite fields.

$$\text{Let } \lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1}, & \text{if } x_1 \neq x_2, \\ \frac{3x_1^2+a}{2y_1}, & \text{if } Q = R, \end{cases} \text{ and } v = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

Then $Q + R = (x_3, y_3)$ where $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = -\lambda x_3 - v$.

Consider the curve $y^2 = x^3 + x + 1$ over the field Z_5. Let $Q = (3, 1)$ and $R = (3, 1)$, then $\lambda = 14$ and $v = -41$ giving $Q + R = (190, 1) \equiv (0, 1)$ modulo 5. Observe that $Q = R$; hence, $Q + R = [2]Q = [2]R$, where the values inside the square brackets indicate the number of times the point is added to itself.

For the remainder of this paper, we will consider non-singular elliptic curves over the field of integers modulo p, where $p > 2$ is a prime. For $p > 2$ it is known that $x^3 + ax + b$ has distinct roots if and only if p does not divide the discriminant $-4a^3 - 27b^2$.

Figure 2. Chord-and-tangent addition on $y^2 = x^3 - x + 9$.

6. THE (Q, R)-FIBONACCI SEQUENCES ON ELLIPTIC CURVES

Given points Q and R on a non-singular elliptic curve over p, we define the (Q, R)-Fibonacci sequence by the following: $H_0 = Q$, $H_1 = R$, and $H_{n+1} = H_n + H_{n-1}$. Our notation is similar to the regular (q, r)-Fibonacci sequence notation: we will suppress Q, R, and the prime p that is implicit in the choice of elliptic curve. First, we establish some basic properties of H_n.

Proposition 10: Let Q and R be points on a non-singular elliptic curve E over $p > 2$,
(a) The (Q, R)-Fibonacci sequence H_n is given by $H_n = [F_{n-1}]Q + [F_n]R$.
(b) The (O, R)-Fibonacci sequence is $H_n = [F_n]R$.
(c) The (Q, R)-Fibonacci sequence H_n is purely periodic.

Proof: (a). This is easily seen from a straightforward induction. (b). This is a special case of (a) with $Q = O$. (c). The proof follows from an argument similar to the proof of Proposition 2(b) using the fact that the number of points on the elliptic curve over p is finite. □

As stated in Proposition 10(b), a (Q, R)-Fibonacci sequence on E is purely periodic. We will denote the period as $K(Q, R, E)$.

Lemma 11: Given a point R on a non-singular elliptic curve E over $p > 2$ and integers m and n, then $[m]R = [n]R$ if and only if $m \equiv n \bmod ord(R)$.

Proof: Notice $[m]R = [n]R$ if and only if $[m - n]R = [0]R$, so $(m - n) \mid ord(R)$ and the result follows. □

We can now make the connection between the periods on elliptic curves and periods of ordinary Fibonacci sequences. The next theorem shows that the period of the (O, R) sequence depends only on $ord(R)$ so that any points R with the same order will generate Fibonacci sequences with exactly the same length. Once this connection is made, we can generalize properties of Fibonacci numbers to the (O, R)-Fibonacci sequences on elliptic curves.

Theorem 12: Let R and Q be points on a non-singular elliptic curve E over $p > 2$, then
(a) $K(O, R, E) = K(R, O, E) = k(ord(R))$.
(b) $K(Q, R, E) \mid lcm(K(O, Q, E), K(O, R, E))$.
(c) $K(Q, R, E) \mid k(ord(E))$.

Proof: (a). The $(R, 0)$ sequence begins R, O, R and hence $K(O, R, E) = K(R, O, E)$. Proposition 10(b) tells us that the (O, R)-sequence has the form $[F_n]R$. The period $K(O, R, E)$ is the smallest positive c such that $[0]R = H_c = [F_c]R$ and $[1]R = H_{c+1} = [F_{c+1}]R$ with $c > 0$. By Lemma 11, this happens if and only if $F_c \equiv 0$ and $F_{c+1} \equiv 1$ modulo $ord(R)$. Since c is the smallest such integer, $c = k(ord(R))$. (b). The proof is analogous to that of Proposition 3. (c). We know that $ord(R) \mid ord(E)$ and $ord(Q) \mid ord(E)$, hence the $lcm(K(O, Q, E), K(O, R, E)) \mid ord(E)$ and the result follows from part (b). □

Since $k(ord(R))$ is equal to $K(O, R, E)$, some properties of the standard Fibonacci sequences may be translated to analogous properties for (O, R)-Fibonacci sequences on an elliptic curve.

Theorem 13: Let Q, R, be points on a non-singular elliptic curve E over prime $p > 2$.
(a) If $ord(R)$ is prime and $ord(R) \equiv \pm 1 \ mod\ 10$, then $K(O, R, E) \mid ord(R) - 1$.
(b) If $ord(R)$ is prime and $ord(R) \equiv \pm 3 \ mod\ 10$, then $K(O, R, E) \mid 2(ord(R) + 1)$.
(c) If $ord(R)$ has prime factorization $\prod p_i^{e_i}$, then $K(O, R, E) = lcm(k(p_i^{e_i}))$.
(d) If $ord(Q) \mid ord(R)$, then $K(O, Q, E) \mid K(O, R, E)$.

Proof: Use the result of Theorem 12 in Theorem 1. □

We now give the analogous notion of an equivalence class for (Q, R)-Fibonacci sequences defined on elliptic curves. We say that (A, B) is *equivalent* to (Q, R) if A and B appear as successive points in the (Q, R)-sequence on a non-singular elliptic curve E over prime p. We know the size of an equivalence class containing (Q, R) is $K(Q, R, E)$. We define $C_d(E)$ to be the number of distinct equivalence classes of size d for the elliptic curve E.

Theorem 14: Let Q and R be points on a non-singular elliptic curve E over a prime $p > 2$ and w_c be the magnitudes of the determinants of the Fibonacci circulant matrices as before.
(a) $C_1(E) = 1$.
(b) $C_2(E) = 0$.
(c) If $c = K(Q, R, E)$, then $gcd(w_c, ord(E)) > 1$.

Proof: (a) and (b) follow from arguments analogous to those from the proof of Proposition 4. (c) follows from a proof analogous to the proof of Theorem 6. Note that the matrix equation involving the W_n only uses integer multiples of elliptic curve points and hence is meaningful. In light of Lemma 11 and the fact that every R on E has order dividing $ord(E)$, we may consider

W_n modulo $ord(E)$ and the system will have only trivial solutions when w_n is relatively prime to $ord(E)$. □

Note that not all the properties we saw for ordinary Fibonacci sequences generalize to the elliptic curve case. We consider the elliptic curve $y^2 = x^3 + 1$ over $p = 7$. One can check that $C_3(E) = 5$. The five classes of length three are: $\{O, (3,0), (3,0)\}$, $\{O, (5,0), (5,0)\}$, $\{O, (6,0), (6,0)\}$, $\{(3,0), (5,0), (6,0)\}$, and $\{(3,0), (6,0), (5,0)\}$. Thus we can see that the freedom provided by the elliptic curve addition allows multiple non-trivial solutions to congruences described in the proof of Proposition 4(c), which does not allow the result of Proposition 4(c) to carry over to elliptic curves.

Equivalence classes partition $E \times E$, and hence we get a theorem analogous to Theorem 7.

Theorem 15: Let E be a non-singular finite elliptic curve over a prime $p > 2$ and $C_d(E)$ be defined as above, then

$$ord(E)^2 = \sum_{d|k(ord(E))} C_d(E)d.$$

Proof: The equivalence classes form a partition of $E \times E$ and each class will have a size that divides $k(ord(E))$ by Theorem 12. By summing the number of elements in each class of length d for all $d \mid k(ord(E))$, we get the number of possible pairs, which is $ord(E)^2$. □

Table 5 illustrates Theorem 15 for the elliptic curve $y^2 = x^3 + 1$ modulo 7.

Divisor d	1	2	3	4	6	8	12	24
$C_d(E)$	1	0	5	0	0	1	0	5

Table 5. Lengths and Number of Equivalence Classes for $y^2 = x^3 + 1$ modulo 7.

CONCLUSION

We have seen that the periods of Fibonacci sequences with generalized initial conditions modulo m satisfy many properties. We have seen how a sequence of determinants arrising from circulant matrices restricts the period lengths and have introduced a sense of equivalence that gives rise to a partition theorem. There are many analogous properties for generalized Fibonacci sequences on elliptic curves. However, the elliptic curve groups are richer and may have more elements of low order and Fibonacci sequences on elliptic curves exhibit some properties of periods not seen modulo m.

ACKNOWLEDGMENTS

This work was supported by NSF grant DMS-0243763 and Lafayette College.

REFERENCES

[1] M. Baake, J. Hermisson, and P. Pleasants. "The Torus Parametrization of Quasiperiodic LI-classes." *Journal of Physics A* **30** (1997): 3029-3056.

[2] R. Crandall and C. Pomerance. *Prime Numbers: A Computational Perspective.* New York: Springer-Verlag New York Inc., 2001.

[3] P. J. Davis, *Circulant Matrices.* John Wiley & Sons, Inc., New York, 1979.
[4] L. E. Dickson. *History of the Theory of Numbers.* Vol. 1. New York: Chelsea Publishing Company, Reprint 1971.
[5] R. Guy and N. J. A. Sloane. *On-Line Encyclopedia of Integer Sequences* http://www.research.att.com/cgi-bin/access.cgi/as/njas/sequences/eismum.cgi. (2003): A001350.
[6] V. E. Hoggatt, Jr., *Fibonacci and Lucas Numbers*, The Fibonacci Association, Santa Clara, 1969.
[7] A. F. Horadam. "Basic Properties of a Certain Generalized Sequence of Numbers." *The Fibonacci Quarterly* **3** (1965): 161-76.
[8] S. Knox. "Fibonacci Sequences in Finite Groups." *The Fibonacci Quarterly* **30** (1992): 116-20.
[9] J. Minkus. "Circulants and Horadam's Sequences." *A Collection of Manuscripts Related to the Fibonacci Sequence*, Santa Clara: The Fibonacci Association, 1980, 48-52.
[10] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* New York: Springer-Verlag New York Inc., 1992.
[11] J. Vinson. "The Relation of the Period Modulo to the Rank of Apparition of m in the Fibonacci Sequence." *The Fibonacci Quarterly* **1.1** (1963): 37-46.
[12] D. D. Wall. "Fibonacci Series Modulo m." *American Mathematical Monthly* **67** (1960): 525-32.
[13] H. Wilcox. "Fibonacci Sequences of Period n in Groups." *The Fibonacci Quarterly* **24.4** (1986): 356-61.

AMS Classification Numbers: 11B39, 11B50, 14H52

✠ ✠ ✠