Algebra and Discrete Mathematics
Volume **25** (2018). Number 1, pp. 1–17

RESEARCH ARTICLE

Periods of Tribonacci sequences and elliptic curves

Lyes Ait-Amrane and Hacène Belbachir

Communicated by V. V. Kirichenko

Abstract. We will study the periods of Tribonacci sequences associated to elliptic curves. This work is motivated by a paper of Coleman *et al.* who did it for classical Fibonacci sequences. We are convinced that similar results modulo a deeper work are accessible. Our aim is to explore the Tribonacci case.

1. Introduction and preliminaries

Several works which make links between elliptic curves and linear recurrence sequences were done, essentially with Fibonacci sequences and their generalizations, for example, the work of Ribenboim [13] which provides the points with integral coordinates in certain elliptic curves. An other link is to determine perfect powers in elliptic divisibility sequences, as mentioned in the paper of Reynolds [12], where he presents the use of Fibonacci numbers in elliptic divisibility sequences. Bugeaud *et al.* [8] showed, by modular techniques inspired from the proof of Fermat's last theorem, that the only perfect powers in the Fibonacci sequence are $1, 8$ and 144. Also, there was studies of periods of generalized Fibonacci sequences, for example, the work of Brent [7].

The purpose of this work is to make a link between enumerative combinatorics and number theory through elliptic curves. More specifically,

2010 MSC: Primary 11B50; Secondary 11G05, 11A07, 11A41, 11B37, 11B39.
Key words and phrases: elliptic curves, periods of sequences, Tribonacci sequence, generalized Fibonacci sequences, prime numbers, congruences.

the study of periods of linear recurrence sequences over elliptic curves. There is a first work which was done by Coleman *et al.* [9] who studied periods of classical Fibonacci sequences on elliptic curves and it appears that this work can be viewed in a more general framework. We know that the Fibonacci sequence can be recovered as the sum of the main rays of Pascal's triangle, that is, we can consider that each element F_{n+1} of the Fibonacci sequence $(F_n)_n$ is the sum of the binomial coefficients $\binom{n-k}{k}$. In this context there are two ways to generalize the work of Coleman *et al.* [9]. Knowing that the Fibonacci sequence is a linear recurrence sequence of order 2, we are interested to see whether we could understand and reproduce this work for linear recurrence sequences of order s. However, determining properties related to the divisibility of primes for linear sequences of order s is not an easy thing. So, for showing that it can be generalized and have a first step towards a broader program, we will do the work at first for Tribonacci sequences, that is, the linear recurrence sequence of order 3, see for instance [2]. Still in relation to Pascal's triangle, each element of the linear recurrence sequence of order 3 is the sum of the main rays of a generalized Pascal's triangle, named the bi^{2}nomial coefficients (for the appellation see [3]) and denoted by $\binom{n}{a}_2$, for a complete overview see [1, 4]. We can recovered this Pascal's triangle through the generating function $(1+x+x^2)^n$ and therefore, the elements of the Tribonacci sequence $(T_n)_n$ are given by $T_{n+2} = \sum_k \binom{n-k}{k}_2$ and satisfy $T_0 = T_1 = 0, T_2 = 1$ and the linear recurrence relation $T_{n+1} = T_n + T_{n-1} + T_{n-2}$. It is known that $(T_n \mod m)$ is finite and simply periodic for any modulus $m > 1$, see [14, 16]. That is, the first three terms which are repeated in $(T_n \mod m)_n$ are $0, 0, 1$. We denote by $k(m)$ the least positive integer satisfying $T_{k(m)} \equiv T_{k(m)+1} \equiv 0 \mod m$ and $T_{k(m)+2} \equiv 1 \mod m$. It is easy to see that if τ is a positive integer satisfying $T_\tau \equiv T_{\tau+1} \equiv 0 \mod m$ and $T_{\tau+2} \equiv 1 \mod m$, then $k(m)|\tau$. We will define Tribonacci sequences on an elliptic curve, then make the link between periods of classical Tribonacci sequences modulo m and periods of Tribonacci sequences on an elliptic curve, which will allow us to apply the known results in the classical case to the case of elliptic curves. Let $t(x) = x^3 - x^2 - x - 1$ be the Tribonacci polynomial and let $I = \{3, 5, 23, 31, \dots\}$ be the set of all primes p for which $t(x)$ is irreducible over $\mathbb{F}_p$, $Q = \{7, 13, 17, 19, \dots\}$ be the set of all primes p for which $t(x)$ splits over $\mathbb{F}_p$ into the product of a linear factor and an irreducible quadratic factor and $L = \{2, 11, 47, 53, \dots\}$ be the set of all primes p for which $t(x)$ completely splits over $\mathbb{F}_p$ into linear factors, see [11] for more details about the sets I, Q and L. Then we have

the following theorem that contains some of the fundamental properties known about the periods of the Tribonacci sequence modulo m.

Theorem 1. *Let $p \neq 2, 11$ be a prime. Then*
(a) *If $p \in L$, then $k(p)|(p-1)$.*
(b) *If $p \in Q$, then $k(p)|(p^2-1)$.*
(c) *If $p \in I$, then $k(p)|(p^2+p+1)$.*
(d) *If m has prime factorization $\prod p_i^{e_i}$, then $k(m) = \operatorname{lcm}(k(p_i^{e_i}))$.*
(e) *If $n|m$, then $k(n)|k(m)$.*

Proof. See [11] for (a)-(c) and [14, 16] for (d). For (e) Suppose that $n|m$ and let $\sigma = k(n), \tau = k(m)$. Then σ is the least positive integer satisfying $T_\sigma \equiv T_{\sigma+1} \equiv 0 \mod n, T_{\sigma+2} \equiv 1 \mod n$ and τ is the least positive integer satisfying $T_\tau \equiv T_{\tau+1} \equiv 0$ and $T_{\tau+2} \equiv 1 \mod m$. By hypothesis, we have $n|m$ from which we deduce that $T_\tau \equiv T_{\tau+1} \equiv 0 \mod n, T_{\tau+2} \equiv 1 \mod n$ and therefore $\sigma|\tau$. □

For instance, the Tribonacci sequence modulo 3 is given by 0, 0, 1, 1, 2, 1, 1, 1, 0, 2, 0, 2, 1, 0, 0, 1, ..., which implies that $k(3) = 13|(3^2+3+1) = 13$ and so (c) is satisfied. The Tribonacci sequence modulo 6 is 0, 0, 1, 1, 2, 4, 1, 1, 0, 2, 3, 5, 4, 0, 3, 1, 4, 2, 1, 1, 4, 0, 5, 3, 2, 4, 3, 3, 4, 4, 5, 1, 4, 4, 3, 5, 0, 2, 1, 3, 0, 4, 1, 5, 4, 4, 1, 3, 2, 0, 5, 1, 0, 0, ..., and thus $k(6) = 52$. Modulo 2 the sequence is 0, 0, 1, 1, 0, 0, 1, ..., and thus $k(2) = 4$. Hence, part (d) is also satisfied since $\operatorname{lcm}(k(2), k(3)) = \operatorname{lcm}(4, 13) = 52 = k(6)$. We see also that (e) is satisfied because 2, 3|6 and $k(2)$, $k(3)|k(6)$.

2. The (a, b, c)-Tribonacci sequence

The (a, b, c)-Tribonacci sequence is a sequence $(G_n)_n$ defined by a triple of initial conditions values $G_0 = a$, $G_1 = b$, $G_2 = c$, and a recurrence relation $G_{n+1} = G_n + G_{n-1} + G_{n-2}$, where a, b, c are integers. The $(4, 4, 2)$-Tribonacci sequence modulo 6 is 4, 4, 2, 4, 4, 4, 0, 2, 0, 2, 4, 0, 0, 4, 4, 2, ... We see that the three initial conditions are repeated and hence, the $(4, 4, 2)$-Tribonacci sequence modulo 6 is simply periodic. The following proposition tells us that the (a, b, c)-Tribonacci sequence modulo m is simply periodic and we can express it in terms of the Tribonacci sequence.

Proposition 1. *Let a, b, c and m be integers with $m > 1$.*
(a) *The (a, b, c)-Tribonacci sequence satisfies*

$$G_n = aT_{n-1} + b(T_{n-1} + T_{n-2}) + cT_n \quad \text{for } n \geqslant 0, \tag{1}$$

with $T_{-1} = 1$ and $T_{-2} = -1$.

(b) *The (a,b,c)-Tribonacci sequence modulo m is simply periodic.*

Proof. (a) This follows from a straightforward induction.

(b) The same proof as for the Tribonacci sequence (T_n) holds, see [14, 16] for the case of the $(0,0,1)$-sequence. We can also check it directly from (1) and the simply periodicity of the Tribonacci sequence (T_n). □

We denote by $k(a,b,c;m)$ the period of $(G_n \mod m)_n$. That is, the least positive integer k satisfying $T_k \equiv T_0 \mod m$, $T_{k+1} \equiv T_1 \mod m$ and $T_{k+2} \equiv T_2 \mod m$. We can see in the previous examples that $k(4,4,2;6) = 13|52 = k(6)$. The following proposition tells us, among other, that we have $k(a,b,c;m)|k(m)$.

Proposition 2. *Let (G_n) be the (a,b,c)-Tribonacci sequence where a, b, c and m are any integers with $m > 1$.*

(a) *If $G_n \equiv G_0 \mod m$, $G_{n+1} \equiv G_1 \mod m$ and $G_{n+2} \equiv G_2 \mod m$, then $k(a,b,c;m)|n$.*
(b) *$k(a,b,c;m)|k(m)$.*
(c) *$k(0,0,c;m) = k(c,0,0;m)$ and $k(0,0,c;m)|k(m)$.*
(d) *If $\gcd(c,m) = 1$, then $k(0,0,c;m) = k(m)$.*
(e) *$k(a,b,c;m)|\operatorname{lcm}(k(a,0,0;m), k(0,b,0;m), k(0,0,c;m))$.*

Proof. (a) It follows from the definition of periodicity and Proposition 1(b).

(b) Relation (1) implies that

$$\begin{aligned} G_{k(m)} &= aT_{k(m)-1} + b(T_{k(m)-1} + T_{k(m)-2}) + cT_{k(m)}, \\ G_{k(m)+1} &= aT_{k(m)} + b(T_{k(m)} + T_{k(m)-1}) + cT_{k(m)+1}, \\ G_{k(m)+2} &= aT_{k(m)+1} + b(T_{k(m)+1} + T_{k(m)}) + cT_{k(m)+2}, \end{aligned}$$

which imply that

$$\begin{aligned} G_{k(m)} &\equiv aT_{-1} + b(T_{-1} + T_{-2}) + cT_0 \mod m, \\ G_{k(m)+1} &\equiv aT_0 + b(T_0 + T_{-1}) + cT_1 \mod m, \\ G_{k(m)+2} &\equiv aT_1 + b(T_1 + T_0) + cT_2 \mod m, \end{aligned}$$

so we obtain $G_{k(m)} \equiv G_0, G_{k(m)+1} \equiv G_1, G_{k(m)+2} \equiv G_2 \mod m$, and the result follows from (a).

(c) The part one follows from the fact that the $(c,0,0)$-Tribonacci sequence begins by c, 0, 0, c giving the same sequence as the $(0,0,c)$-Tribonacci sequence except for the staring point. Part two is a special case of (b).

(d) Relation (1) implies that the general term of the $(0,0,c)$-Tribonacci sequence is $G_n = cT_n$. If $\gcd(c,m) = 1$, then c is invertible modulo m and so $cT_i \equiv cT_j \mod m$ if and only if $T_i \equiv T_j \mod m$. Thus, $k(0,0,c;m) = k(m)$.

(e) Let $\sigma = k(a,0,0;m)$, $\tau = k(0,b,0;m)$ and $\theta = k(0,0,c;m)$. Relation (1) implies, by considering general terms of the $(a,0,0)$, $(0,b,0)$ and $(0,0,c)$-sequences, that $aT_{\sigma-1} \equiv a$, $aT_\sigma \equiv 0$, $aT_{\sigma+1} \equiv 0 \mod m$, $b(T_{\tau-1} + T_{\tau-2}) \equiv 0$, $b(T_\tau + T_{\tau-1}) \equiv b$, $b(T_{\tau+1} + T_\tau) \equiv 0 \mod m$ and $cT_\theta \equiv 0, cT_{\theta+1} \equiv 0, cT_{\theta+2} \equiv c \mod m$. Let $\rho = \operatorname{lcm}(\sigma,\tau,\theta)$. Since $\sigma|\rho, \tau|\rho$ and $\theta|\rho$, then $aT_{\rho-1} \equiv a$, $aT_\rho \equiv 0$, $aT_{\rho+1} \equiv 0 \mod m$, $b(T_{\rho-1}+T_{\rho-2}) \equiv 0$, $b(T_\rho + T_{\rho-1}) \equiv b$, $b(T_{\rho+1} + T_\rho) \equiv 0 \mod m$ and $cT_\rho \equiv 0$, $cT_{\rho+1} \equiv 0$, $cT_{\rho+2} \equiv c \mod m$. These facts and relation (1) give $G_\rho \equiv a$, $G_{\rho+1} \equiv b$ and $G_{\rho+2} \equiv c \mod m$. Hence $k(a,b,c;m)|\rho$. □

Let us now consider a binary relation $\sim$ on the set $(\mathbb{Z}/m\mathbb{Z})^3$ defined by $(a,b,c) \sim (q,r,t)$ if and only if, in the (a,b,c)-Tribonacci sequence, there is an index i such that $G_i \equiv q \mod m$, $G_{i+1} \equiv r \mod m$ and $G_{i+2} \equiv t \mod m$. Since three successive terms completely determine the sequence modulo m, this is an equivalence on $(\mathbb{Z}/m\mathbb{Z})^3$. Table 1 gives all the equivalence classes modulo 6.

A Tribonacci sequence of period d modulo m is of the form x_1, x_2, x_3, …, x_d, $x_{d+1} \equiv x_1$, $x_{d+2} \equiv x_2$, …. Hence, the distinct triples which are composed from three consecutive terms in this sequence are (x_1,x_2,x_3), (x_2,x_3,x_4), …, (x_d,x_1,x_2). Thus, we have d triples and we deduce that the size of the equivalence class containing (a,b,c) is $d = k(a,b,c;m)$. 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 that $c_1(6) = 2$, $c_2(6) = 1$, $c_4(6) = 1$, $c_{13}(6) = 4$, $c_{26}(6) = 2$, $c_{52}(6) = 2$, and all other $c_d(6) = 0$ for all other d.

The following Theorem counts the elements of $(\mathbb{Z}/m\mathbb{Z})^3$ corresponding to the partition of that set into equivalence classes.

Theorem 2. *Let $m > 1$ and $c_d(m)$ be defined as above, then*

$$m^3 = \sum_{d|k(m)} c_d(m)d.$$

Proof. The same proof as in the Fibonacci case holds, see [9], or see [10]. □

We have seen in Table 1 that modulo 6, there are classes that have different sizes. However, except for the $(0,0,0)$-classes which always has

$k(a,b,c;6)$	(a,b,c)
1	$(0,0,0)$
52	$(0,0,1),(0,1,1),(1,1,2),(1,2,4),(2,4,1),(4,1,1),(1,1,0),$ $(1,0,2),(0,2,3),(2,3,5),(3,5,4),(5,4,0),(4,0,3),(0,3,1),$ $(3,1,4),(1,4,2),(4,2,1),(2,1,1),(1,1,4),(1,4,0),(4,0,5),$ $(0,5,3),(5,3,2),(3,2,4),(2,4,3),(4,3,3),(3,3,4),(3,4,4),$ $(4,4,5),(4,5,1),(5,1,4),(1,4,4),(4,4,3),(4,3,5),(3,5,0),$ $(5,0,2),(0,2,1),(2,1,3),(1,3,0),(3,0,4),(0,4,1),(4,1,5),$ $(1,5,4),(5,4,4),(4,4,1),(4,1,3),(1,3,2),(3,2,0),(2,0,5),$ $(0,5,1),(5,1,0),(1,0,0).$
13	$(0,0,2),(0,2,2),(2,2,4),(2,4,2),(4,2,2),(2,2,2),(2,2,0),$ $(2,0,4),(0,4,0),(4,0,4),(0,4,2),(4,2,0),(2,0,0).$
4	$(0,0,3),(0,3,3),(3,3,0),(3,0,0).$
13	$(0,0,4),(0,4,4),(4,4,2),(4,2,4),(2,4,4),(4,4,4),(4,4,0),$ $(4,0,2),(0,2,0),(2,0,2),(0,2,4),(2,0,4),(4,0,0).$
52	$(0,0,5),(0,5,5),(5,5,4),(5,4,2),(4,2,5),(2,5,5),(5,5,0),$ $(5,0,4),(0,4,3),(4,3,1),(3,1,2),(1,2,0),(2,0,3),(0,3,5),$ $(3,5,2),(5,2,4),(2,4,5),(4,5,5),(5,5,2),(5,2,0),(2,0,1),$ $(0,1,3),(1,3,4),(3,4,2),(4,2,3),(2,3,3),(3,3,2),(3,2,2),$ $(2,2,1),(2,1,5),(1,5,2),(5,2,2),(2,2,3),(2,3,1),(3,1,0),$ $(1,0,4),(0,4,5),(4,5,3),(5,3,0),(3,0,2),(0,2,5),(2,5,1),$ $(5,1,2),(1,2,2),(2,2,5),(2,5,3),(5,3,4),(3,4,0),(4,0,1),$ $(0,1,5),(1,5,0),(5,0,0).$
26	$(1,4,1),(4,1,0),(1,0,5),(0,5,0),(5,0,5),(0,5,4),(5,4,3),$ $(4,3,0),(3,0,1),(0,1,4),(1,4,5),(4,5,4),(5,4,1),(4,1,4),$ $(1,4,3),(4,3,2),(3,2,3),(2,3,2),(3,2,1),(2,1,0),(1,0,3),$ $(0,3,4),(3,4,1),(4,1,2),(1,2,1),(2,1,4).$
2	$(0,3,0),(3,0,3).$
13	$(5,5,5),(5,5,3),(5,3,1),(3,1,3),(1,3,1),(3,1,5),(1,5,3),$ $(5,3,3),(3,3,5),(3,5,5),(5,5,1),(5,1,5),(1,5,5).$
1	$(3,3,3)$
13	$(1,1,1),(1,1,3),(1,3,5),(3,5,3),(5,3,5),(3,5,1),(5,1,3),$ $(1,3,3),(3,3,1),(3,1,1),(1,1,5),(1,5,1),(5,1,1).$
26	$(5,0,3),(0,3,2),(3,2,5),(2,5,4),(5,4,5),(4,5,2),(5,2,5),$ $(2,5,0),(5,0,1),(0,1,0),(1,0,1),(0,1,2),(1,2,3),(2,3,0),$ $(3,0,5),(0,5,2),(5,2,1),(2,1,2),(1,2,5),(2,5,2),(5,2,3),$ $(2,3,4),(3,4,3),(4,3,4),(3,4,5),(4,5,0).$

Table 1. The (a,b,c)-equivalence classes modulo 6.

Divisor d	1	31
$c_d(10)$	1	4

Table 2. Lengths and number of equivalence classes modulo 5.

length 1, we may have every class has length $k(m)$, as exhibited in Table 2 by the case when $m = 5$, with $k(m) = 31$.

The small equivalence classes are described by the following proposition.

Proposition 3. *Let $m > 1$ be an integer.*

(a) $c_1(m) = 1$ *if m is odd and* $c_1(m) = 2$ *if m is even.*
(b) $c_2(m) = 0$ *if m is odd and* $c_2(m) = 1$ *if m is even.*
(c) $c_3(m) = 0$.
(d) $c_4(m) = 0$ *if* $m \equiv 1, 3 \mod 4$, $c_4(m) = 1$ *if* $m \equiv 2 \mod 4$ *and* $c_4(m) = 3$ *if* $m \equiv 0 \mod 4$.

Proof. (a) A sequence of period 1 is of the form a, a, a, a, ... modulo m. Thus, $a + a + a \equiv a \mod m$, so $2a \equiv 0 \mod m$. If m is odd, we get that $a \equiv 0 \mod m$ and the sequence is in fact 0, 0, 0,.... Hence, $c_1(m) = 1$. If m is even, we get that $a \equiv 0 \mod \frac{m}{2}$. In this case, we have the two sequences 0, 0, 0,... and $\frac{m}{2}$, $\frac{m}{2}$, $\frac{m}{2}$, ... Hence, $c_1(m) = 2$.

(b) A sequence of period 2 is of the form a, b, a, b, a, ... $\mod m$. Thus, $a + b + a \equiv b \mod m$ and $b + a + b \equiv a \mod m$, which gives us $2a \equiv 2b \equiv 0 \mod m$. If m is odd, we get that $a \equiv b \equiv 0 \mod m$. This yields the sequence 0, 0, 0, ..., which is in fact a sequence of period 1. Hence, $c_2(m) = 0$. If m is even, we get that $a \equiv b \equiv 0 \mod \frac{m}{2}$. This yields a sequence of period 2, which is (up to order) 0, $\frac{m}{2}$, 0, $\frac{m}{2}$, ..., and two sequences of period 1, which are 0, 0, 0, ... and $\frac{m}{2}$, $\frac{m}{2}$, $\frac{m}{2}$, ... Hence $c_2(m) = 1$.

(c) A sequence of period 3 is of the form a, b, c, a, b, c, ... $\mod m$. Thus we have $a+b+c \equiv a \mod m$, $b+c+a \equiv b \mod m$ and $c+a+b \equiv c \mod m$, which gives us $2a \equiv 2b \equiv 2c \equiv 0 \mod m$. If m is odd, we get that $a \equiv b \equiv c \equiv 0 \mod m$. This yields the sequence 0, 0, 0, ..., which is in fact a sequence of period 1. Hence, $c_3(m) = 0$. If m is even, we get that $a \equiv b \equiv c \equiv 0 \mod \frac{m}{2}$. This yields a sequence of period 2 which is (up to order) 0, $\frac{m}{2}$, 0, $\frac{m}{2}$, ..., two sequences of period 1 which are 0, 0, 0, ... and $\frac{m}{2}$, $\frac{m}{2}$, $\frac{m}{2}$, ..., the other cases give the same sequence of order 4 which is (up to order) $\frac{m}{2}$, $\frac{m}{2}$, 0, 0, $\frac{m}{2}$, $\frac{m}{2}$, ... Hence, $c_3(m) = 0$.

(d) A sequence of period 4 may be written as a, b, c, $a+b+c$, $a+2b+2c$, $2a + 3b + 4c$, $4a + 6b + 7c$, ... $\mod m$. Thus we have $a + 2b + 2c \equiv a \mod m$, $2a + 3b + 4c \equiv b \mod m$ and $4a + 6b + 7c \equiv c \mod m$, which implies $2b + 2c \equiv 2a + 2c \equiv 2a + 2b \equiv 0 \mod m$. If m is odd, we get that $b + c \equiv a + c \equiv a + b \equiv 0 \mod m$, which implies that $2a \equiv 2b \equiv 2c \equiv 0 \mod m$ and hence $a \equiv b \equiv c \equiv 0 \mod m$. Thus, we have a sequence of period 1 which is 0, 0, 0, ... and $c_4(m) = 0$. If m is even, we get that

$b+c \equiv a+c \equiv a+b \equiv 0 \mod \frac{m}{2}$, which implies that $2a \equiv 2b \equiv 2c \equiv 0 \mod \frac{m}{2}$, here too, we distinguish two cases. If $\frac{m}{2}$ is odd, then we have $a \equiv b \equiv c \equiv 0 \mod \frac{m}{2}$ and we obtain a class of size 4 which is $(0,0,\frac{m}{2})$, two classes of size 1 which are $(0,0,0)$, $(\frac{m}{2},\frac{m}{2},\frac{m}{2})$ and one class of size 2 which is $(0,\frac{m}{2},0)$. Hence $c_4(m)=1$. If $\frac{m}{2}$ is even, then $a \equiv b \equiv c \equiv 0 \mod \frac{m}{4}$ and we obtain 2 classes of size 1 which are $(0,0,0,)$, $(\frac{m}{2},\frac{m}{2},\frac{m}{2})$, one class of size 2 which is $(0,\frac{m}{2},0)$, three classes of size 4 which are $(0,0,\frac{m}{2})$, $(\frac{m}{4},\frac{m}{4},\frac{m}{4})$, $(\frac{m}{4},\frac{3m}{4},\frac{3m}{4})$ and six classes of size 8 which are $(0,0,\frac{m}{4})$, $(0,0,\frac{3m}{4})$, $(0,\frac{m}{4},0)$, $(0,\frac{m}{2},\frac{3m}{4})$, $(0,\frac{m}{2},\frac{3m}{4})$, $(0,\frac{3m}{4},0)$. Hence, $c_4(m)=3$. □

Now we consider, in a general manner, an (x_1,x_2,x_3)-Tribonacci sequence of period d modulo m, then we have $x_1+x_2+x_3 \equiv x_4, x_2+x_3+x_4 \equiv x_5, \ldots, x_{d-1}+x_d+x_1 \equiv x_2$. Thus, we obtain

$$\begin{pmatrix} 1 & 1 & 1 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & -1 & \cdots & 0 & 0 & 0 \\ \vdots & & \vdots & & & & \ddots & & & \vdots \\ -1 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \\ 1 & 1 & -1 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{d-2} \\ x_{d-1} \\ x_d \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix} \mod m.$$

We call the $d \times d$ matrix above, the circulant Tribonacci matrix, and we denote it by W_d. The standard circulant matrix is the following $n \times n$ matrix

$$\pi_n = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

We denote by $w_n = \det(W_n)$ the determinant of the Tribonacci circulant matrix. Since the matrix π_n has n distinct eigenvalues which are the n^{th} roots of unity and $W_n = I_n + \pi_n + \pi_n^2 - \pi_n^3$, where I_n is the identity matrix, we deduce that the eigenvalues of W_n are $1 + e^{2i\pi j/n} + e^{4i\pi j/n} - e^{6i\pi j/n}$ for $0 \leqslant j \leqslant n-1$, and so $w_n = \prod_{j=0}^{n-1}(1 + e^{2i\pi j/n} + e^{4i\pi j/n} - e^{6i\pi j/n})$. The next theorem gives us a relation between w_n and the period of the Tribonacci sequence modulo m.

Theorem 3. *Let a, b and c be integers with $(a,b,c) \not\equiv (0,0,0) \mod m$, where $m > 1$ is an integer. If $l = k(a,b,c;m)$, then* $\gcd(w_l, m) \neq 1$.

Proof. Assume that $\gcd(w_l, m) = 1$, then W_l is invertible modulo m. Thus, the system $W_l X \equiv 0 \mod m$ has only $X \equiv 0 \mod m$ as solution. But if we let (G_n) denotes the (a, b, c)-Tribonacci sequence modulo m, then $X = (G_1, \ldots, G_l)$ is a non trivial solution of $W_l X \equiv 0 \mod m$, which gives the desired contradiction. □

Table 3 gives some values of the sequence (w_n). For instance, if we consider $w_{13} = 2862 = 2 \cdot 3^3 \cdot 53$, then Theorem 5 tells us that if a sequence has period length 13 modulo m, then $2, 3$ or $53|m$. As an example, it is easy to see that $k(2, 2, 4; 6) = 13$ and we have $\gcd(w_{13}, 6) = 6$. Thus, the prime factors of w_n give a finite list of primes, if none of them divides m, then n can not be a period of a Tribonacci sequence modulo m.

n	w_n	n	w_n
4	$16 = 2^4$	20	$195536 = 2^4 \cdot 11^2 \cdot 101$
5	$22 = 2 \cdot 11$	21	$361286 = 2 \cdot 43 \cdot 4201$
6	$28 = 2^2 \cdot 7$	22	$665372 = 2^2 \cdot 397 \cdot 419$
7	$86 = 2 \cdot 43$	23	$1219462 = 2 \cdot 47 \cdot 12973$
8	$128 = 2^7$	24	$2248064 = 2^7 \cdot 7 \cdot 13 \cdot 193$
9	$218 = 2 \cdot 109$	25	$4134922 = 2 \cdot 11 \cdot 187951$
10	$484 = 2^2 \cdot 11^2$	26	$7595748 = 2^2 \cdot 3^3 \cdot 53 \cdot 1327$
11	$794 = 2 \cdot 397$	27	$13985354 = 2 \cdot 109 \cdot 64153$
12	$1456 = 2^4 \cdot 7 \cdot 13$	28	$25718128 = 2^4 \cdot 29 \cdot 43 \cdot 1289$
13	$2862 = 2 \cdot 3^3 \cdot 53$	29	$47283806 = 2 \cdot 23641903$
14	$4988 = 2^2 \cdot 29 \cdot 43$	30	$87007228 = 2^2 \cdot 7 \cdot 11^2 \cdot 61 \cdot 421$
15	$9262 = 2 \cdot 11 \cdot 421$	31	$160006750 = 2 \cdot 5^3 \cdot 640027$
16	$17408 = 2^10 \cdot 17$	32	$294264832 = 2^{13} \cdot 17 \cdot 2113$
17	$31282 = 2 \cdot 15641$	33	$541334114 = 2 \cdot 397 \cdot 681781$
18	$57988 = 2^2 \cdot 7 \cdot 19 \cdot 109$	34	$995580932 = 2^2 \cdot 15641 \cdot 15913$
19	$107314 = 2 \cdot 53657$	35	$1831116386 = 2 \cdot 11 \cdot 43 \cdot 1935641$

Table 3. The w_n numbers and their prime factorizations.

3. Tribonacci sequences on elliptic curves

Let $E : y^2 = x^3 + ax + b$ be a non-singular elliptic curve over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where p is a prime such that $p > 2$. Let α, β, γ be the roots of the cubic which are distinct since E is non-singular, these roots may be in an extension of $\mathbb{F}_p$. We recall that the points of order 2 in E are $(\alpha, 0), (\beta, 0)$ and $(\gamma, 0)$. The identity element is the point at infinity denoted by O. We set $E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + ax + b\} \cup \{O\}$.

See [15] for more details about the addition of points on such an elliptic curve. In what follows, p will denote an odd prime, $h = ord\big(E(\mathbb{F}_p)\big)$ and $h_R = ord(R)$, for any point $R \in E(\mathbb{F}_p)$.

Let A, B and C be three points of $E(\mathbb{F}_p)$. We define the (A, B, C)-Tribonacci sequence, denoted by $(H_n)_n$, by $H_0 = A, H_1 = B, H_2 = C$ and the linear recurrence relation $H_{n+1} = H_n + H_{n-1} + H_{n-2}$. First, we establish some basic properties of (H_n).

Proposition 4. *Let A, B and C be three points of $E(\mathbb{F}_p)$.*
(a) *The (A, B, C)-Tribonacci sequence (H_n) is given by*

$$H_n = [T_{n-1}]A + [T_{n-2} + T_{n-1}]B + [T_n]C. \tag{2}$$

(b) *The (O, O, C)-Tribonacci sequence is $H_n = [T_n]C$.*
(c) *The (O, B, O)-Tribonacci sequence is $H_n = [T_{n-2} + T_{n-1}]B$.*
(d) *The (A, B, C)-Tribonacci sequence (H_n) is simply periodic.*

Proof. (a) This follows from a straightforward induction. (b) and (c) are special cases of (a) with $A = B = O$ for (b) and $A = C = O$ for (c). The proof of (d) follows from an argument similar to the proof of Proposition 1(b) since the group $E(\mathbb{F}_p)$ is finite. □

We denote by $K(A, B, C; E)$ the period of the (A, B, C)-Tribonacci sequence. That is, the least positive integer k satisfying $H_k = A, H_{k+1} = B$ and $H_{k+2} = C$.

Lemma 1. *If P is a point of E and m, n are integers, then $[m]P = [n]P$ if and only if $m \equiv n \mod h_P$.*

Proof. See [9]. □

Lemma 1 allows us to make the connection between the periods of elliptic curves and periods of ordinary Tribonacci sequences. We will see that the period of the (O, O, C) sequence depends only on h_C so that any points C with the same order will generate Tribonacci sequences with exactly the same length. Once this connection is made, we cane generalize properties of Tribonacci numbers to the (O, O, C)-Tribonacci sequences on elliptic curves.

Theorem 4. *Let A, B and C be points of $E(\mathbb{F}_p)$. Then:*
(a) *$K(O, O, C; E) = K(C, O, O; E) = k(h_C)$. If h_C is odd, then we have $K(O, C, O; E) = k(h_C)$.*
(b) *$K(O, C, O; E) | k(h_C)$.*

(c) $K(A,B,C;E) \mid \operatorname{lcm}(K(A,O,O;E), K(O,B,O;E), K(O,O,C;E))$.

Proof. (a) The equality $K(O,O,C;E) = K(C,O,O;E)$ is obvious since the two sequences are the same. Proposition 4(b) tells us that the (O,O,C)-sequence is $H_n = [T_n]C$. Let $c = K(O,O,C;E)$, then $[0]C = H_c = [T_c]C, [0]C = H_{c+1} = [T_{c+1}]C$ and $[1]C = H_{c+2} = [T_{c+2}]C$. By Lemma 1, this happens if and only if $T_c \equiv 0, T_{c+1} \equiv 0$ and $T_{c+2} \equiv 1$ modulo h_C. Since c is the smallest such integer, $c = k(h_C)$. Suppose now that h_C is odd and let $c = K(O,C,O;E)$. Proposition 4(c) tells us that the (O,C,O)-sequence is $H_n = [T_{n-2} + T_{n-1}]C$. Hence, we have the following equivalent systems where the second equivalence comes from Lemma 1.

$$\begin{cases} H_0 = H_c \\ H_1 = H_{c+1} \\ H_2 = H_{c+2} \end{cases} \iff \begin{cases} [0]C = [T_{c-2} + T_{c-1}]C \\ [1]C = [T_{c-1} + T_c]C \\ [0]C = [T_c + T_{c+1}]C \end{cases}$$

$$\iff \begin{cases} T_{c-2} + T_{c-1} \equiv 0 \mod (h_C) \\ T_{c-1} + T_c \equiv 1 \mod (h_C) \\ T_c + T_{c+1} \equiv 0 \mod (h_C) \end{cases}$$

$$\iff \begin{cases} 2T_{c+1} \equiv 0 \mod (h_C) \\ T_{c-1} + T_c \equiv 1 \mod (h_C) \\ T_c + T_{c+1} \equiv 0 \mod (h_C) \end{cases}$$

$$\iff \begin{cases} T_{c+1} \equiv 0 \mod (h_C) \\ T_{c-1} \equiv 1 \mod (h_C) \\ T_c \equiv 0 \mod (h_C) \end{cases}$$

$$\iff \begin{cases} T_{c+1} \equiv 0 \mod (h_C) \\ T_{c+2} \equiv 1 \mod (h_C) \\ T_c \equiv 0 \mod (h_C) \end{cases}$$

Since c is the smallest integer verifying the last system, then $c = k(h_C)$.

(b) If h_C is arbitrary, then the fourth equivalence above becomes an implication since

$$T_{c+1} \equiv 0 \mod (h_C) \Longrightarrow 2T_{c+1} \equiv 0 \mod (h_C).$$

Hence, the last system implies the first system, so $K(O,C,O;E) | k(h_C)$.

(c) The proof is analogue to that of Proposition 2(e). □

Since we have $k(h_C) = K(O,O,C;E)$, Some properties of the standard Tribonacci sequence may be translated to analogous properties for (O,O,C)-Tribonacci sequences on an elliptic curve.

Theorem 5. *Let A, B and C be three points of $E(\mathbb{F}_p)$.*
(a) *If $h_C \in L \setminus \{2, 11\}$, then $K(O, O, C; E) | (h_C - 1)$.*
(b) *If $h_C \in Q$, then $K(O, O, C; E) | (h_C^2 - 1)$.*
(c) *If $h_C \in I$, then $K(O, O, C; E) | (h_C^2 + h_C + 1)$.*
(d) *If h_C has prime factorization $\prod p_i^{e_i}$, then $K(O, O, C; E) = \operatorname{lcm}(k(p_i^{e_i}))$.*
(e) *If $h_A | h_C$, then $K(O, O, A; E) | K(O, O, C; E)$.*
(f) $K(A, B, C; E) \mid k(h)$.

Proof. (a)–(e) use the result of Theorem 4(a) in Theorem 1. For (f), we know that $h_A | h$, $h_B | h$ and $h_C | h$, we deduce from (e) and Theorem 4(a) and (b) that

$$\operatorname{lcm}(K(A, O, O; E), K(O, B, O; E), K(O, O, C; E)) | k(h).$$

The result follows from Theorem 4(c). □

Now we define, as for the ordinary Tribonacci sequences, an equivalence relation on Tribonacci sequences defined on elliptic curves. We say that (A', B', C') is equivalent to (A, B, C) if, in the (A, B, C)-Tribonacci sequence, there is an index i such that $H_i = A'$, $H_{i+1} = B'$ and $H_{i+2} = C'$. As for the ordinary case, the size of an equivalence class containing (A, B, C) is $K(A, B, C; E)$. We define $C_d(E)$ to be the number of distinct equivalence classes of size d.

We will see in the following theorem that we may not always have the same results as for the ordinary Tribonacci sequence modulo m.

Theorem 6. *Let A, B and C be three points of $E(\mathbb{F}_p)$ and w_c be the determinants of the Tribonacci circulant matrices as before.*

(a) $C_1(E) = \begin{cases} 1 & \text{if the cubic has no root in } \mathbb{F}_p, \\ 2 & \text{if the cubic has one root in } \mathbb{F}_p, \\ 4 & \text{if the cubic has three roots in } \mathbb{F}_p. \end{cases}$

(b) $C_2(E) = \begin{cases} 0 & \text{if the cubic has no root in } \mathbb{F}_p, \\ 1 & \text{if the cubic has one root in } \mathbb{F}_p, \\ 6 & \text{if the cubic has three roots in } \mathbb{F}_p. \end{cases}$

(c) *If $c = K(A, B, C; E)$, then $\gcd(w_c, h) \neq 1$.*

Proof. (a) and (b) follow from arguments analogous to those from the proof of Proposition 3. Indeed, if the cubic has no root in $\mathbb{F}_p$ and hence, no point of order 2 in $E(\mathbb{F}_p)$, then we have one sequence of period 1 which is (O, O, O) and no sequence of period 2. If there is one point P of order

2 in $E(\mathbb{F}_p)$, then we have two sequences of period 1 which are (O, O, O), (P, P, P) and one sequence of period 2 which is (O, P, O). If there are three points P_i, with $i = 1, 2, 3$, of order two in $E(\mathbb{F}_p)$, then we have four sequences of period 1 which are (O, O, O), (P_i, P_i, P_i) with $i = 1, 2, 3$, and six sequences of period 2 which are (O, P_i, O), (P_i, P_j, P_i) with $i, j = 1, 2, 3$ and $i < j$. (c) The same proof as in the Fibonacci case holds. See [9]. □

The next theorem is analogous to Theorem 2.

Theorem 7. *Let E be an elliptic curve over $\mathbb{F}_p$ with $p > 2$ and $C_d(E)$ be defined as before, then*

$$h^3 = \sum_{d|k(h)} C_d(E)d.$$

Proof. It follows from the fact that equivalence classes form a partition of $E(\mathbb{F}_p)^3$ and that, by Theorem 5(f), all classes have a size that divides $k(h)$. □

Example 1. On the elliptic curve $E : y^2 = x^3 + x + 1$ considered on $\mathbb{F}_5$ we have $E(\mathbb{F}_5) = \{O, P_i, 1 \leqslant i \leqslant 8\}$, where $P_1 = (0, 1)$, $P_2 = (4, 2)$, $P_3 = (2, 1)$, $P_4 = (3, 4)$, $P_5 = (3, 1)$, $P_6 = (2, 4)$, $P_7 = (7, 3)$, $P_8 = (0, 4)$. The point P_1 has order 9 and generates this group. We have $P_j = [j]P_1$ with $1 \leqslant j \leqslant 8$. Hence, $E(\mathbb{F}_5) \simeq \mathbb{Z}/9\mathbb{Z}$. Therefore, work on $E(\mathbb{F}_5)$ returns to work on the ordinary Tribonacci sequence modulo 9. This group has no point of order 2, hence $C_1(E) = 1 = c_1(9)$, $C_2(E) = 0 = c_2(9)$.

Example 2. On the elliptic curve $E : y^2 = x^3 + x$ considered on $\mathbb{F}_3$, the cubic has one root $x = 0$ in $\mathbb{F}_3$ and so, one point of order 2 in $E(\mathbb{F}_3)$ which is $(0, 0)$. The other non trivial points are $(2, 1)$, $(2, 2)$ which are of order 4. Hence, $E(\mathbb{F}_3) \simeq \mathbb{Z}/4\mathbb{Z}$. Therefore, work on $E(\mathbb{F}_3)$ returns to work on the ordinary Tribonacci sequence modulo 4 and we have $C_1(E) = 2 = c_1(4)$, $C_2(E) = 1 = c_2(4)$. Table 4 illustrates Theorem 7 for this elliptic curve. We have $ord(E(\mathbb{F}_3)) = 4$ and $k(4) = 8$.

Divisor d	1	2	4	8
$C_d(E)$	2	1	3	6

Table 4. Lengths and number of equivalence classes for $y^2 = x^3 + x$ on $\mathbb{F}_3$.

Example 3. On the elliptic curve $E : y^2 = x^3 - x$ considered on $\mathbb{F}_3$, the cubic has three roots in $\mathbb{F}_3$, so we have three points of order 2 in $E(\mathbb{F}_3) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In this case, we have $C_1(E) = 4$ and $C_2(E) = 6$, which does not occur on a ordinary Tribonacci sequence modulo m.

The following theorem tells us when we get the same results as in the ordinary case.

Theorem 8. *Let E be an elliptic curve over the finite field $\mathbb{F}_p$. Then*

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z} \quad or \quad \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

for some integer $n \geqslant 1$, or for some integers $n_1, n_2 \geqslant 1$ with n_1 dividing n_2.

Proof. See [15]. □

Corollary 1. *Let A, B and C be three points of $E(\mathbb{F}_p)$ and assume that $E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ for some integers $n_1, n_2 \geqslant 1$ with n_1 dividing n_2. Then $K(A, B, C; E)|k(n_2)$.*

Proof. It follows from a proof analogous to the proof of Theorem 5(f) with the fact that any point in $E(\mathbb{F}_p)$ has order dividing $n_2 = \frac{h}{n_1}$. □

Corollary 2. *Suppose that we have $E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ for some integers $n_1, n_2 \geqslant 1$ with n_1 dividing n_2. Then*

$$h^3 = \sum_{d|k(n_2)} C_d(E)d.$$

Proof. It follows from Theorem 7 and Corollary 1. □

Table 5 illustrates Corollary 2 for the elliptic curve $y^2 = x^3 + 2$ on $\mathbb{F}_7$. We have $E(\mathbb{F}_7) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, ord(E(\mathbb{F}_7)) = 9, k(3) = 13$ and $k(9) = 39$.

Divisor d	1	3	13	39
$C_d(E)$	1	0	56	0

Table 5. Lengths and number of equivalence classes for $y^2 = x^3 + 2$ on $\mathbb{F}_7$.

Conclusion and perspectives

We exhibit the periods of Tribonacci sequences with generalized initial conditions, modulo m, they satisfy many properties. We define Tribonacci matrices and we show how the determinants of these matrices restricts the period lengths. We give the concept of Tribonacci sequences on an elliptic curve and we make the link between the period of a regular Tribonacci sequence modulo m and the period of a Tribonacci sequence on an elliptic

curve, which allowed us to transfer some known properties in the ordinary case to the case of elliptic curves. Finally, we establish that Theorem 8 gives us the two classifications of the types of groups associated to elliptic curves over finite fields and interpret them in enumerative combinatorics. That is, express the number of distinct classes of the same size by recurrence linear sequences. Hence, Theorem 8 tells us when we have the same properties in both cases, that is to say, the classical case and the case of elliptic curves, and allow us to refine Theorem 7 when $E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$.

Our first perspective is to generalize what we do to the linear recurrence sequence (u_n) of order s, see [2], defined by

$$u_{n+1} = u_n + u_{n-1} + \cdots + u_{n-s},$$

with $n \geqslant s,\ u_0 = u_1 = \cdots = u_{s-1} = 0$ and $u_s = 1$. The elements of this linear recurrence sequence are the sum of principal rays of a generalized Pascal's triangle and given by $u_{n+s} = \sum_k \binom{n-k}{k}_s$, where $\binom{n}{k}_s$ are given by the generating function $(1 + x + \cdots + x^s)^n$, see [1, 4].

Our second perspective is to generalize to the linear recurrence sequence $(v_n)_n$, associated to different directions of the rays in Pascal's triangle, defined for $p, n, r \in \mathbb{N}, q \in \mathbb{Z}$ such that $0 \leqslant p \leqslant r-1$ and $q + r > 0$, by

$$v_{n+1} = \sum_{k=0}^{\lfloor (n-p)/(q+r) \rfloor} \binom{n-qk}{p+rk} x^{n-p-(q+r)k} y^{p+rk},$$

which satisfies the linear recurrence relation, see [5, 6]

$$v_n - x\binom{r}{1}v_{n-1} + x^2\binom{r}{2}v_{n-2} + \cdots + (-1)^r x^r \binom{r}{r} v_{n-r} = y^r v_{n-r-q}.$$

In the first instance, we will look for $r = 2$, which gives us the sequence of Morgan-Voyce, then we will see in a more general framework.

Acknowledgements

The authors would like to thank the anonymous reviewer for valuable remarks and suggestions to improve the original manuscript.

References

[1] H. Belbachir, *Determining the mode for convolution powers of discrete uniform distribution*, Probab. Engrg. Inform. Sci. 25 (2011), no. **4**, 469–475.

[2] H. Belbachir, F. Bencherif, *Linear recurrence sequences and powers of a square matrix*, Integers 6 (2006), A12, 17 pp.

[3] H. Belbachir, A. Benmezaï, *A q-analogue for bi-s-nomial coefficients and generalized Fibonacci sequences*, C. R. Math. Acad. Sci. Paris 352 (2014), no. **3**, 167–171.

[4] H. Belbachir, S. Bouroubi, A. Khelladi, *Connection between ordinary multinomials, Fibonacci numbers, Bell polynomials and discrete uniform distribution*, Ann. Math. Inform. 35 (2008), 21–30.

[5] H. Belbachir, T. Komatsu, L. Szalay, *Characterization of linear recurrences associated to rays in Pascal's triangle*, Diophantine analysis and related fields 2010, 90–99, AIP Conf. Proc., 1264, *Amer. Inst. Phys., Melville, NY*, 2010.

[6] H. Belbachir, T. Komatsu, L. Szalay, *Linear recurrences associated to rays in Pascal's triangle and combinatorial identities*, Math. Slovaca. 64 (2014), no. **2**, 287–300.

[7] P. R. Brent, *On the periods of generalized Fibonacci recurrences*, Math. Comp. 63 (1994), no. **207**, 389–401.

[8] Y. Bugeaud, M. Mignotte, S. Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers*, Ann. of Math. (2) 163 (2006), no. **3**, 969–1018.

[9] D. A. Coleman, C. J. Dugan, R. A. McEwen, C. A. Reiter, T. T. Tang, *Periods of (q, r)-Fibonacci sequences and elliptic curves*, Fibonacci Quart. 44 (2006), no. **1**, 59–70.

[10] J. Klaška, *Tribonacci partition formulas modulo m*, Acta Math. Sin. (Engl. Ser.) 26 (2010), no. **3**, 465–476.

[11] J. Klaška, L. Skula, *Periods of the Tribonacci sequence modulo a prime $p \equiv 1 \pmod 3$*, *Fibonacci Quart.* 48 (2010), no. **3**, 228–235.

[12] J. Reynolds, *Perfect powers in elliptic divisibility sequences*, J. Number Theory 132 (2012), no. **5**, 998–1015.

[13] P. Ribenboim, *An algorithm to determine the points with integral coordinates in certain elliptic curves*, J. Number Theory 74 (1999), no. **1**, 19–38.

[14] M. E. Waddill, *Some properties of a generalized Fibonacci sequence modulo m*, Fibonacci Quart. 16 (1978), no. **4**, 344–353.

[15] L. C. Washington, *Elliptic curves: Number theory and cryptography. Second edition. Discrete Mathematics and its Applications (Boca Raton)*, Chapman & Hall/CRC, Boca Raton, FL, 2008.

[16] C. C. Yalavigi, *Properties of Tribonacci numbers*, Fibonacci Quart. 10 (1972), no. **3**, 231–246.

Contact information

L. Ait-Amrane University of Sciences and Technology Houari Boumediene, Faculty of Mathematics, LATN Laboratory, BP 32, El Alia, 16111, Bab Ezzouar, Algiers, Algeria;
Ecole nationale Supérieure d'Informatique, BP 68M Oued Smar, 16270, El Harrach, Algiers, Algeria
E-Mail(*s*): lyesait@gmail.com, l_ait_amrane@esi.dz

H. Belbachir University of Sciences and Technology Houari Boumediene, Faculty of Mathematics, RECITS Laboratory, BP 32, El Alia, 16111, Bab Ezzouar, Algiers, Algeria
E-Mail(*s*): hacenebelbachir@gmail.com, hbelbachir@usthb.dz

Received by the editors: 28.10.2015
and in final form 25.02.2018.