# SEQUENCES ASSOCIATED TO ELLIPTIC CURVES

BETÜL GEZER

*Communicated by Alexandru Zaharescu*

Let $E$ be an elliptic curve defined over a field $K$ (with $char(K) \neq 2$) given by a Weierstrass equation and let $P = (x, y) \in E(K)$ be a point. Then for each $n \geq 1$ and some $\gamma \in K^*$ we can write the $x$- and $y$-coordinates of the point $[n]P$ as

$$[n]P = \left(\frac{\phi_n(P)}{\psi_n^2(P)}, \frac{\omega_n(P)}{\psi_n^3(P)}\right) = \left(\frac{\gamma^2 G_n(P)}{F_n^2(P)}, \frac{\gamma^3 H_n(P)}{F_n^3(P)}\right)$$

where $\phi_n, \psi_n, \omega_n \in K[x, y]$, $\gcd(\phi_n, \psi_n) = 1$ and

$$F_n(P) = \gamma^{1-n^2}\psi_n(P), G_n(P) = \gamma^{-2n^2}\phi_n(P), H_n(P) = \gamma^{-3n^2}\omega_n(P)$$

are suitably normalized division polynomials of $E$. In this work we show the coefficients of the elliptic curve $E$ can be defined in terms of the sequences of values $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ of the suitably normalized division polynomials of $E$ evaluated at a point $P \in E(K)$. Then we give the general terms of the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ associated to Tate normal form of an elliptic curve. As an application of this we determine square and cube terms in these sequences.

*AMS 2020 Subject Classification:* 14H52, 11B37, 11G07.

*Key words:* elliptic curves, rational points on elliptic curves, division polynomials, elliptic divisibility sequences, squares, cubes.

## 1. INTRODUCTION

Let $E$ be an elliptic curve defined over a field $K$ given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

For background on elliptic curves, see [28] and [29]. Let $E(K)$ be the group of $K$-rational points on $E$, let $\mathcal{O}$ denote the point at infinity, the identity for the group $K$-rational points. Let $K(E)$ denote the function field of $E$ over $K$. Then $z = -x/y \in K(E)$ is a uniformizer at $\mathcal{O}$ and the invariant differential $\omega = \mathrm{d}x/(2y + a_1x + a_3)$ has an expansion as a formal Laurent series in a formal neighborhood of $\mathcal{O}$ such that

$$\omega(z) = (1 + a_1z + (a_1^2 + a_2)z^2 + \cdots)\, dz.$$

This series has coefficients in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$, and the uniformizer $z$ and the differential $\omega$ at $\mathcal{O}$ satisfy $(\omega/dz)(\mathcal{O}) = 1$. Let $n \geq 1$ be an integer, and let $[n](z) \in K[[z]]$ be the power series defining the multiplication-by-$n$ map on the formal group of $E$. The *n-division polynomial* $F_n$ (normalized relative to the uniformizer $z$) is the unique function $F_n \in K(E)$ with divisor $[n]^{-1}(\mathcal{O}) - n^2(\mathcal{O})$ such that

$$\left(\frac{z^{n^2} F_n}{[n](z)}\right)(\mathcal{O}) = 1$$

as defined in [30, Definition 1], see also [18] for details.

If $E$ is an elliptic curve over $\mathbb{C}$, then $E$ has a complex uniformization $\Phi : \mathbb{C}/L \to E(\mathbb{C})$ with a lattice $L \subset \mathbb{C}$. The classical *n-division polynomial* $\psi_n$ of an elliptic curve $\mathbb{C}/L$ can be expressed in terms of the Weierstrass $\sigma$-function:

$$\psi_n(z) = \psi_n(z, L) = \frac{\sigma(nz, L)}{\sigma(z, L)^{n^2}} \quad \text{for all } n \geq 1,$$

where $\sigma(z, L)$ is the Weierstrass $\sigma$-function associated to the lattice $L$. Moreover, the classical $n$-division polynomial $\psi_n$ for the elliptic curve $E$ evaluated at point $P = (x, y)$ is defined using the initial values

$$\begin{aligned}
\psi_0(P) &= 0,\\
\psi_1(P) &= 1,\\
\psi_2(P) &= 2y + a_1x + a_3,\\
\psi_3(P) &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
\psi_4(P) &= \psi_2(P)(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2\\
&\quad +(b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)),
\end{aligned}$$

where the point $P$ correspond to $z \in \mathbb{C}/L$ and $b_i$ are the usual quantities [28, Chapter III.1], and by the formulas

$$\psi_{2n+1}(P) = \psi_{n+2}(P)\psi_n(P)^3 - \psi_{n-1}(P)\psi_{n+1}(P)^3, \quad \text{for } n \geq 2,$$
$$\psi_{2n}(P)\psi_2(P) = \psi_{n-1}(P)^2\psi_n(P)\psi_{n+2}(P) - \psi_{n-2}(P)\psi_n(P)\psi_{n+1}(P)^3, \text{ for } n \geq 3.$$

Let $P = (x, y)$ be a point of $E(K)$ (with $char(K) \neq 2$), and $n \geq 1$. The coordinates of the point $[n]P$ can be expressed in terms of the point $P$, that is, for some $\gamma \in K^*$

$$[n]P = \left(\frac{\phi_n(P)}{\psi_n(P)^2}, \frac{\omega_n(P)}{\psi_n(P)^3}\right) = \left(\frac{\gamma^2 G_n(P)}{F_n(P)^2}, \frac{\gamma^3 H_n(P)}{F_n(P)^3}\right) \tag{2}$$

where $\phi_n$, $\psi_n$, $\omega_n \in K[x, y]$, $\gcd(\phi_n, \psi_n^2) = 1$, and

$$F_n(P) = \gamma^{1-n^2}\psi_n(P), G_n(P) = \gamma^{-2n^2}\phi_n(P), H_n(P) = \gamma^{-3n^2}\omega_n(P) \tag{3}$$

are suitably normalized division polynomials of $E$. Note that $F_0(P) = 0$ and $F_1(P) = 1$. Furthermore the polynomials $\phi_n(P)$ and $\omega_n(P)$ are given by the recursion formulas

$$\begin{aligned} \phi_0(P) &= 1,\ \phi_1(P) = x, \\ \omega_0(P) &= 1,\ \omega_1(P) = y, \end{aligned}$$

and

$$\begin{aligned} \phi_n(P) &= x\psi_n(P)^2 - \psi_{n+1}(P)\psi_{n-1}(P), \\ \omega_n(P) &= (\psi_{n-1}(P)^2\psi_{n+2}(P) - \psi_{n-2}(P)\psi_{n+1}(P)^2 \\ &\quad -\psi_2(P)\psi_n(P)(a_1\phi_n(P) + a_3\psi_n(P)))(2\psi_2(P))^{-1}. \end{aligned}$$

for all $n \geq 2$. The normalized division polynomials $G_n(P)$ and $H_n(P)$ satisfy the following relations for some $\gamma \in K^*$

$$G_0(P) = 1,\ G_1(P) = \gamma^{-2}x, \tag{4}$$

$$H_0(P) = 1,\ H_1(P) = \gamma^{-3}y, \tag{5}$$

and

$$G_n(P) = x\gamma^{-2}F_n(P)^2 - F_{n+1}(P)F_{n-1}(P), \tag{6}$$

$$\begin{aligned} H_n(P) &= (F_{n-1}(P)^2F_{n+2}(P) - F_{n-2}(P)F_{n+1}(P)^2 \\ &\quad -\gamma^{-1}F_2(P)F_n(P)(a_1G_n(P) + \gamma^{-2}a_3F_n(P)))(2F_2(P))^{-1} \end{aligned} \tag{7}$$

for all $n \geq 2$.

Division polynomials play crucial role in the theory of elliptic functions, elliptic curves [26], elliptic divisibility sequences [35], [36]. Ayad [1] used explicit addition formulas to prove that the sequence of values $(F_n(P))_{n\geq 0}$ of the division polynomials of an elliptic curve $E$ at a point $P$ is purely periodic, i.e., the sequence is periodic for all $n$, modulo prime powers. Cheon and Hahn [5] estimate the valuations of division polynomials $F_n(P)$. Complete formulas for explicit valuations of division polynomials at primes of good or bad reduction are given in [32]. Silverman [30] used sophisticated methods to study the arithmetic properties of the sequence $(F_n(P))_{n\geq 0}$. Silverman [30] also studied $p$-adic properties of the sequence $(F_n(P))_{n\geq 0}$, and proved that the existence and algebraicity of the $p$-adic limit of certain subsequences of the sequence $(F_n(P))_{n\geq 0}$. More precisely, Silverman proved if the elliptic curve $E$ has good reduction, then there is a power $q = p^e$ such that for every $m \geq 1$, the limit

$$\lim_{i\to\infty} F_{mq^i}(P) \ \text{ converges in } \mathbb{Z}_p \text{ and is algebraic over } \mathbb{Q}.$$

The sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ that are generated by the numerators of the $x$- and $y$-coordinates of the multiples of a point $P$ on an elliptic

curve $E$ defined over a field $K$ are also interesting and have properties similar to the sequence $(F_n(P))_{n\geq 0}$. In [12], the author and Bizim study periodicity properties and $p$-adic properties of the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$. The authors show that the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ are periodic when $K$ is a finite field. Moreover, they prove that certain subsequences of these sequences converge in $\mathbb{Z}_p$ and the limits are algebraic over $\mathbb{Q}$.

In this paper, we continue to study the properties of the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ of values of the suitably normalized division polynomials of $E$ evaluated at a point $P \in E(K)$. Let $L$ be a lattice in $\mathbb{C}$ and let $E$ be an elliptic curve defined over $\mathbb{C}$ given by the equation

$$E : y^2 = x^3 - \frac{1}{4}g_2(L)x - \frac{1}{4}g_3(L).$$

Ward [35, equations 13.6, 13.7], proved that the modular invariants $g_2(L)$ and $g_3(L)$ associated to the lattice $L$ and the Weierstrass values $\wp(z, L)$ and $\wp'(z, L)$ associated to the point $z$ on the elliptic curve $\mathbb{C}/L$ are rational functions of $F_2$, $F_3$, and $F_4$, with $F_2F_3 \neq 0$, see also [31, Appendix]. Our first main theorem shows that $g_2(L)$, $g_3(L)$, $\wp(z, L)$ and $\wp'(z, L)$ are all defined in the same field as the terms of the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ similar to that of the sequence $(F_n(P))_{n\geq 0}$. The proof of the theorem uses properties of elliptic functions.

Theorem 1. *Let $L$ be a lattice in $\mathbb{C}$, let $E$ be an elliptic curve defined over $\mathbb{C}$ given by the equation*

$$E : y^2 = x^3 - \frac{1}{4}g_2(L)x - \frac{1}{4}g_3(L)$$

*and let $P \in E(\mathbb{C})$. Let $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ be the sequences generated by the numerators of the $x$- and $y$-coordinates of the multiples of $P$ as in (2), respectively. Then the modular invariants $g_2(L)$ and $g_3(L)$ associated to the lattice $L$ and the Weierstrass values $\wp(z, L)$ and $\wp'(z, L)$ associated to the point $z$ on the elliptic curve $\mathbb{C}/L$ are in the field $\mathbb{Q}(G_1, G_2, H_1, H_2)$.*

Section 2 provides background on elliptic divisibility sequences and elliptic curves. In Section 3, we give a representation of the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ by means of the elliptic functions and give the proof of Theorem 1. In Section 4 and Appendix A, we consider the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ associated to elliptic curves with a torsion point of order $N$. Ward [35, Theorem 23.1] studied the case $N = 2$ for elliptic divisibility sequences. It is a classical result that all elliptic curves with a torsion point of order $N$ lie in a one-parameter family where $N \in \{4, ..., 10, 12\}$, see [14, 28] for more details. In [9, Theorem 3.2], we use Tate normal form of an elliptic curve to give a complete description of elliptic divisibility sequences arising from a point

of order $N$. In Theorem 4 and Appendix A, we give a complete description of sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ arising from points of order $N$. We will also use Tate normal form of an elliptic curve to give the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ arising from points of order $N$. As an application, in Theorem 6 and Appendix B, we determine square and cube terms in the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ associated to a Tate normal form.

## 2. ELLIPTIC DIVISIBILITY SEQUENCES

An *elliptic divisibility sequence* (EDS) is a sequence $(h_n)_{n\geq 0}$ of integers satisfying a recurrence relation of the form

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 \ - h_{n+1}h_{n-1}h_m^2$$

and the divisibility property

$$h_n | h_m \text{ whenever } n|m$$

for all $m \geq n \geq 1$. An elliptic divisibility sequence is called *proper* if $h_0 = 0$, $h_1 = 1$, and $h_2h_3 \neq 0$. The *discriminant* of an EDS $(h_n)_{n\geq 0}$ is the quantity

$$\begin{aligned}\Delta(h_n) \ &= \ h_4h_2^{15} - h_3^3h_2^{12} + 3h_4^2h_2^{10} - 20h_4h_3^3h_2^7 + 3h_4^3h_2^5 \\ &\quad + 16h_3^6h_2^4 + 8h_4^2h_3^3h_2^2 + h_4^4,\end{aligned}$$

(this is the formula in [30] or [31], see also [35]). A proper EDS is called *nonsingular* if $\Delta(h_n) \neq 0$. The arithmetic properties of EDSs were first studied by Morgan Ward in 1948 [35, 36]. For more details on EDSs, see also [6, 27, 34].

Ward defined the division polynomials over the field $\mathbb{C}$ and using the complex analytic theory of elliptic functions showed that nonsingular elliptic divisibility sequences can be expressed in terms of elliptic functions. More precisely, Ward [35, Theorem 12.1] proved that if $(h_n)_{n\geq 0}$ is a nonsingular elliptic divisibility sequence, then there exist a lattice $L \subset \mathbb{C}$ and a complex number $z \in \mathbb{C}$ such that

$$h_n = \psi_n(z, L) = \frac{\sigma(nz,\, L)}{\sigma(z,\, L)^{n^2}} \text{ for all } n \geq 1,$$

where $\psi_n(z,\, L)$ and $\sigma(z,\, L)$ are the $n$-division polynomial and the Weierstrass $\sigma$-function associated to the lattice $L$, respectively. Further, Ward showed that the modular invariants $g_2(L)$ and $g_3(L)$ associated to the lattice $L$ and the Weierstrass values $\wp(z)$ and $\wp'(z)$ associated to the point $z$ on the elliptic curve $\mathbb{C}/L$ can be given by the terms $h_2$, $h_3$ and $h_4$ of the sequence $(h_n)$, see [35, equations 13.6, 13.7, 13.5 and 13.1]. Silverman [30, Proposition 18] reformulated Ward's result and showed that if $(h_n)_{n\geq 0}$ is a nonsingular EDS

associated to an elliptic curve $E$ given by a minimal Weierstrass equation over $\mathbb{Q}$ and a point $P \in E(\mathbb{Q})$, then there is a constant $\gamma \in \mathbb{Q}^*$ such that

$$h_n = \gamma^{n^2-1} F_n(P) \quad \text{for all } n \geq 1 \tag{8}$$

where $F_n$ is the normalized $n$-division polynomial on $E$.

## 3. THE REPRESENTATION OF THE SEQUENCES $(G_n(P))_{n\geq 0}$ AND $(H_n(P))_{n\geq 0}$ BY ELLIPTIC FUNCTIONS

Let $E$ be an elliptic curve defined over a field $K$ with Weierstrass equation

$$E : y^2 = x^3 + ax + b.$$

It is clear that the coefficients of the elliptic curve $E$ can be defined in terms of the sequence $(F_n(P))_{n\geq 0}$ of values of the division polynomials of $E$ at a point $P$ by using the relation (8) and Ward's formulas for the modular invariants $g_2(L)$ and $g_3(L)$ [35, equations 13.6, 13.7]; see also [31, Appendix]. In this section, we give a representation of the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ of values of the suitably normalized division polynomials of $E$ evaluated at a point $P \in E(K)$ by means of the elliptic functions and prove that the coefficients of the elliptic curve $E$ can be defined in terms of these sequences. In this section, we will also assume $\psi_2(P)\psi_3(P) \neq 0$ so that $F_2(P)F_3(P) \neq 0$.

We first state some results from the elliptic function theory that will be needed. Let $L$ be a lattice in $\mathbb{C}$. Recall from the elliptic function theory that the Weierstrass $\wp$-function associated to the lattice $L$ and its derivative $\wp'$ satisfy

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L) \tag{9}$$

where $g_2(L)$ and $g_3(L)$ are modular invariants associated to the lattice $L$. If we take the derivative of the both sides of (9) we have the following relation

$$\wp''(z) = 6\wp(z)^2 - \frac{1}{2} g_2(L). \tag{10}$$

Then we obtain

$$g_2(L) = 12\wp(z)^2 - 2\wp''(z). \tag{11}$$

by (10) and so

$$g_3(L) = 2\wp(z)[\wp''(z) - 4\wp(z)^2] - \wp'(z)^2 \tag{12}$$

by (9) and (10). Moreover recall that

$$\psi_2(z) = -\wp'(z), \tag{13}$$

$$\psi_3(z) = 3\wp(z)^4 - \frac{3}{2}g_2(L)\wp(z)^2 - 3g_3(L)\wp(z) - \frac{1}{16}g_2(L)^2,$$

and

$$\wp(2z) - \wp(z) = \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 - 3\wp(z),$$

$$\wp(3z) - \wp(z) = \frac{\wp'(z)^2[\wp'(z)^4 - \psi_3(z)\wp''(z)]}{\psi_3(z)^2}. \tag{14}$$

Furthermore, one can derive a formula for $\wp(nz)$ in terms of $\wp(z)$, $\psi_n(z)$ and $\psi_{n\pm1}(z)$, more explicitly the following relation holds

$$\wp(nz) = \wp(z) - \frac{\psi_{n+1}(z)\psi_{n-1}(z)}{\psi_n(z)^2} \tag{15}$$

for all $n \geq 2$. Thus substituting $n = 2$ and $n = 3$ into (15) we have

$$\wp(2z) - \wp(z) = -\frac{\psi_3(z)}{\psi_2(z)^2} \tag{16}$$

since $\psi_1(z) = 1$, and

$$\wp(3z) - \wp(z) = -\frac{\psi_4(z)\psi_2(z)}{\psi_3(z)^2}. \tag{17}$$

Now by (14), (13) and (17) we have

$$-\frac{\psi_4(z)\psi_2(z)}{\psi_3(z)^2} = \frac{\psi_2(z)^2[\psi_2(z)^4 - \psi_3(z)\wp''(z)]}{\psi_3(z)^2}$$

and so

$$\wp''(z) = \frac{\psi_2(z)^5 + \psi_4(z)}{\psi_2(z)\psi_3(z)}. \tag{18}$$

Let $E$ be an elliptic curve over $\mathbb{C}$. Then the points $(\wp(z), \wp'(z))$ lie on the elliptic curve

$$y^2 = 4x^3 - g_2(L)x - g_3(L) \tag{19}$$

by (9). Now let $(F_n(P))_{n\geq0}$, $(G_n(P))_{n\geq0}$ and $(H_n(P))_{n\geq0}$ be the sequences of values of the normalized division polynomials of $E$ at a point $P$. Then by second part of (4) we have

$$\wp(z) = \gamma^2 G_1(P). \tag{20}$$

On the other hand by (6),

$$G_2(P) = x\gamma^{-2}F_2(P)^2 - F_3(P) \tag{21}$$

since $F_1(P) = 1$. By first part of (3), and (16) we obtain

$$\wp(2z) = \frac{\wp(z)F_2(P)^2 - \gamma^2 F_3(P)}{F_2(P)^2}.$$

Hence by second part of (4), (20) and (21) we have

$$\wp(2z) = \frac{\gamma^2 G_2(P)}{F_2(P)^2}.$$

Thus one can easily derive inductively that

$$\wp(nz) = \frac{\gamma^2 G_n(P)}{F_n(P)^2} \tag{22}$$

for all $n \geq 1$.

We are now ready to prove our first main result. From now on, for simplicity of notation, we write $G_n$ and $H_n$ for $G_n(P)$ and $H_n(P)$, respectively, unless otherwise specified.

*Proof of Theorem 1.* By the first part of (3) we have

$$\psi_2(z) = \gamma^3 F_2 \tag{23}$$

and

$$\psi_3(z) = \gamma^8 F_3.$$

Thus by (23) and (13) we obtain

$$\wp'(z) = -\gamma^3 F_2. \tag{24}$$

On the other hand (22) implies that

$$\wp(3z) = \gamma^2 G_3 / F_3^2.$$

Now (18) and the first part of (3) imply that

$$\wp''(z) = \frac{\gamma^4 (F_2^5 + F_4)}{F_2 F_3}. \tag{25}$$

On the other hand by (23) we have

$$F_2 = 2\gamma^{-3} y$$

since $\psi_2 = 2y$, for the elliptic curve $E : y^2 = x^3 - \frac{1}{4} g_2(L)x - \frac{1}{4} g_3(L)$. Thus by the second part of (5) we derive that

$$F_2 = 2H_1. \tag{26}$$

Now by putting $n = 2$ into (7) and then using (26) we obtain

$$F_4 = 4H_1 H_2 \tag{27}$$

since $F_0 = 0$ and $F_1 = 1$. Thus

$$\wp'(z) = -2\gamma^3 H_1, \tag{28}$$

by (24) and (26). Now by setting $n = 2$ in (6) and then using (24) and the second part of (4) we have

$$F_3 = \gamma^{-6} \wp'(z)^2 G_1 - G_2$$

since $F_1 = 1$. Thus

$$F_3 = 4G_1H_1^2 - G_2 \tag{29}$$

by (28). Therefore by (25), (26), (27) and (29) we have

$$\wp''(z) = \frac{2\gamma^4(8H_1^4 + H_2)}{4G_1H_1^2 - G_2}. \tag{30}$$

On combining (11) with (20) and (30) we obtain the following formula for $g_2(L)$,

$$g_2(L) = \frac{4\gamma^4(12G_1^3H_1^2 - 3G_1^2G_2 - 8H_1^4 - H_2)}{4G_1H_1^2 - G_2}. \tag{31}$$

Similarly combining (12) with (20), (28) and (30) we have

$$g_3(L) = \frac{4\gamma^6(4G_1H_1^4 + G_1H_2 - 8G_1^4H_1^2 + 2G_1^3G_2 + H_1^2G_2)}{4G_1H_1^2 - G_2}. \tag{32}$$

Now if $E$ is an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation

$$E : y^2 = x^3 + ax + b,$$

then (19) imply that

$$a = -\frac{g_2(L)}{4} \text{ and } b = -\frac{g_3(L)}{4}$$

where $g_2(L)$ and $g_3(L)$ are the rational expressions in $G_1$, $G_2$, $H_1$ and $H_2$ by relations (31) and (32) respectively. Finally rational expressions for $\wp(z, L)$ and $\wp'(z, L)$ are given by equations (20) and (28), which completes the proof of the theorem. □

## 4. THE SEQUENCES $(G_n)_{n\geq 0}$ AND $(H_n)_{n\geq 0}$ ASSOCIATED TO TATE NORMAL FORMS

The study of the group $E(\mathbb{Q})$ has been playing important roles in number theory. The modern number theory originated in 1922 when L. J. Mordell proved that the group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group. This result was generalized in 1928 to abelian varieties over number fields by A. Weil. Moreover, the characterization of torsion subgroups of $E(\mathbb{Q})$ is always interesting. A uniform bound was studied for the order of the torsion subgroup $E_{tors}(\mathbb{Q})$ of $E(\mathbb{Q})$ by Shimura, Ogg, and others. The following result conjectured by Ogg, was proved by B. Mazur.

THEOREM 2 ([16]). *Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then the torsion subgroup $E_{tors}(\mathbb{Q})$ is either isomorphic to $\mathbb{Z}/N\mathbb{Z}$ for $N = 1, 2, ..., 10, 12$ or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ for $N = 1, 2, 3, 4$. Further, each of these groups does occur as an $E_{tors}(\mathbb{Q})$.*

It is a classical result that all elliptic curves with a torsion point of order $N$ lie in a one-parameter family where $N \in \{4, ..., 10, 12\}$. The *Tate normal form* of an elliptic curve $E$ with point $P = (0, 0)$ is given by

$$E_N : y^2 + (1 - c)xy - by = x^3 - bx^2$$

where the point $P$ has given order $N$.

If an elliptic curve in normal form has a point of order $N > 3$, then an admissible change of variables transforms the curve to the Tate normal form, in this case, the point $P = (0, 0)$ is a torsion point of maximal order. Kubert [14] gives a list of parameterizable torsion structures, which includes one-parameter family of elliptic curves $E$ defined over $\mathbb{Q}$ with a torsion point of order $N$ where $N = 4, ..., 10, 12$. Some algorithms are given by using the existence of such a family, see [7] for more details. To describe when an elliptic curve defined over $\mathbb{Q}$ has a point of given order $N$, we need the following result on the parametrization of torsion structures. Most cases of the following parameterizations are proved by Husemöller [13].

THEOREM 3 ([7]). *Every elliptic curve with point $P = (0, 0)$ of order $N = 4, ..., 10, 12$ can be written in the following Tate normal form*

$$E_N : y^2 + (1 - c)xy - by = x^3 - bx^2,$$

*with the following relations:*

1. *If $N = 4$, then $b = \alpha$ and $c = 0$, $\alpha \neq 0$.*
2. *If $N = 5$, then $b = \alpha$ and $c = \alpha$, $\alpha \neq 0$.*
3. *If $N = 6$, then $b = \alpha + \alpha^2$ and $c = \alpha$, $\alpha \neq -1, 0$.*
4. *If $N = 7$, then $b = \alpha^3 - \alpha^2$ and $c = \alpha^2 - \alpha$, $\alpha \neq 0, 1$.*
5. *If $N = 8$, then $b = (2\alpha - 1)(\alpha - 1)$ and $c = b/\alpha$, $\alpha \neq 0, \frac{1}{2}, 1$.*
6. *If $N = 9$, then $c = \alpha^2(\alpha - 1)$ and $b = c(\alpha(\alpha - 1) + 1)$, $\alpha \neq 0, 1$.*
7. *If $N = 10$, then $c = (2\alpha^3 - 3\alpha^2 + \alpha)/(\alpha - (\alpha - 1)^2)$ and $b = c\alpha^2/(\alpha - (\alpha - 1)^2)$, $\alpha \neq 0, \frac{1}{2}, 1$.*
8. *If $N = 12$, then $c = (3\alpha^2 - 3\alpha + 1)(\alpha - 2\alpha^2)/(\alpha - 1)^3$ and $b = c(-2\alpha^2 + 2\alpha - 1)/(\alpha - 1)$, $\alpha \neq 0, \frac{1}{2}, 1$.*

Theorem 3 says that every elliptic curve with a point of order $N$ is birationally equivalent to one of the Tate normal forms given above. We will assume that the parameter $\alpha \in \mathbb{Z}$ and the coefficients of $E_N$ are chosen to lie in $\mathbb{Z}$. Hence for $N = 8, 10, 12$, we transform $E_N$ into a birationally equivalent curve $E'_N$ having an equation with integral coefficients. The equations of the birationally equivalent curves for $N = 8, 10, 12$ are given, respectively, as follows:

$$E'_8 \quad : \quad y^2 + (\alpha - \beta)xy - \alpha^3\beta y = x^3 - \alpha^2\beta x^2,$$

$$E'_{10} \ : \ y^2+(\zeta^2-\alpha\beta\zeta)xy-\alpha^3\beta\zeta^4 y = x^3-\alpha^3\beta\zeta^2x^2,$$
$$E'_{12} \ : \ y^2+(\alpha-1)((\alpha-1)^3-\lambda)xy-(\alpha-1)^8\lambda\theta y = x^3-(\alpha-1)^4\lambda\theta x^2,$$

where $\alpha \neq 0,\, 1$,

$$\beta = (2\alpha-1)(\alpha-1),\ \zeta = -\alpha^2+3\alpha-1, \tag{33}$$

and

$$\lambda = (3\alpha^2-3\alpha+1)(\alpha-2\alpha^2),\ \theta = 2\alpha-2\alpha^2-1. \tag{34}$$

From now on, for simplicity of notation, we write $E_8$, $E_{10}$, $E_{12}$ for $E'_8$, $E'_{10}$, $E'_{12}$, respectively.

In [9, Theorem 3.2], we give the general terms of the elliptic divisibility sequences $(h_n)_{n\geq 0}$ associated to a Tate normal form $E_N$ of an elliptic curve for some integer parameter $\alpha$. For example, the general term of $(h_n)_{n\geq 0}$ for $N=8$ is

$$h_n = \varepsilon\alpha^{\{(15n^2-p)/16\}}(\alpha-1)^{\{(7n^2-q)/16\}}(2\alpha-1)^{\{(3n^2-r)/8\}} \tag{35}$$

where

$$\varepsilon = \begin{cases} +1, & \text{if } n \equiv 1,4,5,9,10,13,14 \ (16) \\ -1, & \text{if } n \equiv 2,3,6,7,11,12,15 \ (16), \end{cases}$$

and

$$p = \begin{cases} 15, & \text{if } n \equiv 1,7 \ (8) \\ 12, & \text{if } n \equiv 2,6 \ (8) \\ 7, & \text{if } n \equiv 3,5 \ (8) \\ 16, & \text{if } n \equiv 4 \ (8), \end{cases} \qquad q = \begin{cases} 7, & \text{if } n \equiv 1,7 \ (8) \\ 12, & \text{if } n \equiv 2,6 \ (8) \\ 15, & \text{if } n \equiv 3,5 \ (8) \\ 16, & \text{if } n \equiv 4 \ (8), \end{cases}$$

$$r = \begin{cases} 3, & \text{if } n \equiv 1,3,5,7 \ (8) \\ 4, & \text{if } n \equiv 2,6 \ (8) \\ 0, & \text{if } n \equiv 4 \ (8). \end{cases}$$

In Section 2, we recall that if $(h_n)_{n\geq 0}$ is a nonsingular EDS associated to an elliptic curve $E$ given by a minimal Weierstrass equation over $\mathbb{Q}$ and a point $P \in E(\mathbb{Q})$, then there is a constant $\gamma \in \mathbb{Q}^*$ such that

$$h_n = \gamma^{n^2-1}F_n(P) \quad \text{for all } n \geq 0.$$

Therefore, one can easily obtain the general term of the sequence $(F_n)_{n\geq 0}$ associated to a Tate normal form $E_N$, by using the relation above.

In this section, we consider $(G_n)_{n\geq 0}$ and $(H_n)_{n\geq 0}$ sequences associated to a Tate normal form $E_N$ with torsion point $P=(0,0)$ and give the general terms of these sequences. We take $\gamma = 1$ in (3) so that $G_n = \phi_n$, $H_n = \omega_n$, and

$$F_n = h_n \quad \text{for all } n \geq 0 \tag{36}$$

by (8).

In the following theorem, we determine general terms of the sequences $(G_n)_{n\geq 0}$ and $(H_n)_{n\geq 0}$ associated to an elliptic curve in Tate normal form with a torsion point $P=(0,0)$ of order 8. For the convenience of the reader, we have given the other cases in Appendix A. The proof uses the general terms of sequences in [9, Theorem 3.2].

THEOREM 4. *Let $E_8$ be a Tate normal form of an elliptic curve with a torsion point $P=(0,0)$ of order 8. Let $(G_n)_{n\geq 0}$ and $(H_n)_{n\geq 0}$ be the sequences generated by the numerators of the $x$- and $y$-coordinates of the multiples of $P$ as in (2). Then the general terms of the sequences $(G_n)_{n\geq 0}$ and $(H_n)_{n\geq 0}$ can be given by the following formulas:*

(37)
$$G_n=\begin{cases} 0, & \text{if } n\equiv 1,7\ (8)\\ \alpha^{\{(15n^2+a_1)/8\}}(\alpha-1)^{\{(7n^2-b_1)/8\}}(2\alpha-1)^{\{(3n^2+c_1)/4\}}, & \text{otherwise,}\end{cases}$$

*and*

$$H_n=\begin{cases} 0, & \text{if } n\equiv 1,6\ (8)\\ \varepsilon\alpha^{\{(45n^2+a_2)/16\}}(\alpha-1)^{\{(21n^2-b_2)/16\}}(2\alpha-1)^{\{(9n^2-c_2)/8\}}, & \text{otherwise,}\end{cases}$$

*where $\alpha\neq 0,\ 1$,*

$$a_1=\begin{cases} 0, & \text{if } n\equiv 0\ (8)\\ 4, & \text{if } n\equiv 2,6\ (8)\\ 1, & \text{if } n\equiv 3,5\ (8)\\ 8, & \text{if } n\equiv 4\ (8),\end{cases}\qquad b_1=\begin{cases} 0, & \text{if } n\equiv 0\ (8)\\ 4, & \text{if } n\equiv 2,6\ (8)\\ 7, & \text{if } n\equiv 3,5\ (8)\\ 8, & \text{if } n\equiv 4\ (8),\end{cases}$$

$$c_1=\begin{cases} 0, & \text{if } n\equiv 0,2,4,6\ (8)\\ 1, & \text{if } n\equiv 3,5\ (8).\end{cases}$$

*and*

$$\varepsilon=\begin{cases} +1, & \text{if } n\equiv 0,4,5,10,13\ (16)\\ -1, & \text{if } n\equiv 2,3,7,8,11,12,15\ (16),\end{cases}$$

$$a_2=\begin{cases} 0, & \text{if } n\equiv 0\ (8)\\ -4, & \text{if } n\equiv 2\ (8)\\ 11, & \text{if } n\equiv 3\ (8)\\ 16, & \text{if } n\equiv 4\ (8)\\ -5, & \text{if } n\equiv 5\ (8)\\ 3, & \text{if } n\equiv 7\ (8),\end{cases}\quad b_2=\begin{cases} 0, & \text{if } n\equiv 0\ (8)\\ 4, & \text{if } n\equiv 2\ (8)\\ 13, & \text{if } n\equiv 3,5\ (8)\\ 16, & \text{if } n\equiv 4\ (8)\\ 5, & \text{if } n\equiv 7\ (8),\end{cases}$$

$$c_2 = \begin{cases} 0, & \text{if } n \equiv 0,4 \ (8) \\ 4, & \text{if } n \equiv 2 \ (8) \\ 1, & \text{if } n \equiv 3,7 \ (8) \\ -7, & \text{if } n \equiv 5 \ (8). \end{cases}$$

*Proof.* We give the proof only for the sequence $(G_n)_{n\geq 0}$ as the proof for $(H_n)_{n\geq 0}$ is similar.

Let $n \equiv 1 \ (8)$. Then by (6)

$$G_{8k+1} = -F_{8k+2}F_{8k} \ \text{ for all } k \geq 0,$$

since $x = 0$. We note that $F_n = 0$ if and only if the order $N$ of the point $P$ divides $n$. It follows that $F_{8k} = 0$ for all $k \geq 0$, hence $G_{8k+1} = 0$.

Now let $n \equiv 2 \ (8)$. Then by (6)

$$G_{8k+2} = -F_{8k+3}F_{8k+1} \text{ for all } k \geq 0. \tag{38}$$

By (35) and (36) we obtain

$$F_{8k+1} = \alpha^{60k^2+15k}(\alpha-1)^{28k^2+7k}(2\alpha-1)^{24k^2+6k} \ \text{ for all } k \geq 0,$$

and

$$F_{8k+3} = -\alpha^{60k^2+45k+8}(\alpha-1)^{28k^2+21k+3}(2\alpha-1)^{24k^2+18k+3} \text{ for all } k \geq 0.$$

Now substituting these expressions into (38) we derive that

$$G_{8k+2} = \alpha^{120k^2+60k+8}(\alpha-1)^{56k^2+28k+3}(2\alpha-1)^{48k^2+24k+3}.$$

for all $k \geq 0$. On the other hand by the general term formula in (37) we have

$$G_{8k+2} = \alpha^{120k^2+60k+8}(\alpha-1)^{56k^2+28k+3}(2\alpha-1)^{48k^2+24k+3},$$

which completes the proof for $n \equiv 2 \ (8)$. The remaining cases can be proved in a similar manner. □

*Remark* 1. There is no Tate normal form of an elliptic curve with the torsion point of order two or three, but in [14], Kubert gives a list of elliptic curves with torsion point of order two or three are

$$E_2 : y^2 = x^3 + a_2x^2 + a_4x, \ \ a_4 \neq 0, \tag{39}$$

and

$$E_3 : y^2 + a_1xy + a_3y = x^3, \ \ a_3 \neq 0, \tag{40}$$

respectively.

The following theorem gives the general term of the sequence $(G_n)_{n\geq 0}$ associated to $E_2$ and $E_3$, respectively and the general term of the sequence $(H_n)_{n\geq 0}$ associated to elliptic curve $E_3$. We note the sequence $(H_n)_{n\geq 0}$ associated to elliptic curve $E_2$ is not defined since $F_2 = 0$; see relation (7). The proof of the theorem is similar to the proof of Theorem 4.

THEOREM 5. *Let $E_N$ be an elliptic curve with the torsion point $P = (0, 0)$ of order $N$ as in (39) and (40). Let $(G_n)_{n\geq 0}$ and $(H_n)_{n\geq 0}$ be the sequences generated by the numerators of the $x$- and $y$-coordinates of the multiples of $P$ as in (2). Then the general term of the sequences $(G_n)_{n\geq 0}$ and $(H_n)_{n\geq 0}$ can be given by the following formulas:* 1. *If $N = 2$, then*

$$G_n = \begin{cases} 0, & \text{if } n \text{ is odd} \\ a_4^{\{n^2/2\}}, & \text{if } n \text{ is even.} \end{cases}$$

2. *If $N = 3$, then*

$$G_n = \begin{cases} 0, & \text{if } n \equiv 1, 2 \ (3) \\ a_3^{\{2n^2/3\}}, & \text{if } n \equiv 0 \ (3). \end{cases}$$

*and*

$$H_n = \begin{cases} 0, & \text{if } n \equiv 1 \ (3) \\ \varepsilon a_3^{n^2}, & \text{if } n \equiv 0, 2 \ (3) \end{cases}$$

*where*

$$\varepsilon = \begin{cases} +1, & \text{if } n \equiv 0, 5 \ (6) \\ -1, & \text{if } n \equiv 2, 3 \ (6). \end{cases}$$

## 5. SQUARES AND CUBES IN $(G_n)_{n\geq 0}$ AND $(H_n)_{n\geq 0}$ SEQUENCES

The problem of determining square and cube terms in linear sequences has been considered by various authors, see [20], [23], [24], [25], and see also [3], [4]. Similar problem has also been considered for non-linear sequences, see [10], [11], [9], see also [22], [17]. In this section, we determine square and cube terms in the sequences $(G_n)_{n\geq 0}$ and $(H_n)_{n\geq 0}$ associated to a Tate normal form $E_N$ of an elliptic curve with a torsion point $P = (0, 0)$ of order $N$. Throughout this paper the symbol $\square$ means a square of a non-zero integer, i.e., $\square = \pm\beta^2$ where $\beta$ is a non-zero integer, and $C$ means a cube of a non-zero integer. Determining square and cube terms in these sequences leads to some equations and these equations are similar to equations in [9, Table 3]. Therefore we use similar techniques in [9] for determining square and cube terms in these sequences. We observe that the irreducible factors appearing in the left hand side (if they

are at least two) of these equations are pairwise relatively prime (for example, one can easily show that the irreducible factors in the

$$\alpha(\alpha-1)(2\alpha-1)(2\alpha^2-2\alpha+1)(3\alpha^2-3\alpha+1)=\square,$$

are pairwise relatively prime, see [9, p. 498]). It follows that, if the right hand side of the equation is $\square$ (or $C$), then every irreducible factor is $\square$ (or $C$). It turns out that it is not necessary to consider all irreducible factors in the left hand side. For example, the equation

$$\alpha(2\alpha-1)(2\alpha^2-2\alpha+1)=C$$

implies that all three $\alpha$, $2\alpha-1$, and $2\alpha^2-2\alpha+1$ are $C$, we only use the fact that the third one is $C$.

We use the tables in [21] when our equations turned into Mordell's equation. In some cases we will apply *Elliptic Logarithm Method* to find all integral solutions of our equations (this method has been developed in [33] and, independently, in [8] and now is implemented in MAGMA [15]; see also [2]).

Theorem 6 answers the following three questions:

(1) Which terms of the sequence $(G_n)_{n\geq 0}$ (or $(H_n)_{n\geq 0}$) can be $\square$ (or $C$) independent of $\alpha$?

(2) Which terms of the sequence $(G_n)_{n\geq 0}$ (or $(H_n)_{n\geq 0}$) can be $\square$ (or $C$) with admissible choice of $\alpha$?

(3) Which terms of the sequence $(G_n)_{n\geq 0}$ (or $(H_n)_{n\geq 0}$) can not be $\square$ (or $C$) independent of $\alpha$?

Here again, we only consider the case $N=8$, for the convenience of the reader, we have given the other cases in Appendix B.

THEOREM 6. *Let $E_8$ be a Tate normal form of an elliptic curve with a torsion point $P=(0,0)$ of order 8. Let $(G_n)_{n\geq 0}$ and $(H_n)_{n\geq 0}$ be the sequences generated by the numerators of the $x$- and $y$-coordinates of the multiples of $P$ as in (2). Let $G_n$ and $H_n\neq 0$.*

1.

(i) ◇ *If $n\equiv 0$ (8), then $G_n=\square$ for all $\alpha\neq 0,\ 1$,*
◇ *if $n\equiv 2,\ 6$ (8), then $G_n=\square$ iff $(\alpha-1)(2\alpha-1)=\square$,*
◇ *otherwise $G_n\neq\square$ for all $\alpha\neq 0,\ 1$.*

(ii) ◇ *If $n\equiv 0$ (24), then $G_n=C$ for all $\alpha\neq 0,\ 1$,*
◇ *if $n\equiv 2,\ 10,\ 14,\ 22$ (24), then $G_n=C$ iff $\alpha=C$,*
◇ *if $n\equiv 8,\ 16$ (24), then $G_n=C$ iff $\alpha-1=C$,*
◇ *otherwise $G_n\neq C$ for all $\alpha\neq 0,\ 1$.*

2.

(i) ◇ *If $n\equiv 0,\ 4,\ 8,\ 12$ (16), then $H_n=\square$ for all $\alpha\neq 0,\ 1$,*
◇ *if $n\equiv 3$ (16), then $H_n=\square$ iff $\alpha-1=\square$,*

◇ *if* $n \equiv 5,\ 7\ (16)$, *then* $H_n = \square$ *iff* $2\alpha - 1 = \square$,
◇ *if* $n \equiv 11\ (16)$, *then* $H_n = \square$ *iff* $\alpha = \square$,
◇ *otherwise* $H_n \neq \square$ *for all* $\alpha \neq 0,\ 1$.

(ii) ◇ *If* $n \equiv 0\ (8)$, *then* $H_n = C$ *for all* $\alpha \neq 0,\ 1$,
◇ *otherwise* $H_n \neq C$ *for all* $\alpha \neq 0,\ 1$.

*Proof.* We give the proof only for the sequence $(G_n)_{n\geq 0}$ as the proof for $(H_n)_{n\geq 0}$ is similar.

1. *i.* We note that $G_n = 0$ for $n \equiv 1,\ 7\ (\mathrm{mod}8)$, by (37). It can easily be seen that $G_n = \square$ for every $\alpha \neq 0,\ 1$ for $n \equiv 0\ (8)$, by using (37).

If $n \equiv 2,\ 6\ (8)$, then $G_n = \square$ iff

$$(\alpha - 1)(2\alpha - 1) = \square$$

by (37). This equation leads to

$$(4\alpha - 3)^2 - 8\beta^2 = 1$$

or

$$(4\alpha - 3)^2 + 8\beta^2 = 1,$$

where $\beta$ is a non zero-integer. The last equation is a trivial equation and the solutions of this equation do not provide any acceptable $\alpha$. The first equation leads to Pell equation

$$\tau^2 - 8\beta^2 = 1$$

where $\tau = 4\alpha - 3$. The solutions of this equation are $(3, 1)$, $(17, 6)$, ... . Note that only the solutions of form $\tau + 3 \equiv 0\ (4)$ give the acceptable $\alpha$, and their number is infinite.

If $n \equiv 3,\ 5\ (8)$, then $G_n = \square$ iff

$$\alpha(\alpha - 1)(2\alpha - 1) = \square,$$

and if $n \equiv 4\ (8)$, then $G_n = \square$ iff

$$\alpha(\alpha - 1) = \square$$

by (37). These last two equations lead to trivial equations

$$(2\alpha - 1)^2 \pm \beta^2 = 1$$

where $\beta$ is a non-zero integer. The solutions of these trivial equations do not provide any acceptable $\alpha$, which completes the proof of $(i)$.

*ii.* If $n \equiv 1,\ 7,\ 9,\ 15,\ 17,\ 23\ (24)$, then $G_n = 0$, if $n \equiv 0\ (24)$, then $G_n = C$ for every $\alpha \neq 0,\ 1$, if $n \equiv 2,\ 10,\ 14,\ 22\ (24)$, then $G_n = C$ iff $\alpha = C$, and if $n \equiv 8,\ 16\ (24)$, then $G_n = C$ iff $\alpha - 1 = C$, by (37).

If $n \equiv 3,\ 21\ (24)$, then $G_n = C$ iff

$$\alpha^2(\alpha - 1)(2\alpha - 1) = C,$$

and if $n \equiv 4,\ 20\ (24)$, then $G_n = C$ iff

$$\alpha(\alpha - 1) = C,$$

if $n \equiv 6,\ 18\ (24)$, then $G_n = C$ iff

$$\alpha^2(\alpha - 1) = C,$$

and if $n \equiv 12\ (24)$, then $G_n = C$ iff

$$\alpha(\alpha - 1)^2 = C$$

by (37). These equations lead to

$$\alpha(\alpha - 1) = C.$$

This equation leads to trivial equation

$$\beta_1^3 - \beta_2^3 = 1,$$

where $\alpha = \beta_1^3$, $\alpha - 1 = \beta_2^3$, and $\beta_1$, $\beta_2$ are non-zero integers. The solutions of this equation do not provide any acceptable $\alpha$.

If $n \equiv 5,\ 11,\ 19,\ 13\ (24)$, then $G_n = C$ iff

$$\alpha^2(2\alpha - 1) = C$$

by (37), or equivalently

$$\alpha(2\alpha - 1) = C.$$

The last equation leads to classical equation*

$$2\beta_1^3 + (-\beta_2)^3 = 1,$$

where $\alpha = \beta_1^3$, $2\alpha - 1 = \beta_2^3$, and $\beta_1$, $\beta_2$ are non-zero integers. The solution of this equation does not provide any acceptable $\alpha$, which completes the proof of (*ii*). □

In the following theorem, we determine square and cube terms in the sequence $(G_n)_{n\geq 0}$ associated to elliptic curves $E_2$ and $E_3$, respectively, and square and cube terms in the sequence $(H_n)_{n\geq 0}$ associated to elliptic curve $E_3$. The proof is similar to the proof of Theorem 6.

THEOREM 7. *$E_N$ be an elliptic curve with the torsion point $P = (0, 0)$ of order $N$ as in (39) and (40). Let $(G_n)_{n\geq 0}$ and $(H_n)_{n\geq 0}$ be the sequences generated by the numerators of the $x$- and $y$-coordinates of the multiples of $P$ as in (2), and let $G_n \neq 0$.*

1. *Let $N = 2$.*

(i) $\diamond$ *$G_n = \square$ for every non-zero $a_4$.*

*The equation $x^3 + 2y^3 = 1$ has the integer solution $(x, y) = (-1, 1)$, hence, by Theorem 5, Chapter 24 of [19] can not have further solutions with $xy \neq 0$.

(ii) $\diamond$ *If* $n \equiv 0\ (6)$, *then* $G_n = C$ *for every non-zero* $a_4$,
$\diamond$ *otherwise* $G_n = C$ *iff* $a_4 = C$.

2. *Let* $N = 3$.
(i) $\diamond$ $G_n = \square$ *for every non-zero* $a_3$.
(ii) $\diamond$ $G_n = C$ *for every non-zero* $a_3$.
(iii) $\diamond$ *If* $n \equiv 0,\ 2\ (6)$, *then* $H_n = \square$ *for every non-zero* $a_3$,
$\diamond$ *otherwise* $H_n = \square$ *iff* $a_3 = \square$,
(iv) $\diamond$ *If* $n \equiv 0\ (3)$, *then* $H_n = C$ *for every non-zero* $a_3$,
$\diamond$ *otherwise* $H_n = C$ *iff* $a_3 = C$.

## APPENDIX A

In the following theorems, we determine general terms of the sequences $(G_n)_{n\geq 0}$ and $(H_n)_{n\geq 0}$ associated to an elliptic curve in Tate normal form with a torsion point $P = (0,0)$ of order $N$. The proofs are similar to the proof of Theorem 4.

THEOREM 8. *Let* $E_N$ *be a Tate normal form of an elliptic curve with a torsion point* $P = (0,0)$ *of order* $N$. *Let* $(G_n)_{n\geq 0}$ *be the sequence generated by the numerators of the* $x$*-coordinates of the multiples of* $P$ *as in (2). Let* $\zeta, \lambda, \theta$ *be as in (33) and (34). Then the general term of the sequence* $(G_n)_{n\geq 0}$ *can be given by the following formulas:*

1. *If* $N = 4$, *then*

$$G_n = \begin{cases} 0, & \text{if } n \text{ is odd} \\ \alpha^{\{3n^2/4\}}, & \text{if } n \text{ is even,} \end{cases}$$

*where* $\alpha \neq 0$.

2. *If* $N = 5$, *then*

$$G_n = \begin{cases} 0, & \text{if } n \equiv 1,4\ (5) \\ \alpha^{\{(4n^2-a)/5\}}, & \text{otherwise,} \end{cases}$$

*where* $\alpha \neq 0$, *and*

$$a = \begin{cases} 0, & \text{if } n \equiv 0\ (5) \\ 1, & \text{if } n \equiv 2,3\ (5). \end{cases}$$

3. *If* $N = 6$, *then*

$$G_n = \begin{cases} 0, & \text{if } n \equiv 1,5\ (6) \\ \alpha^{\{(5n^2-a)/6\}}(\alpha+1)^{\{(2n^2+b)/3\}}, & \text{otherwise,} \end{cases}$$

*where* $\alpha \neq -1,\ 0$, *and*

$$a = \begin{cases} 0, & \text{if } n \equiv 0\ (6) \\ 2, & \text{if } n \equiv 2,4\ (6) \\ 3, & \text{if } n \equiv 3\ (6), \end{cases} \quad b = \begin{cases} 0, & \text{if } n \equiv 0,3\ (6) \\ 1, & \text{if } n \equiv 2,4\ (6). \end{cases}$$

4. *If* $N = 7$, *then*

$$G_n = \begin{cases} 0, & \text{if } n \equiv 1, 6 \ (7) \\ \alpha^{\{(10n^2+a)/7\}}(\alpha-1)^{\{(6n^2-b)/7\}}, & \text{otherwise,} \end{cases}$$

*where* $\alpha \neq 0, 1$, *and*

$$a = \begin{cases} 0, & \text{if } n \equiv 0 \ (7) \\ 2, & \text{if } n \equiv 2, 5 \ (7) \\ 1, & \text{if } n \equiv 3, 4 \ (7), \end{cases} \quad b = \begin{cases} 0, & \text{if } n \equiv 0 \ (7) \\ 3, & \text{if } n \equiv 2, 5 \ (7) \\ 5, & \text{if } n \equiv 3, 4 \ (7). \end{cases}$$

5. *If* $N = 9$, *then*

$$G_n = \begin{cases} 0, & \text{if } n \equiv 1, 8 \ (9) \\ \alpha^{\{(14n^2-a)/9\}}(\alpha-1)^{\{(8n^2-b)/9\}}\eta^{\{(2n^2+c)/3\}}, & \text{otherwise} \end{cases}$$

*where* $\alpha \neq 0, 1$, $\eta = \alpha^2 - \alpha + 1$, *and*

$$a = \begin{cases} 0, & \text{if } n \equiv 0, 3, 6 \ (9) \\ 2, & \text{if } n \equiv 2, 7 \ (9) \\ -1, & \text{if } n \equiv 4, 5 \ (9), \end{cases} \quad b = \begin{cases} 0, & \text{if } n \equiv 0 \ (9) \\ 5, & \text{if } n \equiv 2, 7 \ (9) \\ 9, & \text{if } n \equiv 3, 6 \ (9) \\ 11, & \text{if } n \equiv 4, 5 \ (9), \end{cases}$$

$$c = \begin{cases} 0, & \text{if } n \equiv 0, 3, 6 \ (9) \\ 1, & \text{if } n \equiv 2, 4, 5, 7 \ (9). \end{cases}$$

6. *If* $N = 10$, *then*

$$G_n = \begin{cases} 0, & \text{if } n \equiv 1, 9 \ (10) \\ \alpha^{\{(21n^2+a)/10\}}(\alpha-1)^{\{(9n^2-b)/10\}} & \\ \times(2\alpha-1)^{\{(4n^2-c)/5\}}\zeta^{\{(5n^2+d)/5\}}, & \text{otherwise,} \end{cases}$$

*where* $\alpha \neq 0, 1$,

$$a = \begin{cases} 0, & \text{if } n \equiv 0 \ (10) \\ 6, & \text{if } n \equiv 2, 8 \ (10) \\ 1, & \text{if } n \equiv 3, 7 \ (10) \\ 4, & \text{if } n \equiv 4, 6 \ (10) \\ 5, & \text{if } n \equiv 5 \ (10), \end{cases} \quad b = \begin{cases} 0, & \text{if } n \equiv 0 \ (10), \\ 6, & \text{if } n \equiv 2, 8 \ (10) \\ 11, & \text{if } n \equiv 3, 7 \ (10) \\ 14, & \text{if } n \equiv 4, 6 \ (10) \\ 15, & \text{if } n \equiv 5 \ (10), \end{cases}$$

*and*

$$c = \begin{cases} 0, & \text{if } n \equiv 0, 5 \ (10) \\ 1, & \text{if } n \equiv 2, 3, 7, 8 \ (10) \\ -1, & \text{if } n \equiv 4, 6 \ (10), \end{cases} \quad d = \begin{cases} 0, & \text{if } n \equiv 0, 2, 4, 6, 8 \ (10) \\ 1, & \text{if } n \equiv 3, 5, 7 \ (10). \end{cases}$$

7. *If* $N = 12$, *then*

$$G_n = \begin{cases} 0, & \text{if } n \equiv 1, 11 \ (12) \\ \varepsilon\alpha^{\{(n^2-\ a)/6\}}(\alpha-1)^{\{(59n^2+b)/12\}} & \\ \times(2\alpha-1)^{\{(n^2-c)/12\}}\lambda^{\{(3n^2+d)/4\}}\theta^{\{(2n^2+e)/3\}}, & \text{otherwise,} \end{cases}$$

*where* $\alpha \neq 0,\ 1,$

$$\varepsilon = \begin{cases} +1, & \text{if } n \equiv 0,2,3,9,10\ (12) \\ -1, & \text{if } n \equiv 4,5,6,7,8\ (12), \end{cases}$$

$$a = \begin{cases} 0, & \text{if } n \equiv 0\ (12) \\ 4, & \text{if } n \equiv 2,10\ (12) \\ 9, & \text{if } n \equiv 3,9\ (12) \\ 10, & \text{if } n \equiv 4,8\ (12) \\ 13, & \text{if } n \equiv 5,7\ (12) \\ 12, & \text{if } n \equiv 6\ (12), \end{cases} \quad b = \begin{cases} 0, & \text{if } n \equiv 0\ (12) \\ 4, & \text{if } n \equiv 2,10\ (12) \\ 9, & \text{if } n \equiv 3,9\ (12) \\ 16, & \text{if } n \equiv 4,8\ (12) \\ 1, & \text{if } n \equiv 5,7\ (12) \\ 24, & \text{if } n \equiv 6\ (12), \end{cases}$$

$$c = \begin{cases} 0, & \text{if } n \equiv 0,6\ (12), \\ 4, & \text{if } n \equiv 2,4,8,10\ (12) \\ 9, & \text{if } n \equiv 3,9\ (12) \\ 1, & \text{if } n \equiv 5,7\ (12), \end{cases} \quad d = \begin{cases} 0, & \text{if } n \equiv 0,2,4,6,8,10\ (12) \\ 1, & \text{if } n \equiv 3,5,7,9\ (12), \end{cases}$$

*and*

$$e = \begin{cases} 0, & \text{if } n \equiv 0,3,6,9\ (12) \\ 1, & \text{if } n \equiv 2,4,5,7,8,10\ (12). \end{cases}$$

THEOREM 9. *Let $E_N$ be a Tate normal form of an elliptic curve with a torsion point $P = (0,0)$ of order $N$. Let $(H_n)_{n\geq 0}$ be the sequence generated by the numerators of the y-coordinates of the multiples of $P$ as in (2). Let $\zeta, \lambda, \theta$ be as in (33) and (34). Then the general term of the sequence $(H_n)_{n\geq 0}$ can be given by the following formulas:*

1. *If $N = 4$, then*

$$H_n = \begin{cases} 0, & \text{if } n \equiv 1,2\ (4) \\ \varepsilon\alpha^{\{(9n^2-a)/8\}}, & \text{otherwise,} \end{cases}$$

*where $\alpha \neq 0$, and*

$$\varepsilon = \begin{cases} +1, & \text{if } n \equiv 0\ (8) \\ -1, & \text{if } n \equiv 3,4,7\ (8), \end{cases} \quad a = \begin{cases} 0, & \text{if } n \equiv 0\ (4) \\ 1, & \text{if } n \equiv 3\ (4). \end{cases}$$

2. *If $N = 5$, then*

$$H_n = \begin{cases} 0, & \text{if } n \equiv 1,3\ (5), \\ \varepsilon\alpha^{\{(6n^2-a)/5\}}, & \text{otherwise,} \end{cases}$$

*where $\alpha \neq 0$, and*

$$\varepsilon = \begin{cases} +1, & \text{if } n \equiv 0,4,7\ (10) \\ -1, & \text{if } n \equiv 2,5,9\ (10), \end{cases} \quad a = \begin{cases} 0, & \text{if } n \equiv 0\ (5) \\ -1, & \text{if } n \equiv 2\ (5) \\ 1, & \text{if } n \equiv 4\ (5). \end{cases}$$

3. *If* $N = 6$, *then*

$$H_n = \begin{cases} 0, & \text{if } n \equiv 1,4 \ (6), \\ \varepsilon\alpha^{\{(5n^2-a)/4\}}(\alpha+1)^{n^2}, & \text{otherwise,} \end{cases}$$

*where* $\alpha \neq -1,\ 0$, *and*

$$\varepsilon = \begin{cases} +1, & \text{if } n \equiv 0,5,6,9 \ (12) \\ -1, & \text{if } n \equiv 2,3,8,11 \ (12), \end{cases} \quad a = \begin{cases} 0, & \text{if } n \equiv 0,2 \ (6) \\ 1, & \text{if } n \equiv 3,5 \ (6). \end{cases}$$

4. *If* $N = 7$, *then*

$$H_n = \begin{cases} 0, & \text{if } n \equiv 1,5 \ (7) \\ \varepsilon\alpha^{\{(15n^2-a)/7\}}(\alpha-1)^{\{(9n^2-b)/7\}}, & \text{otherwise,} \end{cases}$$

*where* $\alpha \neq 0,\ 1$,

$$\varepsilon = \begin{cases} +1, & \text{if } n \equiv 0,4,7,11 \ (14) \\ -1, & \text{if } n \equiv 2,3,6,9,10,13 \ (14), \end{cases}$$

*and*

$$a = \begin{cases} 0, & \text{if } n \equiv 0 \ (7) \\ -3, & \text{if } n \equiv 2 \ (7) \\ 2, & \text{if } n \equiv 3 \ (7) \\ -5, & \text{if } n \equiv 4 \ (7) \\ 1, & \text{if } n \equiv 6 \ (7), \end{cases} \quad b = \begin{cases} 0, & \text{if } n \equiv 0 \ (7) \\ 1, & \text{if } n \equiv 2 \ (7) \\ 4, & \text{if } n \equiv 3,4 \ (7) \\ 2, & \text{if } n \equiv 6 \ (7). \end{cases}$$

5. *If* $N = 9$, *then*

$$H_n = \begin{cases} 0, & \text{if } n \equiv 1,7 \ (9) \\ \varepsilon\alpha^{\{(7n^2+a)/3\}}(\alpha-1)^{\{(4n^2-b)/3\}}\eta^{(n^2+c)}, & \text{otherwise} \end{cases}$$

*where* $\alpha \neq 0,\ 1$, $\eta = \alpha^2 - \alpha + 1$,

$$\varepsilon = \begin{cases} +1, & \text{if } n \equiv 0,4,5,8,11,12,15 \ (18) \\ -1, & \text{if } n \equiv 2,3,6,9,13,14,17 \ (18), \end{cases}$$

*and*

$$a = \begin{cases} 0, & \text{if } n \equiv 0,3 \ (9) \\ 2, & \text{if } n \equiv 2,5 \ (9) \\ -1, & \text{if } n \equiv 4,8 \ (9) \\ 3, & \text{if } n \equiv 6 \ (9), \end{cases} \quad b = \begin{cases} 0, & \text{if } n \equiv 0 \ (9) \\ 1, & \text{if } n \equiv 2,8 \ (9) \\ 3, & \text{if } n \equiv 3,6 \ (9) \\ 4, & \text{if } n \equiv 4,5 \ (9), \end{cases} \quad c = \begin{cases} 1, & \text{if } n \equiv 4 \ (9) \\ 0, & \text{otherwise.} \end{cases}$$

6. *If* $N = 10$, *then*

$$H_n = \begin{cases} 0, & \text{if } n \equiv 1,8 \ (10) \\ \varepsilon\alpha^{\{(63n^2+a)/20\}}(\alpha-1)^{\{(27n^2-b)/20\}} & \\ \times(2\alpha-1)^{\{(6n^2+c)/5\}}\zeta^{\{(15n^2+d)/4\}}, & \text{otherwise,} \end{cases}$$

*where* $\alpha \neq 0,\ 1,$

$$\varepsilon = \begin{cases} +1, & \text{if } n \equiv 0,4,5,9,10,13,14,17\ (20) \\ -1, & \text{if } n \equiv 2,3,6,7,12,15,16,19\ (20), \end{cases}$$

*and*

$$a = \begin{cases} 0, & \text{if } n \equiv 0\ (10) \\ 8, & \text{if } n \equiv 2\ (10) \\ -7, & \text{if } n \equiv 3\ (10) \\ 32, & \text{if } n \equiv 4\ (10) \\ 25, & \text{if } n \equiv 5\ (10) \\ -8, & \text{if } n \equiv 6\ (10) \\ 13, & \text{if } n \equiv 7\ (10) \\ -3, & \text{if } n \equiv 9\ (10), \end{cases} \quad b = \begin{cases} 0, & \text{if } n \equiv 0\ (10), \\ 8, & \text{if } n \equiv 2\ (10) \\ 23, & \text{if } n \equiv 3,\ 7\ (10) \\ 32, & \text{if } n \equiv 4,\ 6\ (10) \\ 35, & \text{if } n \equiv 5\ (10) \\ 7, & \text{if } n \equiv 9\ (10), \end{cases}$$

$$c = \begin{cases} 0, & \text{if } n \equiv 0,5\ (10) \\ 1, & \text{if } n \equiv 2,3,7\ (10) \\ -1, & \text{if } n \equiv 4,9\ (10) \\ 4, & \text{if } n \equiv 6\ (10), \end{cases} \quad d = \begin{cases} 0, & \text{if } n \equiv 0,2,4,6\ (10) \\ 1, & \text{otherwise.} \end{cases}$$

7. *If* $N = 12$, *then*

$$H_n = \begin{cases} 0, & \text{if } n \equiv 1,10\ (12) \\ \varepsilon\alpha^{\{(n^2-a)/4\}}(\alpha-1)^{\{(59n^2+b)/8\}} & \\ \times(2\alpha-1)^{\{(n^2-c)/8\}}\lambda^{\{(9n^2-d)/8\}}\theta^{(n^2+e)}, & \text{otherwise,} \end{cases}$$

*where* $\alpha \neq 0,\ 1,$

$$\varepsilon = \begin{cases} +1, & \text{if } n \equiv 0,3,5,7,8,11,14,16,18,21\ (24) \\ -1, & \text{if } n \equiv 2,4,6,9,12,15,17,19,20,23\ (24), \end{cases}$$

*and*

$$a = \begin{cases} 0, & \text{if } n \equiv 0\ (12) \\ 4, & \text{if } n \equiv 2\ (12) \\ 5, & \text{if } n \equiv 3\ (12) \\ 8, & \text{if } n \equiv 4,8\ (12) \\ 13, & \text{if } n \equiv 5\ (12) \\ 12, & \text{if } n \equiv 6\ (12) \\ 9, & \text{if } n \equiv 7,9\ (12) \\ 1, & \text{if } n \equiv 11\ (12), \end{cases} \quad b = \begin{cases} 0, & \text{if } n \equiv 0,4\ (12) \\ -4, & \text{if } n \equiv 2\ (12) \\ 13, & \text{if } n \equiv 3\ (12) \\ 5, & \text{if } n \equiv 5,11\ (12) \\ 12, & \text{if } n \equiv 6\ (12) \\ -3, & \text{if } n \equiv 7,9\ (12) \\ 16, & \text{if } n \equiv 8\ (12), \end{cases}$$

$$c = \begin{cases} 0, & \text{if } n \equiv 0,4,8\ (12) \\ 4, & \text{if } n \equiv 2,6\ (12) \\ 1, & \text{if } n \equiv 3,11\ (12) \\ 9, & \text{if } n \equiv 5,9\ (12) \\ -7, & \text{if } n \equiv 7\ (12), \end{cases} \quad d = \begin{cases} 0, & \text{if } n \equiv 0,4,8\ (12) \\ -4, & \text{if } n \equiv 2,6\ (12) \\ 1, & \text{if } n \equiv 3,7,11\ (12) \\ -7, & \text{if } n \equiv 5,9\ (12), \end{cases}$$

*and*

$$e = \begin{cases} 1, & \text{if } n \equiv 4, 7 \ (12) \\ 0, & \text{otherwise.} \end{cases}$$

## APPENDIX B

In the following theorems, we determine square and cube terms in the sequences $(G_n)_{n\geq 0}$ and $(H_n)_{n\geq 0}$ associated to an elliptic curve in Tate normal form with a torsion point $P = (0, 0)$ of order $N$. The proofs are similar to the proof of Theorem 6.

THEOREM 10. *Let $E_N$ be a Tate normal form of an elliptic curve with a torsion point $P = (0, 0)$ of order $N$. Let $(G_n)_{n\geq 0}$ be the sequence generated by the numerators of the $x$-coordinates of the multiples of $P$ as in (2), and let $G_n \neq 0$.*

1. *Let $N = 4$.*
   - (i) $\diamond$ *If $n \equiv 0$ (4), then $G_n = \square$ for all non-zero $\alpha$,*
     $\diamond$ *otherwise $G_n = \square$ iff $\alpha = \square$.*
   - (ii) $\diamond$ *$G_n = C$ for all non-zero $\alpha$.*
2. *Let $N = 5$.*
   - (i) $\diamond$ *If $n \equiv 0$ (5), then $G_n = \square$ for all non-zero $\alpha$,*
     $\diamond$ *otherwise $G_n = \square$ iff $\alpha = \square$.*
   - (ii) $\diamond$ *If $n \equiv 0, 2, 7, 8, 13$ (15), then $G_n = C$ for all non-zero $\alpha$,*
     $\diamond$ *otherwise $G_n = C$ iff $\alpha = C$.*
3. *Let $N = 6$.*
   - (i) $\diamond$ *If $n \equiv 0$ (6), then $G_n = \square$ for all $\alpha \neq -1, 0$,*
     $\diamond$ *if $n \equiv 3$ (6), then $G_n = \square$ iff $\alpha = \square$,*
     $\diamond$ *otherwise $G_n \neq \square$ for all $\alpha \neq -1, 0$.*
   - (ii) $\diamond$ *If $n \equiv 0, 2, 6, 12, 16$ (18), then $G_n = C$ for all $\alpha \neq -1, 0$,*
     $\diamond$ *if $n \equiv 3, 9, 15$ (18), then $G_n = C$ iff $\alpha = C$,*
     $\diamond$ *otherwise $G_n \neq C$ for all $\alpha \neq -1, 0$.*
4. *Let $N = 7$.*
   - (i) $\diamond$ *If $n \equiv 0$ (7), then $G_n = \square$ for all $\alpha \neq 0, 1$,*
     $\diamond$ *if $n \equiv 2, 5$ (7), then $G_n = \square$ iff $\alpha - 1 = \square$,*
     $\diamond$ *otherwise $G_n \neq \square$ for all $\alpha \neq 0, 1$.*
   - (ii) $\diamond$ *If $n \equiv 0, 2, 5, 16, 19$ (21), then $G_n = C$ for all $\alpha \neq 0, 1$,*
     $\diamond$ *if $n \equiv 7, 9, 12, 14$ (21), then $G_n = C$ iff $\alpha = C$,*
     $\diamond$ *otherwise $G_n \neq C$ for all $\alpha \neq 0, 1$.*
5. *Let $N = 9$.*
   - (i) $\diamond$ *If $n \equiv 0$ (9), then $G_n = \square$ for all $\alpha \neq 0, 1$,*
     $\diamond$ *if $n \equiv 3, 6$ (9), then $G_n = \square$ iff $\alpha - 1 = \square$,*
     $\diamond$ *otherwise $G_n \neq \square$ for all $\alpha \neq 0, 1$.*

(ii) ◇ *If* $n \equiv 0,\ 2,\ 9,\ 18,\ 25\ (27)$, *then* $G_n = C$ *for all* $\alpha \neq 0,\ 1$,
◇ *if* $n \equiv 5,\ 22\ (27)$, *then* $G_n = C$ *iff* $\alpha^2 - \alpha + 1 = C$,
◇ *otherwise* $G_n \neq C$ *for all* $\alpha \neq 0,\ 1$.

6. *Let* $N = 10$.
(i) ◇ *If* $n \equiv 0\ (10)$, *then* $G_n = \square$ *for all* $\alpha \neq 0,\ 1$,
◇ *if* $n \equiv 4,\ 6\ (10)$, *then* $G_n = \square$ *iff* $(\alpha - 1)(2\alpha - 1) = \square$,
◇ *otherwise* $G_n \neq \square$ *for all* $\alpha \neq 0,\ 1$.
(ii) ◇ *If* $n \equiv 0\ (30)$, *then* $G_n = C$ *for all* $\alpha \neq 0,\ 1$,
◇ *if* $n \equiv 2,\ 8,\ 22,\ 28\ (30)$, *then* $G_n = C$ *iff* $\alpha^2 - 3\alpha + 1 = C$,
◇ *if* $n \equiv 12,\ 18\ (30)$, *then* $G_n = C$ *iff* $2\alpha - 1 = C$,
◇ *otherwise* $G_n \neq C$ *for all* $\alpha \neq 0,\ 1$.

7. *Let* $N = 12$.
(i) ◇ *If* $n \equiv 0\ (12)$, *then* $G_n = \square$ *for all* $\alpha \neq 0,\ 1$,
◇ *otherwise* $G_n \neq \square$ *for all* $\alpha \neq 0,\ 1$.
(ii) ◇ *If* $n \equiv 0,\ 12,\ 24\ (36)$, *then* $G_n = C$ *for all* $\alpha \neq 0,\ 1$,
◇ *if* $n \equiv 16,\ 20\ (36)$, *then* $G_n = C$ *iff* $\alpha = C$,
◇ *if* $n \equiv 2,\ 34\ (36)$, *then* $G_n = C$ *iff* $\alpha - 1 = C$,
◇ *otherwise* $G_n \neq C$ *for all* $\alpha \neq 0,\ 1$.

THEOREM 11. *Let* $E_N$ *be a Tate normal form of an elliptic curve with a torsion point* $P = (0, 0)$ *of order* $N$. *Let* $(H_n)_{n \geq 0}$ *be the sequence generated by the numerators of the y-coordinates of the multiples of* $P$ *as in (2), and let* $H_n \neq 0$.

1. *Let* $N = 4$.
(i) ◇ *If* $n \equiv 0,\ 3,\ 4\ (8)$, *then* $H_n = \square$ *for all non-zero* $\alpha$,
◇ *otherwise* $H_n = \square$ *iff* $\alpha = \square$.
(ii) ◇ *If* $n \equiv 0\ (4)$, *then* $H_n = C$ *for all non-zero* $\alpha$,
◇ *otherwise* $H_n = C$ *iff* $\alpha = C$.

2. *Let* $N = 5$.
(i) ◇ *If* $n \equiv 0\ (5)$, *then* $H_n = \square$ *for all non-zero* $\alpha$,
◇ *otherwise* $H_n = \square$ *iff* $\alpha = \square$.
(ii) ◇ *If* $n \equiv 0\ (5)$, *then* $H_n = C$ *for all non-zero* $\alpha$,
◇ *otherwise* $H_n = C$ *iff* $\alpha = C$.

3. *Let* $N = 6$.
(i) ◇ *If* $n \equiv 0,\ 8\ (12)$, *then* $H_n = \square$ *for all* $\alpha \neq -1,\ 0$,
◇ *if* $n \equiv 2,\ 6\ (12)$, *then* $H_n = \square$ *iff* $\alpha = \square$,
◇ *otherwise* $H_n \neq \square$ *for all* $\alpha \neq -1,\ 0$.
(ii) ◇ *If* $n \equiv 0\ (6)$, *then* $H_n = C$ *for all* $\alpha \neq -1,\ 0$,
◇ *if* $n \equiv 3\ (6)$, *then* $H_n = C$ *iff* $\alpha = C$,
◇ *otherwise* $H_n \neq C$ *for all* $\alpha \neq -1,\ 0$.

4. *Let* $N = 7$.
   (i) $\diamond$ *If* $n \equiv 0,\ 9,\ 10\ (14)$, *then* $H_n = \square$ *for all* $\alpha \neq 0,\ 1$,
   $\diamond$ *if* $n \equiv 4,\ 6\ (14)$, *then* $H_n = \square$ *iff* $\alpha = \square$,
   $\diamond$ *if* $n \equiv 11,\ 13\ (14)$, *then* $H_n = \square$ *iff* $\alpha - 1 = \square$,
   $\diamond$ *otherwise* $H_n \neq \square$ *for all* $\alpha \neq 0,\ 1$.
   (ii) $\diamond$ *If* $n \equiv 0\ (7)$, *then* $H_n = C$ *for all* $\alpha \neq 0,\ 1$,
   $\diamond$ *if* $n \equiv 2\ (7)$, *then* $H_n = C$ *iff* $\alpha - 1 = C$,
   $\diamond$ *otherwise* $H_n \neq C$ *for all* $\alpha \neq 0,\ 1$.
5. *Let* $N = 9$.
   (i) $\diamond$ *If* $n \equiv 0,\ 13,\ 14\ (18)$, *then* $H_n = \square$ *for all* $\alpha \neq 0,\ 1$,
   $\diamond$ *if* $n \equiv 2,\ 12\ (18)$, *then* $H_n = \square$ *iff* $\alpha - 1 = \square$,
   $\diamond$ *otherwise* $H_n \neq \square$ *for all* $\alpha \neq 0,\ 1$.
   (ii) $\diamond$ *If* $n \equiv 0\ (9)$, *then* $H_n = C$ *for all* $\alpha \neq 0,\ 1$,
   $\diamond$ *if* $n \equiv 3\ (9)$, *then* $H_n = C$ *iff* $\alpha - 1 = C$,
   $\diamond$ *otherwise* $H_n \neq C$ *for all* $\alpha \neq 0,\ 1$.
6. *Let* $N = 10$.
   (i) $\diamond$ *If* $n \equiv 0,\ 5,\ 15,\ 16\ (20)$, *then* $H_n = \square$ *for all* $\alpha \neq 0,\ 1$,
   $\diamond$ *if* $n \equiv 4,\ 12\ (20)$, *then* $H_n = \square$ *iff* $2\alpha - 1 = \square$,
   $\diamond$ *if* $n \equiv 3,\ 13\ (20)$, *then* $H_n = \square$ *iff* $(\alpha - 1)(2\alpha - 1) = \square$,
   $\diamond$ *otherwise* $H_n \neq \square$ *for all* $\alpha \neq 0,\ 1$.
   (ii) $\diamond$ *If* $n \equiv 0\ (10)$, *then* $H_n = C$ *for all* $\alpha \neq 0,\ 1$,
   $\diamond$ *otherwise* $H_n \neq C$ *for all* $\alpha \neq 0,\ 1$.
7. *Let* $N = 12$.
   (i) $\diamond$ *If* $n \equiv 0,\ 8,\ 12,\ 19,\ 20\ (24)$, *then* $H_n = \square$ *for all* $\alpha \neq 0,\ 1$,
   $\diamond$ *if* $n \equiv 4,\ 16\ (24)$, *then* $H_n = \square$ *iff* $2\alpha - 2\alpha^2 - 1 = \square$,
   $\diamond$ *otherwise* $H_n \neq \square$ *for all* $\alpha \neq 0,\ 1$.
   (ii) $\diamond$ *If* $n \equiv 0\ (12)$, *then* $H_n = C$ *for all* $\alpha \neq 0,\ 1$,
   $\diamond$ *otherwise* $H_n \neq C$ *for all* $\alpha \neq 0,\ 1$.

**Acknowledgments.** This work was supported by the research fund of Bursa Uludağ University project no: KUAP(F)-2017/3.

REFERENCES

[1] M. Ayad, *Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques*. Ann. Inst. Fourier **43** (1993), *3*, 585–618.

[2] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*. J. Symbolic Comput. **24** (1997), *3-4*, 235–265.

[3] A. Bremner and N. Tzanakis, *Lucas sequences whose 12th or 9th term is a square*. J. Number Theory **107** (2004), 215–227.

[4] A. Bremner and N. Tzanakis, *On squares in Lucas sequences*. J. Number Theory **124** (2007), 511–520.

[5] J. Cheon and S. Hahn, *Explicit valuations of division polynomials of an elliptic curve*. Manuscripta Math. **97** (1998), 319–328.

[6] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*. Math. Surveys Monogr. **104**, AMS, Providence, RI, 2003.

[7] I. Garcia-Selfa, M.A. Olalla and J.M. Tornero, *Computing the rational torsion of an elliptic curve using Tate normal form*. J. Number Theory **96** (2002), 76–88.

[8] J. Gebel, A. Pethő and H.G. Zimmer, *Computing integral points on elliptic curves*. Acta Arith. **68** (1994), 171–192.

[9] B. Gezer, *Elliptic divisibility sequences, squares and cubes*. Publ. Math. Debrecen **83** (2013), *3*, 481–515.

[10] B. Gezer and O. Bizim, *Squares in elliptic divisibility sequences*. Acta Arith. **144** (2010), *2*, 125–134.

[11] B. Gezer and O. Bizim, *Cubes in elliptic divisibility sequences*. Math. Rep. (Bucur.) **14 (64)** (2012), *1*, 21–29.

[12] B. Gezer and O. Bizim, *Sequences generated by elliptic curves*. Acta Arith. **188** (2019), *3*, 253–268.

[13] D. Husemöller, *Elliptic Curves*. Springer-Verlag, New York, 1987.

[14] D.S. Kubert, *Universal bounds on the torsion of elliptic curves*. Proc. Lond. Math. Soc. **33** (1976), *3*, 193–237.

[15] `http://magma.maths.usyd.edu.au/calc/`

[16] B. Mazur, *Modular curves and the Eisenstein ideal*. Publ. Math. Inst. Hautes Études Sci. **47** (1977), 33–186.

[17] V. Mahé, *Prime power terms in elliptic divisibility sequences*. Math. Comp. **83** (288) (2014), 1951–1991.

[18] B. Mazur and J. Tate, *The p-adic sigma function*. Duke Math. J. **62** (1991), 663–688.

[19] L.J. Mordell, *Diophantine Equations*. Pure Appl. Math. **30**, Academic Press, London and New York, 1970.

[20] A. Pethő, *Full cubes in the Fibonacci sequence*. Publ. Math. Debrecen **30** (1983), 117–127.

[21] A. Pethő, *On Mordell's equation*. https://arato.inf.unideb.hu/petho.attila/cikkek/67_MORDELL.pdf

[22] J. Reynolds, *Perfect powers in elliptic divisibility sequences*. J. Number Theory **132** (2012), 998–1015.

[23] P. Ribenboim, *Pell numbers, squares and cubes*. Publ. Math. Debrecen **54** (1999), 131–152.

[24] P. Ribenboim and W. McDaniel, *The square terms in Lucas sequences*. J. Number Theory **58** (1996), 104–123.

[25] P. Ribenboim and W. McDaniel, *Squares in Lucas sequences having an even first parameter*. Colloq. Math. **78** (1998), 29–34.

[26] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p.* Math. Comp. **44** (170) (1985), 483–494.

[27] R. Shipsey, *Elliptic divisibility sequences.* Ph. D. Thesis, University of London, 2000.

[28] J.H. Silverman, *The Arithmetic of Elliptic Curves.* Second Edition. Grad. Texts in Math. **106**, Springer-Verlag, New York, 2009.

[29] J.H. Silverman and J. Tate, *Rational Points on Elliptic Curves.* Undergrad. Texts Math., Springer, 1992.

[30] J.H. Silverman, *p-adic properties of division polynomials and elliptic divisibility sequences.* Math. Ann. **332** (2005), *2*, 443–471, addendum 473–474.

[31] J.H. Silverman and N. Stephens, *The sign of an elliptic divisibility sequence.* J. Ramanujan Math. Soc. **21** (2006), *1*, 1–17.

[32] K. Stange, *Integral points on elliptic curves and explicit valuations of division polynomials.* Canad. J. Math. **68** (2016), *5*, 1120–1158.

[33] R.J. Stroeker and N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms.* Acta Arith. **67** (1994), 177–196.

[34] C.S. Swart, *Elliptic curves and related sequences.* Ph.D. Thesis, University of London, 2003.

[35] M. Ward, *Memoir on elliptic divisibility sequences.* Amer. J. Math. **70** (1948), 31–74.

[36] M. Ward, *The law of repetition of primes in an elliptic divisibility sequences.* Duke Math. J. **15** (1948), 941–946.

*Received March 12, 2019*

*Bursa Uludağ University*
*Faculty of Science*
*Department of Mathematics*
*Gorukle, 16059, Bursa, Turkiye*
betulgezer@uludag.edu.tr