ACTA ARITHMETICA
188.3 (2019)

Sequences generated by elliptic curves

by

Betül Gezer and Osman Bizim (Bursa)

1. Introduction. Let E be an elliptic curve defined over a field K given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

let $E(K)$ denote the group of K-rational points on the elliptic curve E and let $\mathcal{O}$ denote the point at infinity, the identity element of the group $E(K)$. For a deeper discussion of elliptic curves, see [8, 11]. 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 differential $\omega = dx/(2y + a_1x + a_3)$ has an expansion as a formal Laurent series in a formal neighborhood of $\mathcal{O}$ such that

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

Note that the series $\omega(z)$ has coefficients in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$. Furthermore the uniformizer z and the differential ω 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 [9, Definition 1] (see also [4] for more details).

Recall that an elliptic curve over $\mathbb{C}$ has a complex uniformization $\Phi : \mathbb{C}/L \to E(\mathbb{C})$ with a lattice $L \subset \mathbb{C}$. Then the classical n-division polynomial

2010 *Mathematics Subject Classification*: Primary 14H52; Secondary 11G07, 14G20, 11B37.
Key words and phrases: elliptic curves, division polynomials, elliptic divisibility sequences.
Received 4 May 2017; revised 16 May 2018.
Published online 7 March 2019.

DOI: 10.4064/aa170504-25-6

is given by

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

where $\sigma(z, L)$ is the Weierstrass σ-function associated to the lattice L. Silverman [9] showed that there is a relationship between the normalized n-division polynomial F_n and the classical n-division polynomial ψ_n: there is a constant $\gamma \in \mathbb{C}^*$ such that

$$F_n(\Phi(z)) = \gamma^{1-n^2}\psi_n(z,\, L)$$

for all $z \in \mathbb{C}$ and all $n \geq 1$.

Division polynomials also arise in expressing the coordinates of $[n]P$ in terms of a point $P = (x, y) \in E(K)$ (with $\mathrm{char}(K) \neq 2$): for some $\gamma \in K^*$, we can write the multiples of P as

$$[n]P = \left(\frac{\phi_n(P)}{\psi_n^2(P)}, \frac{\omega_n(P)}{\psi_n^3(P)}\right) = \left(\frac{\gamma^2 G_n(P)}{F_n^2(P)}, \frac{\gamma^3 H_n(P)}{F_n^3(P)}\right) \tag{1.2}$$

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

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

are suitably normalized division polynomials of E. Furthermore the polynomials ϕ_n and ω_n are given by the recursion formulas

$$\phi_0 = 1, \quad \phi_1 = x,$$
$$\omega_0 = 1, \quad \omega_1 = y,$$

and for $n \geq 2$,

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1},$$
$$\omega_n = (\psi_{n-1}^2\psi_{n+2} - \psi_{n-2}\psi_{n+1}^2 - \psi_2\psi_n(a_1\phi_n + a_3\psi_n^2))(2\psi_2)^{-1}.$$

Then the normalized division polynomials G_n and H_n satisfy the following relations for some $\gamma \in K^*$:

$$G_0 = 1, \quad G_1 = \gamma^{-2}x,$$
$$H_0 = 1, \quad H_1 = \gamma^{-3}y,$$

and for $n \geq 2$,

$$\begin{aligned} G_n &= x\gamma^{-2}F_n^2 - F_{n+1}F_{n-1}, \\ H_n &= (F_{n-1}^2F_{n+2} - F_{n-2}F_{n+1}^2 - \gamma^{-1}F_2F_n(a_1G_n + \gamma^{-2}a_3F_n^2))(2F_2)^{-1}. \end{aligned} \tag{1.3}$$

Division polynomials play important roles in the theory of elliptic curves, e.g. in counting points on an elliptic curve defined over a finite field [5], and in the theory of elliptic divisibility sequences [13]. Silverman [9] considered the sequence $(F_n(P))_{n\geq 0}$ of values of the division polynomials of E at a point $P \in E(K)$ and studied the periodicity properties and the p-adic behavior of this sequence. See also [2], [7] for more work on the division polynomials.

The purpose of this paper is to study 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, i.e., the sequences of values $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ of suitably normalized division polynomials of E evaluated at a point $P \in E(K)$. We study the periodicity properties of $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ when K is a finite field. Then we consider the p-adic behavior of these sequences when K is a local field. We will obtain many results for these sequences similar to those for $(F_n(P))_{n\geq 0}$.

Our first main theorem shows that $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ are purely periodic.

THEOREM 1.1. *Let p be an odd prime, let E be an elliptic curve defined over the finite field $\mathbb{F}_p$ and let $P \in E(\mathbb{F}_p)$ be a point of order* ([1]) *$r > 3$. 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* (1.2)*, respectively. Then the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ are purely periodic with periods rt and rt' for some integers t and t', respectively. In particular, the integers t and t' divide $p-1$.*

The proof of Theorem 1.1 uses [9, Theorem 8] which is similar to a result of Ward for elliptic divisibility sequences [13, Theorems 8.1, 8.2 and 9.2]. We can generalize Theorem 1.1 to the case of modulo prime powers.

THEOREM 1.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be a point of infinite order. Let p be an odd prime such that P modulo p is nonsingular and let $r > 3$ be the order of P modulo p. Write $v = \mathtt{ord}_p(F_r(P))$ and $r_l = p^{l-v}r$ for $l \geq v$. 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* (1.2)*, respectively. Then the sequences*

$$(G_n(P) \bmod p^l)_{n\geq 0} \quad \text{and} \quad (H_n(P) \bmod p^l)_{n\geq 0}$$

are purely periodic with periods $r_l t_l$ and $r_l t'_l$ for some integers t_l and t'_l, respectively. In particular, the integers t_l and t'_l divide $p^{l-1}(p-1)$ for all positive integers l.

We will prove that $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ possess certain periodicity properties and we will use similar techniques to [9] to show that some of their subsequences have p-adic limits. Furthermore, if E is an elliptic curve defined over $\mathbb{Q}$ and ordinary at p, then the limits of these convergent sequences are algebraic numbers.

THEOREM 1.3. *Let E be an elliptic curve defined over the field $\mathbb{Q}_p$, let $P \in E(\mathbb{Q}_p)$ be a point whose reduction modulo p has order $r \geq 3$ and let*

([1]) That is, the smallest positive integer such that $[r]P = \mathcal{O}$.

$(G_n(P))_{n\geq 0}$ 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 (1.2), respectively. Suppose further that p is an odd prime and $p \nmid r$. Then there exists a power $q = p^N$ such that for all $m \geq 1$, the limits

$$\lim_{i\to\infty} G_{mq^i}(P) \text{ and } \lim_{i\to\infty} H_{mq^i}(P) \quad \text{exist in } \mathbb{Z}_p.$$

If in addition E is defined over $\mathbb{Q}$, ordinary at p and $P \in E(\mathbb{Q})$, then the limits of these sequences are algebraic numbers.

2. Elliptic divisibility sequences. An *elliptic divisibility sequence* (EDS) is a sequence $(h_n)_{n\geq 0}$ of integers satisfying a nonlinear recursion of the form

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \tag{2.1}$$

and the divisibility property

$$h_n \mid h_m \quad \text{whenever} \quad n \mid m$$

for all $m \geq n \geq 1$. See [13], [14], and [3] for more details on EDSs. 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

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

(see [9], [10] or [13]). A proper elliptic divisibility sequence is called *nonsingular* if $\Delta(h_n) \neq 0$.

Ward was the first to study the arithmetic properties of elliptic divisibility sequences in a series of papers in 1948 [13, 14]. He showed that nonsingular elliptic divisibility sequences arise as values of the division polynomials of an elliptic curve. More precisely, in [13, Theorem 12.1] he 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

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

where $\psi_n(z, L)$ and $\sigma(z, L)$ are the n-division polynomial and the Weierstrass σ-function associated to the lattice L, respectively. Assume now that the lattice L determines an elliptic curve E and the point z determines a point P on E. Then the elliptic divisibility sequence $(h_n)_{n\geq 0}$ is said to be *associated* to the elliptic curve E and the point P. Silverman [9, Proposition 18] reformulated Ward's result and proved 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

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

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

3. Periodicity of division polynomials. Let $(h_n)_{n\geq 0}$ be a sequence and let m be a positive integer. Then m is called a *divisor* of the sequence $(h_n)_{n\geq 0}$ if it divides some term h_k with $k > 0$. If m divides h_r but does not divide h_l when l is a proper divisor of r, then r is called a *rank of apparition* of m in $(h_n)_{n\geq 0}$. Ward [13] showed that an elliptic divisibility sequence $(h_n)_{n\geq 0}$ admits every prime p as a divisor and p has at least one rank of apparition r in $(h_n)_{n\geq 0}$ with $r \leq 2p+1$. Ward also proved that elliptic divisibility sequences modulo a prime are periodic and the period is a multiple of a rank of apparition r [13, Theorem 11.1]. Ward used the properties of the Weierstrass σ-function to show that elliptic divisibility sequences possess certain periodicity properties. These properties are called *symmetry properties* after Ward.

Let E be an elliptic curve defined over a finite field $\mathbb{F}$ and let $P \in E(\mathbb{F})$. Silverman [9] used a lift to characteristic zero and the Lefschetz principle to prove that the sequence $(F_n(P))_{n\geq 0}$ of values of the normalized n-division polynomials of E at P is purely periodic, which is inspired by a similar result of Ward for elliptic divisibility sequences. Silverman showed that the symmetry properties hold for the sequence $(F_n(P))_{n\geq 0}$.

THEOREM 3.1 ([9, Theorem 8]). *Let $\mathbb{F}$ be a finite field, let E be an elliptic curve defined over $\mathbb{F}$ and let $P \in E(\mathbb{F})$ be a point of order $r \geq 3$. Let $(F_n(P))_{n\geq 0}$ be the sequence of values of the normalized n-division polynomials of E at P as in* (1.2)*. Then there exist units $a, b \in \mathbb{F}^*$, depending on P, such that for all nonnegative integers k, n,*

$$F_{r+n}(P) = a^n b F_n(P), \tag{3.1}$$

$$F_{kr+n}(P) = a^{kn} b^{k^2} F_n(P). \tag{3.2}$$

Furthermore, the units a and b satisfy

$$a = \frac{F_{r+2}(P)}{F_2(P)F_{r+1}(P)}, \quad b = \frac{F_2(P)F_{r+1}(P)^2}{F_{r+2}(P)} \quad \text{and} \quad a^r = b^2. \tag{3.3}$$

From Theorem 3.1, Silverman [9, Corollary 9] immediately deduced the periodicity of $(F_n(P))_{n\geq 0}$. Here we restate a theorem of Ward for explicit computation of the period of $(F_n(P))_{n\geq 0}$.

THEOREM 3.2 ([13, Theorem 11.1]). *Let p be an odd prime and let E be an elliptic curve over the finite field $\mathbb{F}_p$ having a point $P \in E(\mathbb{F}_p)$ of order $r \geq 3$. Let $(F_n(P))_{n\geq 0}$ be the sequence of values of the normalized n-division*

polynomials of E at P. Suppose

$$e = \frac{F_2(P)}{F_{r+2}(P)}, \qquad k = F_{r+1}(P), \tag{3.4}$$

and let ε, κ be the orders of e and k in $\mathbb{F}_p^*$, respectively. Then the sequence $(F_n(P))_{n\geq 0}$ is purely periodic with period rt where $t = 2^\mu \operatorname{lcm}[\varepsilon, \kappa]$ and the exponent μ is determined as follows:

$$\mu = \begin{cases} -1 & \text{if } \varepsilon \text{ and } \kappa \text{ are both even and both divisible} \\ & \text{by } 2^x \text{ with exactly the same power } x \geq 2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The proof uses Theorem 3.1 and [13, Theorem 11.1]. ∎

4. Periodicity of $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$. In this section, we will prove that the sequences $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ of values of suitably normalized division polynomials evaluated at a fixed point $P \in E(\mathbb{F}_p)$ on an elliptic curve E are purely periodic. We will give some formulas for explicit computation of the periods of $(G_n(P) \pmod p)_{n\geq 0}$ and $(H_n(P) \pmod p)_{n\geq 0}$. First, in the following theorem we show that symmetry properties hold for these sequences similar to Ward's symmetry properties.

THEOREM 4.1. *Let p be an odd prime, let E be an elliptic curve defined over the finite field $\mathbb{F}_p$ and let $P \in E(\mathbb{F}_p)$ be a point of order $r \geq 3$. 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 (1.2), respectively. Then there exist units $a, b \in \mathbb{F}_p^*$, depending on P, such that for all nonnegative integers k, n,*

$$G_{r+n}(P) = a^{2n}b^2 G_n(P), \qquad H_{r+n}(P) = a^{3n}b^3 H_n(P), \tag{4.1}$$

$$G_{kr+n}(P) = a^{2kn}b^{2k^2} G_n(P), \quad H_{kr+n}(P) = a^{3kn}b^{3k^2} H_n(P). \tag{4.2}$$

Furthermore, the units a and b satisfy

$$a^2 = \frac{G_2(P)G_{r+3}(P)}{G_3(P)G_{r+2}(P)}, \quad b^2 = \frac{G_3(P)^2 G_{r+2}(P)^3}{G_2(P)^3 G_{r+3}(P)^2}, \tag{4.3}$$

$$a^3 = \frac{H_{r+1}(P)}{H_1(P)H_r(P)}, \qquad b^3 = H_r(P), \tag{4.4}$$

for nonzero $G_i(P)$ and $H_i(P)$.

Proof. Replacing n by $r+n$ in (1.3) and then using the equation in (3.1) we derive the formulas in (4.1). Similarly replacing n by $kr+n$ in (1.3) and then using the equation in (3.2) we obtain the formulas in (4.2).

Finally, setting $n = 2$ and then $n = 3$ in the first equation of (4.1) we obtain

$$G_{r+2}(P) = a^4b^2G_2(P) \quad \text{and} \quad G_{r+3}(P) = a^6b^2G_3(P). \tag{4.5}$$

Thus, the values a^2 and b^2 can be obtained from these equations for non-zero $G_i(P)$.

Similarly putting $n = 0$ and then $n = 1$ in the second equation of (4.1) we have

$$H_r(P) = b^3 \quad \text{and} \quad H_{r+1}(P) = a^3b^3H_1(P), \tag{4.6}$$

since $H_0(P) = 1$. Hence we derive the second equation in (4.4), and so the value a^3 can be obtained from the second equation of (4.6) for non-zero $H_i(P)$. ∎

Remark 4.2. (i) It is clear that the equations in (4.5) (or the second equation in (4.6)) cannot be used to find the values a^2, b^2 (or a^3) when both sides of the equations in (4.5) (or the second equation in (4.6)) are zero. In any case, these values can be obtained directly from the first and second equations in (3.3). It follows that

$$a^2 = \frac{F_{r+2}(P)^2}{F_2(P)^2F_{r+1}(P)^2}, \quad b^2 = \frac{F_2(P)^2F_{r+1}(P)^4}{F_{r+2}(P)^2}, \tag{4.7}$$

$$a^3 = \frac{F_{r+2}(P)^3}{F_2(P)^3F_{r+1}(P)^3}, \quad b^3 = \frac{F_2(P)^3F_{r+1}(P)^6}{F_{r+2}(P)^3}. \tag{4.8}$$

(ii) It can easily be seen that $F_{-n}(P) = -F_n(P)$ for all $n \geq 0$. From this fact and by (1.3) one can obtain

$$\begin{aligned} G_{-n}(P) &= G_n(P), \\ H_{-n}(P) &= H_n(P) + \gamma^{-1}F_n(P)F_2(P)(a_1G_n(P) + a_3\gamma^{-2}F_n(P)^2), \end{aligned}$$

for all $n \geq 0$.

(iii) Replacing n by $-n$ in (3.1), (3.2), (4.1), (4.2) and then using the relations in (ii) we obtain

$$\begin{aligned} F_{r-n}(P) &= -a^{-n}bF_n(P), & F_{kr-n}(P) &= -a^{-kn}b^{k^2}F_n(P), \\ G_{r-n}(P) &= a^{-2n}b^2G_n(P), & G_{kr-n}(P) &= a^{-2kn}b^{2k^2}G_n(P), \\ H_{r-n}(P) &= a^{-3n}b^3H_{-n}(P), & H_{kr-n}(P) &= a^{-3kn}b^{3k^2}H_{-n}(P), \end{aligned}$$

for $n = 0, 1, \ldots, r$.

Now we will prove our first main theorem.

Proof of Theorem 1.1. Let a and b as in Theorem 3.1 and let t be the smallest integer such that

$$a^{2t} = 1, \quad b^{2t^2} = 1. \tag{4.9}$$

It is clear that t divides the least common multiple of the orders of a and b in $\mathbb{F}_p^*$, therefore $t \mid p-1$. The first equation of (4.2) implies that

$$G_{rt+n}(P) = a^{2tn}b^{2t^2}G_n(P) = G_n(P) \quad \text{for all } n \geq 0.$$

Thus the sequence $(G_n(P))_{n\geq 0}$ is periodic and rt is a period.

Let $(F_n(P))_{n\geq 0}$ be the sequence of values of the normalized n-division polynomials of E at P. Then

$$F_n(P) = 0 \quad \text{if and only if} \quad r \mid n$$

since $P \in E(\mathbb{F}_p)$ has order r. Now write $n = mr$ for some integer $m \geq 1$. Then by (1.3) we have

$$G_{mr}(P) = G_n(P) = -F_{mr+1}(P)F_{mr-1}(P)$$

since $F_{mr}(P) = 0$. Therefore by (3.2) and Remark 4.2(iii), we obtain

$$G_n(P) = b^{2m^2} \tag{4.10}$$

since $F_1(P) = 1$. It follows that $G_n(P) = b^{2m^2}$ for some $m \geq 1$ when $n = mr$, i.e., $r \mid n$. Let $\pi \geq 1$ be the least period of $(G_n(P))_{n\geq 0}$. Then by (4.10),

$$G_{\pi+r}(P) = G_r(P) = b^2.$$

It follows that $r \mid \pi$. Now write $\pi = rs$ for some integer $s \geq 1$. Then $s \mid t$, since rt is a period. On the other hand, by the first equation in (4.2) we have

$$G_n(P) = G_{rs+n}(P) = a^{2sn}b^{2s^2}G_n(P)$$

and so $a^{2sn}b^{2s^2} = 1$ for all $n \geq 0$. Now setting $n = 1$ and then $n = 2$ in the last equation we obtain $a^{2s} = 1$ and so $b^{2s^2} = 1$. Therefore $s \geq t$ and hence $s = t$, which completes the proof for $(G_n(P))_{n\geq 0}$.

Now let t' be the smallest integer such that

$$a^{3t'} = 1,\ b^{3t'^2} = 1. \tag{4.11}$$

Thus t' divides the least common multiple of the orders of a and b in $\mathbb{F}_p^*$, and so $t' \mid p-1$. The second equation of (4.2) implies that

$$H_{rt'+n}(P) = a^{3t'n}b^{3t'^2}H_n(P) = H_n(P) \quad \text{for all } n \geq 0,$$

thus $(H_n(P))_{n\geq 0}$ is periodic and rt' is a period. The rest of the proof is similar to the proof of the periodicity of $(G_n(P))_{n\geq 0}$. ∎

Theorem 1.1 tells us that $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$ are purely periodic with periods rt and rt', respectively. Now we will give explicit formulas for t and t'. To do this we first state a useful lemma.

LEMMA 4.3 ([13, Lemma 11.1]). *Let p be an odd prime and d be an integer such that $\gcd(p, d) = 1$. Let δ be the least positive integer such that $d^\delta \equiv 1 \pmod{p}$. If δ is odd, then there exists no integer x such that the*

congruence $d^x \equiv -1 \pmod p$ *is satisfied. But if* δ *is even, the congruence is satisfied if and only if* x *is an odd multiple of* $\delta/2$.

THEOREM 4.4. *Let* E *be an elliptic curve defined over* $\mathbb{Q}$ *and let* $P \in E(\mathbb{Q})$ *be a point of infinite order. Let* p *be an odd prime such that* P *modulo* p *is nonsingular, and suppose* $r > 3$ *is the order of* P *modulo* p. *Let* $(F_n(P))_{n\geq 0}$ *be the sequence of values of the normalized* n*-division polynomials of* E *at* P *and let* $(G_n(P))_{n\geq 0}$ *be the sequence generated by the numerators of the* x*-coordinates of the multiples of* P *as in* (1.2). *Suppose*

$$e \equiv \frac{F_2(P)^2}{F_{r+2}(P)^2}, \quad k \equiv F_{r+1}(P)^2 \pmod p, \tag{4.12}$$

and let ε *and* κ *be the least positive integers such that* $e^\varepsilon \equiv 1$, $k^\kappa \equiv 1 \pmod p$. *Then the sequence* $(G_n(P) \bmod p)_{n\geq 0}$ *is purely periodic with period* rt *where* $t = 2^\mu \operatorname{lcm}[\varepsilon, \kappa]$ *and*

$$\mu = \begin{cases} -1 & \text{if } \varepsilon \text{ and } \kappa \text{ are both even and both divisible} \\ & \text{by } 2^x \text{ with exactly the same power } x \geq 2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. One can observe that the equations in (4.7) imply that

$$k \equiv a^2 b^2, \quad e \equiv 1/a^4 b^2 \pmod p \tag{4.13}$$

and hence

$$k^t \equiv b^{2t}, \quad e^t \equiv 1/b^{2t} \pmod p, \tag{4.14}$$

since t is the smallest integer such that $a^{2t} \equiv 1 \pmod p$, by (4.9). On the other hand, since $a^{2t} \equiv 1 \pmod p$ we have $a^{2rt} \equiv 1 \pmod p$. Therefore

$$a^{2rt} \equiv b^{4t} \equiv 1 \pmod p,$$

as $a^r \equiv b^2 \pmod p$ by (3.3). It follows that $b^{2t} \equiv 1 \pmod p$ or $b^{2t} \equiv -1 \pmod p$.

Assume now that $b^{2t} \equiv 1 \pmod p$. Then by (4.14) we obtain

$$k^t \equiv e^t \equiv 1 \pmod p. \tag{4.15}$$

Now let ε and κ be the least positive integers such that $e^\varepsilon \equiv 1$, $k^\kappa \equiv 1 \pmod p$, and let $s = \operatorname{lcm}[\varepsilon, \kappa]$. Then (4.15) implies that $\varepsilon \mid t$ and $\kappa \mid t$, and hence $s \mid t$. Furthermore, $k^s \equiv 1$ and $e^s \equiv 1 \pmod p$. Then by (4.13) we obtain $a^{2s} \equiv 1 \pmod p$, and so $b^{2s} \equiv 1 \pmod p$. The last congruence implies that $b^{2s^2} \equiv 1 \pmod p$. Hence $t \mid s$, since t is the smallest integer such that $a^{2t} \equiv 1$, $b^{2t^2} \equiv 1 \pmod p$, by (4.9). Thus $s = t$.

Suppose that $b^{2t} \equiv -1 \pmod p$. Then by (4.9), $b^{2t^2} \equiv (b^{2t})^t \equiv (-1)^t \equiv 1 \pmod p$. Hence t must be even. On the other hand, (4.14) implies that $k^t \equiv e^t \equiv -1 \pmod p$. By Lemma 4.3, ε and κ are both even and t is an

odd multiple of both $\varepsilon/2$ and $\kappa/2$. Let $s = \frac{1}{2}\operatorname{lcm}[\varepsilon, \kappa]$. Then

$$s \mid t. \tag{4.16}$$

By Lemma 4.3, s is an odd multiple of both $\varepsilon/2$ and $\kappa/2$, that is, $s = (\varepsilon/2)m$ and $s = (\kappa/2)n$ for odd integers m, n. Let x be an integer such that $\operatorname{ord}_2(s) = x$ with $x \geq 2$. It follows that $\operatorname{ord}_2(\varepsilon/2) = x$ and $\operatorname{ord}_2(\kappa/2) = x$, since m and n are odd. Thus if $b^{2t} \equiv -1 \pmod{p}$, then ε and κ are both even and both divisible by 2^x with exactly the same power $x \geq 2$. Conversely, if ε and κ are both even and both divisible by 2^x with exactly the same power $x \geq 2$, then we have $\varepsilon = 2^y u$ and $\kappa = 2^y v$ where $y > 1$ and u, v are odd integers. Thus

$$s = \tfrac{1}{2}\operatorname{lcm}[\varepsilon, \kappa] = 2^{y-1}\operatorname{lcm}[u, v].$$

As $\operatorname{lcm}[u, v] = uw$ and $\operatorname{lcm}[u, v] = vz$ for certain odd integers w and z, we can write $s = 2^{y-1}uw = (\varepsilon/2)w$ and $s = 2^{y-1}vz = (\kappa/2)z$. Therefore s is an odd multiple of both $\varepsilon/2$ and $\kappa/2$, and s is even, since ε and κ are both even and both divisible by 2^x with exactly the same power $x \geq 2$. Thus

$$k^s \equiv e^s \equiv 1 \pmod{p}.$$

Then $a^{2s} \equiv 1 \pmod{p}$ by (4.13), and so $b^{2s} \equiv 1 \pmod{p}$. Hence $b^{2s^2} \equiv (b^{2s})^s \equiv 1 \pmod{p}$. But by (4.9), t is the smallest integer such that $a^{2t} \equiv 1$, $b^{2t^2} \equiv 1 \pmod{p}$, hence $t \mid s$. Thus $s = t$ by (4.16), which completes the proof. ∎

THEOREM 4.5. *Let E be an elliptic curve defined over $\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be a point of infinite order. Let p be an odd prime such that P modulo p is nonsingular, and suppose $r > 3$ is the order of P modulo p. Let $(F_n(P))_{n\geq 0}$ be the sequence of values of the normalized n-division polynomials of E at P and let $(H_n(P))_{n\geq 0}$ be the sequence generated by the numerators of the y-coordinates of the multiples of P as in* (1.2). *Let*

$$e' \equiv \frac{F_2(P)^3}{F_{r+2}(P)^3}, \quad k' \equiv F_{r+1}(P)^3 \pmod{p}, \tag{4.17}$$

and let ε' and κ' be the least positive integers such that $e^{\varepsilon'} \equiv 1$, $k^{\kappa'} \equiv 1 \pmod{p}$. Then the sequence $(H_n(P) \pmod{p})_{n\geq 0}$ is purely periodic with period rt' where $t' = 2^\mu \operatorname{lcm}[\varepsilon', \kappa']$ and

$$\mu = \begin{cases} -1 & \text{if } \varepsilon' \text{ and } \kappa' \text{ are both even and both divisible} \\ & \text{by } 2^x \text{ with exactly the same power } x \geq 2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. One can observe that the equations in (4.8) imply that

$$k' \equiv a^3 b^3, \quad e' \equiv 1/a^6 b^3 \pmod{p} \tag{4.18}$$

and so

$$b^{3t'} \equiv k'^{t'}, \quad 1/b^{3t'} \equiv e'^{t'} \pmod{p} \tag{4.19}$$

since t' is the smallest integer such that $a^{3t'} \equiv 1 \pmod{p}$ by (4.11). Since $a^r \equiv b^2 \pmod{p}$ by (3.3), we infer that $a^{3r} \equiv b^6 \pmod{p}$ and so

$$a^{3rt'} \equiv b^{6t'} \equiv 1 \pmod{p},$$

as $a^{3t'} \equiv 1 \pmod{p}$ by (4.11). Therefore $b^{3t'} \equiv 1 \pmod{p}$ or $b^{3t'} \equiv -1 \pmod{p}$. The rest of the proof is similar to the proof of Theorem 4.4. ∎

REMARK 4.6. Notice that the congruences (4.12) and (4.17) are obtained by taking the squares and cubes of both sides of (3.4), respectively. It follows that the periods π_G and π_H of $(G_n(P) \pmod{p})_{n\geq 0}$ and $(H_n(P) \pmod{p})_{n\geq 0}$ cannot be greater than the period π_F of $(F_n(P) \pmod{p})_{n\geq 0}$, since the order of the square (or cube) of an element equals either the order of the element or half (or one third) of that order. More precisely,

$$\pi_G = \pi_F \quad \text{or} \quad \pi_G = \pi_F/2$$

and

$$\pi_H = \pi_F \quad \text{or} \quad \pi_H = \pi_F/3.$$

If in addition the period π_F of $(F_n(P) \pmod{p})_{n\geq 0}$ is equal to the order of P modulo p, then $\pi_F = \pi_G = \pi_H$.

5. Periodicity modulo p^l. In [14], Ward studied elliptic divisibility sequences modulo p^l for primes $p > 3$ with ranks of apparition greater than three and with positive integers l. Ward proved that if $r > 3$ is a rank of apparition of a prime in an elliptic divisibility sequence (h_n) and p^k is the highest power of p dividing h_r, or equivalently $\mathtt{ord}_p(h_r) = k$, then the rank of apparition of p^l in (h_n) is r or $p^{l-k}r$ according as $l \leq k$ or $l > k$ by using elliptic function theory. Shipsey [6] studied periodicity properties of an elliptic divisibility sequence (h_n) modulo p^2 for some prime $p > 3$ and gave a symmetry formula for h_{mr} modulo p^2 for $m \geq 1$, where r is the rank of apparition of p in (h_n) [6, Theorem 3.5.4]. Then Shipsey obtained the periodicity of $(h_{mr})_{m\geq 1}$ modulo p^2 by using the symmetry formula. Ayad [1] and Swart [12] generalized Shipsey's symmetry properties to the case of modulo prime powers. Ayad [1] used explicit addition formulas to prove that the sequence $(F_n(P))_{n\geq 0}$ of values of the division polynomials modulo p^l is purely periodic with period $\pi_l = \min\{1, p^{l-v}\}\pi_1$, where π_1 is the period of $(F_n(P))_{n\geq 0}$ modulo p, $v = \mathtt{ord}_p(F_r(P))$ and r is the rank of apparition of p in $(F_n(P))_{n\geq 0}$, or equivalently the order of P modulo p. Moreover, Ayad proved the following result.

THEOREM 5.1 ([1, Théorème C]). *Let E be an elliptic curve defined over $\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be a point of infinite order. Suppose p is an odd prime*

such that P modulo p is nonsingular. Let $(F_n(P))_{n\geq 0}$ be the sequence of values of the normalized n-division polynomials of E at P as in (1.2). *Let $r \geq 3$ be the order of P modulo p and write $v = \mathtt{ord}_p(F_r(P))$. Then there exist integers A_l and B_l, relatively prime to p, such that for all nonnegative integers k, n and all $l \geq v$,*

$$F_{kp^{l-v}r+n}(P) \equiv A_l^{kn} B_l^{k^2} F_n(P) \pmod{p^l}. \tag{5.1}$$

Furthermore the integers A_l and B_l satisfy

$$A_l \equiv \frac{F_{r_l+2}(P)}{F_2(P)F_{r_l+1}(P)}, \quad B_l \equiv \frac{F_{r_l+1}(P)^2 F_2(P)}{F_{r_l+2}(P)}, \quad A^{r_l} \equiv B_l^2 \pmod{p^l} \tag{5.2}$$

where $l \geq v$ and $r_l = p^{l-v}r$.

The next theorem shows that similarly to Theorem 5.1, symmetry properties hold for $(G_n(P))_{n\geq 0}$ and $(H_n(P))_{n\geq 0}$.

THEOREM 5.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be a point of infinite order. Suppose p is an odd prime such that P modulo p is nonsingular. Let $(F_n(P))_{n\geq 0}$ be the sequence of values of the normalized n-division polynomials of E at P, and 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* (1.2). *Let $r \geq 3$ be the order of P modulo p and write $v = \mathtt{ord}_p(F_r(P))$. Then there exist integers A_l and B_l, relatively prime to p, such that for all nonnegative integers k, n and all $l \geq v$,*

$$G_{kp^{l-v}r+n}(P) \equiv A_l^{2kn} B_l^{2k^2} G_n(P) \pmod{p^l}, \tag{5.3}$$

$$H_{kp^{l-v}r+n}(P) \equiv A_l^{3kn} B_l^{3k^2} H_n(P) \pmod{p^l}. \tag{5.4}$$

Furthermore, for nonzero $G_i(P)$ and $H_i(P)$ values the integers A_l and B_l satisfy

$$A_l^2 \equiv \frac{G_2(P)G_{r_l+3}(P)}{G_3(P)G_{r_l+2}(P)}, \quad B_l^2 \equiv \frac{G_3(P)^2 G_{r_l+2}(P)^3}{G_2(P)^3 G_{r_l+3}(P)^2} \pmod{p^l}, \tag{5.5}$$

$$A_l^3 \equiv \frac{H_{r_l+1}(P)}{H_1(P)H_{r_l+1}(P)}, \quad B_l^3 \equiv H_{r_l} \pmod{p^l}, \tag{5.6}$$

where $l \geq v$ and $r_l = p^{l-v}r$.

Proof. Replacing n by $kp^{l-v}r + n$ in (1.3) and then using the expressions in (5.1) we derive the formulas in (5.3) and (5.4), respectively. Putting $n = 2$ and then $n = 3$ in (5.3) we obtain the relations in (5.5) for nonzero $G_i(P)$. Similarly, putting $n = 0$ and then $n = 1$ in (5.4) we have the congruences in (5.6) for nonzero $H_i(P)$ since $H_0(P) = 1$. ∎

Now we can give the proof of Theorem 1.2.

Proof of Theorem 1.2. One can show that the sequences $(G_n(P))_{n\ge0}$ and $(H_n(P))_{n\ge0}$ of values of the division polynomials modulo p^l are purely periodic with periods $r_l t_l$ and $r_l t'_l$, respectively, and t_l and t'_l divide $p^{l-1}(p-1)$, by using the congruences (5.2)–(5.4) similarly to the proof of Theorem 1.1. ∎

Theorem 1.2 says that the sequences $(G_n(P) \bmod p^l)_{n\ge0}$ and $(H_n(P) \bmod p^l)_{n\ge0}$ are purely periodic with periods $r_l t_l$ and $r_l t'_l$. In the following theorems we give explicit formulas for t_l and t'_l. The proofs can easily be obtained similarly to the proofs of Theorems 4.4 and 4.5.

THEOREM 5.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be a point of infinite order. Suppose p is an odd prime such that P modulo p is nonsingular. Let $(F_n(P))_{n\ge0}$ be the sequence of values of the normalized n-division polynomials of E at P and let $(G_n(P))_{n\ge0}$ be the sequence generated by the numerators of the x-coordinates of the multiples of P as in* (1.2). *Let $r > 3$ be the order of P modulo p and write $v = \mathtt{ord}_p(F_r(P))$ and $r_l = p^{l-v}r$ for $l \ge v$. Let E_l and K_l be integral solutions of the congruences*

$$E_l \equiv \frac{F_2(P)^2}{F_{r_l+2}(P)^2}, \qquad K_l \equiv F_{r_l+1}(P)^2 \pmod{p^l}, \tag{5.7}$$

and let ε_l and κ_l be the orders of E_l and K_l in $\mathbb{Z}^*_{p^l}$, respectively. Then the sequence $(G_n(P) \bmod p^l)_{n\ge0}$ is purely periodic with period $\pi_l = r_l t_l$ where $t_l = 2^\mu \operatorname{lcm}[\varepsilon_l, \kappa_l]$ and

$$\mu = \begin{cases} -1 & \text{if } \varepsilon_l \text{ and } \kappa_l \text{ are both even and both divisible} \\ & \text{by } 2^x \text{ with exactly the same power } x \ge 2, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, $t_l \mid p^{l-1}(p-1)$.

THEOREM 5.4. *Let E be an elliptic curve defined over $\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be a point of infinite order. Suppose p is an odd prime such that P modulo p is nonsingular. Let $(F_n(P))_{n\ge0}$ be the sequence of values of the normalized n-division polynomials of E at P and let $(H_n(P))_{n\ge0}$ be the sequences generated by the numerators of the y-coordinates of the multiples of P as in* (1.2). *Let $r > 3$ be the order of P modulo p and write $v = \mathtt{ord}_p(F_r(P))$ and $r_l = p^{l-v}r$ for $l \ge v$. Let E'_l and K'_l be integral solutions of the congruences*

$$E'_l \equiv \frac{F_2(P)^3}{F_{r_l+2}(P)^3}, \qquad K'_l \equiv F_{r_l+1}(P)^3 \pmod{p^l}$$

and let ε'_l and κ'_l be the orders of E'_l and K'_l modulo p^l, respectively. Then the sequence $(H_n(P) \bmod p^l)_{n\ge0}$ is purely periodic with period $\pi'_l = r_l t'_l$ where

$t_l' = 2^\mu \operatorname{lcm}[\varepsilon_l', \kappa_l']$ *and*

$$\mu = \begin{cases} -1 & \text{if } \varepsilon_l' \text{ and } \kappa_l' \text{ are both even and both divisible} \\ & \text{by } 2^x \text{ with exactly the same power } x \geq 2, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, $t_l \mid p^{l-1}(p-1)$.

6. p-adic convergence. Silverman [9] used the Mazur–Tate p-adic σ-function to prove the existence and algebraicity of the p-adic limit of certain subsequences of the sequence $(F_n(P))_{n\geq 1}$ of values of the division polynomials of an elliptic curve E evaluated at a point P on E. More precisely, in [9, Theorem 2] he showed that if E is an elliptic curve defined over $\mathbb{Q}_p$ with good ordinary reduction and $P \in E(\mathbb{Q}_p)$, then there is a power $q = p^N$ such that $(F_{mq^i}(P))_{i\geq 1}$ converges in $\mathbb{Z}_p$ as $i \to \infty$ for all $m \geq 1$. In addition, if E is defined over $\mathbb{Q}$ and $P \in E(\mathbb{Q})$, then the limit of this convergent sequence is an algebraic number. Furthermore, in an addendum to [9], Silverman used Ayad's formula (5.1) to show that $(F_{mq^i}(P))$ is $\mathbb{Z}_p$-Cauchy without the ordinary reduction hypothesis.

We use similar techniques to [9] to prove Theorem 1.3.

Proof of Theorem 1.3. By Theorem 5.2 we know that there exist integers A_l, B_l, relatively prime to p, such that for all nonnegative integers k, n and all $l \geq v$,

$$G_{kp^{l-v}r+n}(P) \equiv A_l^{2kn} B_l^{2k^2} G_n(P) \pmod{p^l}$$

where $v = \mathtt{ord}_p(F_r(P))$ is an integer specified in Theorem 5.1. Let $q = p^N$ be a power such that $q \equiv 1 \pmod{(p-1)r}$. Now as $q^{i-j} \equiv 1 \pmod{(p-1)r}$, we have

$$G_{mq^i}(P) = G_{mq^j(1+(p-1)rt)}(P)$$

for all $i > j \geq 2l/N$, all $l > v$, and some $t \in \mathbb{Z}$. Thus we can write

$$G_{mq^i}(P) = G_{mt(p-1)p^{Nj-l+v}p^{l-v}r+mq^j}(P) = G_{sp^{l-v}r+mq^j}(P)$$

where $s = mt(p-1)p^{Nj-l+v}$. Then by (5.3) we have

$$G_{mq^i}(P) \equiv A_l^{2smq^j} B_l^{2s^2} G_{mq^j}(P) \pmod{p^l}$$

and so

$$G_{mq^i}(P) \equiv G_{mq^j}(P) \pmod{p^l}$$

since $s \in \mathbb{Z}_{p^l}^*$ and p is an odd prime. Therefore

$$\|G_{mq^i}(P) - G_{mq^j}(P)\|_p \leq q^{-j/2+1} \quad \text{for all } i > j > 2(v/N+1)$$

where $j = \lceil 2l/N \rceil$ and hence the sequence $(G_{mq^i}(P))$ is $\mathbb{Z}_p$-Cauchy. It follows that it converges in $\mathbb{Z}_p$. Similarly we can use the formula (5.4) to show that $(H_{mq^i}(P))$ converges in $\mathbb{Z}_p$. If in addition E is defined over $\mathbb{Q}$, ordinary at p and $P \in E(\mathbb{Q})$, then [9, Theorem 2] implies that the limit of $(F_{mq^i}(P))$ is an algebraic number. Then by (1.3) the limit

$$\lim_{i\to\infty} G_{mq^i}(P) = \lim_{i\to\infty} x\gamma^{-2}F^2_{mq^i}(P) - \lim_{i\to\infty} F_{mq^i+1}(P)F_{mq^i-1}(P)$$

is an algebraic number since the limit of $(F_{mq^i}(P))$ is an algebraic number and the sum and product of algebraic numbers are algebraic. Similarly one can show that the limit of $(H_{mq^i}(P))_{n\geq 0}$ is an algebraic number by (1.3). ∎

Acknowledgments. The authors would like to thank the anonymous referee for valuable comments and suggestions that improved the quality of the paper.

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), 585–618.

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

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

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

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

[6] R. Shipsey, *Elliptic divisibility sequences*, PhD thesis, Goldsmith's College (Univ. of London), 2000.

[7] I. E. Shparlinski and K. E. Stange, *Character sums with division polynomials*, Canad. Math. Bull. 55 (2012), 850–857.

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves,* 2nd ed., Grad. Texts in Math. 106, Springer, Dordrecht, 2009.

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

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

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

[12] C. S. Swart, *Elliptic curves and related sequences*, PhD thesis, Royal Holloway (Univ. of London), 2003.

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

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

Betül Gezer, Osman Bizim
Department of Mathematics
Faculty of Science
Bursa Uludağ University
Görükle, 16059, Bursa, Turkey
E-mail: betulgezer@uludag.edu.tr
obizim@uludag.edu.tr