New York Journal of Mathematics

New York J. Math. **31** (2025) 568–588.

Periods modulo p of integer sequences associated with division polynomials of genus 2 curves

Yasuhiro Ishitsuka, Tetsushi Ito, Tatsuya Ohshita, Takashi Taniguchi and Yukihiro Uchida

Abstract. We study an integer sequence associated with Cantor's division polynomials of a genus 2 curve having an integral point. We show that the reduction modulo p of such a sequence is periodic for all but finitely many primes p, and describe the relation between the period of the reduction modulo p of the sequence and the order of the integral point on the reduction modulo p in the Jacobian variety explicitly. This generalizes Ward's results on elliptic divisibility sequences associated with division polynomials of elliptic curves.

Contents

1. Introduction

An integer sequence $\{a_n\}_{n\in\mathbb{Z}}$ is called a *divisibility sequence* if $a_m \mid a_n$ whenever $m \mid n$. An *elliptic divisibility sequence* is a divisibility sequence $\boldsymbol{W} := \{W_n\}_{n\in\mathbb{Z}}$ satisfying

$$W_{n+m}W_{n-m} = W_{n+1}W_{n-1}W_m^2 - W_{m+1}W_{m-1}W_n^2$$

for all integers $m, n \in \mathbb{Z}$. Elliptic divisibility sequences were introduced by Ward [17]. Ward proved that for an arbitrary "non-degenerate" elliptic divisibility sequence $\boldsymbol{W}$, there exist an elliptic curve E defined over $\mathbb{Q}$ and $P =$

Received March 15, 2024.

2020 *Mathematics Subject Classification.* Primary 11G30; Secondary 11B50, 14H25.

Key words and phrases. Curves of genus 2, Jacobian, division polynomials.

ISSN 1076-9803/2025

$(x_P, y_P) \in E(\mathbb{Q})$ such that $\psi_n(x_P, y_P) = W_n$, where $\psi_n(X, Y) \in \mathbb{Q}[X, Y]$ is the n-th division polynomial of E. Using them, he also proved that the reduction modulo p of the sequence $\boldsymbol{W}$ is periodic for all but finitely many primes p. More precisely, he proved the following: let $\mathrm{Per}_p(\boldsymbol{W})$ be the period of the reduction modulo p of the sequence $\boldsymbol{W}$. Let $\mathrm{ord}_p(P)$ be the order of the point $\overline{P} \in E(\mathbb{F}_p)$, where $\overline{P}$ is the reduction of P modulo p. Then $\mathrm{ord}_p(P)$ divides $\mathrm{Per}_p(\boldsymbol{W})$, and $\mathrm{Per}_p(\boldsymbol{W})$ divides $(p-1)\,\mathrm{ord}_p(P)$, i.e.

$$\mathrm{ord}_p(P) \mid \mathrm{Per}_p(\boldsymbol{W}) \mid (p-1)\,\mathrm{ord}_p(P)$$

(see [17, Theorem 10.1]).

The aim of this paper is to generalize these results to genus 2 curves with integral points. In order to state our results, let us introduce some notation. Let C be a hyperelliptic curve of genus 2 over $\mathbb{Q}$ defined by

$$Y^2 = F(X) := X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0,$$

where $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}$. Let $\mathrm{disc}(F) \in \mathbb{Z}$ be the discriminant of $F(X)$, and $\mathrm{Jac}(C)$ be the Jacobian variety of C. For an integer $n \geq 0$, let $\psi_n(X) \in \mathbb{Z}[X]$ be the division polynomial of C defined by Cantor [4]. Let $P = (x_P, y_P)$ $(x_P, y_P \in \mathbb{Z})$ be an integral point on $C \backslash \{\infty\}$. We put

$$D_P := [P] - [\infty] \in \mathrm{Jac}(C)(\mathbb{Q}) \qquad \text{and} \qquad c_n := \psi_n(x_P) \in \mathbb{Z}.$$

The main results of this paper are as follows.

Theorem 1.1. *Let $\boldsymbol{c} := \{c_n\}_{n\in\mathbb{Z}} := \{\psi_n(x_P)\}_{n\in\mathbb{Z}}$ be the integer sequence associated with the division polynomials of a hyperelliptic curve C and its integral point P on $C\backslash\{\infty\}$ defined as above. Assume that $c_3c_4c_5c_6c_7(c_4^3 - c_3^3c_5) \neq 0$. Let p be an odd prime which divides neither $\mathrm{disc}(F)$ nor $c_3c_4c_5c_6c_7(c_4^3 - c_3^3c_5)$. Then the following assertions hold.*

1. *The reduction modulo p of the sequence $\boldsymbol{c}$ is periodic.*
2. *Let $\mathrm{Per}_p(\boldsymbol{c})$ be the period of the reduction modulo p of the sequence $\boldsymbol{c}$. Let $\overline{D_P} \in \mathrm{Jac}(C)(\mathbb{F}_p)$ be the reduction modulo p of D_P, and $\mathrm{ord}_p(D_P)$ be the order of the point $\overline{D_P} \in \mathrm{Jac}(C)(\mathbb{F}_p)$. Then $\mathrm{ord}_p(D_P)$ divides $\mathrm{Per}_p(\boldsymbol{c})$, and $\mathrm{Per}_p(\boldsymbol{c})$ divides $(p-1)\,\mathrm{ord}_p(D_P)$, i.e.*

$$\mathrm{ord}_p(D_P) \mid \mathrm{Per}_p(\boldsymbol{c}) \mid (p-1)\,\mathrm{ord}_p(D_P).$$

Since $|\mathrm{Jac}(C)(\mathbb{F}_p)| \leq (1+\sqrt{p})^4$ by the Hasse–Weil bound (see [10, Theorem 19.1, (b) and (c)]), we obtain the following upper bound of $\mathrm{Per}_p(\boldsymbol{c})$.

Corollary 1.2. *The period $\mathrm{Per}_p(\boldsymbol{c})$ of the reduction modulo p of the sequence $\boldsymbol{c}$ is bounded above by $(p-1)(1+\sqrt{p})^4$.*

Theorem 1.1 (2) means that the ratio $\mathrm{Per}_p(\boldsymbol{c})/\,\mathrm{ord}_p(D_P)$ is an integer and a divisor of $p-1$. The method in this paper in fact allows us to give an explicit description of this ratio, which is an analogue of Ward's result for elliptic divisibility sequences [17, Theorem 10.1]. As a precise version of Theorem 1.1 (2), we prove the following.

Theorem 1.3. *Under the assumptions in Theorem* 1.1*, let* $r := \operatorname{ord}_p(D_P)$ *be the order of* $\overline{D_P} \in \operatorname{Jac}(C)(\mathbb{F}_p)$*, and* $\alpha_p, \beta_p \in \mathbb{F}_p$ *be elements satisfying* $\alpha_p \equiv c_{r+3}/(c_3 c_{r+2}) \pmod p$ *and* $\beta_p \equiv (c_3^2 c_{r+2}^3)/c_{r+3}^2 \pmod p$*, where we know that* $c_{r+2}, c_{r+3} \not\equiv 0 \pmod p$ *(see Claim* 3.4*). Let* d *be the least positive integer such that* $\alpha_p^d \equiv \beta_p^{d^2} \equiv 1 \pmod p$*. Then we have*

$$\operatorname{Per}_p(\boldsymbol{c}) = d \operatorname{ord}_p(D_P).$$

For a given sequence $\boldsymbol{c}$, the behavior of $d = \operatorname{ord}_p(D_P)/\operatorname{Per}_p(\boldsymbol{c})$ as a divisor of $p-1$, in varying p, does not seem to have an obvious pattern. It might thus be interesting to seek the behavior from, e.g., a statistical point of view (see Remark B.3).

Remark 1.4. The order $r = \operatorname{ord}_p(D_P)$ can be calculated as the least positive integer r such that $c_{r-1} \equiv c_r \equiv c_{r+1} \equiv 0 \pmod p$ (see Theorem 2.1 (2)).

Remark 1.5. The condition $c_3 c_4 c_5 c_6 c_7 (c_4^3 - c_3^3 c_5) \neq 0$ in Theorem 1.1 seems technical. We need to assume it in order to prove properties of the reduction modulo p of the sequence $\boldsymbol{c}$ by induction (see the proof of Theorem 3.1). In fact, under a weaker assumption, we can prove the periodicity of the reduction modulo p of the sequence $\boldsymbol{c}$ by the pigeonhole principle. We demonstrate it in Proposition 4.1. Meanwhile, the upper bound of $\operatorname{Per}_p(\boldsymbol{c})$ obtained by the pigeonhole principle is p^{11}, which is (much) larger than the upper bound obtained in Corollary 1.2.

Although Theorem 1.1 and Theorem 1.3 are analogous to Ward's results for elliptic divisibility sequences, the proofs are quite different. Ward's proof does not seem applicable to our case. Our proofs of Theorem 1.1 and Theorem 1.3 are similar to the proofs for elliptic divisibility sequences given by Shipsey and Swart [13]. They used recurrence relations to prove Ward's results. For genus 2 curves, Cantor proved that $\boldsymbol{c}$ satisfies a bilinear recurrence relation of Somos 8 type [4, p.143], where a recurrence relation is said to be of Somos k type if it is of the form

$$c_n c_{n+k} = \sum_{i=1}^{\lfloor k/2 \rfloor} \alpha_i c_{n+i} c_{n+k-i}.$$

However, the recurrence relation of Somos 8 type alone does not seem to imply Theorem 1.1 and Theorem 1.3.

In this paper, we shall first show that $\boldsymbol{c}$ satisfies the following recurrence relations for all integers m and n (see Theorem 2.5):

$$\begin{aligned} c_4 c_{n+m} c_{n-m} &= c_{m+1} c_{m-1} c_{n+3} c_{n-3} \\ &\quad + (c_4 c_m^2 - c_3^2 c_{m+1} c_{m-1}) c_{n+2} c_{n-2} \\ &\quad + (c_3^2 c_{m+2} c_{m-2} - c_{m+3} c_{m-3}) c_{n+1} c_{n-1} \\ &\quad - c_4 c_{m+2} c_{m-2} c_n^2, \\ c_3 c_5 c_{n+m+1} c_{n-m} &= c_3 c_{m+2} c_{m-1} c_{n+4} c_{n-3} \\ &\quad + (c_5 c_{m+1} c_m - c_3 c_4 c_{m+2} c_{m-1}) c_{n+3} c_{n-2} \\ &\quad + (c_3 c_4 c_{m+3} c_{m-2} - c_3 c_{m+4} c_{m-3}) c_{n+2} c_{n-1} \\ &\quad - c_5 c_{m+3} c_{m-2} c_{n+1} c_n. \end{aligned}$$

In fact, these recurrence relations are satisfied by Cantor's division polynomials $\{\psi_n(X)\}_{n\in\mathbb{Z}}$, which may be of independent interest. Specializing to $m = 4$ and 5, we obtain bilinear recurrence relations of Somos 8, 9, 10 and 11 type satisfied by $\boldsymbol{c}$ (see Corollary 2.6), which includes Cantor's recurrence relation mentioned above. Using these as key ingredients, we prove Theorem 1.1 and Theorem 1.3 by inductive arguments.

Note that some other sequences satisfying relations of Somos type have appeared in the literature. As examples of recent results, Hone [8] proved that certain Hankel determinants corresponding to a genus 2 curve satisfy a relation of Somos 8 type. Doliwa [6] proved some bilinear relations for multipole orthogonal polynomials via their determinantal expressions.

Independently of our work, Ustinov [16, Theorem 1] recently proved that the reduction modulo an arbitrary integer of a sequence satisfying a relation of Somos type are eventually periodic if the sequence has finite rank. Here, a sequence $\{s_n\}_{n\in\mathbb{Z}}$ has *finite rank* if the matrices

$$M_s^{(0)} = (s_{m+n} s_{m-n})_{m,n\in\mathbb{Z}}, \quad M_s^{(1)} = (s_{m+n+1} s_{m-n})_{m,n\in\mathbb{Z}}$$

have finite rank. This result is proved by several recurrence relations of Somos type and the pigeonhole principle similarly to Proposition 4.1. Ustinov's theorem can be applied to the case a modulus is not prime. On the other hand, the upper bound of the period, although it is not given explicitly in [16], is larger than our bound as discussed in Remark 1.5.

The outline of this paper is as follows. In Section 2, we recall Cantor's division polynomials of a genus 2 curve and their basic properties. Cantor's division polynomials are described by the hyperelliptic sigma function. A classical formula of theta functions proved by Caspary and Frobenius shows that the sequence $\boldsymbol{c}$ satisfies some recurrence relations. In Section 3, using the recurrence relation obtained in Section 2, we prove the periodicity of the reduction modulo p of the sequence $\boldsymbol{c}$. In Section 4, we prove Theorem 1.1 and Theorem 1.3. In Appendix A, we prove a formula relating Cantor's division polynomials and hyperelliptic sigma functions. In Appendix B, we give a numerical example. For the integer sequence introduced by Cantor (OEIS A058231), we give numerical results on the period of the reduction modulo p of the sequence $\boldsymbol{c}$ and the order of a point on the reduction modulo p of the Jacobian variety.

2. Cantor's division polynomials

In this section, we prove some properties of Cantor's division polynomials used in the proof of Theorem 1.1.

Let K be a field of characteristic different from 2. Let C be a hyperelliptic curve of genus 2 defined by

$$Y^2 = F(X) := X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0,$$

where $a_0, a_1, a_2, a_3, a_4 \in K$. Let $\mathrm{Jac}(C)$ be the Jacobian variety of C. Let $\infty \in C$ be the point at infinity of C. We embed C into $\mathrm{Jac}(C)$ by $P \mapsto D_P := [P] - [\infty]$. The image of C is written as Θ, which is called the *theta divisor* on $\mathrm{Jac}(C)$.

For an integer $n \geq 0$, let $\psi_n(X) \in K[X]$ be the division polynomials of C defined by Cantor; see [4] for details. We extend the division polynomials for $n < 0$ by $\psi_n(X) := -\psi_{-n}(X)$. For $-1 \leq n \leq 3$, they are given by

$$\psi_{-1}(X) = \psi_0(X) = \psi_1(X) = 0, \quad \psi_2(X) = 1, \quad \psi_3(X) = 4F(X).$$

Theorem 2.1. *Let $P = (x_P, y_P) \in C(K)$ be a K-rational point with $y_P \neq 0$, and $n \geq 3$. The following assertions hold.*

(1) *$nD_P \in \Theta$ if and only if $\psi_n(x_P) = 0$.*
(2) *$nD_P = 0$ if and only if $\psi_{n-1}(x_P) = \psi_n(x_P) = \psi_{n+1}(x_P) = 0$.*

Proof. See [4, pp. 140–141]. □

Lemma 2.2. *Let $P = (x_P, y_P) \in C(K)$ be a point with $y_P \neq 0$. For every integer $n \in \mathbb{Z}$, at least one of*

$$\psi_n(x_P),\ \psi_{n+1}(x_P),\ \psi_{n+2}(x_P),\ \psi_{n+3}(x_P)$$

is not zero.

Proof. Since $\psi_{-n}(X) = -\psi_n(X)$, $\psi_2(X) = 1 \neq 0$, and $\psi_{-2}(X) = -1 \neq 0$, we may assume $n \geq 3$. By [4, Lemma 3.29], at least one of $f_n, f_{n+1}, f_{n+2}, f_{n+3}$ is not zero, where f_r is a rational function on C defined in [4, Section 3, Section 8]. We have $\psi_r(X) = (2Y)^{(r^2-r-2)/2} f_r$; see [4, p.133, (8.7)]. Since $y_P \neq 0$, at least one of $\psi_n(x_P), \psi_{n+1}(x_P), \psi_{n+2}(x_P), \psi_{n+3}(x_P)$ is not zero. □

In the rest of this section, let K be a subfield of $\mathbb{C}$. Cantor's division polynomials $\psi_n(X)$ can be expressed by using the hyperelliptic sigma function. Let $\sigma : \mathbb{C}^2 \to \mathbb{C}$ be the hyperelliptic sigma function associated with C. (For recent developments on the theory of sigma functions, see [3] and references therein. We adopt the notation used in [11, 12].) We define

$$\sigma_2(u) := \frac{\partial \sigma(u)}{\partial u_2},$$

where $u = (u_1, u_2) \in \mathbb{C}^2$.

The following theorem essentially follows from the description of Cantor's division polynomials in [12, Appendix A] (see also [9, p. 518]), but there are sign errors in the literature. For the convenience of the readers, we correct a proof in Appendix A.

Theorem 2.3. *Let $P = (x_P, y_P) \in C(\mathbb{C})$ be a point and let $u \in \mathbb{C}^2$ be the point corresponding to P (for the definition of u, see Lemma* A.2*). Then we have*

$$2y_P\psi_n(x_P) = (-1)^n \frac{\sigma(nu)}{\sigma_2(u)^{n^2}}.$$

The following argument is almost the same as that in [15, Section 6].

Proposition 2.4. *Let $d \geq 6$ be an even integer and $u^{(1)}, u^{(2)}, \dots, u^{(d)} \in \mathbb{C}^2$. Then we have*

$$\operatorname{pf}\left(\sigma(u^{(i)} + u^{(j)})\sigma(u^{(i)} - u^{(j)})\right)_{1\leq i,j\leq d} = 0, \tag{2.1}$$

where pf A *is the Pfaffian of A.*

Proof. See [15, Corollary 6.2] or [1, p. 473, Ex. v]. The proposition follows from similar formulas for theta functions proved by Caspary [5] and Frobenius [7]. □

Let $P = (x_P, y_P) \in C(\mathbb{C})$ be a point and we put $c_n := \psi_n(x_P)$.

Theorem 2.5. *For all integers m and n, we have*

$$\begin{aligned} c_4c_{n+m}c_{n-m} = {} & c_{m+1}c_{m-1}c_{n+3}c_{n-3} \\ & + (c_4c_m^2 - c_3^2c_{m+1}c_{m-1})c_{n+2}c_{n-2} \\ & + (c_3^2c_{m+2}c_{m-2} - c_{m+3}c_{m-3})c_{n+1}c_{n-1} \\ & - c_4c_{m+2}c_{m-2}c_n^2, \end{aligned} \tag{2.2}$$

$$\begin{aligned} c_3c_5c_{n+m+1}c_{n-m} = {} & c_3c_{m+2}c_{m-1}c_{n+4}c_{n-3} \\ & + (c_5c_{m+1}c_m - c_3c_4c_{m+2}c_{m-1})c_{n+3}c_{n-2} \\ & + (c_3c_4c_{m+3}c_{m-2} - c_3c_{m+4}c_{m-3})c_{n+2}c_{n-1} \\ & - c_5c_{m+3}c_{m-2}c_{n+1}c_n. \end{aligned} \tag{2.3}$$

Proof. Setting $d = 6$, $u^{(1)} = nu$, $u^{(2)} = mu$, $u^{(3)} = 3u$, $u^{(4)} = 2u$, $u^{(5)} = u$ and $u^{(6)} = 0$ in (2.1), we obtain (2.2) by Theorem 2.3 and Proposition 2.4. Similarly, setting $u^{(1)} = (n + 1/2)u$, $u^{(2)} = (m + 1/2)u$, $u^{(3)} = 7u/2$, $u^{(4)} = 5u/2$, $u^{(5)} = 3u/2$ and $u^{(6)} = u/2$ in (2.1), we obtain (2.3) by Theorem 2.3 and Proposition 2.4. Note that we used $c_0 = c_1 = 0$ and $c_2 = 1$. □

By letting $m = 4$ and 5 in each of the above, we obtain bilinear recurrence relations of Somos 8, 9, 10 and 11 type satisfied by $\boldsymbol{c}$.

Corollary 2.6.

$$\begin{aligned} c_4 c_{n+4} c_{n-4} &= c_3 c_5 c_{n+3} c_{n-3} + (c_4^3 - c_3^3 c_5) c_{n+2} c_{n-2} \\ &\quad + c_3^2 c_6 c_{n+1} c_{n-1} - c_4 c_6 c_n^2, \end{aligned} \tag{2.4}$$

$$\begin{aligned} c_3 c_5 c_{n+5} c_{n-4} &= c_3^2 c_6 c_{n+4} c_{n-3} + c_4 (c_5^2 - c_3^2 c_6) c_{n+3} c_{n-2} \\ &\quad + c_3 c_4 c_7 c_{n+2} c_{n-1} - c_5 c_7 c_{n+1} c_n, \end{aligned} \tag{2.5}$$

$$\begin{aligned} c_4 c_{n+5} c_{n-5} &= c_4 c_6 c_{n+3} c_{n-3} + c_4 (c_5^2 - c_3^2 c_6) c_{n+2} c_{n-2} \\ &\quad + (c_3^3 c_7 - c_8) c_{n+1} c_{n-1} - c_3 c_4 c_7 c_n^2, \end{aligned} \tag{2.6}$$

$$\begin{aligned} c_3 c_5 c_{n+6} c_{n-5} &= c_3 c_4 c_7 c_{n+4} c_{n-3} + (c_5^2 c_6 - c_3 c_4^2 c_7) c_{n+3} c_{n-2} \\ &\quad + c_3 (c_3 c_4 c_8 - c_9) c_{n+2} c_{n-1} - c_3 c_5 c_8 c_{n+1} c_n. \end{aligned} \tag{2.7}$$

Note that the Somos 8 type relation (2.4) was proved by Cantor [4, p. 143].

3. Periodicity of the values of Cantor's division polynomials

In this section, we prove the periodicity of the reduction modulo p of the values of Cantor's division polynomials. As in Section 1, let C be a hyperelliptic curve of genus 2 over $\mathbb{Q}$ defined by

$$Y^2 = F(X) := X^5 + a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X + a_0,$$

where $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}$. For an integer $n \geq 0$, let $\psi_n(X) \in \mathbb{Z}[X]$ be the division polynomial of C defined by Cantor. Let $P = (x_P, y_P)$ $(x_P, y_P \in \mathbb{Z})$ be an integral point on $C \backslash \{\infty\}$. We put

$$D_P := [P] - [\infty] \in \mathrm{Jac}(C)(\mathbb{Q}) \quad \text{and} \quad c_n := \psi_n(x_P) \in \mathbb{Z}.$$

Theorem 3.1. *Let p be an odd prime which is not a divisor of the discriminant of $F(X)$. We also assume that p is not a divisor of $c_3 c_4 c_5 c_6 c_7 (c_4^3 - c_3^3 c_5)$. Let $\overline{D_P} \in \mathrm{Jac}(C)(\mathbb{F}_p)$ be the reduction modulo p of D_P, and $r := \mathrm{ord}_p(D_P)$ be the order of $\overline{D_P}$. Then we have the following:*

(1) *We have $c_{r+2}, c_{r+3} \not\equiv 0 \pmod{p}$.*
(2) *Let $\alpha_p, \beta_p \in \mathbb{F}_p$ be elements satisfying*

$$\alpha_p \equiv c_{r+3}/(c_3 c_{r+2}) \pmod{p}, \quad \beta_p \equiv (c_3^2 c_{r+2}^3)/c_{r+3}^2 \pmod{p}.$$

Then, we have the following relations for all integers n and k:

$$c_{kr+n} \equiv \alpha_p^{kn} \beta_p^{k^2} c_n \pmod{p}. \tag{3.1}$$

(3) *We have $\alpha_p^r = \beta_p^2$ in $\mathbb{F}_p$.*

Note that the conditions in Theorem 3.1 are satisfied for all but finitely many p.

The proof of Theorem 3.1 is divided into several steps. In principle, the strategy of our proof is similar to the proof for elliptic divisibility sequences by Shipsey and Swart [13, Theorem 2]. However, our proof is more involved than theirs. We need to analyze the reduction modulo p of the sequence using recurrence relations of Somos 8, 9, 10, 11 type together.

In order to simplify the notation, we omit "(mod p)" in the rest of this section. All the congruences are taken modulo p.

Claim 3.2. $y_P \not\equiv 0$.

Proof. Since $c_3 = \psi_3(x_P) = 4F(x_P)$ and $c_3 \not\equiv 0$, we have $F(x_P) \not\equiv 0$. This implies $y_P \not\equiv 0$. □

Claim 3.3. *The order* $r = \mathrm{ord}_p(D_P)$ *satisfies* $r \geq 9$.

Proof. Note that $\overline{D_P} \neq 0 \in \mathrm{Jac}(C)(\mathbb{F}_p)$ since $x_P, y_P \in \mathbb{Z}$. Since $y_P \not\equiv 0$, we have $r \geq 3$. By Theorem 2.1 (2) with $n = r$, we have $c_{r-1} \equiv c_r \equiv c_{r+1} \equiv 0$. Since $c_3c_4c_5c_6c_7 \not\equiv 0$ by our assumption, we have $r \geq 9$. □

Claim 3.4. $c_{r+2}, c_{r+3} \not\equiv 0$.

Proof. Since $c_{r-1} \equiv c_r \equiv c_{r+1} \equiv 0$, by Lemma 2.2, we have $c_{r+2} \not\equiv 0$. By our assumption, $c_3 \not\equiv 0$. By Theorem 2.1 (1) with $n = 3$, we have $3\overline{D_P} \notin \Theta$. Since $r\overline{D_P} = 0$, we have $(r+3)\overline{D_P} \notin \Theta$. Therefore, again by Theorem 2.1 (1) with $n = r + 3$, we have $c_{r+3} \not\equiv 0$. □

This finishes the proof of the first assertion, and it allows us to define $\alpha_p, \beta_p \in \mathbb{F}_p^\times$ as above. We continue the proof of Theorem 3.1. As the base case of the induction, we first prove (3.1) for $k = 1$ and $-3 \leq n \leq 7$:

Claim 3.5. *For integers n satisfying* $-3 \leq n \leq 7$, *we have*

$$c_{r+n} \equiv \alpha_p^n \beta_p c_n. \tag{3.2}$$

Proof. Since $c_{r-1} \equiv c_r \equiv c_{r+1} \equiv 0$, (3.2) holds for $n = -1, 0, 1$. Meanwhile, (3.2) holds for $n = 2, 3$ by the definitions of α_p and β_p.

Setting $n = r + 3$ in (2.4), we obtain

$$0 \equiv c_3^2 c_6 c_{r+4} c_{r+2} - c_4 c_6 c_{r+3}^2$$

since $c_{r-1} \equiv c_r \equiv c_{r+1} \equiv 0$. By the assumption of Theorem 3.1, we have $c_3c_6 \not\equiv 0$. Since (3.2) holds for $n = 2, 3$ and $c_2 = 1$, we obtain

$$c_{r+4} \equiv \frac{c_4 c_{r+3}^2}{c_3^2 c_{r+2}} \equiv \frac{c_4(\alpha_p^3 \beta_p c_3)^2}{c_3^2 \cdot \alpha_p^2 \beta_p c_2} \equiv \alpha_p^4 \beta_p c_4.$$

Hence, (3.2) holds for $n = 4$.

Setting $n = r + 3$ in (2.5), we obtain

$$0 \equiv c_3 c_4 c_7 c_{r+5} c_{r+2} - c_5 c_7 c_{r+4} c_{r+3}.$$

By assumption, we have $c_3c_4c_7 \not\equiv 0$. Since (3.2) holds for $n = 2, 3, 4$ and $c_2 = 1$, we obtain

$$c_{r+5} \equiv \frac{c_5 c_{r+4} c_{r+3}}{c_3 c_4 c_{r+2}} \equiv \frac{c_5 \cdot \alpha_p^4 \beta_p c_4 \cdot \alpha_p^3 \beta_p c_3}{c_3 c_4 \cdot \alpha_p^2 \beta_p c_2} \equiv \alpha_p^5 \beta_p c_5.$$

Hence, (3.2) holds for $n = 5$.

Setting $n = r + 4$ in (2.4), we obtain

$$0 \equiv (c_4^3 - c_3^3 c_5) c_{r+6} c_{r+2} + c_3^2 c_6 c_{r+5} c_{r+3} - c_4 c_6 c_{r+4}^2.$$

By the assumption of Theorem 3.1, we have $c_4^3 - c_3^3 c_5 \not\equiv 0$. Since (3.2) holds for $n = 2, 3, 4, 5$ and $c_2 = 1$, we obtain

$$c_{r+6} \equiv \frac{-c_3^2 c_6 c_{r+5} c_{r+3} + c_4 c_6 c_{r+4}^2}{(c_4^3 - c_3^3 c_5) c_{r+2}} \equiv \frac{-\alpha_p^8 \beta_p^2 c_3^3 c_5 c_6 + \alpha_p^8 \beta_p^2 c_4^3 c_6}{(c_4^3 - c_3^3 c_5) \alpha_p^2 \beta_p c_2} \equiv \alpha_p^6 \beta_p c_6.$$

Hence, (3.2) holds for $n = 6$.

Setting $n = r + 2$ in (2.4), we obtain

$$c_4 c_{r+6} c_{r-2} \equiv -c_4 c_6 c_{r+2}^2.$$

By the assumption of Theorem 3.1, we have $c_4 c_6 \not\equiv 0$. Since $c_{-2} = -c_2 = -1$ and (3.2) holds for $n = 2, 6$, we obtain

$$c_{r-2} \equiv -\frac{c_6 c_{r+2}^2}{c_{r+6}} \equiv -\frac{\alpha_p^4 \beta_p^2 c_2^2 c_6}{\alpha_p^6 \beta_p c_6} \equiv \alpha_p^{-2} \beta_p c_{-2}.$$

Hence, (3.2) holds for $n = -2$.

Setting $n = r + 2$ in (2.5), we obtain

$$c_3 c_5 c_{r+7} c_{r-2} \equiv -c_5 c_7 c_{r+3} c_{r+2}.$$

By the assumption of Theorem 3.1, we have $c_3 c_5 \not\equiv 0$. Since $c_{-2} = -c_2$ and (3.2) holds for $n = -2, 2, 3$,

$$c_{r+7} \equiv -\frac{c_7 c_{r+3} c_{r+2}}{c_3 c_{r-2}} \equiv -\frac{\alpha_p^5 \beta_p^2 c_2 c_3 c_7}{\alpha_p^{-2} \beta_p c_3 c_{-2}} \equiv \alpha_p^7 \beta_p c_7.$$

Hence, (3.2) holds for $n = 7$.

Setting $n = r + 1$ in (2.5), we obtain

$$c_3 c_5 c_{r+6} c_{r-3} \equiv c_3^2 c_6 c_{r+5} c_{r-2}.$$

By assumption, we have $c_3 c_5 c_6 \not\equiv 0$. Since $c_{-3} = -c_3$ and (3.2) holds for $n = -2, 5, 6$, we obtain

$$c_{r-3} \equiv \frac{c_3 c_6 c_{r+5} c_{r-2}}{c_5 c_{r+6}} \equiv \frac{\alpha_p^3 \beta_p^2 c_{-2} c_3 c_5 c_6}{\alpha_p^6 \beta_p c_5 c_6} \equiv \alpha_p^{-3} \beta_p c_{-3}.$$

Hence, (3.2) holds for $n = -3$.

Summarizing the above, we see that (3.2) holds for $-3 \le n \le 7$. □

Next, we shall prove (3.1) for $k = 1$ and for all n by induction:

Claim 3.6. *For all integers $n \in \mathbb{Z}$, we have*

$$c_{r+n} \equiv \alpha_p^n \beta_p c_n. \tag{3.3}$$

Proof. Suppose that (3.3) holds for $m \le n \le m+10$ for some $m \ge -3$. We shall prove that the assertion holds for $n = m+11$. By Lemma 2.2, at least one of c_m, c_{m+1}, c_{m+2} or c_{m+3} is not congruent to 0 modulo p. So it is enough to consider the following four cases:

- $c_m \not\equiv 0$
- $c_{m+1} \not\equiv 0$
- $c_{m+2} \not\equiv 0$
- $c_{m+3} \not\equiv 0$

We first consider the case $c_m \not\equiv 0$. From (2.7) for $n = m+5$, we have

$$c_3 c_5 c_{m+11} c_m = \sum_{i=0}^{3} S_i c_{m+6+i} c_{m+5-i}, \tag{3.4}$$

where

$$S_0 := -c_3c_5c_8, \quad S_1 := c_3(c_3c_4c_8 - c_9), \quad S_2 := c_5^2c_6 - c_3c_4^2c_7, \quad S_3 := c_3c_4c_7.$$

Similarly, from (2.7) for $n = r+m+5$, we have

$$c_3 c_5 c_{r+m+11} c_{r+m} = \sum_{i=0}^{3} S_i c_{r+m+6+i} c_{r+m+5-i} \tag{3.5}$$

where S_0, S_1, S_2, S_3 are the same constants as above.

By (3.4), since $c_3c_5c_m \not\equiv 0$, we have

$$c_{m+11} \equiv \frac{1}{c_3c_5c_m} \sum_{i=0}^{3} S_i c_{m+6+i} c_{m+5-i}.$$

On the other hand, by the induction hypothesis, we have $c_{r+n} \equiv \alpha_p^n \beta_p c_n$ for $m \le n \le m+10$. Hence, by (3.5), we obtain

$$\begin{aligned} c_{r+m+11} &\equiv \frac{1}{c_3c_5c_{r+m}} \sum_{i=0}^{3} S_i c_{r+m+6+i} c_{r+m+5-i} \\ &\equiv \frac{1}{\alpha_p^m \beta_p c_3c_5c_m} \sum_{i=0}^{3} S_i \cdot \alpha_p^{m+6+i} \beta_p c_{m+6+i} \cdot \alpha_p^{m+5-i} \beta_p c_{m+5-i} \\ &\equiv \frac{1}{\alpha_p^m \beta_p c_3c_5c_m} \sum_{i=0}^{3} S_i \alpha_p^{2m+11} \beta_p^2 \cdot c_{m+6+i} c_{m+5-i} \\ &\equiv \frac{\alpha_p^{m+11}\beta_p}{c_3c_5c_m} \sum_{i=0}^{3} S_i c_{m+6+i} c_{m+5-i}. \end{aligned}$$

Comparing two equations, we have

$$c_{r+m+11} \equiv \alpha_p^{m+11} \beta_p c_{m+11} \pmod{p},$$

and thus (3.3) is true for $n = m+11$.

The other cases are proved in a similar manner. Note that when $c_{m+1} \not\equiv 0$, $c_{m+2} \not\equiv 0$, $c_{m+3} \not\equiv 0$, we shall use (2.6), (2.5), (2.4), respectively. By induction, (3.3) holds for all $n \geq -3$.

The assertion for $n \leq -4$ is proved by similar arguments. Let $m \leq -4$ and assume that the assertion holds for every $n > m$. By Lemma 2.2, at least one of c_{m+8}, c_{m+9}, c_{m+10} or c_{m+11} is not congruent to 0 modulo p. So it is enough to consider the following four cases:

- $c_{m+8} \not\equiv 0$
- $c_{m+9} \not\equiv 0$
- $c_{m+10} \not\equiv 0$
- $c_{m+11} \not\equiv 0$

When $c_{m+11} \not\equiv 0$, we obtain

$$c_m = \frac{1}{c_3 c_5 c_{m+11}} \sum_{i=0}^{3} S_i c_{m+6+i} c_{m+5-i}$$

from (2.7) for $n = m+5$. Thus, we prove the assertion for c_m from the assertions for c_n for $n > m$. Similarly, when $c_{m+10} \not\equiv 0$, $c_{m+9} \not\equiv 0$, $c_{m+8} \not\equiv 0$, we shall use (2.6), (2.5), (2.4), respectively. □

Next, we shall prove part (3) of Theorem 3.1.

Claim 3.7. $\alpha_p^r = \beta_p^2 \in \mathbb{F}_p$.

Proof. Setting $n = 2$ and $n = -r-2$ in (3.2), we have

$$c_{r+2} \equiv \alpha_p^2 \beta_p c_2, \quad c_{-2} \equiv \alpha_p^{-r-2} \beta_p c_{-r-2}.$$

Since $c_{-2} = -c_2 = -1$ and $c_{-r-2} = -c_{r+2}$, we have $\alpha_p^r = \beta_p^2$ in $\mathbb{F}_p$. □

Finally, we prove (3.1) for all integers $k \in \mathbb{Z}$.

Claim 3.8. *For all integers n and k, we have*

$$c_{kr+n} \equiv \alpha_p^{kn} \beta_p^{k^2} c_n.$$

Proof. By Claim 3.6, the assertion holds for $k = 1$. We shall prove the assertion by induction on k. Assume that the assertion holds for some k. Then we have

$$c_{(k+1)r+n} = c_{kr+(r+n)} \equiv \alpha_p^{k(r+n)} \beta_p^{k^2} c_{r+n}.$$

Since $\alpha_p^r = \beta_p^2 \in \mathbb{F}_p$ by Claim 3.7, we have

$$\alpha_p^{k(r+n)} \beta_p^{k^2} c_{r+n} \equiv (\beta_p^2)^k \alpha_p^{kn} \beta_p^{k^2} c_{r+n} \equiv \alpha_p^{kn} \beta_p^{k^2+2k} c_{r+n}.$$

By the assertion for $k = 1$, we have $c_{r+n} \equiv \alpha_p^n \beta_p c_n$. Hence, we have

$$\alpha_p^{kn} \beta_p^{k^2+2k} c_{r+n} \equiv \alpha_p^{kn} \beta_p^{k^2+2k} \cdot \alpha_p^n \beta_p c_n \equiv \alpha_p^{(k+1)n} \beta_p^{(k+1)^2} c_r.$$

The assertion is proved for $k+1$. By induction, the assertion is proved for all $k \geq 1$.

Since we have

$$c_{-kr+n} \equiv -c_{kr-n} \equiv -\alpha_p^{k\cdot(-n)}\beta_p^{k^2}c_{-n} \equiv \alpha_p^{(-k)\cdot n}\beta_p^{(-k)^2}c_n,$$

the assertion for $k < 0$ follows. □

The proof of Theorem 3.1 is complete.

4. Proof of the main theorems

We are now ready to prove Theorem 1.1 and Theorem 1.3.

Proof of Theorem 1.1. Let p be a prime satisfying the assumption in Theorem 3.1. Substituting $k = p-1$ in Theorem 3.1 (2), we have

$$c_{(p-1)r+n} \equiv \alpha_p^{(p-1)n}\beta_p^{(p-1)^2}c_n \equiv c_n \pmod{p}$$

for all integers $n \in \mathbb{Z}$. Hence, $\{c_n \pmod{p}\}_{n\in\mathbb{Z}}$ is periodic, and the period $\mathrm{Per}_p(\boldsymbol{c})$ is a divisor of $(p-1)r = (p-1)\,\mathrm{ord}_p(D_P)$.

Next, we shall prove that $r = \mathrm{ord}_p(D_P)$ divides $s := \mathrm{Per}_p(\boldsymbol{c})$. Since $c_{-1} = c_1 = c_1 = 0$ and $c_2 = 1$, we have $s \geq 4$. Recall that $y_P \not\equiv 0 \pmod{p}$. Since s is the period of the reduction modulo p of the sequence $\boldsymbol{c}$, we have $c_{s+i} \equiv c_i \equiv 0 \pmod{p}$ for $i = -1, 0, 1$. Therefore, by Theorem 2.1 (2), we obtain $s\overline{D_P} = 0$ in $\mathrm{Jac}(C)(\mathbb{F}_p)$. Hence, r divides s. □

Proof of Theorem 1.3. Let $r := \mathrm{ord}_p(D_P)$, $s := \mathrm{Per}_p(\boldsymbol{c})$, and $k := s/r$. By Theorem 1.1 (2), k is a positive integer. By Theorem 3.1 (2), we have $c_{dr+n} \equiv c_n \pmod{p}$ for all integers $n \in \mathbb{Z}$. Hence, we have $s = kr \mid dr$, which implies $k \mid d$.

Setting $n = 2, 3$ in the relation in Theorem 3.1 (2), we have

$$c_{kr+2} \equiv \alpha_p^{2k}\beta_p^{k^2}c_2 \pmod{p}, \quad c_{kr+3} \equiv \alpha_p^{3k}\beta_p^{k^2}c_3 \pmod{p}.$$

Since $s = kr$ is the period and $c_2, c_3 \not\equiv 0 \pmod{p}$, we have

$$\alpha_p^k \equiv \beta_p^{k^2} \equiv 1 \pmod{p}.$$

Hence, we obtain $d \mid k$ since d is the least positive integer satisfying such a condition (see [17, Lemma 10.1]). Therefore, we have $d = k$, which implies $\mathrm{Per}_p(\boldsymbol{c}) = d\,\mathrm{ord}_p(D_P)$. □

As we mentioned in Remark 1.5, we can prove Theorem 1.1 (1) and a half of Theorem 1.1 (2) by using the pigeonhole principle instead of using Theorem 3.1:

Proposition 4.1. *Let p be an odd prime which divides neither* $\mathrm{disc}(F)$ *nor* $c_3c_4c_5$. *Then the reduction modulo p of the sequence* $\boldsymbol{c}$ *is periodic, and we have* $\mathrm{ord}_p(D_P) \mid \mathrm{Per}_p(\boldsymbol{c})$.

Proof. By Lemma 2.2, there exists no integer m such that

$$c_m \equiv c_{m+1} \equiv c_{m+2} \equiv c_{m+3} \equiv 0 \pmod{p}.$$

Since $c_3c_4c_5 \not\equiv 0 \pmod{p}$, by the bilinear recurrence relations of Somos 8, 9, 10 and 11 type in Corollary 2.6, the values $c_{m+11} \pmod{p}$ and $c_{m-1} \pmod{p}$

are uniquely determined by the values $c_{m+i} \pmod{p}$ for $0 \leq i \leq 10$. By the pigeonhole principle, there exist an integer $k \in \mathbb{Z}$ and a positive integer $s \geq 1$ such that $c_{s+k+i} \equiv c_{k+i} \pmod{p}$ for $0 \leq i \leq 10$. Thus, we obtain $c_{n+s} \equiv c_n \pmod{p}$ for all $n \in \mathbb{Z}$ by induction.

The proof of "$\mathrm{ord}_p(D_P) \mid \mathrm{Per}_p(\boldsymbol{c})$" is the same as Theorem 1.1 (2). (Note that the proof of "$\mathrm{ord}_p(D_P) \mid \mathrm{Per}_p(\boldsymbol{c})$" does not require Theorem 3.1.) □

Remark 4.2. In contrast to Theorem 1.1, in the above proof of Proposition 4.1, we do not require the assumption that $c_6c_7(c_4^3 - c_3^3c_5) \not\equiv 0 \pmod{p}$. However, the upper bound for the period $\mathrm{Per}_p(\boldsymbol{c})$ we can obtain from the pigeonhole principle is p^{11}, which is much larger than the upper bound in Corollary 1.2. In particular, without Theorem 3.1, it seems difficult to prove the divisibility "$\mathrm{Per}_p(\boldsymbol{c}) \mid (p-1)\,\mathrm{ord}_p(D_P)$."

Appendix A. Proof of Theorem 2.3

In this appendix, we give a proof of Theorem 2.3. This result essentially follows from the description of Cantor's division polynomials in [12, Appendix]. However, the sign in the formula in [12, Theorem A 1] is incorrect. In fact, the sign $(-1)^{(2n-g)(g-1)/2}$ in [12, Proposition 8.2 (ii)] should be replaced by $(-1)^{(n-g-1)(n+g^2+2g)/2}$ as in [15, Theorem 5.1]. Moreover, the sign $(-1)^{r(r-1)/2}$ in [12, p. 738] should be read $(-1)^{(r-g)(r-g+1)/2}$. Here we supply necessary arguments to correct the sign errors in the literature.

For details on the hyperelliptic sigma function, we refer the readers to [3] and references therein. We adopt the definitions in [11, 12]. In an expression for the Laurent expansion of a function, the symbol $(d^\circ(z_1, z_2, \dots, z_m) \geq n)$ stands for the terms of total degree at least n with respect to the variables $z_1, z_2, \dots, z_m$.

We define differential forms

$$\omega_1 := \frac{dX}{2Y}, \quad \omega_2 := \frac{XdX}{2Y}, \quad \eta_1 := \frac{(3X^3 + 2a_1X^2 + a_2X)dX}{2Y}, \quad \eta_2 := \frac{X^2dX}{2Y}.$$

Let $\{\alpha_1, \alpha_2, \beta_1, \beta_2\}$ be a symplectic basis of $H_1(C(\mathbb{C}), \mathbb{Z})$. We define 2×2 matrices by

$$\omega' := \begin{pmatrix} \int_{\alpha_1}\omega_1 & \int_{\alpha_2}\omega_1 \\ \int_{\alpha_1}\omega_2 & \int_{\alpha_2}\omega_2 \end{pmatrix}, \qquad \omega'' := \begin{pmatrix} \int_{\beta_1}\omega_1 & \int_{\beta_2}\omega_1 \\ \int_{\beta_1}\omega_2 & \int_{\beta_2}\omega_2 \end{pmatrix},$$

$$\eta' := \begin{pmatrix} \int_{\alpha_1}\eta_1 & \int_{\alpha_2}\eta_1 \\ \int_{\alpha_1}\eta_2 & \int_{\alpha_2}\eta_2 \end{pmatrix}, \qquad \eta'' := \begin{pmatrix} \int_{\beta_1}\eta_1 & \int_{\beta_2}\eta_1 \\ \int_{\beta_1}\eta_2 & \int_{\beta_2}\eta_2 \end{pmatrix},$$

which are called the *period matrices*.

We define the *hyperelliptic sigma function* by

$$\sigma(u) := c\exp\left(-\frac{1}{2}\,{}^t u\,\eta'\,\omega'^{-1}\,u\right)\vartheta\begin{bmatrix}\delta''\\ \delta'\end{bmatrix}(\omega'^{-1}u,\ \omega'^{-1}\omega''),$$

where $u = \binom{u_1}{u_2} \in \mathbb{C}^2$, c is some constant, δ', δ'' are the Riemann constants, and ϑ is the Riemann theta function with characteristics. The constant c is determined so that the following lemma holds. For details, see [11, Lemma 1.2] and the references cited there.

Lemma A.1. *The function $\sigma(u)$ has the Taylor expansion*

$$\sigma(u) = u_1 + \frac{1}{6}a_2 u_1^3 - \frac{1}{3}u_2^3 + (d^\circ(u_1, u_2) \geq 5)$$

at $u = \binom{0}{0}$.

We also use the following lemmas.

Lemma A.2. *Let $P = (x_P, y_P) \in C(\mathbb{C})$ and*

$$u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \begin{pmatrix} \int_\infty^P \omega_1 \\ \int_\infty^P \omega_2 \end{pmatrix}.$$

Assume that u is in a neighborhood of $\binom{0}{0}$. Then we have

$$u_1 = \frac{1}{3}u_2^3 + (d^\circ(u_2) \geq 4), \tag{A.1}$$

$$\sigma_2(u) = -u_2^2 + (d^\circ(u_2) \geq 3), \tag{A.2}$$

$$x_P = \frac{1}{u_2^2} + (d^\circ(u_2) \geq -1), \tag{A.3}$$

$$y_P = -\frac{1}{u_2^5} + (d^\circ(u_2) \geq -4). \tag{A.4}$$

Proof. See [11, Lemmas 1.7, 1.9, and 1.12]. □

Lemma A.3. *The polynomial $\psi_n(X) \in \mathbb{Z}[X]$ is of degree $n^2 - 4$, and its leading coefficient is $\binom{n+1}{3}$.*

Proof. The lemma follows from [4, Theorem 8.17]. □

Proof of Theorem 2.3. Comparing the definition of $\psi_n(X)$ and the determinant expression of $\sigma(nu)/\sigma_2(u)^{n^2}$ in [12, Theorem A 1], we have

$$2y_P\psi_n(x_P) = \pm\frac{\sigma(nu)}{\sigma_2(u)^{n^2}}.$$

To determine the sign, we compare the leading term of the Laurent expansion of both sides at $u_2 = 0$. By Lemmas A.2 and A.3, we have

$$2y_P\psi_n(x_P) = -2\binom{n+1}{3}\frac{1}{u_2^{2n^2-3}} + (d^\circ(u_2) \geq -2n^2 + 4). \tag{A.5}$$

By Lemmas A.1 and A.2, we have

$$\begin{aligned}\sigma(nu) &= nu_1 + \frac{1}{6}a_2(nu_1)^3 - \frac{1}{3}(nu_2)^3 + (d^\circ(u_1,u_2) \geq 5)\\ &= \frac{1}{3}nu_2^3 + \frac{1}{6}a_2\left(\frac{1}{3}nu_2^3\right)^3 - \frac{1}{3}n^3u_2^3 + (d^\circ(u_2) \geq 4)\\ &= -2\binom{n+1}{3}u_2^3 + (d^\circ(u_2) \geq 4).\end{aligned}$$

By Lemma A.2, we have

$$\sigma_2(u)^{n^2} = (-1)^{n^2}u_2^{2n^2} + (d^\circ(u_2) \geq 2n^2+1).$$

Since $(-1)^{n^2} = (-1)^n$, we have

$$\frac{\sigma(nu)}{\sigma_2(u)^{n^2}} = 2(-1)^{n+1}\binom{n+1}{3}\frac{1}{u_2^{2n^2-3}} + (d^\circ(u_2) \geq -2n^2+4). \tag{A.6}$$

Therefore, by (A.5) and (A.6), we obtain

$$2y_P\psi_n(x_P) = (-1)^n\frac{\sigma(nu)}{\sigma_2(u)^{n^2}}. \qquad \square$$

Appendix B. Numerical calculation of periods and orders

Here we give an example illustrating Theorem 1.1. We study the integer sequence introduced by Cantor (see OEIS A058231)[1]. It is an integer sequence $\{c_n\}_{n\geq 0}$ satisfying

$$\begin{aligned}&c_0 = c_1 = 0, \quad c_2 = 1, \quad c_3 = 36, \quad c_4 = -16,\\ &c_5 = 5041728, \quad c_6 = -19631351040, \quad c_7 = -62024429150208,\\ &c_8 = -2805793044443561984, \quad c_9 = -1213280369793911777918976\end{aligned}$$

and the recurrence relation of Somos 8 type

$$\begin{aligned}-16c_nc_{n+8} - 181502208c_{n+1}c_{n+7} + 235226865664c_{n+2}c_{n+6}&\\ + 25442230947840c_{n+3}c_{n+5} + 314101616640c_{n+4}^2 &= 0.\end{aligned}$$

It is a non-trivial fact that such an integer sequence $\{c_n\}_{n\geq 0}$ exists. In fact, this sequence consists of values of Cantor's division polynomials; see also [4]. We set

$$C:\ Y^2 = X^5 - 3X^4 - 2X + 9, \quad P = (0,3).$$

Let $\psi_n(X) \in \mathbb{Z}[X]$ be Cantor's division polynomial for C. Then we can verify

$$c_n = \psi_n(0).$$

We extend the sequence c_n to $n < 0$ by $c_n = -c_{-n}$ (see OEIS A058231). In particular, we have $c_{-1} = c_0 = c_1 = 0$.

From Theorem 1.1 and Corollary 1.2, we obtain the following results.

[1] https://oeis.org/A058231

Corollary B.1. *Let p be a prime not in the following list:*

$$2, 3, 5, 7, 29, 41, 47, 379, 509, 853, 8059, 8753, 49711, 140891.$$

Then the following assertions hold.

(1) *The reduction modulo p of the sequence $\boldsymbol{c} = \{c_n\}_{n\in\mathbb{Z}}$ is periodic.*
(2) *Let $\mathrm{Per}_p(\boldsymbol{c})$ be the period of the reduction modulo p of the sequence $\boldsymbol{c}$. Let $\mathrm{ord}_p(D_P)$ be the order of the point $\overline{D_P} \in \mathrm{Jac}(C)(\mathbb{F}_p)$. Then we have*
$$\mathrm{ord}_p(D_P) \mid \mathrm{Per}_p(\boldsymbol{c}) \mid (p-1)\,\mathrm{ord}_p(D_P).$$
(3) *We have $\mathrm{Per}_p(\boldsymbol{c}) \le (p-1)(1+\sqrt{p})^4$.*

Proof. By Theorem 1.1 and Corollary 1.2, it is enough to determine the set of excluded primes. The discriminant of $X^5 - 3X^4 - 2X + 9$ is $-36040475 = -5^2 \times 29 \times 49711$. (By Magma, the conductor of C is $4613180800 = 2^7 \times 5^2 \times 29 \times 49711$.) We calculate

$$\begin{aligned}
c_3 &= 2^2 \times 3^2,\\
c_4 &= -2^4,\\
c_5 &= 2^6 \times 3^2 \times 8753,\\
c_6 &= -2^8 \times 3 \times 5 \times 7 \times 41 \times 47 \times 379,\\
c_7 &= -2^{13} \times 3^2 \times 7 \times 853 \times 140891,\\
c_4^3 - c_3^3 c_5 &= -2^{13} \times 7 \times 509 \times 8059.
\end{aligned}$$

□

In the following table, for prime $p \le 400$, we give numerical results on the number of $\mathbb{F}_p$-rational points on the reduction modulo p of $\mathrm{Jac}(C)$, the order $\mathrm{ord}_p(D_P)$ of the point $\overline{D_P} \in \mathrm{Jac}(C)(\mathbb{F}_p)$, the period $\mathrm{Per}_p(\boldsymbol{c})$ of the reduction modulo p of the sequence $\boldsymbol{c}$, the ratio $\mathrm{Per}_p(\boldsymbol{c})/\mathrm{ord}_p(D_P)$, and the elements $\alpha_p, \beta_p \in \mathbb{F}_p$ in Theorem 1.3.

The calculations of $|\mathrm{Jac}(C)(\mathbb{F}_p)|$ and $\mathrm{ord}_p(D_P)$ are done by Magma [2]. The calculations of $\mathrm{Per}_p(\boldsymbol{c})$ are done by Sage [14] using the bilinear recurrence relations of Somos 8, 9, 10 and 11 type satisfied by $\boldsymbol{c}$ in Corollary 2.6.

Table 1: Numerical verification of Theorem 1.1 for the case of Cantor's sequence (OEIS A058231).

p	$\lvert\mathrm{Jac}(C)(\mathbb{F}_p)\rvert$	$\mathrm{ord}_p(D_P)$	$\mathrm{Per}_p(\boldsymbol{c})$	$\mathrm{Per}_p(\boldsymbol{c})/\mathrm{ord}_p(D_P)$	α_p	β_p
2						
3	12	2	6	3		
5			12			
7	28	7	21	3	4	2
11	112	56	280	5	4	9

13	127	127	762	6	10	7
17	272	136	2176	16	10	4
19	405	135	405	3	7	1
23	692	173	3806	22	12	10
29			2100			
31	997	997	997	1	1	1
37	1684	842	3368	4	6	31
41	1693	1693	8465	5	10	37
43	1186	1186	2372	2	42	1
47	2433	2433	55959	23	18	17
53	3284	821	10673	13	16	16
59	3512	439	12731	29	45	19
61	3910	3910	234600	60	26	40
67	5056	632	41712	66	6	2
71	5064	2532	88620	35	10	36
73	5840	730	13140	18	37	57
79	5825	5825	75725	13	18	52
83	7324	3662	150142	41	78	77
89	6762	2254	198352	88	60	75
97	9884	9884	948864	96	90	2
101	9900	275	13750	50	82	10
103	10112	5056	10112	2	102	1
107	12944	3236	343016	106	46	81
109	11349	11349	306423	27	3	45
113	12332	12332	1381184	112	12	41
127	15272	15272	30544	2	126	1
131	18724	9362	243412	26	45	86
137	19104	9552	1299072	136	21	15
139	20687	20687	2854806	138	71	72
149	20696	5174	382876	74	37	64
151	22010	22010	3301500	150	51	2
157	27456	2288	118976	52	29	156
163	26138	26138	4234356	162	137	122
167	30036	7509	1246494	166	19	30

173	26673	26673	2293878	86	54	62
179	32388	2699	480422	178	60	132
181	35447	35447	638046	18	138	149
191	38384	19192	3646480	190	28	163
193	37210	37210	7144320	192	114	120
197	34920	4365	427770	98	61	22
199	41888	10472	1036728	99	65	180
211	45849	15283	229245	15	134	137
223	49121	49121	5452431	111	9	126
227	56510	28255	6385630	226	33	162
229	54829	54829	6250506	114	3	62
233	53520	4460	1034720	232	212	207
239	56584	7073	1683374	238	202	207
241	66112	33056	793344	24	32	226
251	64724	32362	1618100	50	226	204
257	63176	31588	4043264	128	143	165
263	70608	35304	9249648	262	258	189
269	71024	8878	1189652	134	170	24
271	73020	4868	262872	54	266	188
277	74418	24806	6846456	276	24	115
281	80956	80956	22667680	280	259	267
283	80436	6703	1890246	282	81	272
293	84592	21148	3087608	146	172	267
307	94816	47408	4835616	102	155	51
311	105052	52526	16283060	310	289	124
313	97720	24430	635180	26	255	265
317	108842	108842	34394072	316	126	115
331	102800	25700	1413500	55	172	274
337	116852	29213	2453892	84	196	147
347	125596	31399	10864054	346	38	280
349	113967	5427	314766	58	110	115
353	125906	62953	5539864	88	336	317
359	129600	64800	23198400	358	105	254
367	136161	45387	16611642	366	268	360

373	146336	4573	283526	62	31	97
379	143613	143613	54285714	378	189	293
383	153214	76607	29263874	382	64	157
389	160166	80083	15536102	194	311	355
397	165192	6883	1362834	198	121	119

Remark B.2. Among the primes $p \leq 400$, for $p \neq 2, 3, 5, 7, 29, 41, 47, 379$, we have

$$\mathrm{ord}_p(D_P) \mid \mathrm{Per}_p(\boldsymbol{c}) \mid (p-1)\,\mathrm{ord}_p(D_P)$$

by Theorem 1.1. For the excluded primes, the curve C has bad reduction at $p = 2, 5, 29$. For $p = 7, 41, 47, 379$, although we cannot apply Theorem 1.1 because p divides $c_3c_4c_5c_6c_7(c_4^3 - c_3^3c_5)$, we observe that the above divisibilities hold for such p. However, for $p = 3$, we observe that the divisibility $\mathrm{ord}_p(D_P) \mid \mathrm{Per}_p(\boldsymbol{c})$ holds, but the divisibility $\mathrm{Per}_p(\boldsymbol{c}) \mid (p-1)\,\mathrm{ord}_p(D_P)$ does not.

Remark B.3. For primes ≤ 400, we have $\mathrm{Per}_p(\boldsymbol{c}) = \mathrm{ord}_p(D_P)$ for $p = 31$ only. We have $\mathrm{Per}_p(\boldsymbol{c}) = (p-1)\,\mathrm{ord}_p(D_P)$ for $p =$ 17, 23, 61, 67, 89, 97, 107, 113, 137, 139, 151, 163, 167, 179, 191, 193, 227, 233, 239, 263, 277, 281, 283, 311, 317, 347, 359, 367, 379, 383.

Acknowledgements. The authors would like to thank the referee for useful comments and suggestions. The work of Y. I. was supported by JSPS KAKENHI Grant Number 21K18577, 24K21512 and 21K13773. The work of T. I. was supported by JSPS KAKENHI Grant Number 21K18577, 24K21512 and 23K20786. The work of T. O. was supported by JSPS KAKENHI Grant Number 18H05233, 20K14295, 21K18577 and 24K21512. The work of T. T. was supported by JSPS KAKENHI Grant Number 21K18577, 24K21512 and 22H01115. The work of Y. U. was supported by JSPS KAKENHI Grant Number 21K18577, 24K21512 and 20K03517. A part of this work was done while the authors were supported by the Sumitomo Foundation FY2018 Grant for Basic Science Research Projects (Grant Number 180044). Most of calculations were done with the aid of the computer algebra systems Magma [2] and Sage [14].

References

[1] Baker, Henry F. Abelian functions. Abel's theorem and the allied theory of theta functions. Cambridge Mathematical Library. *Cambridge University Press, Cambridge*, 1995. MR1386644 (97b:14038), JFM 28.0331.01. 573

[2] Bosma, Wieb; Cannon, John; Playoust, Catherine. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24** (1997), no. 3-4, 235–265. MR1484478, Zbl 0898.68039, doi: 10.1006/jsco.1996.0125. 583, 586

[3] Buchstaber, Viktor M.; Enolski, Victor Z.; Leykin, D. V. σ-functions: old and new results. *Integrable systems and algebraic geometry. Vol. 2*, 175–214. London Math. Soc. Lecture Note Ser., 459. *Cambridge Univ. Press, Cambridge*, 2020. ISBN:978-1-108-71577-5, ISBN:978-1-108-78549-5. MR4421431, Zbl 1473.14057, arXiv:1810.11079, doi: 10.1017/9781108773355.007. 572, 580

[4] CANTOR, DAVID G. On the analogue of the division polynomials for hyperelliptic curves. *J. Reine Angew. Math.* **447** (1994), 91–145. MR1263171 (94m:11071), Zbl 0788.14026, doi: 10.1515/crll.1994.447.91. 569, 570, 572, 574, 581, 582

[5] CASPARY, FERDINAND. Zur Theorie der Thetafunctionen mehrerer Argumente. *J. Reine Angew. Math.* **96** (1884), 324–326. MR1579999, JFM 16.0443.01, doi: 10.1515/crll.1884.96.324. 573

[6] DOLIWA, ADAM. Determinantal approach to multiple orthogonal polynomials and the corresponding integrable equations. *Stud. Appl. Math.* **153** (2024), no. 2, Paper No. e12726, 26 pp. MR4788479, Zbl 1546.42021, arXiv:2312.15509, doi: 10.1111/sapm.12726. 571

[7] FROBENIUS, G. Ueber Thetafunctionen mehrerer Variabeln. *J. Reine Angew. Math.* **96** (1884), 100–122. MR1579993, JFM 16.0440.01, doi: 10.1515/crll.1884.96.100. 573

[8] HONE, ANDREW N. W. Continued fractions and Hankel determinants from hyperelliptic curves. *Comm. Pure Appl. Math.* **74** (2021), no. 11, 2310–2347. MR4373159, Zbl 1485.39030, arXiv:1907.05204, doi: 10.1002/cpa.21923. 571

[9] MATSUTANI, SHIGEKI. Recursion relation of hyperelliptic psi-functions of genus two. *Integral Transforms Spec. Funct.* **14** (2003), no. 6, 517–527. MR2017658 (2004m:14097), Zbl 1041.11047, arXiv:math-ph/0105031, doi: 10.1080/10652460310001600609. 573

[10] MILNE, JAMES S. Abelian varieties. *Arithmetic geometry* (Storrs, Conn., 1984), 103–150. *Springer-Verlag, New York*, 1986. ISBN:0-387-96311-1. MR0861974, Zbl 0604.14028, doi: 10.1007/978-1-4613-8655-1_5. 569

[11] ÔNISHI, YOSHIHIRO. Determinant expressions for abelian functions in genus two. *Glasg. Math. J.* **44** (2002), no. 3, 353–364. MR1956544 (2003k:11103), Zbl 1101.14312, arXiv:math/0105188, doi: 10.1017/S001708950203001X. 572, 580, 581

[12] ÔNISHI, YOSHIHIRO. Determinant expressions for hyperelliptic functions. With an appendix by Shigeki Matsutani. *Proc. Edinb. Math. Soc. (2)* **48** (2005), no. 3, 705–742. MR2171194 (2007b:14065), Zbl 1148.14303, doi: 10.1017/S0013091503000695. 572, 573, 580, 581

[13] SHIPSEY, RACHEL; SWART, CHRISTINE. Elliptic divisibility sequences and the elliptic curve discrete logarithm problem. Cryptology ePrint Archive, Paper 2008/444, 2008. https://eprint.iacr.org/2008/444. 570, 574

[14] THE SAGE DEVELOPERS. SageMath, the Sage Mathematics Software System (Version 9.5). https://www.sagemath.org. doi: 10.5281/zenodo.6259615. 583, 586

[15] UCHIDA, YUKIHIRO. Division polynomials and canonical local heights on hyperelliptic Jacobians. *Manuscripta Math.* **134** (2011), no. 3-4, 273–308. MR2765713 (2012h:14083), Zbl 1226.14039, doi: 10.1007/s00229-010-0394-9. 573, 580

[16] USTINOV, ALEXEY V. On periodicity of the Somos sequences modulo m. *Mat. Zametki* **115** (2024), no. 3, 439–449; translation in *Math. Notes* **115** (2024), no. 3-4, 405–413. MR4767914, Zbl 1548.11048, doi: 10.4213/mzm14120. 571

[17] WARD, MORGAN. Memoir on elliptic divisibility sequences. *Amer. J. Math.* **70** (1948), 31–74. MR0023275 (9,332j), Zbl 0035.03702, doi: 10.2307/2371930. 568, 569, 579

(Y. Ishitsuka) Institute of Mathematics for Industry, Kyushu University, Fukuoka, 819-0395, Japan
yishi1093@gmail.com

(T. Ito) Department of Mathematics, Faculty of Science, Kyoto University, Kyoto 606-8502, Japan
tetsushi@math.kyoto-u.ac.jp

(T. Ohshita) Department of Mathematics, Cooperative Faculty of Education, Gunma University, Maebashi, Gunma 371-8510, Japan
ohshita@gunma-u.ac.jp

(T. Taniguchi) Department of Mathematics, Graduate School of Science, Kobe University, Kobe 657-8501, Japan
tani@math.kobe-u.ac.jp

(Y. Uchida) Department of Mathematical Sciences, Graduate School of Science, Tokyo Metropolitan University, 1-1 Minami-Osawa, Hachioji, Tokyo 192-0397, Japan
yuchida@tmu.ac.jp

This paper is available via http://nyjm.albany.edu/j/2025/31-19.html.