E. S. Malygina, S. A. Novoselov, Division polynomials for hyperelliptic curves defined by Dickson polynomials, *Mat. Vopr. Kriptogr.*, 2020, Volume 11, Issue 2, 69–81

DOI: https://doi.org/10.4213/mvk322

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2020 Т. 11 № 2 С. 69–81

УДК 519.719.2+512.742.72 DOI https://doi.org/10.4213/mvk322

Division polynomials for hyperelliptic curves defined by Dickson polynomials

E. S. Malygina, S. A. Novoselov

Immanuel Kant Baltic Federal University, *Kaliningrad*

Получено 05.XI.2019

Abstract. In this paper, we investigate division polynomials for hyperelliptic curves of genus 2 defined by the Dickson polynomial. For the case of $\ell = 3$, we obtain explicit formulae.

Keywords: hyperelliptic curve, division polynomials, Mumford–Cantor's coordinates, l-torsion, Dickson polynomials

Многочлены деления для гиперэллиптических кривых, определяемых многочленами Диксона

Е. С. Малыгина, С. А. Новоселов

Балтийский федеральный университет им. И. Канта, *Калининград*

Аннотация. Выводятся формулы для многочленов деления класса гиперэллиптических кривых рода 2, задаваемых многочленами Диксона. В случае $\ell = 3$ формулы представлены в явном виде.

Ключевые слова: гиперэллиптические кривые, многочлены деления, координаты Мамфорда–Кантора, группа ℓ-кручения, многочлены Диксона

Citation: Matematicheskie Voprosy Kriptografii, 2020, v. 11, № 2, pp. 69–81 (Russian)

1. Introduction

Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, where $p > 2$. A hyperelliptic curve C of genus g is a nonsingular curve defined by equation

$$Y^2 = f(X),$$

where f is a monic polynomial of degree $2g+1$ or $2g+2$.

Hyperelliptic curves were first proposed for use in cryptography by Koblitz [2] for constructing cryptosystems based on discrete logarithm problem (DLP). At the present time only curves of genus 2 and 3 are considered for constructing of cryptosystems based on DLP due to index-calculus attacks [7].

On the other side, in the post-quantum cryptography on isogenies there is no limitation on genus. The main problem in this field is the absence of effective formulas for a computation of isogenies in general case of degree ℓ. Recently, Flynn and Yan Bo Ti [10] proposed a first post-quantum isogeny-based scheme on genus 2 curves. The authors used the Richelot isogenies for a computing of degree 2 isogenies and the Kummer surfaces for degree 3 case.

In this work, we develop a direct approach for degree 3 case to remove a dependency on the Kummer surface in scheme. It consist of two steps. The first step is to give an explicit formulas for the division polynomials which describe kernels of degree 3 isogenies. The second step is a computation of an isogeny from the division polynomial. The division polynomials provide explicit formulas for a scalar multiplication in the Jacobian of hyperelliptic curve. Since it is known that $[\ell] = \psi \circ \hat{\psi}$ for any isogeny ψ of degree ℓ computation of an isogeny may be done by factoring or decomposing the division polynomials.

As the first step, in this paper, we give explicit formulas for the division polynomials which describe kernels of degree 3 isogenies. We do this for interesting class of curves defined by the Dickson polynomials.

The division polynomials were first introduced for elliptic curves ($g = 1$) and later were described for hyperelliptic curves by Cantor [4]. The division polynomials are used in Schoof–Pila-like [3] algorithms for counting points on the Jacobian of the curve and in the computation of modular equations [6]. By theorem of Tate [1], point-counting allows us to determine whether two hyperelliptic curves have the isogenous Jacobians or not. Counting points on the Jacobian of curve involves a computation modulo division ideal generated by the division polynomials. Because of that, a degrees and a form of the division polynomials directly affects the complexity of point-counting algorithms.

In this paper we investigate the division polynomials for special classes of curves, which are defined by the Dickson polynomials. These classes arise in the decomposition of Jacobians of curves with equation $C\colon Y^2 = X^{2g+1} + aX^{g+1} + bX$. We denote the Jacobian of the curve C by $\mathrm{Jac}_C(k)$, where $k = \mathbb{F}_q(\sqrt[g]{b})$ or $k = \mathbb{F}_q(\sqrt[2g]{b})$ (depends on the case) is an extension of the finite field $\mathbb{F}_q$.

Theorem 1 ([8]). *If genus g of the curve C is odd then*

$$\mathrm{Jac}_C(\mathbb{F}_q(\sqrt[g]{b})) \sim \mathrm{Jac}_{C_1}(\mathbb{F}_q(\sqrt[g]{b})) \times \mathrm{Jac}_{C_2}(\mathbb{F}_q(\sqrt[g]{b})),$$

where

$$C_1\colon Y^2 = D_g(X, \sqrt[g]{b}) + a$$

and

$$C_2\colon Y^2 = (X^2 - 4\sqrt[g]{b})(D_g(X, \sqrt[g]{b}) + a).$$

If genus g of the curve C is even then

$$\mathrm{Jac}_C(\mathbb{F}_q(\sqrt[2g]{b})) \sim \mathrm{Jac}_{C_3}(\mathbb{F}_q(\sqrt[2g]{b})) \times \mathrm{Jac}_{\tilde{C}_3}(\mathbb{F}_q(\sqrt[2g]{b})),$$

where

$$C_3\colon Y^2 = (X + 2\sqrt[2g]{b})(D_g(X, \sqrt[g]{b}) + a)$$

and

$$\tilde{C}_3\colon Y^2 = (X - 2\sqrt[2g]{b})(D_g(X, \sqrt[g]{b}) + a).$$

Here, $D_g(X, \alpha) = \sum_{i=0}^{\lfloor \frac{g}{2} \rfloor} \frac{g}{g-i}\binom{g-i}{i}(-\alpha)^i X^{g-2i}$ for some constant α denotes the Dickson polynomial of degree g. If $\alpha = 1$, we simply write $D_g(X)$ instead of $D_g(X, 1)$. We refer to [5] for properties of the Dickson polynomials. Because of the theorem, the computation of the number of points on the $\mathrm{Jac}_C(\mathbb{F}_q)$ may be reduced to the computation of the number of points on $\mathrm{Jac}_{C_1}, \mathrm{Jac}_{C_2}, \mathrm{Jac}_{C_3}, \mathrm{Jac}_{\tilde{C}_3}$.

2. Background and notation

Let k be a perfect field, $\mathrm{char}(k) \neq 2$ and a hyperelliptic curve C/k of genus g be defined by the equation

$$C\colon Y^2 = f(X) = \sum_{i=0}^{2g+1} f_i X^i, \quad f_{2g+1} = 1.$$

We denote by $\mathrm{Jac}_C(\bar{k})[\ell]$ the ℓ-torsion subgroup of elements from the Jacobian $\mathrm{Jac}_C(\bar{k})$ of the curve C, where ℓ is a prime and $\ell \neq \mathrm{char}(k)$.

Let $\tau : (x, y) \mapsto (x, -y)$ be a hyperelliptic involution and $\sigma\colon C/k \to \mathrm{Jac}_C(k)$ be a canonical injection such that a point P corresponds to a divisor class $[P - \infty]$. Any element of $\mathrm{Jac}_C(k)$ may be uniquely represented by a divisor $D = \sum_{i=1}^{t} \sigma(P_i)$, $t \in \mathbb{N}$, such that the following holds:

$$P_i \in C(\bar{k}) \text{ and } P_i \neq \infty,$$

$$P_i \neq \tau(P_{i'}) \text{ with } i \neq i',$$

$$t \leqslant g.$$

Let $P_i = (x_i, y_i) \in C(\overline{k})$. Then the Mumford–Cantor representation of the divisor D has a form

$$D = (d(X), e(X)) = \left(X^r + d_{r-1}X^{r-1} + \ldots + d_0, e_{r-1}X^{r-1} + \ldots + e_0\right),$$

where $d(X) = \prod_{i=1}^{r}(X - x_i)$, $e(x_i) = y_i$, $\deg e(X) < \deg d(X) \leqslant g$, and $d(X)|(e^2(X) - f(X))$. Group law on the Jacobian is given by the Cantor's algorithm [9]. More details on hyperelliptic curves and their arithmetic may be found in [11].

The number t in the representation above is called the weight of the divisor. In fact, all generic non-zero divisors $D \in [D] \in \mathrm{Jac}_C(k)[\ell]$ have a weight g. In this work we consider the case $g = 2$. Then for the divisor $D = P_1 + P_2 - 2\infty$ we have

$$[\ell]D = 0 \;\Leftrightarrow\; [\ell](P_1 - \infty) = -[\ell](P_2 - \infty).$$

Set $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. So, the Mumford–Cantor coordinates for divisors $[\ell](P_i - \infty)$, $i = 1, 2$, may be represented by the pair of polynomials

$$\left(\delta_\ell\left(\frac{x_i - X}{4y_i^2}\right), \epsilon_\ell\left(\frac{x_i - X}{4y_i^2}\right)\right).$$

We remark that $\delta_\ell\left(\frac{x_i - X}{4y_i^2}\right)$ is not necessarily a monic polynomial. Thus, we need to divide by the leading coefficient to obtain the Mumford–Cantor representation.

The main result of this paper is explicit formulae for δ_3 and ϵ_3 in the case of genus 2 hyperelliptic curve defined by the Dickson polynomials.

3. Padé approximation

To find the polynomials δ_ℓ and ϵ_ℓ, we can use an algorithm for group law from [9] for adding divisors in Mumford–Cantor representation. But there is a more efficient way due to Cantor [4] which use Padé approximation. We specialize these formulas to the case of curves defined by the Dickson polynomials and $\ell = 3$ and obtain them in explicit form.

Throughout this paper, we assume $g = 2$. We consider a hyperelliptic curve $C/\mathbb{F}_q$ defined by the equation

$$Y^2 = (X \pm 2)(D_4(X, \alpha) + c),$$

where $D_4(X, \alpha) = X^4 - 4X^2\alpha + 2\alpha^2$ is the Dickson polynomial and $\alpha, c \in \mathbb{F}_q$. Let $P = (x, y) \in C(\mathbb{F}_q)$. We make the change of variables

$$P = (x, y) \mapsto \tilde{P} = (0, -y).$$

Then by setting

$$X = x - Z, \;\; \tilde{f}(Z) = f(x - Z),$$

the original curve

$$C\colon Y^2 = X^5 \pm 2X^4 - 4\alpha X^3 \mp 8\alpha X^2 + (2\alpha^2 + c)X \pm (4\alpha^2 + 2c)$$

passing through the point P is replaced with the curve

$$\begin{aligned}\tilde{C}\colon \tilde{Y}^2 = (x - Z)^5 \pm 2(x - Z)^4 - 4\alpha(x - Z)^3 \mp 8\alpha(x - Z)^2 \\ + (2\alpha^2 + c)(x - Z) \pm (4\alpha^2 + 2c)\end{aligned}$$

passing through the point $\tilde{P}$. This change of variable simplifies the expressions in the further formulas. Denote by $\tilde{f}(Z)$ the right part of the equation of the new curve $\tilde{C}$. Expand the expression $\sqrt{\tilde{f}(Z)}$ in a formal Taylor series

$$S(Z) := \sqrt{\tilde{f}(Z)} = \sum_{i=1}^{\infty} s_i(x)Z^i$$

with constant term $s_0 = -y$. Since $p > 2$, the coefficients of $S(Z)$ are defined over the finite field $\mathbb{F}_q$.

Let $m_r = \left\lfloor \frac{r+g}{2} \right\rfloor$ and $n_r = \left\lfloor \frac{r-g-1}{2} \right\rfloor$ for $r \geqslant g+1$. Let $A_r(Z)$ and $B_r(Z)$ be non-zero polynomials such that the formal power series $A_r(Z) - B_r(Z)S(Z)$ is divided by $Z^{m_r+n_r+1}$ and $\deg A_r \leqslant m_r$, $\deg B_r \leqslant n_r$, then a pair (A_r, B_r) is (m_r, n_r)-Padé approximants of series $S(Z)$, namely $\frac{A_r(Z)}{B_r(Z)} = S(Z)$ up to order $m_r + n_r$. So, the Padé approximation problem may be reduced to the searching for polynomials $A_r(Z)$ and $B_r(Z)$.

Let us introduce the following notation which will be used in the next section:

$$G_r(Z) = -\frac{A_r(Z) - B_r(Z)S(Z)}{Z^r},$$
$$H_r(Z) = -(A_r(Z) + B_r(Z)S(Z))G_r(Z).$$

Here $G_r(Z)$ is an error value showing how far $\frac{A_r(Z)}{B_r(Z)}$ is from $S(Z)$. The zeroes of the polynomial $H_r(Z)$ correspond to Z-coordinates of the divisor representation $[r](\tilde{P} - \infty)$.

4. Explicit formulae

In this section we obtain the explicit formulae for the division polynomials ψ_r and as a consequence we obtain explicit formulae for the Mumford–Cantor coordinates via coefficients of the series $S(Z)$, the division polynomials ψ_r, the Padé approximants $A_r(Z), B_r(Z)$, and the values $G_r(Z)$, $H_r(Z)$ for $g = 2$. Let $P = (x, y) \in C(\mathbb{F}_p)$, where

$$y = \pm\sqrt{x^5 \pm 2x^4 - 4\alpha x^3 \mp 8\alpha x^2 + (2\alpha^2 + c)x \pm (4\alpha^2 + 2c)}$$

and as above we have

$$S(Z) = \sum_{i=1}^{\infty} s_i(x) Z^i.$$

Denote

$$\det(S)_{mn} = \begin{vmatrix} s_{m-n+1} & s_{m-n+2} & \cdots & s_m \\ s_{m-n+2} & s_{m-n+3} & \cdots & s_{m+1} \\ \vdots & \vdots & \cdots & \vdots \\ s_{m-1} & s_m & \cdots & s_{m+n-2} \\ s_m & s_{m+1} & \cdots & s_{m+n-1} \end{vmatrix}.$$

The first four division polynomials are

$$\psi_1 = 0, \quad \psi_2 = 1, \quad \psi_3 = (2y)^2, \quad psi_4 = (2y)^5 s_3.$$

As above we have $m_r = \left\lfloor \frac{r+g}{2} \right\rfloor$, $n_r = \left\lfloor \frac{r-g-1}{2} \right\rfloor$ and for $r \geqslant 5$ we may express ψ_r in terms of $\det(S)_{m_r n_r}$:

$$\psi_r = (2y)^{\frac{r^2-r-2}{2}} \cdot \det(S)_{m_{r+1} n_{r+1}}.$$

Besides, the polynomial ψ_r may be calculated by the recursion formula with $s \geqslant r$ (see [4]):

$$\psi_s \cdot \psi_r \cdot \psi_{s+r} \cdot \psi_{s-r} = \begin{vmatrix} \psi_{s-2} & \psi_{s-1} \cdot \psi_{r+1} & \psi_s \cdot \psi_{r+2} \\ \psi_{s-1} \cdot \psi_{r-1} & \psi_r \psi_s & \psi_{s+1} \cdot \psi_{r+1} \\ \psi_s \cdot \psi_{r-2} & \psi_{s+1} \cdot \psi_{r-1} & \psi_{s+2} \cdot \psi_r \end{vmatrix}.$$

Also according to [4] the first non-trivial values for the Padé approximants A_r, B_r and the error value C_r with $r = 0, \dots 4$ are

$$A_0(Z) = -1, \quad A_1(Z) = -Z, \quad A_2(Z) = -Z^2,$$

$$A_3(Z) = \sum_{i=0}^{2} s_i Z^i, \quad A_4(Z) = \sum_{i=0}^{3} s_i Z^i,$$

$$B_0(Z) = 0, \quad B_1(Z) = 0, \quad B_2(Z) = 0, \quad B_3(Z) = 1, \quad B_4(Z) = 1,$$

$$G_0(Z) = 1, \quad G_1(Z) = 1, \quad G_2(Z) = 1,$$

$$G_3(Z) = \sum_{i=3}^{\infty} s_i Z^{i-3}, \; G_4(Z) = \sum_{i=4}^{\infty} s_i Z^{i-4}.$$

Knowing only ψ_r and the initial values given above, we obtain recursive formulae for A_r, B_r, G_r with $r \geqslant 5$:

$$A_r(Z) = (2y)^{-r+2} \cdot \frac{\psi_{r-1}}{\psi_{r-2}} \cdot A_{r-1}(Z) - (2y)^{-2r+3} \cdot \frac{\psi_r}{\psi_{r-2}} \cdot A_{r-2}(Z) \cdot Z,$$

$$B_r(Z) = (2y)^{-r+2} \cdot \frac{\psi_{r-1}}{\psi_{r-2}} \cdot B_{r-1}(Z) - (2y)^{-2r+3} \cdot \frac{\psi_r}{\psi_{r-2}} \cdot B_{r-2}(Z) \cdot Z,$$

$$G_r(Z) = \left((2y)^{-r+2} \cdot \frac{\psi_{r-1}}{\psi_{r-2}} \cdot G_{r-1}(Z) - (2y)^{-2r+3} \cdot \frac{\psi_r}{\psi_{r-2}} \cdot G_{r-2}(Z) \right) / Z.$$

In a similar way we define the initial values for $H_r(Z)$ with $r = 2, 3, 4$:

$$H_2(Z) = -Z^2,$$

$$H_3(Z) = 2(s_0 s_5 + s_1 s_4 + s_2 s_3) Z^2 + 2(s_0 s_4 + s_1 s_3) Z + 2 s_0 s_3,$$

$$H_4(Z) = 2(s_0 s_6 + s_1 s_5 + s_2 s_4) Z^2 + 2(s_0 s_5 + s_1 s_4) Z + 2 s_0 s_4.$$

A recursive formula for $H_r(Z)$ with $r \geqslant 5$ is

$$H_r(Z) = 2\Bigg(\frac{(2y)^{-2r+4} \cdot \frac{\psi_{r-1}^2}{\psi_{r-2}^2} \cdot A_{r-1}(Z) \cdot G_{r-1}(Z)}{Z} - \frac{(2y)^{-3r+5} \cdot \frac{\psi_{r-1}\psi_r}{\psi_{r-2}^2} \cdot A_{r-1}(Z) \cdot G_{r-2}(Z)}{Z} + (2y)^{-4r+6} \cdot \frac{\psi_{r-1}^2}{\psi_{r-2}^2} \cdot A_{r-2}(Z) \cdot G_{r-2}(Z) - (2y)^{-3r+5} \cdot \frac{\psi_{r-1}\psi_r}{\psi_{r-2}^2} \cdot A_{r-2}(Z) \cdot G_{r-1}(Z)\Bigg)\{i_2\} = 2(A_r(Z) \cdot G_r(Z))\{i_2\},$$

where the symbol $\{i_2\}$ denotes omitting all terms of degree more than 2.

Finally, we reformulate one of the central Cantor's theorems in our notation.

Theorem 2 ([4])**.** *If $r \geqslant 3$ then element $[r](\tilde{P}-\infty)$ in the Jacobian $\mathrm{Jac}_{\tilde{C}}(\bar{k})$ of the curve $\tilde{C}$ may be represented by the pair $(H_r(Z), E_r(Z))$, where*

$$E_r(Z) = 2y \cdot \frac{\psi_{r-1}\psi_{r+1}}{\psi_r^2} \cdot Z \cdot \left(\frac{(2y)^{r^2+r-2} H_{r+1}(Z)}{\psi_{r+1}^2} - \frac{(2y)^{r^2-3r} H_{r-1}(Z)}{\psi_{r-1}^2}\right) \ (\mathrm{mod}\, H_r(Z)).$$

Returning to the original curve C and divisor $[r](P-\infty)$ with $r \geqslant 3$, the Mumford–Cantor coordinates are the polynomials of the following form:

$$\delta_r(Z) = (2y)^{r^2-r-2} \cdot H_r(4y^2 Z),$$

$$\epsilon_r(Z) = \frac{y \cdot (\psi_{r-1}^2 \cdot \delta_{r+1}(Z) - \psi_{r+1}^2 \cdot \delta_{r-1}(Z)) \cdot Z}{\psi_{r-1} \cdot \psi_r^2 \cdot \psi_{r+1}} \ (\mathrm{mod}\ \delta_r(Z)).$$

4.1. Case $\ell = 3$

Consider a hyperelliptic curve $C/\mathbb{F}_p$ of genus $g = 2$ with equation

$$Y^2 = (X-2)(D_4(X,\alpha)+c) = X^5-2X^4-4\alpha X^3+8\alpha X^2+(2\alpha^2+c)X-4\alpha^2-2c,$$

where $D_4(X,\alpha) = X^4 - 4\alpha X^2 + 2\alpha^2$ is the Dickson polynomial. Set $\alpha = 1$, then our equation takes a form

$$Y^2 = X^5 - 2X^4 - 4X^3 + 8X^2 + (c+2)X + (-2c-4).$$

For a divisor $D = P_1 + P_2 - 2\infty$ with points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, we have a relation

$$[\ell]D = 0 \Leftrightarrow [\ell](P_1 - \infty) = -[\ell](P_2 - \infty).$$

For $\ell = 3$ we denote the Mumford–Cantor representation as

$$[3](P_1 - \infty) = \left(\delta_3\left(\frac{x_1 - X}{4y_1^2}\right), \epsilon_3\left(\frac{x_1 - X}{4y_1^2}\right)\right),$$

$$[3](P_2 - \infty) = \left(\delta_3\left(\frac{x_2 - X}{4y_2^2}\right), \epsilon_3\left(\frac{x_2 - X}{4y_2^2}\right)\right).$$

For simplicity we set

$$\begin{aligned} &[3](P_1 - \infty) \\ &\quad = \left(d_2(x_1, y_1)X^2 + d_1(x_1, y_1)X + d_0(x_1, y_1), e_1(x_1, y_1)X + e_0(x_1, y_1)\right), \end{aligned}$$

$$\begin{aligned} &[3](P_2 - \infty) \\ &\quad = \left(d_2(x_2, y_2)X^2 + d_1(x_2, y_2)X + d_0(x_2, y_2), e_1(x_2, y_2)X + e_0(x_2, y_2)\right), \end{aligned}$$

where d_2, d_1, d_0, e_1, e_0 are rational functions in variables x_i, y_i, $i = 1, 2$:

$$\begin{aligned} d_2 = -\frac{1}{4y^4}\Big(& 64x^{20} - 512x^{19} + 512x^{18} + 6144x^{17} + (256c - 16896)x^{16} + (-2048c - 20480)x^{15} \\ & + (120832 + 3072c)x^{14} + (-32768 + 16384c)x^{13} + (-391680 - 55808c + 384c^2)x^{12} \\ & + (-3072c^2 - 12288c + 380928)x^{11} + (6144c^2 + 253952c + 614400)x^{10} \\ & + (12288c^2 - 212992c - 999424)x^9 + (-439296c + 256c^3 - 59904c^2 - 374784)x^8 \\ & + (1228800 + 36864c^2 + 696320c - 2048c^3)x^7 \\ & + (129024c^2 + 5120c^3 + 192512c - 90112)x^6 \\ & + (-786432 - 786432c - 196608c^2)x^5 \\ & + (-19968c^3 - 23040c^2 + 230400 + 64c^4 + 149504c)x^4 \\ & + (253952 - 512c^4 + 28672c^3 + 184320c^2 + 376832c)x^3 \\ & + (-4096c^3 - 106496 - 147456c + 1536c^4 - 61440c^2)x^2 \\ & + (-65536c - 49152c^2 - 2048c^4 - 16384c^3 - 32768)x \\ & + 16384 + 8192c^3 + 1024c^4 + 24576c^2 + 32768c\Big), \end{aligned}$$

$$\begin{aligned}
d_1 = -\frac{1}{4y^4}\Big(& -128x^{21} + 1024x^{20} - 1024x^{19} - 12288x^{18} + (33792 - 512c)x^{17} \\
& + (4096c + 95y^2 + 40960)x^{16} + (-608y^2 - 241664 - 6144c)x^{15} \\
& + (144y^2 + 65536 - 32768c)x^{14} + (783360 - 768c^2 + 111616c + 6464y^2)x^{13} \\
& + (24576c - 761856 + 6144c^2 + 60cy^2 - 9960y^2)x^{12} \\
& + (-1228800 - 12288c^2 - 26688y^2 - 507904c + 96cy^2)x^{11} \\
& + (70240y^2 - 3408cy^2 + 425984c - 24576c^2 + 1998848)x^{10} \\
& + (25216y^2 + 119808c^2 + 878592c + 11072cy^2 - 512c^3 + 749568)x^9 \\
& + (90c^2y^2 + 552cy^2 + 4096c^3 - 2457600 - 192024y^2 - 73728c^2 - 1392640c)x^8 \\
& + (-59520cy^2 - 10240c^3 + 180224 - 258048c^2 - 385024c + 104320y^2 + 480c^2y^2)x^7 \\
& + (142528y^2 + 393216c^2 + 98240cy^2 + 1572864c + 1572864 - 6992c^2y^2)x^6 \\
& + (-128c^4 + 23232c^2y^2 - 460800 + 39936c^3 \\
& - 134400y^2 - 20736cy^2 - 299008c + 46080c^2)x^5 \\
& + (-368640c^2 + 380c^3y^2 + 1024c^4 - 507904 - 69552cy^2 - 753664c \\
& - 15776y^2 - 57344c^3 - 30072c^2y^2)x^4 \\
& + (39296cy^2 - 3072c^4 + 122880c^2 - 2272c^3y^2 + 8192c^3 + 294912c \\
& + 32000y^2 + 212992 + 7104c^2y^2)x^3 \\
& + (65536 + 4096c^4 + 32768c^3 + 131072c + 4752c^3y^2 \\
& + 7872cy^2 + 16224c^2y^2 + 98304c^2 - 11136y^2)x^2 \\
& + (-65536c - 11136c^2y^2 + 2304cy^2 - 16384c^3 \\
& - 2048c^4 - 32768 - 49152c^2 - 3904c^3y^2 + 17920y^2)x \\
& + 888c^3y^2 - c^4y^2 - 9232y^2 - 5664cy^2 + 1256c^2y^2\Big),
\end{aligned}$$

$$\begin{aligned}
d_0 = -\frac{1}{4y^4}\Big(& 64x^{22} - 512x^{21} + 512x^{20} + 6144x^{19} + (-16896 + 256c)x^{18} \\
& + (-95y^2 - 20480 - 2048c)x^{17} \\
& + (120832 + 608y^2 + 3072c)x^{16} + (-32768 - 144y^2 + 16384c)x^{15} \\
& + (-391680 - 55808c - 6464y^2 + 384c^2)x^{14} \\
& + (-60cy^2 + 9960y^2 - 12288c - 3072c^2 + 380928)x^{13} \\
& + (6144c^2 + 40y^4 + 253952c + 26688y^2 - 96cy^2 + 614400)x^{12} \\
& + (-192y^4 - 999424 - 70240y^2 + 12288c^2 + 3408cy^2 - 212992c)x^{11} \\
& + (-11072cy^2 - 374784 + 256c^3 - 439296c - 160y^4 - 25216y^2 - 59904c^2)x^{10} \\
& + (-90c^2y^2 + 1920y^4 + 696320c - 2048c^3 - 552cy^2 + 36864c^2 + 192024y^2 + 1228800)x^9 \\
& + (5120c^3 + 192512c - 480c^2y^2 + 59520cy^2 - 40cy^4 \\
& - 90112 + 129024c^2 - 720y^4 - 104320y^2)x^8
\end{aligned}$$

$$
\begin{aligned}
&+(-786432-98240cy^2-8960y^4-196608c^2\\
&-142528y^2+640cy^4-786432c+6992c^2y^2)x^7\\
&+(-19968c^3+149504c+20736cy^2-23232c^2y^2+230400-23040c^2\\
&+64c^4+12672y^4-3136cy^4+134400y^2)x^6\\
&+(376832c+253952+184320c^2-380c^3y^2+15776y^2+2560y^4+69552cy^2\\
&+28672c^3+6400cy^4-512c^4+30072c^2y^2)x^5\\
&+(2272c^3y^2-106496-147456c-61440c^2-32000y^2-9760y^4+440c^2y^4\\
&-39296cy^2-7104c^2y^2-4000cy^4+1536c^4-4096c^3)x^4\\
&+(-2240c^2y^4-16384c^3-4752c^3y^2-49152c^2-32768+11136y^2-16224c^2y^2\\
&-3840cy^4+1280y^4-2048c^4-65536c-7872cy^2)x^3\\
&+(1024c^4+11136c^2y^2-2304cy^2+32768c+16384+24576c^2+3680c^2y^4\\
&+8192c^3-17920y^2+4480cy^4-5760y^4+3904c^3y^2)x^2\\
&+(-1664c^2y^4+1536cy^4+c^4y^2+5664cy^2+9232y^2+9728y^4-888c^3y^2-1256c^2y^2)x\\
&-1952cy^4+8c^3y^4-464c^2y^4-1984y^4\biggr),
\end{aligned}
$$

$$
\begin{aligned}
e_1=\frac{1}{(2y)^9}\biggl(&145x^{24}-1392x^{23}+2472x^{22}+16288x^{21}+(-1626c-59460)x^{20}\\
&+(20880c-89952)x^{19}\\
&+(689296-96568c)x^{18}+(116064c-459072)x^{17}\\
&+(-5649c^2+597564c-3226692)x^{16}\\
&+(81568c^2-2566528c+7090816)x^{15}+(-456816c^2+3031872c+659520)x^{14}\\
&+(1116480c^2+3700992c-20189952)x^{13}\\
&+(1684c^3-194792c^2-15568016c+25595680)x^{12}\\
&+(13344c^3-5577792c^2+18238848c+2370816)x^{11}\\
&+(-274800c^3+13458528c^2-5592384c-38119296)x^{10}\\
&+(1462208c^3-11625856c^2-8844032c+34221568)x^9\\
&+(8991c^4-3706056c^3-2898072c^2+15915744c+13631472)x^8\\
&+(-90672c^4+4540032c^3+12815232c^2-16344576c-46179072)x^7\\
&+(366920c^4-1101504c^3-7272256c^2+3210496c+20827264)x^6\\
&+(-738528c^4-3791616c^3-1289472c^2+16708608c+20058624)x^5\\
&+(-666c^5+692076c^4+4279152c^3+2916960c^2-17482272c-23493696)x^4\\
&+(4432c^5-51040c^4-798592c^3-1639168c^2+1038592c+3203584)x^3\\
&+(-10968c^5-466032c^4-1618368c^3+597120c^2+7773312c+7316736)x^2\\
&+(12000c^5+378048c^4+1364736c^3+75264c^2-4938240c-4924416)x
\end{aligned}
$$

$$+ (c^6 - 4916c^5 - 102468c^4 - 360800c^3 - 99088c^2 + 1047744c + 1087552)\Bigg),$$

$$\begin{aligned}
e_0 = \frac{1}{(2y^9)}\Bigg(& - 145x^{25}1392x^{24} - 2472x^{23} - 16288x^{22} + (1626c + 59460)x^{21} \\
&+ (88y^2 - 20880c + 89952)x^{20} + (-704y^2 + 96568c - 689296)x^{19} \\
&+ (480y^2 - 116064c + 459072)x^{18} \\
&+ (9600y^2 + 5649c^2 - 597564c + 3226692)x^{17} \\
&+ (-1448cy^2 - 17488y^2 - 81568c^2 + 2566528c - 7090816)x^{16} \\
&+ (17664cy^2 - 87552y^2 + 456816c^2 - 3031872c - 659520)x^{15} \\
&+ (-80512cy^2 + 333568y^2 - 1116480c^2 - 3700992c + 20189952)x^{14} \\
&+ (133632cy^2 - 138240y^2 - 1684c^3 + 194792c^2 + 15568016c - 25595680)x^{13} \\
&+ (2288c^2y^2 + 173248cy^2 - 1106496y^2 - 13344c^3 + 5577792c^2 - 18238848c - 2370816)x^{12} \\
&+ (-6272c^2y^2 - 1120768cy^2 + 2223616y^2 + 274800c^3 \\
&- 13458528c^2 + 5592384c + 38119296)x^{11} \\
&+ (-79552c^2y^2 + 1846528cy^2 - 1403648y^2 - 1462208c^3 + 11625856c^2 + 8844032c \\
&- 34221568)x^{10} + (535808c^2y^2 - 961536cy^2 - 822272y^2 - 8991c^4 \\
&+ 3706056c^3 + 2898072c^2 - 15915744c - 13631472)x^9 \\
&+ (11312c^3y^2 - 1333728c^2y^2 - 664000cy^2 + 3310976y^2 + 90672c^4 - 4540032c^3 \\
&- 12815232c^2 + 16344576c + 46179072)x^8 \\
&+ (-101120c^3y^2 + 1371648c^2y^2 + 834560cy^2 - 4626432y^2 - 366920c^4 + 1101504c^3 \\
&+ 7272256c^2 - 3210496c - 20827264)x^7 \\
&+ (354688c^3y^2 + 148736c^2y^2 - 581120cy^2 + 1080320y^2 + 738528c^4 + 3791616c^3 \\
&+ 1289472c^2 - 16708608c - 20058624)x^6 \\
&+ (-585216c^3y^2 - 1508352c^2y^2 + 1775616cy^2 + 4902912y^2 + 666c^5 - 692076c^4 - 4279152c^3 \\
&- 2916960c^2 + 17482272c + 23493696)x^5 \\
&+ (-712c^4y^2 + 355520c^3y^2 + 855872c^2y^2 - 1914112cy^2 - 4396160y^2 - 4432c^5 + 51040c^4 \\
&+ 798592c^3 + 1639168c^2 - 1038592c - 3203584)x^4 \\
&+ (5440c^4y^2 + 209408c^3y^2 + 470528c^2y^2 - 456704cy^2 - 1207296y^2 + 10968c^5 \\
&+ 466032c^4 + 1618368c^3 - 597120c^2 - 7773312c - 7316736)x^3 \\
&+ (-15392c^4y^2 - 413952c^3y^2 - 672512c^2y^2 + 1784832cy^2 + 3194368y^2 - 12000c^5 \\
&- 378048c^4 - 1364736c^3 - 75264c^2 + 4938240c + 4924416)x^2 \\
&+ (18816c^4y^2 + 199680c^3y^2 + 222208c^2y^2 - 905216cy^2 - 1402880y^2 - c^6 + 4916c^5 \\
&+ 102468c^4 + 360800c^3 + 99088c^2 - 1047744c - 1087552)x \\
&- 8c^5y^2 - 8272c^4y^2 - 33088c^3y^2 - 640c^2y^2 + 130432cy^2 + 130816y^2\Bigg).
\end{aligned}$$

Conclusion

In this paper we obtain explicit formulae for 3-division polynomials for the class of curves defined by the Dickson polynomials. This gives us an explicit description of the 3-torsion in the Jacobian of the curve and allows to find the points of order 3. Therefore, we can find $\#\mathrm{Jac}_C(\mathbb{F}_q) \pmod 3$. The formulae were obtained using Maple software. The source code may be found on the authors homepage[1].

In further works, we will use this formulae to describe isogenies of degree 3 for our class of curves with applications to the scheme of Flynn and Yan Bo Ti.

Acknowledgement: Semyon Novoselov gratefully acknowledges the support of Russian Foundation for Basic Research, research project №18-31-00244.

References

[1] Tate J., “Endomorphisms of Abelian varieties over finite fields”, *Invent. math.*, **2**:2 (1966), 134—144.

[2] Koblitz N., “Hyperelliptic cryptosystems”, *J. Cryptology*, **1**:3 (1989), 139—150.

[3] Pila J., “Frobenius maps of Abelian varieties and finding roots of unity in finite fields”, *Math. Comput.*, **55**:192 (1990), 745—763.

[4] Cantor D. G., “On the analogue of the division polynomials for hyperelliptic curves”, *J. reine und angew. Math.*, **447** (1994), 91—146.

[5] Lidl R., Mullen G. L., Turnwald G., *Dickson polynomials*, Longman Sci. & Tech., Harlow, Essex, England, 1993, 207 pp.

[6] Gaudry P., Schost É., “Modular equations for hyperelliptic curves”, *Math. Comput.*, **74**:249 (2005), 429—454.

[7] Gaudry P., Thomé E., Thériault N., Diem C., “A double large prime variation for small genus hyperelliptic index calculus”, *Math. Comput.*, **76**:257 (2007), 475—492.

[8] Novoselov S.A., *Counting points on hyperelliptic curves of type* $y^2 = x^{2g+1} + ax^{g+1} + bx$, 2019, arXiv: 1902.05992.

[9] Cantor D. G., “Computing in the Jacobian of a hyperelliptic curve”, *Math. Comput.*, **48**:177 (1987), 95—101.

[10] Flynn E.V., Yan Bo Ti, *Genus two isogeny cryptography*, Cryptology ePrint Archive, Report 2019/177, https://eprint.iacr.org/2019/177.

[11] Cohen H., Frei G. et al., *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, 2005, 848 pp.

[1] https://crypto-kantiana.com/ekaterina.malygina/