Indian J Pure Appl Math (2022) 53:989–992
https://doi.org/10.1007/s13226-021-00204-7

ORIGINAL RESEARCH

Supersingular elliptic curves over $\overline{\mathbb{F}}_5$

Nabila Belhamra

Received: 28 March 2021 / Accepted: 12 November 2021 / Published online: 29 November 2021

Abstract In this note we propose an explicit proof that there is a unique supersingular elliptic curve up to isomorphism over $\overline{\mathbb{F}}_5$, and its $\jmath$-invariant is equal to zero.

Keywords Supersingular elliptic curve · Torsion group · $\jmath$-invariant

1 Introduction

Let K be a perfect field of characteristic $p > 0$. An elliptic curve E/K is called supersingular if its endomorphism ring is an order in a quaternion algebra [2]. The determination of supersingular elliptic curves in a given finite characteristic p is considered by many mathematicians. The case $p = 2$ was treated by Washington [5], the case $p = 3$ was treated by Silverman [2] and for the the general case $p \geq 5$ we have various demontrations [3,4,7]. In this note we propose an explicit proof for the particular case $p = 5$, that is stated in the following theorem

Theorem 1 *There is a unique supersingular elliptic curve up to isomorphism over $\overline{\mathbb{F}}_5$, and its $\jmath$-invariant is equal to zero.*

Our proof is based on some explicit rational functions coming up from the explicit group law of elliptic curves, called division polynomials.

1.1 Statements

Let E/K be an elliptic curve defined by its Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with its point at infinity $\mathcal{O} = [0, 1, 0]$.

For ease of notations we define the following quantities

$$\begin{aligned} b_2 &= a_1^2 + 4a_2^2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6^2, \end{aligned}$$

Communicated by Eknath Ghate.

N. Belhamra (✉)
Algebra, USTHB, El Alia, Bab Ezzouar 16111, Algiers, Algeria
E-mail: belhamranabilaa@gmail.com

$$b_8 = \frac{1}{4}(b_2b_6 - b_4^2).$$

Let $n \geq 0$ be an integer. The multiplication by n-isogeny can be defined explicitly by rational functions ϕ_n, ψ_n, ω_n, called the n^{th} division polynomials

$$\begin{aligned}[n] : E &\to E\\ P &\mapsto [n]P = \left(\frac{\phi_n(P)}{\psi_n^2(P)}, \frac{\omega_n(P)}{\psi_n^3(P)}\right)\end{aligned}$$

The division polynomials ψ_n are defined recursively via [1]:

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

and for $m \geq 2$, we have

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geq 2, \tag{4}$$

$$\psi_{2m} = \psi_m\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+2}^2\right)/\psi_2, \quad m > 2, \tag{5}$$

and the polynomials ϕ_n are defined by [1]

$$\begin{aligned}
&\phi_0 = 1,\\
&\phi_1 = x,\\
&\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \quad n \geq 1.
\end{aligned}$$

These polynomials satisfy the following relation [1]:

$$\phi_r\psi_m^2 - \phi_m\psi_r^2 = \psi_{m-r}\psi_{m+r}, \quad 1 \leq r \leq m, \tag{6}$$

and for $p > 2$ the polynomial ω_n can be written as [1]

$$\omega_n = [(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)/\psi_2 - (a_1\phi_n + a_3\psi_n^2)\psi_n]/2 \tag{7}$$

The kernel of $[n]$, denoted by $E[n]$, is called the n-torsion subgroup of E. Every point in $E[n]$ is called a n-torsion point on E. We have the following theorem

Theorem 2 [2] *Let E/K be an elliptic curve. Then the p-torsion subgroup is either reduced to $\{\mathcal{O}\}$, or isomorphic to $\frac{\mathbb{Z}}{p\mathbb{Z}}$.*

There are many characterizations of supersingular elliptic curves. We give the following

Theorem 3 [6] *Let E/K be an elliptic curve. E is supersingular over $\overline{K}$ if and only if $E[p]$ is reduced to $\{\mathcal{O}\}$.*

The following proposition represents the key tool for our proof.

Proposition 4 [2]

(a) *Two elliptic curves E_1/K, E_2/K are isomorphic if and only if $\jmath(E_1) = \jmath(E_2)$.*
(b) *Let $\jmath \in \overline{K}$. There exists an elliptic curve defined over $K(\jmath)$ whose $\jmath$-invariant is equal to $\jmath$, denoted by $E_\jmath$ and defined as follows:*

$$\begin{aligned}
E_\jmath &: y^2 + xy = x^3 + \frac{36}{1728 - \jmath}x + \frac{1}{1728 - \jmath} \ \text{ if } \jmath \neq 0 \text{ and } \jmath \neq 1728,\\
E_0 &: y^2 + y = x^3,\\
E_{1728} &: y^2 = x^3 + x.
\end{aligned}$$

2 Proof of theorem 1

From Proposition 4 we have for all $\jmath \in \overline{\mathbb{F}}_5$, an elliptic curve $E_\jmath$ of $\jmath$-invariant equal to $\jmath$ is defined over $\overline{\mathbb{F}}_5$ as follows:

$$E_\jmath : y^2 + xy = x^3 + \frac{1}{3-j}x + \frac{1}{3-j} \text{ if } j \neq 0 \text{ and } \jmath \neq 3, \tag{8}$$

$$E_0 : y^2 + y = x^3, \tag{9}$$

$$E_3 : y^2 = x^3 + x. \tag{10}$$

The following change of variables

$$(x, y) \mapsto (x + 2, y + 2x - 1)$$

transforms the equation (8) into the following

$$y^2 = x^3 + \frac{2\jmath}{3-\jmath}x + \frac{\jmath}{3-\jmath}, \tag{11}$$

and the following change of variables

$$(x, y) \mapsto (x, y + 2)$$

transforms the equation (9) into the following

$$y^2 = x^3 - 1. \tag{12}$$

Now we require the following proposition

Proposition 5 *Let $\jmath \in \overline{\mathbb{F}}_5$. Let P be a point on $E_\jmath$. Then*

$$[5]P = \mathcal{O} \Leftrightarrow \psi_5(P) = 0.$$

Proof From (11), (10) and (12) we have for all $\jmath \in \overline{\mathbb{F}}_5$, the elliptic curve $E_\jmath$ is defined by an equation of the form

$$y^2 = x^3 + A_\jmath x + B_\jmath.$$

Let P be a point on $E_\jmath$. Then

$$[5]P = \mathcal{O} \Leftrightarrow [3]P = -[2]P \Leftrightarrow \frac{\phi_3(P)}{\psi_3(P)^2} = \frac{\phi_2(P)}{\psi_2(P)^2} \text{ and } \frac{\omega_3(P)}{\psi_3(P)^3} = -\frac{\omega_2(P)}{\psi_2(P)^3}. \tag{13}$$

From (6) we have

$$\frac{\phi_3(P)}{\psi_3(P)^2} = \frac{\phi_2(P)}{\psi_2(P)^2} \Leftrightarrow \phi_3(P)\psi_2(P)^2 - \phi_2(P)\psi_3(P)^2 = 0 \Leftrightarrow \psi_5(P) = 0,$$

and from (4) we have

$$\psi_5(P) = 0 \Leftrightarrow \psi_4(P)\psi_2(P)^3 - \psi_3(P)^3 = 0 \Leftrightarrow \frac{1}{\psi_2^3(P)} = \frac{\psi_4(P)}{\psi_3(P)^3}.$$

Therefore, from (7) we obtain

$$\frac{\omega_3(P)}{\psi_3(P)^3} = \frac{\psi_5(P)\psi_2(P)^2 - \psi_4(P)^2}{2\psi_2(P)\psi_3(P)^3} = \frac{-\psi_4(P)^2}{2\psi_2(P)\psi_3(P)^3} = \frac{-\omega_2(P)}{\psi_2(P)^3}.$$

Then the system given by (13) holds for $\psi_5(P) = 0$, which completes the proof. □

In the following theorem we prove that every non zero $\jmath$-invariant defines a non supersingular elliptic curve over $\overline{\mathbb{F}}_5$.

Theorem 6 *Every elliptic curve over $\overline{\mathbb{F}}_5$ of non zero j-invariant is not supersingular.*

Proof In view of Proposition 4 all the $\overline{\mathbb{F}}_5$ -isomorphic elliptic curves have the same j-invariant. Then it suffices to study the supersingularity of the elliptic curve E_j defined by the equation (11) if $j \in \overline{\mathbb{F}}_5^*\backslash\{3\}$, and by the equation (10) if $j = 3$.
Let $P = (x, y)$ be a point in $\mathbb{A}^2_{\overline{\mathbb{F}}_5}$. We have $P \in E_j[5]$ if and only if $P \in E_j$ and $[5]P = \mathcal{O}$. From Proposition 5, we have $\psi_5(x, y) = 0$, i.e.

$$\psi_5(x, y) = 0 \Leftrightarrow \psi_2^3(x, y)\psi_4(x, y) - \psi_3^3(x, y) = 0.$$

Therefore, we obtain

$$P \in E_j[5] \Leftrightarrow \begin{cases} y^2 = x^3 + \frac{2j}{3-j}x + \frac{j}{3-j}, \\ \psi_2^3(x, y)\psi_4(x, y) - \psi_3^3(x, y) = 0. \end{cases} \quad \text{if} \quad j \in \overline{\mathbb{F}}_5^*\backslash\{3\}, \tag{14}$$

$$P \in E_3[5] \Leftrightarrow \begin{cases} y^2 = x^3 + x, \\ \psi_2^3(x, y)\psi_4(x, y) - \psi_3^3(x, y) = 0. \end{cases} \tag{15}$$

From (1), (2) and (3) we get

$$(14) \Leftrightarrow \begin{cases} \frac{j}{3-j}x^{10} + \frac{j}{3-j}x^9 + \frac{4j^3}{(3-j)^3}x^5 + \frac{j^4}{(3-j)^4}x^2 + \left(\frac{j^6}{(3-j)^6} - \frac{2j^4}{(3-j)^5}\right) = 0, \\ y^2 = x^3 + \frac{2j}{3-j}x + \frac{j}{3-j}. \end{cases}$$

$$(15) \Leftrightarrow \begin{cases} 3x^{10} + 4 = 0, \\ y^2 = x^3 + x. \end{cases}$$

Since $\overline{\mathbb{F}}_5$ is algebraically closed, then the two systems given by (14) and (15) have solutions over $\overline{\mathbb{F}}_5$. Therefore, for all $j \in \overline{\mathbb{F}}_5^*$, $E_j[5]$ is larger than $\mathcal{O}$, which implies, by Theorem 3 that E_j is not supersingular over $\overline{\mathbb{F}}_5$. Thus we get the result. □

In the following theorem we prove that the zero j-invariant defines a supersingular elliptic curve over $\overline{\mathbb{F}}_5$.

Theorem 7 *Let E_0 be the elliptic curve defined by the equation (12). Then E_0 is supersingular over $\overline{\mathbb{F}}_5$.*

Proof Assume that E_0 is not supersingular over $\overline{\mathbb{F}}_5$. Then by Theorem 3 and Theorem 2, there exists a 5-torsion point $P = (x, y)$ on E_0. This implies that (x, y) satisfies the equation (12) and by Proposition 5 (x, y) satisfies also the following equation

$$\psi_5(x, y) = \psi_2^3(x, y)\psi_4(x, y) - \psi_3(x, y)^3 = 0.$$

From (1), (2), (3) and (12) we find that

$$\psi_2^3(x, y)\psi_4(x, y) - \psi_3(x, y)^3 = 0 \Leftrightarrow -1 = 0,$$

which is impossible, and then the group $E_0[5]$ must be reduced to $\{\mathcal{O}\}$. Thus E_0 is supersingular over $\overline{\mathbb{F}}_5$. □

In view of Theorem 6 every $\overline{\mathbb{F}}_5$-isomorphism class defined by a nonzero j-invariant is not supersingular, and by Theorem 6 the zero j-invariant defines a supersingular $\overline{\mathbb{F}}_5$-isomorphism class of elliptic curves. Thus, there exists a unique supersinular elliptic curve up to isomorphism over $\overline{\mathbb{F}}_5$ and its j-invariant is equal to zero. Thus We get the proof.

References

1. D. R. Kohel. Endomorphism rings of elliptic curves over finite fields. PhD thesis, University of California, Berkeley, 1996.
2. J. H. Silverman. The arithmetic of elliptic curves, volume 106. Springer Science and Business Media, 2009.
3. J. I. Igusa. Class number of a definite quaternion with prime discriminant. Proc. Nat. Acad. Sci. U.S.A., 44, 312-314, 1958.
4. J. B. Birch, W. Kuyk, Modular functions of one variable. IV, Lecture Notes in Mathematics, 476, Berlin, New York: Springer-Verlag, pp. 142-144, 1975.
5. L. C. Washington. Elliptic Curves: Number Theory and Cryptography, Second Edition. New York, 2003.
6. M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg, 14, 197-272, 1941.
7. N. D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over Q, Inventiones Mathematicae, 89 (3), 561-567, 1987.