On the p -th division polynomial

Josep González *

Abstract

By using the relations between supersingular elliptic curves defined over a finite field of characteristic $p > 3$ and the p -th division polynomial, we present a property about the reduction modulo a prime $p > 3$ of the p -th division polynomial based on a heuristic argument and numerical evidence. We prove this property determining the p -th division polynomial of supersingular elliptic curves. As a consequence of this result, we present a criterion to discard supersingular elliptic curves.

1 Introduction

Let E be an elliptic curve given by a Weierstrass equation defined over a field K of characteristic different from 2 and 3. For an odd prime p , the p -th division polynomial of E , $\psi_{E,p}(X)$, provides the X -coordinates of the nontrivial p -torsion points of E . If $\text{char}(K) \neq p$, then there are exactly $(p^2 - 1)/2$ of such X -coordinates. When $\text{char}(K) = p$, the elliptic curve E is ordinary or supersingular depending on whether the p -torsion group is cyclic of order p or trivial. In the ordinary case, the p -th division polynomial of E has $(p - 1)/2$ roots and, in the supersingular case, $\psi_{E,p}(X)$ is a nonzero constant lying in K . The goal of this paper is to study the relationship between supersingular elliptic curves in characteristic $p > 3$ and the p -division polynomials.

The article is organized as follows. In section 2, we recall some general facts on supersingular elliptic curves and we present two properties about these curves. One of them concerns the roots of the Deuring polynomial in Proposition 2.1 and the other the j -invariant of a supersingular elliptic curve in Proposition 2.2. Moreover, in Corollary 2.1 we present a property of the polynomial $Q(A, B) \in \mathbb{F}_p[A, B]$ whose zeros characterize the supersingular elliptic curves given by equations of the form $Y^2 = X^3 + AX + B$.

In section 3, we investigate the relationship between elliptic curves in characteristic $p > 3$ and the p -th division polynomial of elliptic curves. From these relations, we derive congruences between modular forms for the group $\text{SL}_2(\mathbb{Z})$. Based on a heuristic argument and numerical evidence, in Theorem 3.1 we present a property of the reduction modulo p of the p -th division polynomial. By using the property stated for the polynomial $Q(A, B)$ in section 2, we show that this theorem is equivalent to determine the p -th division polynomial for supersingular elliptic curves. More precisely, it is equivalent to Theorem 3.2, where it is stated that for a supersingular elliptic curve $E : Y^2 = X^3 + AX + B$, one has

$$\psi_{E,p} = (-1)^{(p-1)/2} \left(A^3 + \frac{27}{4} B^2 \right)^{(p^2-1)/12}.$$

We show that it suffices to prove this theorem for supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ and, for these curves, we prove that the p -th division polynomial can

**Keywords:* supersingular elliptic curves, division polynomials.
2020 Mathematics Subject Classification: 11F03, 14H52.

be viewed as an automorphism of the curve that links the Frobenius endomorphism Frob_{p^2} with the p -multiplication. Next, the proof of Theorem 3.2 is split in three propositions according to the order of the automorphism group $\text{Aut}(E)$. As a consequence of the results obtained, in Corollary 3.2 we present a criterion to discard supersingular elliptic curves.

2 Supersingular elliptic curves

Let K be a field such that $\text{char}(K) \neq 2$ and let E be an elliptic curve defined over K with j -invariant $j(E)$. There exists $\lambda \in \overline{K} \setminus \{0, 1\}$ such that

$$j(E) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

As usual, $\overline{K}$ denotes an algebraic closure of K . The elliptic curve E_λ defined by the equation

$$y^2 = x(x - 1)(x - \lambda), \quad (1)$$

is isomorphic to E , i.e. $j(E_\lambda) = j(E)$. Equation (1) is called the Legendre equation.

The map $\overline{K} \setminus \{0, 1\} \rightarrow \overline{K}$, $\lambda \mapsto j(E_\lambda)$ is surjective and the set of pre-images of a value of $j \in \overline{K}$ is

$$\{\lambda, 1/\lambda, 1 - \lambda, 1/(1 - \lambda), \lambda/(\lambda - 1), (\lambda - 1)/\lambda\}.$$

For every value $j \neq 0, 1728$, there are exactly six values of λ . If $\text{char}(K) \neq 3$, then for $j = 0$ there are exactly two values of λ that are the roots of the polynomial $x^2 - x + 1$, while for $j = 1728$ there are the following three values $\lambda \in \{-1, 2, 1/2\}$. When $\text{char}(K) = 3$, then $1728 = 0$ and the only value is $\lambda = -1$.

Now, let E be an elliptic curve defined over a field K with $\text{char}(K) = p > 2$. The curve E is said to be supersingular if the group of points of p -torsion is trivial, i.e. $E[p](\overline{K}) \simeq \{0\}$. It is known that

- (i) If E is supersingular, then $j(E) \in \mathbb{F}_{p^2}$ and the algebra $\text{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra.
- (ii) If E is given by an equation of the form $Y^2 = f(X)$, where $f(X) \in K[X]$ has distinct roots and its degree is 3, then E is supersingular if and only if the coefficient of the monomial X^{p-1} in the polynomial $f(X)^{(p-1)/2}$ is zero.
- (iii) Two supersingular elliptic curves defined over K are $\overline{K}$ -isogenous.
- (iv) The number of supersingular j -invariants is equal to $g+1$, where g is the genus of the modular curve $X_0(p)$. In particular, for $p > 3$ this number agrees with $\lfloor (p-1)/12 \rfloor + \epsilon_p$, where ϵ_p is 0, 1, 1, 2 according to whether $p \equiv 1, 5, 7, 11 \pmod{12}$, respectively.

For instance, for (i), (ii) and (iii) see Chapter V in [Sil86] and for (iv) cf. (2) in [Ogg78]. When part (ii) is applied to a Legendre equation, we obtain that E_λ is supersingular if and only if λ is a root of the polynomial

$$H_p(x) := \sum_{i=0}^r \binom{r}{i}^2 x^i \in \mathbb{F}_p[x], \quad \text{where } r = \frac{p-1}{2},$$

because $(-1)^r H_p(\lambda)$ is the coefficient of x^r in the polynomial $((x-1)(x-\lambda))^r$. The polynomial $H_p(x)$ is called the Deuring polynomial and has the following properties (cf. [Sil86]):

(i) The polynomial $H_p(x)$ has distinct roots and satisfies the differential equation

$$x(1-x)y'' + (1-2x)y' - \frac{y}{4} = 0. \quad (2)$$

(ii) $H_p(x)$ has the factor $x^2 - x + 1$ if and only if $p \equiv 2 \pmod{3}$ and the factor $(x+1)(x-2)(x-1/2)$ if and only if $p \equiv 3 \pmod{4}$. In other words, for $p > 3$ the j -invariants 0 and 1728 are supersingular if and only if $p \equiv 2 \pmod{3}$ and $p \equiv 3 \pmod{4}$ respectively.

(iii) One has

$$H_p(x) = x^r H_p(1/x) \quad \text{and} \quad H_p(1-x) = (-1)^r H_p(x).$$

In Proposition 1 of [BM04], it is proved that if E_λ is supersingular, then $\lambda \in \mathbb{F}_{p^2}$, i.e. $|E_\lambda[2](\mathbb{F}_{p^2})| = 4$. The following property of the Deuring polynomial will allow us to generalize this proposition.

Lemma 2.1 *The polynomial $H_p(x)$ satisfies the following property*

$$H_p(1-x^2) = H_p\left(\left(\frac{1-x}{1+x}\right)^2\right) (1+x)^{p-1}.$$

Proof. Consider the elliptic curve E_{λ^2} for some $\lambda \in \overline{\mathbb{F}_p} \setminus \{0, \pm 1\}$. Let us denote by $E/\overline{\mathbb{F}_p}$ the elliptic curve defined by

$$Y^2 = X(X - (1+\lambda)^2)(X - (1-\lambda)^2) = X^3 - 2(1+\lambda^2)X^2 + (1-\lambda^2)^2X,$$

that is isomorphic to $E_{(\frac{1-\lambda}{1+\lambda})^2}$.

Let $\phi : E_{\lambda^2} \rightarrow E$ be the isogeny of degree 2 defined by $(X, Y) \mapsto (\frac{Y^2}{X^2}, \frac{Y(\lambda^2 - X^2)}{X^2})$. Since E and E_{λ^2} are isogenous, one has that E is supersingular if and only if E_{λ^2} is supersingular. The assignment $\lambda \mapsto \frac{1-\lambda}{1+\lambda}$ is a bijective map of the set $\overline{\mathbb{F}_p} - \{0, 1, -1\}$ onto itself. Therefore, the polynomial $H_p(x^2)$ has the same roots as the polynomial $H_p((\frac{1-x}{1+x})^2)(1+x)^{p-1}$. Since the polynomial $H_p(x^2)$ is monic, the polynomial $(-1)^r H(1-x^2)$ is monic too and, thus, it coincides with the monic polynomial $(-1)^r H_p((\frac{1-x}{1+x})^2)(1+x)^{p-1}$.

Next, we show an alternative proof for this property without using isogenies. Firstly, by applying the fact that $H_p(x)$ satisfies the differential equation (2), it can be checked that the polynomials

$$G(x) := (-1)^r H_p\left(\left(\frac{1-x}{1+x}\right)^2\right) (1+x)^{p-1}, \quad F(x) := H_p(x^2)$$

satisfy the differential equation

$$y'' + \frac{1-3x^2}{x(1-x^2)}y' - \frac{y}{1-x^2} = 0. \quad (3)$$

We have that

$$F(i) = G(i) = H_p(-1) \quad \text{and} \quad F'(i) = G'(i) = 2iH_p'(-1),$$

for $i \in \mathbb{F}_{p^2}$ such that $i^2 = -1$. Since $F(x)$ and $G(x)$ satisfy (3), both polynomials have the same successive derivatives at i and, thus, $F(x) = G(x)$. $\square$

Proposition 2.1 *If E_λ is supersingular, then $|E_\lambda[4](\mathbb{F}_{p^2})| \equiv 0 \pmod{8}$ and λ is a square in $\mathbb{F}_{p^2}$.*

Proof. The point $(\sqrt{\lambda}, (-1 + \sqrt{\lambda})\sqrt{-\lambda})$ lies in $E_\lambda[4] \setminus E_\lambda[2]$. Hence, if λ is a square in $\mathbb{F}_{p^2}$, then $|E_\lambda[4](\mathbb{F}_{p^2})| \equiv 0 \pmod{8}$. Now, assume that E_λ is supersingular. Let $u \in \overline{\mathbb{F}}_p$ such that $u^2 = \lambda$. By the above lemma, $\left(\frac{1-u}{1+u}\right)^2$ is a root of $H_p(x)$. We get

$$\left(\frac{1-u}{1+u}\right)^2 = \frac{1+\lambda-2u}{1+\lambda+2u} \in \mathbb{F}_{p^2},$$

and, thus, $u \in \mathbb{F}_{p^2}$. $\square$

For a supersingular elliptic curve E_λ , λ is a square in $\mathbb{F}_{p^2}$ but its j -invariant has a different property.

Proposition 2.2 *Let $\tilde{j} \in \mathbb{F}_{p^2}$ be a supersingular j -invariant. Then, $\tilde{j}$ is a cube in $\mathbb{F}_p(\tilde{j})$.*

Proof. The ring $\mathcal{Q} := \text{End}_{\mathbb{F}_{p^2}} \tilde{E}$ is a maximal order of a quaternion algebra of discriminant p (cf. Theorem 10.6 in [Was08]). Let D be the discriminant of an imaginary quadratic field coprime to 3 and such that p is inert in $\mathbb{Q}(\sqrt{D})$. Hence, the order $\mathbb{Z}[\sqrt{D}]$ can be embedded in $\mathcal{Q}$ and there is $\tilde{\alpha} \in \mathcal{Q}$ such that $\tilde{\alpha}^2 = D$. By Chapter 13, Theorem 14 in [Lan87], there is an elliptic curve E defined over a number field and an endomorphism $\alpha \in \text{End } E$ whose reductions at a prime $\mathfrak{P}$ over p are $\tilde{E}$ and $\tilde{\alpha}$ respectively. By Theorem 12.2 in [Cox89], there is an algebraic integer j_0 such that $j(E) = j_0^3$ and $\mathbb{Q}(j(E)) = \mathbb{Q}(j_0)$. Hence, if $\tilde{j}_0$ denotes the reduction of j_0 at $\mathfrak{P}$, then $\tilde{j} = \tilde{j}_0^3$ and $\mathbb{F}_p(\tilde{j}) = \mathbb{F}_p(\tilde{j}_0)$. $\square$

In Theorem 2.4 of [Mor11], it is proved that a supersingular j -invariant is a cube in $\mathbb{F}_{p^2}$. The above proposition adds that if $j \in \mathbb{F}_p$, then j is a cube in $\mathbb{F}_p$.

Now, we describe the characterization of the supersingular elliptic curves given by short Weierstrass equations. Set

$$Q(U, V) := \sum_{k=\lfloor \frac{r+1}{2} \rfloor}^{\lfloor \frac{p-1}{3} \rfloor} U^{2r-3k} V^{2k-r} \binom{r}{2r-2k} \binom{2r-2k}{k} \in \mathbb{F}_p[U, V], \quad (4)$$

where $r = (p-1)/2$.

An elliptic curve E defined by an equation of the form $Y^2 = X^3 + AX + B$ with $A, B \in \overline{\mathbb{F}}_p$ is supersingular if and only if $Q(A, B) = 0$ because the value of the coefficient of X^{p-1} in the polynomial $(X^3 + AX + B)^{\frac{p-1}{2}}$ is

$$\sum_{\substack{0 \leq k \leq i \leq r \\ 2k+i=p-1}} A^{i-k} B^{r-i} \binom{r}{i} \binom{i}{k} = \sum_{k=\lfloor \frac{r+1}{2} \rfloor}^{\lfloor \frac{p-1}{3} \rfloor} A^{2r-3k} B^{2k-r} \binom{r}{2r-2k} \binom{2r-2k}{k}.$$

Lemma 2.2 *The polynomial $Q(U, V)$ is square-free. Moreover, if $Q(A, B) = 0$ for $(A, B) \neq (0, 0)$, then $4A^3 + 27B^2 \neq 0$.*

Proof. Transforming the Legendre equation into short Weierstrass form, we get that the elliptic curve E_λ is isomorphic to $E : Y^2 = X^3 + AX + B$ for

$$A = \frac{1}{3}(-1 + \lambda - \lambda^2) \text{ and } B = -\frac{1}{27}(-2 + \lambda)(1 + \lambda)(-1 + 2\lambda).$$

Since $A^{2r-3k}B^{2k-r}$ is a polynomial in λ of degree r , the degree of $Q(A, B)$ in λ is at most r . Due to the fact that $H_p(x)$ has no double roots, $Q(A, B)$ must be $aH_p(\lambda)$ for some $a \in \mathbb{F}_p^*$ and all non constant factors of $Q(U, V)$ are square-free. Moreover, the irreducible polynomial $4U^3 + 27V^2$ does not divide $Q(U, V)$ because $4A^3 + 27B^2 = -(\lambda - 1)^2\lambda^2$ and 0 and 1 are not roots of $H_p(x)$.

The set $S = \{(A, B) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p : Q(A, B) = 0, 4A^3 + 27B^2 = 0\}$ is finite because the polynomial $4U^3 + 27V^2$ does not divide $Q(U, V)$. If $4A^3 + 27B^2 = 0$, then $X^3 + AX + B = (X - a)^2(X - b)$ for some $a, b \in \overline{\mathbb{F}}_p$. Hence, $b = -2a$, $A = -3a^2$ and $B = 2a^3$. One has

$$Q(A, B) = a^r \left(\sum_{k=\lfloor \frac{r+1}{2} \rfloor}^{\lfloor \frac{p-1}{3} \rfloor} (-3)^{2r-3k} 2^{2k-r} \binom{r}{2r-2k} \binom{2r-2k}{k} \right).$$

Since S is finite, if $Q(A, B) = 0$, then a must be zero and, thus, $(A, B) = (0, 0)$. $\square$

By Hilbert's Nullstellensatz, we obtain the following result.

Corollary 2.1 *Let $P(U, V) \in \overline{\mathbb{F}}_p[U, V]$ be such that $P(0, 0) = 0$. If $P(A, B) = 0$ for all pairs $(A, B) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$ such that $Y^2 = X^3 + AX + B$ is a supersingular elliptic curve, then $Q(U, V)$ divides $P(U, V)$.*

The roots of the polynomial $H_p(x)$ provide the values λ corresponding to the supersingular elliptic curves E_λ . In the next proposition, we show that the polynomial $Q(U, V)$ can be used to get the j -invariants of such curves.

Proposition 2.3 *Assume $p > 3$. Consider the polynomial*

$$J_p(z) = \sum_{k=\lfloor \frac{p+1}{4} \rfloor}^{\lfloor \frac{p-1}{3} \rfloor} \left(-\frac{4}{27} \right)^k \binom{r}{2r-2k} \binom{2r-2k}{k} z^{\lfloor \frac{p-1}{3} \rfloor - k} \in \mathbb{F}_p[z].$$

The roots of $J_p(z)$ provide the values $\frac{j}{j-1728}$ for the j -invariants of supersingular elliptic curves such that $j \neq 0, 1728$.

Proof. For $j \neq 0, 1728$, the elliptic curve E given by the equation

$$Y^2 = X^3 + AX + A, \quad \text{with} \quad A = -\frac{27}{4} \frac{j}{j-1728}$$

has $j(E) = j$. Put $z = \frac{j}{j-1728}$. Then, E is supersingular if and only if $Q(A, A) = 0$, i.e. $z^{r-\lfloor \frac{p-1}{3} \rfloor} J_p(z) = 0$. The degree of the polynomial $J_p(z)$ is $\lfloor \frac{p-1}{3} \rfloor - \lfloor \frac{p+1}{4} \rfloor = \lfloor \frac{p-1}{12} \rfloor$. The statement follows from the fact that this degree is equal to the number of supersingular j -invariants different from 0 and 1728. $\square$

3 Division Polynomials

Let E be an elliptic curve defined over an algebraically closed field K of characteristic $\neq 2, 3$ given by an equation of the form $Y^2 = X^3 + AX + B$ with $A, B \in K$. We denote by O the origin of E and $(x(Q), y(Q))$ denote the affine coordinates of the point $Q \in E(K) \setminus \{O\}$.

By the Riemann-Roch theorem, every function on E that is regular away from O belongs in $K[X] \oplus YK[X]$. As in [Sil86], for each integer $m > 0$ the polynomials $\psi_{E,m} \in \mathbb{Z}[A, B, X] \oplus Y\mathbb{Z}[A, B, X]$ denote the m -division polynomials for E . These polynomials, viewed as functions on E , have a unique pole at O and their zeros are

all the points $Q \in E[m] \setminus \{O\}$. One has that $\psi_{E,m} \in \mathbb{Z}[A, B, X]$ if m is odd and $\psi_{E,m} \in Y\mathbb{Z}[A, B, X]$ when m is even. The polynomials $\psi_{E,m}$ are determined by the values:

$$\psi_{E,m} = \begin{cases} 1 & \text{if } m = 1, \\ 2Y & \text{if } m = 2, \\ 3X^4 + 6AX^2 + 12BX - A^2 & \text{if } m = 3, \\ 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3) & \text{if } m = 4, \end{cases}$$

and by the recursive relations

$$\begin{aligned} \psi_{E,2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 & \text{if } m \geq 2, \\ 2Y\psi_{E,2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) & \text{if } m \geq 3. \end{aligned}$$

The polynomials $\psi_{E,m}(X, Y)$ can be written as follows:

$$\psi_{E,m}(X, Y) = \begin{cases} \sum_{i=0}^{(m^2-1)/2-1} a_i X^i + m X^{\frac{m^2-1}{2}} & \text{if } m \text{ is odd,} \\ Y(\sum_{i=0}^{m^2/2-3} a_i X^i + m X^{\frac{m^2}{2}-2}) & \text{if } m \text{ is even.} \end{cases} \quad (5)$$

If $\text{char}(K) = 0$, then $\text{div } \psi_{E,m} = \sum_{Q \in E[m] \setminus \{O\}} (Q) - (m^2 - 1)(O)$ and for m odd we have

$$\psi_{E,m}^2(X) = m^2 \prod_{Q \in E[m] \setminus \{O\}} (X - x(Q)).$$

Note that for an odd integer $m > 1$, the m -th division polynomial can be considered as a polynomial in 3 variables, that is $\psi_m(X, A, B) \in \mathbb{Z}[X, A, B]$, that satisfies $\psi_m(X, 0, 0) = m X^{(m^2-1)/2}$. The following statement is well-known (for instance see Lemma 3 in [Dol18]).

Proposition 3.1 *Let $p > 3$ be a prime and assume that $\tilde{E}$ is an elliptic curve defined over $\mathbb{F}_p$ given by the equation $Y^2 = X^3 + \tilde{A}X + \tilde{B}$. Let*

$$\psi_{\tilde{E},p}(X) = \psi_p(X, \tilde{A}, \tilde{B}) = \sum_{i=0}^{(p^2-1)/2-1} \tilde{a}_i X^i.$$

Then

- (i) *One has $\tilde{a}_i = 0$ for all $i \not\equiv 0 \pmod{p}$.*
- (ii) *$\tilde{E}$ is ordinary if and only if $\tilde{a}_{(p^2-p)/2} \neq 0$. Otherwise $\psi_{\tilde{E},p}(X) = \tilde{a}_0 \neq 0$.*

This proposition can be argued as follows. There exists a number field K with a prime $\mathfrak{P}$ over p for which there are $A, B \in K$ such that their reductions modulo $\mathfrak{P}$ are $\tilde{A}$ and $\tilde{B}$ respectively. The p -th division polynomial of the elliptic curve $E : Y^2 = X^3 + AX + B$ is $\psi_{E,p} = \sum_{i=0}^{(p^2-1)/2-1} a_i X^i + p X^{\frac{p^2-1}{2}}$, where the reduction modulo $\mathfrak{P}$ of a_i is $\tilde{a}_i$. Let C be the kernel of the homomorphism $\pi : E[p] \rightarrow \tilde{E}[p]$ provided by the reduction modulo $\mathfrak{p}$. If $\tilde{E}$ is ordinary, then $\tilde{E}[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and the same occurs for the group C . In this case, the $\mathfrak{P}$ -adic valuation $v_{\mathfrak{P}}(x(Q))$ is < 0 for all $Q \in C \setminus \{O\}$ and ≥ 0 for all $Q \in E[p] \setminus C$. Therefore, every point in $\tilde{E}[p]$ has p pre-images and, thus,

$$\psi_{\tilde{E},p}^2 = \tilde{a}_{(p^2-p)/2}^2 \left(\prod_{\tilde{Q} \in \tilde{E}[p] \setminus \{\tilde{O}\}} (X - x(\tilde{Q})) \right)^p.$$

If $\tilde{E}$ is supersingular, then $C = E[p]$ and $\psi_{\tilde{E},p} = \tilde{a}_0$ that must be non zero, because there is not any point $\tilde{Q} \in \tilde{E} \setminus \{\tilde{O}\}$ satisfying $\psi_{\tilde{E},p}(x(\tilde{Q})) = 0$.

Let $b_i(A, B) \in \mathbb{F}_p[A, B]$ be the coefficient of $X^{p((p-1)/2-i)}$, $0 \leq i \leq (p-3)/2$, in the polynomial $\psi_p(X, A, B) \pmod{p}$. By Corollary 2 in [Deb14], we know that $b_0(A, B) = Q(A, B)$, where $Q(U, V)$ is the polynomial defined in (4). We have that $b_i(0, 0) = 0$ and for all pairs $(a, b) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$ such that $Y^2 = X^3 + aX + b$ is a supersingular elliptic curve one has $b_i(a, b) = 0$. By Corollary 2.1, $Q(A, B)$ divides $b_i(A, B)$ and we have

$$\psi_p(X) \equiv Q(A, B) \left(X^{p((p-1)/2)} + \sum_{i=1}^{(p-3)/2} a_i(A, B) X^{p((p-1)/2-i)} \right) + c(A, B) \pmod{p}, \quad (6)$$

for some $a_i(A, B), c(A, B) \in \mathbb{Z}[A, B]$.

Now, we will review this result from the point of view of modular forms.

3.1 Modular forms

Let E be an elliptic curve defined over $\mathbb{C}$. By the uniformization theorem for elliptic curves, we can take an equation for E of the form

$$Y^2 = X^3 + AX + B,$$

such that there is τ in the upper half-plane satisfying

$$\left(\frac{\wp(z; \tau)'}{2} \right)^2 = \wp(z; \tau)^3 + A\wp(z; \tau) + B,$$

where $\wp(z; \tau)$ is the Weierstrass $\wp$ -function for the lattice $\langle 1, \tau \rangle$, $A = -g_2(\tau)/4$ and $B = -g_3(\tau)/4$. Here, g_2 and g_3 denote the usual modular functions of weight 4 and 6 for the group $\Gamma(1) = \text{SL}_2(\mathbb{Z})$. Let p be a prime > 3 . We have

$$\psi_{E,p}^2(X) = p^2 \prod_{\substack{0 \leq i, j \leq p^2-1, \\ i+j \neq 0}} \left(X - \wp\left(\frac{i\tau + j}{m}; \tau\right) \right).$$

On the one hand

$$\psi_{E,p}^2(X) = p^2 \left(X^{p^2-1} + \sum_{j=1}^{p^2-1} (-1)^j S_j(\tau) X^{p^2-1-j} \right),$$

and we get $p^2 - 1$ functions $S_j(\tau)$. On the other hand

$$\psi_{E,p}^2(X) \in \mathbb{Z}[X, g_2(\tau)/4, g_3(\tau)/4].$$

Hence, for every $1 \leq j \leq p^2 - 1$ there is $P_j \in \mathbb{Z}[U, V]$ such that

$$p^2 \cdot S_j(\tau) = P_j(g_2(\tau)/4, g_3(\tau)/4).$$

It is known that

$$\wp(z; \tau) = \frac{1}{z^2} + \sum_{n \geq 1} (2n+1) G_{2n+2}(\tau) z^{2n},$$

where $G_{2k}(\tau)$ is the Eisenstein series of weight $2k$ for the lattice $\langle 1, \tau \rangle$. By using this fact, it can be checked that the function $S_j(\tau)$ satisfies $S_j(\tau+1) = S_j(\tau)$

and $S_j(-1/\tau) = S_j(\tau)\tau^{2j}$, i.e. it is a modular function of weight $2j$ for the group $\Gamma(1)$. In particular, $P_1(U, V) = 0$ because there are no non-trivial modular forms of weight 2 for $\Gamma(1)$; an alternative reasoning for this assertion can be found in the proof of Proposition 2.2 in [Gon00]. For $j > 1$, $P_j(U, V)$ is a linear combination of polynomials of the form $U^k V^s$ with $2r + 3s = j$, since the set $\{g_2^k g_3^s : 2k + 3s = j\}$ is a $\mathbb{C}$ -basis of the modular forms of weight $2j$ for $\Gamma(1)$.

Note that

$$\psi_{E,p}(X) = p \left(X^{(p^2-1)/2} + \sum_{j=1}^{(p^2-1)/2} (-1)^j s_j(\tau) X^{(p^2-1)/2-j} \right),$$

and $s_j(\tau)$ is also a modular function of weight $2j$ for the group $\Gamma(1)$.

By applying Proposition 3.1, we obtain the following congruences modulo p .

Proposition 3.2 *Let $Q(U, V) \in \mathbb{F}_p[U, V]$ be as in (4), that is*

$$Q(U, V) = \sum_{k=\lfloor \frac{r+1}{2} \rfloor}^{\lfloor \frac{p-1}{3} \rfloor} U^{2r-3k} V^{2k-r} \binom{r}{2r-2k} \binom{2r-2k}{k},$$

where $r = (p-1)/2$. With the above notation, we have

- (i) $P_j(U, V) \equiv 0 \pmod{p}$ when $j \not\equiv -1 \pmod{p}$.
- (ii) $\psi_p(X) \equiv a Q(A, B) X^{p(p-1)/2} + (\text{lower order terms in } X^p) \pmod{p}$, for some $a \in \mathbb{F}_p^*$. In particular, one has

$$P_{p-1}(U, V) \equiv a^2 Q(U, V)^2 \pmod{p}.$$

Proof. We recall that the elliptic curve $Y^2 = X^3 + AX + B$ defined over $\overline{\mathbb{F}}_p$ is supersingular if and only if $Q(A, B)$ is equal to zero, because it is the coefficient of X^{p-1} in $(X^3 + AX + B)^r$. By applying Proposition 3.1 and Corollary 2.1, we obtain

$$\psi_p(X, A, B) \equiv a(A, B) Q(A, B) X^{p(p-1)/2} + (\text{lower order terms in } X^p) \pmod{p},$$

for some polynomial $a(A, B) \in \mathbb{Z}[A, B]$ that is non zero modulo p . Therefore, $p^2 S_j \equiv 0 \pmod{p}$ when $j \not\equiv -1 \pmod{p}$ and $p^2 S_{p-1} \equiv a(A, B)^2 Q(A, B)^2 \pmod{p}$ for some $a(A, B) \in \mathbb{Z}[A, B]$. Since we can view A and B as modular forms of weight 4 and 6 respectively, $Q(A, B)^2$ has weight $2(p-1)$, because

$$4(2r-3k) + 6(2r-k) = 2r = p-1.$$

Hence, $a(A, B)$ must have weight zero and, thus, $a(A, B) \pmod{p} \in \mathbb{F}_p^*$. $\square$

Note that part (ii) is a weak version of Corollary 2 in [Deb14] (there $a = 1$) already used in (6), proved in a simpler way with arguments involving modular forms.

Now, we consider the congruence (6), i.e.

$$\psi_p(X) \equiv Q(A, B) \left(X^{p(p-1)/2} + \sum_{i=1}^{(p-3)/2} a_i(A, B) X^{p((p-1)/2-i)} \right) + c(A, B) \pmod{p},$$

for $a_i(A, B), c(A, B) \in \mathbb{Z}[A, B]$. When $Q(A, B) = 0$, $c(A, B) \pmod{p}$ must be non zero. Since $c(A, B)$ has weight $p^2 - 1$ viewed as a modular form and the discriminant of the elliptic curve E has weight 12, it is reasonable to think that

$$c(A, B) \equiv a_{(p-1)/2}(A, B) Q(A, B) + b(4A^3 + 27B^2)^{(p^2-1)/12} \pmod{p} \quad (7)$$

for some $a_{(p-1)/2}(A, B) \in \mathbb{Z}[A, B]$ and $b \in \mathbb{F}_p^*$.

The computations made by J.-C. Lario and the author for primes $p \leq 59$ provide that the congruence (7) is satisfied for $b = (-1)^{(p-1)/2} 4^{(1-p^2)/12}$.

3.2 The p -th division polynomial modulo p

The above computations lead us to formulate the following statement.

Theorem 3.1 *For a prime $p > 3$, let $Q(U, V) \in \mathbb{F}_p[U, V]$ be as in Proposition 3.2. The polynomial $\psi_p(X, A, B) \pmod{p}$ agrees with the polynomial*

$$Q(A, B) \left(X^{p(p-1)/2} + \sum_{i=1}^{(p-1)/2} a_i(A, B) X^{p((p-1)/2-i)} \right) + \left(\frac{-1}{p} \right) \left(A^3 + \frac{27}{4} B^2 \right)^{(p^2-1)/12}$$

modulo p , for some polynomials $a_i(A, B) \in \mathbb{Z}[A, B]$ and where $\left(\frac{-1}{p} \right)$ denotes the Legendre symbol.

The polynomial $c(A, B)$ in (6) satisfies $c(0, 0) = 0$. By Corollary 2.1, the above theorem is equivalent to the following statement.

Theorem 3.2 *Let $E : Y^2 = X^3 + A X + B$ be a supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$. One has*

$$\psi_{E,p} = \left(\frac{-1}{p} \right) \left(A^3 + \frac{27}{4} B^2 \right)^{(p^2-1)/12}.$$

For every pair $(A, B) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$ such that the elliptic curve $E : Y^2 = X^3 + A X + B$ is supersingular, there exists $\delta \in \overline{\mathbb{F}}_p$ such that $(A \delta^2, B \delta^3) \in \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}$ because $j(E) \in \mathbb{F}_{p^2}$. Moreover, the map $(x, y) \mapsto (\delta x, \delta^{3/2} y)$ provides an isomorphism between E and the elliptic curve $E_\delta : Y^2 = X^3 + A \delta^2 X + B \delta^3$. Since

$$\psi_p(\delta X, \delta^2 A, \delta^3 B) = \delta^{(p^2-1)/2} \psi_p(X, A, B),$$

it suffices to prove Theorem 3.2 for supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. Now, we proceed to do that. We will split the proof in three propositions depending on the order of the automorphism group of the elliptic curve E .

Lemma 3.1 *Let $E : Y^2 = X^3 + A X + B$ be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. The automorphism $u \in \text{Aut } E$ such that $[p] = u \circ \text{Frob}_{p^2}$ acts as follows*

$$u(x, y) = (\psi_{E,p}^{-2} x, \psi_{E,p}^{-3} y).$$

Proof. We know that $\psi_{E,p} \in \mathbb{F}_{p^2}$. By Theorem 3.6 in [Was08], we have

$$[p](x, y) = \left(\frac{\phi_{E,p}}{\psi_{E,p}^2}, \frac{\omega_{E,p}}{\psi_{E,p}^3} \right),$$

where

$$\phi_{E,p} = x \psi_{E,p}^2 - \psi_{E,p+1} \psi_{E,p-1}, \quad \omega_{E,p} = (4y)^{-1} (\psi_{E,p+2} \psi_{E,p-1}^2 - \psi_{E,p-2} \psi_{E,p+1}^2).$$

By Lemma 3.5 in [Was08], we know that $\phi_{E,p} = x^{p^2} + \dots$. Using (5), we obtain that $\omega_{E,p} = y(x^{3(p^2-1)/2} + \dots)$. Since

$$\text{Frob}_{p^2}(x, y) = (x^{p^2}, y^{p^2}) = (x^{p^2}, y(x^3 + A x + B)^{(p^2-1)/2}) = (x^{p^2}, y(x^{3(p^2-1)/2} + \dots)),$$

the statement follows. $\square$

Remark 3.1 Set $n = |\text{Aut } E|$ and let $\zeta \in \mathbb{F}_{p^2}$ be a n -th root of the unity. We can identify ζ as the automorphism of E defined by $(x, y) \mapsto (\zeta^2 x, \zeta^3 y)$. The above lemma can be rewritten as follows

$$\psi_{E,p} \circ [p] = \text{Frob}_{p^2},$$

where $\psi_{E,p}$ is viewed as an automorphism of E .

Proposition 3.3 Let $Y^2 = X^3 + AX + B$, with $A, B \in \mathbb{F}_{p^2}$, be the equation of a supersingular elliptic curve E such that $j(E) \neq 0, 1728$. One has

$$\psi_{E,p} = \left(\frac{-1}{p} \right) \left(A^3 + \frac{27}{4} B^2 \right)^{(p^2-1)/12},$$

where

$$\left(A^3 + \frac{27}{4} B^2 \right)^{(p^2-1)/12} = \begin{cases} 1 & \text{if } |E(\mathbb{F}_{p^2})| \equiv 0 \pmod{8}, \\ -1 & \text{if } |E(\mathbb{F}_{p^2})| \equiv 4 \pmod{8}. \end{cases}$$

Proof. In Lemma 4 of [Dol18], it is proved that $\psi_{E,p} = \pm 1$ for E as in the statement. In fact, this is a consequence from the fact that $\text{Aut } E = \{\pm 1\}$. First, we will prove that

$$\psi_{E,p} = \begin{cases} \left(\frac{-1}{p} \right) & \text{if } |E(\mathbb{F}_{p^2})| \equiv 0 \pmod{8}, \\ -\left(\frac{-1}{p} \right) & \text{if } |E(\mathbb{F}_{p^2})| \equiv 4 \pmod{8}. \end{cases} \quad (8)$$

By Lemma 3.1, $\text{Frob}_{p^2} = \psi_{E,p}[p]$. Hence, the characteristic polynomial of Frob_{p^2} acting on the Tate module of E is $(x - \psi_{E,p}p)^2$ and, thus, the trace of Frob_{p^2} is $2\psi_{E,p}p$. Therefore, we have

$$|E(\mathbb{F}_{p^2})| = p^2 + 1 - 2\psi_{E,p}p = (p - \psi_{E,p})^2,$$

and follows (8).

Now, we complete the proof of the statement. Let E_λ be the elliptic curve such that $E \simeq E_\lambda$. Since $j(E) \neq 0, 1728$, there exists $\delta \in \mathbb{F}_{p^2}$ such that

$$A = \frac{1}{3}\delta^2(-1 + \lambda - \lambda^2) \text{ and } B = -\frac{1}{27}\delta^3(-2 + \lambda)(1 + \lambda)(-1 + 2\lambda).$$

By Proposition 2.2, we know that $j(E) = j_0^3$ for some $j_0 \in \mathbb{F}_{p^2}$. Hence, when $j(E) \neq 0$ one has that $1/4(\lambda - 1)^2\lambda^2$ is a cube in $\mathbb{F}_{p^2}$ and, thus, $1/2(\lambda - 1)\lambda$ is a cube in $\mathbb{F}_{p^2}$. By Proposition 2.1, $1/2(\lambda - 1)\lambda$ is also a square in $\mathbb{F}_{p^2}$ and, thus, $1/2(\lambda - 1)\lambda = u^6$ for some $u \in \mathbb{F}_{p^2}$. Therefore, we have

$$\left(A^3 + \frac{27}{4} B^2 \right)^{\frac{p^2-1}{12}} = (-\delta^6 u^{12})^{\frac{p^2-1}{12}} = \delta^{\frac{p^2-1}{2}} = \begin{cases} 1 & \text{if } \delta \in \mathbb{F}_{p^2}^2, \\ -1 & \text{otherwise.} \end{cases}$$

The curves E and E_λ are isomorphic over $\mathbb{F}_{p^2}$ if and only if δ is a square in $\mathbb{F}_{p^2}$ because $\text{Aut}(E) = \{\pm 1\}$. In such a case, $|E(\mathbb{F}_{p^2})| = |E_\lambda(\mathbb{F}_{p^2})| \equiv 0 \pmod{8}$. If δ is not a square in $\mathbb{F}_{p^2}$, then

$$|E(\mathbb{F}_{p^2})| + |E_\lambda(\mathbb{F}_{p^2})| = 2(p^2 + 1) \equiv 4 \pmod{8},$$

and, thus $|E(\mathbb{F}_{p^2})| \equiv 4 \pmod{8}$. Hence, the statement is proved. $\square$

Next, we prove Theorem 3.2 for the remaining supersingular cases, i.e. for $j(E) = 1728$ and $j(E) = 0$.

Proposition 3.4 *Let $Y^2 = X^3 + AX$, with $A \in \mathbb{F}_{p^2}$ be a supersingular elliptic curve E . One has*

$$\psi_{E,p} = -A^{(p^2-1)/4},$$

Proof. If E is supersingular, then $p \equiv 3 \pmod{4}$. The isogeny $[p]$ acts on $E[4](\overline{\mathbb{F}}_p)$ as -1 . We consider the following point of E

$$P = (A^{1/2}, \sqrt{2} A^{1/2} A^{1/4}) \in E[4].$$

Applying Lemma 3.1 to the point P , we get the equalities

$$\psi_{E,p}^{-2} A^{p^2/2} = A^{1/2} \quad \text{and} \quad \psi_{E,p}^{-3} \sqrt{2} A^{p^2/2} A^{p^2/4} = -\sqrt{2} A^{1/2} A^{1/4},$$

and the statement follows. $\square$

Proposition 3.5 *Let $Y^2 = X^3 + B$, with $B \in \mathbb{F}_{p^2}$, be a supersingular elliptic curve E . One has*

$$\psi_{E,p} = -B^{(p^2-1)/6}.$$

Proof. If E is supersingular, then $p \equiv 2 \pmod{3}$. Note that in this case

$$\left(\frac{-1}{p}\right) 27^{(p^2-1)/12} = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right)^{(p+1)/2} = \left(\frac{-1}{p}\right) \left(-\left(\frac{-1}{p}\right)\right)^{(p+1)/2} = -1,$$

and $4^{(p^2-1)/12} = 2^{(p-1)\frac{p+1}{6}} \equiv 1 \pmod{p}$.

The isogeny $[p]$ acts on $E[4](\overline{\mathbb{F}}_p)$ as $\left(\frac{-1}{p}\right)$. Consider the point

$$P = (-B^{1/3}(1 + \sqrt{3}), \sqrt{3}\sqrt{-(3 + 2\sqrt{3})} \sqrt{B}) \in E[4].$$

We claim that $\sqrt{3 + 2\sqrt{3}} \in \mathbb{F}_{p^2}$ if and only if $\left(\frac{-1}{p}\right) = -1$. Indeed, if $\left(\frac{-1}{p}\right) = -1$, then $\sqrt{3} \in \mathbb{F}_p$, otherwise $3 + 2\sqrt{3}$ is not a square in $\mathbb{F}_{p^2}$ because $(3 + 2\sqrt{3})(3 - 2\sqrt{3}) = -3 \notin \mathbb{F}_p^2$. Hence,

$$\sqrt{3 + 2\sqrt{3}}^{p^2} = -\left(\frac{-1}{p}\right) \sqrt{3 + 2\sqrt{3}}.$$

From the following equalities obtained applying Lemma 3.1 to P

$$\psi_{E,p}^{-2} B^{p^2/3} = B^{1/3} \quad \text{and} \quad -\left(\frac{-1}{p}\right) \psi_{E,p}^{-3} B^{p^2/2} = \left(\frac{-1}{p}\right) B^{1/2},$$

we obtain the statement. $\square$

This proposition concludes the proof of Theorem 3.2.

Since $E(\mathbb{F}_{p^2})$ is isomorphic to the group $(\mathbb{Z}/(p+1)\mathbb{Z})^2$ or $(\mathbb{Z}/(p-1)\mathbb{Z})^2$ when E is supersingular and $j(E) \neq 0, 1728$, the condition $|E(\mathbb{F}_{p^2})| \equiv 0 \pmod{8}$ amounts to saying that $|E[4](\mathbb{F}_{p^2})| = 16$. As a by-product of Proposition 3.3, we obtain the following criterion to discard supersingular elliptic curves.

Corollary 3.1 *If an elliptic curve $E : Y^2 = X^3 + AX + B$ defined over $\mathbb{F}_{p^2}$ with j -invariant different from 0 and 1728 does not satisfy the conditions*

$$E[4](\mathbb{F}_{p^2}) = E[2n] \text{ for } n \in \{1, 2\} \text{ and } \left(A^3 + \frac{27}{4}B^2\right)^{\frac{p^2-1}{12}} = (-1)^n,$$

then E is ordinary.

The probability that a randomly selected $\tilde{j} \in \mathbb{F}_{p^2}$ is a supersingular j -invariant is approximately $\frac{1}{12(p+1)}$, which is very small for large primes. If among the ordinary elliptic curves defined over $\mathbb{F}_{p^2}$ the 12-th root of the unity $(A^3 + \frac{27}{4}B^2)^{\frac{p^2-1}{12}}$ is independent of the condition on $E[4](\mathbb{F}_{p^2})$, then this criterion should be effective for this class of curves with probability $\geq 11/12 = 0.917$.

If $\lambda, 1 - \lambda \in \mathbb{F}_{p^2}^*$, then $\lambda = 4m^2/(1 + m^2)^2$ for some $m \in \mathbb{F}_{p^2}$. In this particular case, it can be checked that $|E_\lambda[4](\mathbb{F}_{p^2})| = 16$. As a consequence of the Propositions 2.1 and 2.2, we can state a criterion, that implies the previous corollary and can be computed easily.

Corollary 3.2 *For $\tilde{j} \in \mathbb{F}_{p^2} \setminus \{0, 1728\}$, let $\lambda \in \overline{\mathbb{F}_p}$ be such that $j(E_\lambda) = \tilde{j}$. If the conditions*

$$\lambda, 1 - \lambda \in \mathbb{F}_{p^2}^* \quad \text{and} \quad \frac{1}{2}(1 - \lambda)\lambda \in \mathbb{F}_{p^2}^*$$

are not satisfied, then $\tilde{j}$ is the j -invariant of an ordinary elliptic curve.

It would be interesting if an expert could evaluate these criteria by comparing with existing ones such as those shown in [Dol18].

References

- [BM04] John Brillhart and Patrick Morton. Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial. *J. Number Theory*, 106(1):79–111, 2004.
- [Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$* . A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. Fermat, class field theory and complex multiplication.
- [Deb14] Christophe Debry. Beyond two criteria for supersingularity: coefficients of division polynomials. *J. Théor. Nombres Bordeaux*, 26(3):595–606, 2014.
- [Dol18] Javad Doliskani. On division polynomial PIT and supersingularity. *Appl. Algebra Engrg. Comm. Comput.*, 29(5):393–407, 2018.
- [Gon00] J. González. On the division polynomials of elliptic curves, 2000. Contributions to the algorithmic study of problems of arithmetic moduli (Spanish).
- [Lan87] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.
- [Mor11] Patrick Morton. The cubic Fermat equation and complex multiplication on the Deuring normal form. *Ramanujan J.*, 25(2):247–275, 2011.
- [Ogg78] A. P. Ogg. On the Weierstrass points of $X_0(N)$. *Illinois J. Math.*, 22(1):31–35, 1978.
- [Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
- [Was08] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.

Josep González Rovira

Departament de Matemàtiques, Universitat Politècnica de Catalunya EPSEVG,
Avinguda Víctor Balaguer 1, 08800 Vilanova i la Geltrú, Catalonia
josep.gonzalez@upc.edu