JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Christophe DEBRY

Beyond two criteria for supersingularity: coefficients of division polynomials

Tome 26, n° 3 (2014), p. 595-605.

<http://jtnb.cedram.org/item?id=JTNB_2014__26_3_595_0>

Journal de Théorie des Nombres
de Bordeaux **26** (2014), 595–605

Beyond two criteria for supersingularity: coefficients of division polynomials

par Christophe DEBRY

Résumé. Soit $f(x)$ un polynôme cubique, unitaire et séparable avec coefficients dans un corps de caractéristique $p \geq 3$, et soit E la courbe elliptique donnée par l'équation $y^2 = f(x)$. Dans cet article on démontre que le coefficient du monôme $x^{\frac{1}{2}p(p-1)}$ dans le p–ième polynôme de division de E est égal au coefficient du monôme x^{p-1} dans $f(x)^{\frac{1}{2}(p-1)}$. Lorsque le corps de base est fini, le premier coefficient est nul si et seulement si E est supersingulière, ce qui, par un critère classique de Deuring (1941), est équivalent à la nullité du deuxième coefficient. Donc les zéros des coefficients sont les mêmes. L'égalité des coefficients qu'on démontre dans cet article entraîne clairement cette égalité de zéros.

Abstract. Let $f(x)$ be a cubic, monic and separable polynomial over a field of characteristic $p \geq 3$ and let E be the elliptic curve given by $y^2 = f(x)$. In this paper we prove that the coefficient at $x^{\frac{1}{2}p(p-1)}$ in the p–th division polynomial of E equals the coefficient at x^{p-1} in $f(x)^{\frac{1}{2}(p-1)}$. For elliptic curves over a finite field of characteristic p, the first coefficient is zero if and only if E is supersingular, which by a classical criterion of Deuring (1941) is also equivalent to the vanishing of the second coefficient. So the zero loci of the coefficients are equal; the main result in this paper is clearly stronger than this last statement.

Introduction

Let K be a finite field of characteristic $p \geq 3$ and let E/K be an elliptic curve given by the equation $y^2 = f(x)$, where $f(x) \in K[x]$ is cubic, monic and separable. Associated to E, one defines division polynomials ψ_m (for every positive integer m), whose properties we shall review in Section 1. One of the properties we need to state the main theorem, is that if m is odd, then ψ_m, as a function on E, is a function of x only. These polynomials can be used to check whether E is supersingular or not:

> *Division polynomial criterion*: E is supersingular if and only if the coefficient at $x^{\frac{1}{2}p(p-1)}$ in ψ_p is zero.

Manuscrit reçu le 2 avril 2013, révisé le 4 septembre 2014, accepté le 5 septembre 2014.

For example, let $E : y^2 = x^3 + Ax + B$ be a model of an elliptic curve over a finite field of characteristic 5. Then ψ_5 is equal to $2Ax^{10} + 4A^2Bx^5 + (4B^4 - 2A^3B^2 + A^6)$. So E is supersingular if and only if $A = 0$. There is also a classical criterion, very similar (in wording) to the one above.

> *Deuring criterion*: E is supersingular if and only if the coefficient at x^{p-1} in $f(x)^{\frac{1}{2}(p-1)}$ is zero.

For a proof of this criterion, one can consult Silverman [8, V.4.1]. We reconsider the above example: an elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_{5^k}$ is supersingular if and only if the coefficient at x^4 in $(x^3 + Ax + B)^2$ is zero, i.e., if and only if $2A = 0$. This is indeed the same criterion as the one we got using division polynomials. The striking similarity between the criteria actually has a deeper reason: not only do these coefficients at different monomials in different polynomials have the same zeros, they actually are equal, as we prove in section 2. More precisely, we show that the following theorem holds:

Theorem 1. *Consider the elliptic curve $E : y^2 = x^3 + ax^2 + bx + c$ over $\mathbb{Q}(a, b, c)$ (where a, b and c are transcendentals). Let $p \geq 3$ be prime and let $\ell_p \in \mathbb{Z}[a, b, c]$ be the coefficient at $x^{\frac{1}{2}p(p-1)}$ in the p–th division polynomial $\psi_p \in \mathbb{Z}[x, a, b, c]$ of E. Let $c_p \in \mathbb{Z}[a, b, c]$ be the coefficient at x^{p-1} in $(x^3 + ax^2 + bx + c)^{\frac{1}{2}(p-1)}$. Then $\ell_p \equiv c_p \pmod{p}$.*

Specializing the indeterminates a, b and c, as well as the $\mathbb{Z}$–coefficients of the polynomials in the theorem immediately implies the following

Corollary 2. *Let K be a field of characteristic $p \geq 3$ and let $f(x)$ be a cubic, monic and separable polynomial over K. Let E be the elliptic curve given by $y^2 = f(x)$. Then the coefficient at $x^{\frac{1}{2}p(p-1)}$ in the p–th division polynomial of E is equal to the coefficient at x^{p-1} in $f(x)^{\frac{1}{2}(p-1)}$.*

In section 3 we apply the above result to a specific elliptic curve to deduce, just for the sake of arithmetic fun, that if k is a positive integer and $4k + 1$ is prime, then this prime divides $k^k - 1$. Finally, in section 4 we look at the other coefficients of the p–th division polynomial in characteristic p, proving that all of them (except for the constant) are divisible by the one at $x^{\frac{1}{2}p(p-1)}$, the leading actor of the above theorem and corollary.

Acknowledgements

The author would like to thank Antonella Perucca for assisting the master's thesis leading to this paper, as well as the anonymous referee for suggestions to state a more general result and to clarify the exposition. The author is supported by a PhD fellowship of the Research Foundation – Flanders (FWO).

1. Division polynomials

Let E be an elliptic curve over a field K and choose a Weierstrass model

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

for E. We denote the neutral element of the group law on E by $\mathcal{O}$, and denote the multiplication–by–m isogeny by $[m]$. The division polynomials $(\psi_m)_{m\geq 1}$ associated to E are defined recursively:

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

and

$$\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,\\
\psi_2\psi_{2m} &= \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2.
\end{aligned}$$

Recall that the b–quantities in the definition of ψ_3 and ψ_4 are polynomials in the a–quantities: $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$ and $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. Every $\psi_m \in K[x,y]$ can be written as a linear polynomial in y over $K[x]$ using the Weierstrass equation. As such, one can prove that if m is odd, then $\psi_m \in K[x]$, and as a polynomial in x, ψ_m has degree at most $\frac{1}{2}(m^2-1)$ and the coefficient at $x^{\frac{1}{2}(m^2-1)}$ equals m. Proofs for these claims can be found in various places, e.g., [5, 3.6]. We also recall the following standard facts:

- The roots of ψ_m are precisely the nontrivial m–torsion points on E, i.e., the points $P \in E(\overline{K}) \setminus \{\mathcal{O}\}$ satisfying $[m]P = \mathcal{O}$.
- The polynomials ψ_m^2 and $\phi_m = x\psi_m^2 - \psi_{m-1}\psi_{m+1}$ are elements of $K[x]$ using the Weierstrass equation, and as such are relatively prime.
- Denoting the Weierstrass x–coordinate function on E by x, the functions $x \circ [m]$ and ϕ_m/ψ_m^2 on E are equal.

We deduce the following result about the p–th division polynomial in characteristic $p \geq 3$.

Proposition 3. *Let E be an ordinary elliptic curve over a finite field K of characteristic $p \geq 3$. Then ψ_p has degree $\frac{1}{2}p(p-1)$ and lies in $K[x^p]$.*

Proof. Note that $[p]$ is not separable and hence factors through the p–th power Frobenius

$$\Phi : E \to E^{(p)} : [X : Y : Z] \mapsto [X^p : Y^p : Z^p],$$

where $E^{(p)}$ is the elliptic curve defined by the Weierstrass equation with coefficients a_i^p. (Cf. [8, II.2.12]) It follows that $x \circ [p]$ is a rational function of x^p and y^p. Since finite fields are perfect, this implies that $x \circ [p]$ is the p–th power of a rational function in x and y. So the coefficients of the divisor of $x \circ [p]$ are all divisible by p. Since $x \circ [p] = \phi_p/\psi_p^2$ where ϕ_p and ψ_p^2 are coprime, we find that the coefficients in $2\mathrm{div}(\psi_p)$ are p–divisible. The zero set $\mathcal{Z}$ of ψ_p is equal to $(\ker[p])(\overline{K}) \setminus \{\mathcal{O}\}$, and ψ_p has only a pole at $\mathcal{O}$, so

$$\mathrm{div}(\psi_p) = \sum_{P \in \mathcal{Z}} n_P \langle P \rangle - n\langle \mathcal{O} \rangle,$$

where $n = \sum_{P \in \mathcal{Z}} n_P$ and each $n_P \geq 1$. By the p–divisibility of the coefficients, we get that p divides each $2n_P$ and therefore divides each n_P (p is odd). It follows that $n_P \geq p$ and $n \geq p \cdot \sharp\mathcal{Z} = p(p-1)$ because E is ordinary. The polynomial $\psi_p \in K[x]$ has degree $\leq \frac{1}{2}(p^2-1)$ and hence has order at least $1-p^2$ in $\mathcal{O}$. In other words, $-n \geq 1-p^2$, which together with $p \mid n$ implies that $n \leq p(p-1)$. We find that $n = p(p-1)$ and hence

$$\mathrm{div}(\psi_p) = \sum_{P \in \mathcal{Z}} p\langle P \rangle - p(p-1)\langle \mathcal{O} \rangle = p\left(\sum_{P \in \mathcal{Z}} \langle P \rangle - (p-1)\langle \mathcal{O} \rangle \right).$$

The first implication is that the degree of $\psi_p \in K[x]$ equals $-\frac{1}{2}\mathrm{ord}_{\mathcal{O}}(\psi_p) = \frac{1}{2}p(p-1)$. One also easily verifies that the sum of the points in $\mathcal{Z}$ is equal to $\mathcal{O}$, so the divisor $\frac{1}{p}\mathrm{div}(\psi_p)$ is principal. Therefore, ψ_p is the p^{th} power of a polynomial in $K[x]$, which (working in characteristic p) implies that $\psi_p \in K[x^p]$. □

Remark. An alternative to prove this proposition is to use the main theorem from [1]. Cheon and Hahn [3] prove the proposition for ordinary elliptic curves over the prime field $\mathbb{F}_p$.

Example. Let $E : y^2 = x^3 + Ax + B$ be a model of an elliptic curve over $\mathbb{F}_{5^k}$. Then ψ_5 is equal to $2Ax^{10} + 4A^2Bx^5 + (4B^4 - 2A^3B^2 + A^6)$. Note that ψ_5 is indeed a function of x^5. It also follows from the proposition that if E is ordinary, then ψ_5 must have degree $5 \cdot 4/2 = 10$, so $A \neq 0$ if E is ordinary.

We can now derive the division polynomial criterion for supersingularity. Let E be an elliptic curve over a finite field of characteristic $p \geq 3$. Since the zeros of ψ_p are precisely the nontrivial p–torsion points, E is supersingular if and only if ψ_p has no zeros, i.e., ψ_p is a constant polynomial. This is equivalent to all nonconstant coefficients of ψ_p being zero. But we know that if E is ordinary, then ψ_p has degree $\frac{1}{2}p(p-1)$. This implies that E is supersingular if and only if the coefficient at $x^{\frac{1}{2}p(p-1)}$ in ψ_p is zero, which is the division polynomial criterion mentioned in the introduction.

2. Proof of Theorem 1

2.1. Setup of a special case. Let $p \geq 3$ be a prime and let A and B be indeterminates. Consider the p–th division polynomial ψ_p of the elliptic curve over $\mathbb{Q}(A, B)$ given by the equation $y^2 = x^3 + Ax + B$. As p is odd, one can prove that $\psi_p \in \mathbb{Z}[x, A, B]$, so we can consider the coefficient $\ell_p(A, B) \in \mathbb{Z}[A, B]$ at $x^{\frac{1}{2}p(p-1)}$ in ψ_p. Let $c_p(A, B)$ be the coefficient at x^{p-1} in $(x^3 + Ax + B)^{\frac{1}{2}(p-1)}$. For example, $\ell_5(A, B) = 62A$ and $c_p(A, B) = 2A$. We first prove the following special case of Theorem 1:

Proposition 4. *We have* $c_p(A, B) \equiv \ell_p(A, B) \pmod{p}$.

The following three subsections will consist of the proof of the above proposition. To simplify notations, write $p = 2q + 1$ with $q \in \mathbb{Z}$. One can easily check the proposition for $p = 3$: both coefficients are zero. So suppose $p \geq 5$ from now on.

2.2. Step 1: $c_p(A, B)$ as a sum. First, we compute $c_p(A, B)$ by using the trinomial identity:

$$(x^3 + Ax + B)^q = \sum_{(i,j,k)\in S} \binom{q}{i, j, k} x^{3i+j} A^j B^k,$$

where $S = \{(i, j, k) \in \mathbb{Z}^3 \mid i, j, k \geq 0, i + j + k = q\}$ and

$$\binom{q}{i, j, k} = \frac{q!}{i!j!k!}.$$

Hence,

$$c_p(A, B) = \sum_{(i,j,k)\in S_0} \binom{q}{i, j, k} A^j B^k,$$

where $S_0 = \{(i, j, k) \in S \mid 3i + j = p - 1 = 2q\}$. Let us determine S_0 more explicitly. The triple (i, j, k) is in S_0 if and only if $i = \frac{1}{3}(2q - j)$, $k = q - i - j = \frac{1}{3}(q - 2j)$, and i, j, k are non–negative integers. So

$$S_0 = \left\{ \left(\frac{1}{3}(2q - j), j, \frac{1}{3}(q - 2j) \right) \mid j \equiv -q \pmod 3, j \in \mathbb{Z} \cap \left[0, \frac{q}{2}\right] \right\}.$$

We find that

$$c_p(A, B) = \sum_{j\in J} \binom{q}{\frac{1}{3}(2q - j), j, \frac{1}{3}(q - 2j)} A^j B^{\frac{1}{3}(q-2j)},$$

where $J = \left\{ j \in \mathbb{Z} \mid j \equiv -q \pmod 3, 0 \leq j \leq \frac{1}{2}q \right\}$.

2.3. Step 2: $\ell_p(A,B)$ as a sum. Write

$$\psi_p = \sum_t \beta_t(A,B)x^t, \quad \text{with} \quad \beta_t(A,B) \in \mathbb{Z}[A,B].$$

Giving x degree 1, A degree 2 and B degree 3 makes $x^3 + Ax + B$ homogeneous of degree 3, so the Weierstrass equation forces us to give y degree $\frac{3}{2}$. One can now prove by induction that $\psi_m(x,y,A,B)$ is homogeneous of (weighted) degree $\frac{1}{2}(m^2-1)$. It follows that $\beta_t(A,B)$ is a homogeneous polynomial of weighted degree $\frac{1}{2}(p^2-1)-t$, and hence, it contains only monomials of the form A^rB^s with $2r+3s = \frac{1}{2}(p^2-1)-t$. Hence write

$$\beta_t(A,B) = \sum_{2r+3s=\frac{1}{2}(p^2-1)-t} \alpha_{r,s}A^rB^s,$$

with $\alpha_{r,s} \in \mathbb{Z}$. Since ψ_p has leading coefficient p as a polynomial in x, we have $\alpha_{0,0} = p$. Also, $\alpha_{r,s} = 0$ if $r < 0$ or $s < 0$. Let $\mathbb{Z}_{(p)}$ be the localization of $\mathbb{Z}$ by $\mathbb{Z} \setminus p\mathbb{Z}$ (invert everything in $\mathbb{Z} \setminus p\mathbb{Z}$) and for all integers r and s we denote by $\overline{\alpha}_{r,s}$ the image of $(4r+6s+1)\alpha_{r,s}$ under the canonical map $\mathbb{Z} \to \mathbb{Z}_{(p)}/p^2\mathbb{Z}_{(p)}$.

Lemma 5. *For all integers r and s, and writing $d = 2r+3s$, we have*

$$2d\overline{\alpha}_{r,s} = -(2d-2)\overline{\alpha}_{r-1,s} - (2d-3)\,\overline{\alpha}_{r,s-1}.$$

Proof. This is a direct consequence of the following formula in [7, Eq. (3)]:

$$\begin{aligned} d\left(d+\frac{1}{2}\right)\alpha_{r,s} = &\left(\frac{p^2+3}{2}-d\right)\left(\frac{p^2}{6}-1+d\right)\alpha_{r-1,s} \\ &- \left(\frac{p^2+5}{2}-d\right)\left(\frac{p^2+3}{2}-d\right)\alpha_{r,s-1} \\ &+ 3(r+1)p^2\alpha_{r+1,s-1} - \frac{2}{3}(s+1)p^2\alpha_{r-2,s+1}. \quad \square \end{aligned}$$

The recursion formula in Lemma 5 enables us to compute $\overline{\alpha}_{r,s}$ from $\overline{\alpha}_{r-1,s}$ and $\overline{\alpha}_{r,s-1}$, as long as $2r+3s$ is not divisible by p (hence invertible in $\mathbb{Z}_{(p)}$).

Proposition 6. *If r and s are non–negative integers with $2r+3s < p$, then in $\mathbb{Z}_{(p)}/p^2\mathbb{Z}_{(p)}$ we have*

$$(r+s)!r!s! \cdot (-4)^{r+s}\overline{\alpha}_{r,s} = (2r+2s)! \cdot p.$$

Proof. We prove this formula by induction on $2r+3s$ using Lemma 5. Since we are using induction, there are some small cases we should handle first. The fact that $\alpha_{r,-1} = 0$ for all r yields that $2r\overline{\alpha}_{r,0} = (1-2r)\overline{\alpha}_{r-1,0}$. This implies for all non–negative integers r that $(2r)(2r-2)\cdots 2\overline{\alpha}_{r,0} = (1-2r)(3-2r)\cdots(-3)(-1)\overline{\alpha}_{0,0}$, which leads to $(2^r \cdot r!)^2 \cdot \overline{\alpha}_{r,0} = (-1)^r \cdot (2r)! \cdot p$.

This is the desired formula for $s = 0$. Proving the formula for $r = 0$ is done in a completely analogous way. So we have proven the formula for $r = 0$, for $s = 0$ and for all $2r + 3s$ in the set $\{0, 1, 2, 3\}$.

So now assume we know the formula to be true for all non–negative r and s such that $2r + 3s \in \{0, 1, \ldots, D\}$ with $3 \leq D < p - 1$. We want to prove the formula for all integers $r, s \geq 1$ satisfying $2r + 3s = D + 1$. Note that $r - 1$ and $s - 1$ are non–negative integers and both $2(r - 1) + 3s = D - 1$ and $2r + 3(s - 1) = D - 2$ are in $\{0, 1, \ldots, D\}$, so, writing $C = (r + s - 1)!(r - 1)!(s - 1)! \cdot (-4)^{r+s-1}$, the induction hypothesis says that $Cr\overline{\alpha}_{r-1,s} = Cs\overline{\alpha}_{r,s-1} = (2r + 2s - 2)! \cdot p$. Lemma 5 now yields

$$\begin{aligned} &Crs \cdot 2(2r + 3s)\overline{\alpha}_{r,s} \\ &\quad = -\left((s(4r + 6s - 2) + r(4r + 6s - 3)\right) \cdot (2r + 2s - 2)! \cdot p \\ &\quad = -(2r + 3s)p \cdot (2r + 2s - 1)! \end{aligned}$$

This implies the formula we want to prove because $2r+3s \in \{1, 2, \ldots, p-1\}$ is invertible in $\mathbb{Z}_{(p)}/p^2\mathbb{Z}_{(p)}$. □

Now let $r, s \geq 1$ be integers satisfying $2r + 3s = q$. Then $2r + 3s < p$, so the above proposition and the fact that $4r+6s+1 = 2q+1 = p$ imply that

$$p \cdot \Big((r + s)!r!s! \cdot (-4)^{r+s}\alpha_{r,s} - (2r + 2s)!\Big) \in p^2\mathbb{Z}_{(p)} \cap \mathbb{Z} = p^2\mathbb{Z}.$$

We deduce that

$$\begin{aligned} \ell_p(A, B) = \beta_{\frac{1}{2}p(p-1)}(A, B) &= \sum_{2r+3s=q} \alpha_{r,s}A^rB^s \\ &\equiv \sum_{2r+3s=q} \left(\frac{-1}{4}\right)^{r+s} \binom{2r + 2s}{r + s, r, s} A^rB^s \pmod{p}. \end{aligned}$$

2.4. Step 3: equality of coefficients in the sums. We have proven that

$$c_p(A, B) = \sum_{j\in J} \binom{q}{\frac{1}{3}(2q - j), j, \frac{1}{3}(q - 2j)} A^jB^{\frac{1}{3}(q-2j)},$$

where $J = \Big\{j \in \mathbb{Z} \mid j \equiv -q \pmod 3, 0 \leq j \leq \frac{1}{2}q\Big\}$, and

$$\ell_p(A, B) \equiv \sum_{2r+3s=q} \left(\frac{-1}{4}\right)^{r+s} \binom{2r + 2s}{r + s, r, s} A^rB^s \pmod{p}.$$

Note that the indices in this last sum are all couples (r, s) of non–negative integers such that $2r + 3s = q$. This condition is equivalent to r and $s = \frac{1}{3}(q-2r)$ being non–negative integers, i.e., $0 \leq r \leqslant \frac{1}{2}q$ and $r \equiv -q \pmod 3$.

(For these r and s we have $r+s=\frac{1}{3}(q+r)$.) It follows that

$$\ell_p(A,B)\equiv\sum_{j\in J}\left(\frac{-1}{4}\right)^{\frac{1}{3}(q+j)}\binom{\frac{2}{3}(q+j)}{\frac{1}{3}(q+j),j,\frac{1}{3}(q-2j)}A^jB^{\frac{1}{3}(q-2j)}\pmod p.$$

Therefore, $c_p(A,B)\equiv\ell_p(A,B)\pmod p$ is equivalent to proving

$$\binom{q}{\frac{1}{3}(2q-j),j,\frac{1}{3}(q-2j)}\equiv\left(\frac{-1}{4}\right)^{\frac{1}{3}(q+j)}\binom{\frac{2}{3}(q+j)}{\frac{1}{3}(q+j),j,\frac{1}{3}(q-2j)}\pmod p$$

for all $j\in J$. To prove this, put $j+q=3k$ with $k\in\mathbb{Z}$ (then $\frac{1}{3}q\le k\le\frac{1}{2}q$) and rewrite the congruence as

$$\binom{q}{q-k,j,q-2k}\equiv\left(\frac{-1}{4}\right)^k\binom{2k}{k,j,q-2k}\pmod p.$$

This is equivalent to

$$\frac{q!}{(q-k)!}\equiv\left(\frac{-1}{4}\right)^k\frac{(2k)!}{k!}\pmod p.$$

We rewrite the left hand side as follows:

$$\begin{aligned}\frac{q!}{(q-k)!}&=q(q-1)\cdots(q-k+1)=\left(\frac{p-1}{2}\right)\left(\frac{p-3}{2}\right)\cdots\left(\frac{p+1-2k}{2}\right)\\&\equiv 2^{-k}\cdot(-1)(-3)\cdots(-2k+1)=(-2)^{-k}1\cdot3\cdots(2k-1)\\&=(-2)^{-k}\frac{(2k)!}{2\cdot4\cdots(2k)}=(-2)^{-k}\frac{(2k)!}{2^k\cdot k!}\pmod p,\end{aligned}$$

the desired congruence. This completes the proof of Proposition 4.

2.5. Proof of Theorem 1. Let $K=\mathbb{Q}(a,b,c)$ be the rational function field in three variables over $\mathbb{Q}$ and consider the polynomial $f(X)=X^3+aX^2+bX+c$ over K. Let E and E' be the elliptic curves given by the equations $y^2=f(x)$ and $z^2=f(t-\frac{a}{3})$ respectively. Let $(\psi_m)_{m\ge1}$ and $(\varphi_m)_{m\ge1}$ be the division polynomials of E and E' respectively. Recall that $\psi_m^2\in K[x]$ and $\varphi_m^2\in K[t]$ and that the representations as univariate polynomials are unique (because $x\in K(E)$ and $t\in K(E')$ are transcendental over K). So we consider the polynomials $\psi_m^2(X),\varphi_m^2(X)\in K[X]$ in a formal variable X. As such, the fact that $E(\overline{K})\to E'(\overline{K}):(x,y)\mapsto(t,z)=(x+\frac{a}{3},y)$ is a group isomorphism, and that K has characteristic zero, implies that

$$\psi_m^2\left(X-\frac{a}{3}\right)=m^2\prod_{P\in E_m}\left(X-\frac{a}{3}-x(P)\right)=m^2\prod_{P\in E'_m}(X-t(P))=\varphi_m^2(X),$$

where $E_m=E[m](\overline{K})\setminus\{\mathcal{O}_E\}$ and $E'_m=E'[m](\overline{K})\setminus\{\mathcal{O}_{E'}\}$. An alternative way to prove that $\psi_m^2(X-\frac{a}{3})=\varphi_m^2(X)$ is explicitly comparing the first four division polynomials of E and E' and then using induction.

The theorem 1 is clearly true for $p = 3$ (the coefficients are $4a$ and a respectively), so now assume that $p \geq 5$. Since p is odd, we can consider $\psi_p(X), \varphi_p(X) \in K[X]$. The equality $\psi_p^2(X - \frac{a}{3}) = \varphi_p^2(X)$ and the fact that ψ_p and φ_p have leading coefficient p imply that $\psi_p(X - \frac{a}{3}) = \varphi_p(X)$. Now consider the following polynomials in a, b and c:

(1) The coefficient at $X^{\frac{1}{2}p(p-1)}$ in $\psi_p(X)$.

(2) The coefficient at $X^{\frac{1}{2}p(p-1)}$ in $\varphi_p(X)$.

(3) The coefficient at X^{p-1} in $f\left(X - \frac{a}{3}\right)^{\frac{1}{2}(p-1)}$.

(4) The coefficient at X^{p-1} in $f(X)^{\frac{1}{2}(p-1)}$.

Since $\psi_p(X - \frac{a}{3}) = \varphi_p(X)$, we know that (1) equals the coefficient at $X^{\frac{1}{2}p(p-1)}$ in $\varphi_p(X + \frac{a}{3})$. Since E' is given in short Weierstrass form, we know by Proposition 6 that $\varphi_p(X)$ is congruent mod p to a polynomial in X of degree at most $\frac{1}{2}p(p-1)$. This implies that (1) and (2) are congruent mod p. Proposition 4 shows that (2) and (3) are congruent mod p. Moreover, (3) and (4) are also congruent mod p because of the following more general elementary result. (Consider $f(X)$ as an element of $\mathbb{F}_p(a, b, c)[X]$)

Lemma 7. *Let F be a field of positive characteristic p and take $f(X) \in F[X]$ of degree at most $2(p-1)$. Then for any $x_0 \in F$, the coefficient at X^{p-1} in $f(X + x_0) - f(X)$ is equal to zero.*

Proof. By the binomial theorem it suffices to show that $\binom{i}{p-1}$ is zero in F, for every $p-1 < i \leq 2(p-1)$. This is true because p divides $i!$ (by $p-1 < i$) but not $(p-1)!$ or $(i-p+1)!$ (by $i - p + 1 \leq p - 1$). □

This proves Theorem 1.

3. A special curve

Let p be a prime congruent to 1 modulo 4 and consider the elliptic curve $y^2 = x^3 + x$ over the finite field $\mathbb{F}_p$. Write $p = 4k + 1$ with $k \in \mathbb{N}$. Then $c_p(1, 0)$ is the coefficient at $x^{p-1} = x^{4k}$ in $(x^3+x)^{2k} = x^{2k}\left(x^2+1\right)^{2k}$, which is clearly $\binom{2k}{k}$. On the other hand,

$$\ell_p(1,0) \equiv \sum_{2r+3s=2k} \left(\frac{-1}{4}\right)^{r+s} \binom{2r+2s}{r+s, r, s} 1^r 0^s \pmod{p},$$

which reduces to $\ell_p(1, 0) \equiv \left(\frac{-1}{4}\right)^k \binom{2k}{k,k,0} \equiv (-4)^{-k}\binom{2k}{k} \pmod{p}$. Theorem 1 states that $c_p(1, 0) \equiv \ell_p(1, 0) \pmod{p}$, which in this case implies that $(-4)^{-k} \equiv 1 \pmod{p}$. Using $(-4)^{-1} \equiv k \pmod{p}$ we get

Proposition 8. *Let k be a positive integer. If $4k + 1$ is prime, then it divides $k^k - 1$.*

Alternative proof. Let $p = 4k+1$ be prime. Then 2 is a quadratic residue mod p if and only if k is even, so $(2/p) = 1$ if k is even and $(2/p) = -1$ if k is odd. It follows that

$$(-1)^k = \left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv 2^{2k} \equiv 4^k \pmod{p},$$

so $k^k \equiv (-4k)^k \equiv (1-p)^k \equiv 1 \pmod{p}$, as desired. □

4. The other coefficients of ψ_p

Consider the elliptic curve given by $y^2 = x^3 + Ax + B$ over $\mathbb{Q}(A,B)$ and let $p \geq 5$ be a prime number. Recall that we can write $\psi_p = \sum_t \beta_t(A,B)x^t$, where $\beta_t(A,B) \in \mathbb{Z}[A,B]$ is homogeneous if A and B are given degree 2 and 3 respectively. We will denote by $\overline{\beta}_t$ the image of β_t under the canonical map $\mathbb{Z}[A,B] \to \mathbb{F}_p[A,B]$.

Proposition 9. *For any $t \geq 1$, the polynomial $\overline{\beta}_t$ is divisible by $\overline{\beta}_{\frac{p(p-1)}{2}}$.*

Proof. Let J be the set of all supersingular j–invariants over $\overline{\mathbb{F}}_p$. As in [2, Lemma 8], Theorem V.4.1 in [8] implies that in $\overline{\mathbb{F}}_p[A,B]$ we have

$$\overline{\beta}_{\frac{p(p-1)}{2}} = cA^{\varepsilon_A}B^{\varepsilon_B} \prod_{j \in J\setminus\{0,1728\}} (B^2 - f(j)A^3),$$

where $f(j) = 4(1728-j)/(27j)$, c is a nonzero constant, $\varepsilon_A = 1$ if $0 \in J$ and $\varepsilon_A = 0$ otherwise, and similary, ε_B is 1 or 0 depending on whether $1728 \in J$ or not.

Fix a positive integer t. We want to prove that $\overline{\beta}_{\frac{p(p-1)}{2}}$ divides $\overline{\beta}_t$, so we may assume that $\overline{\beta}_t \neq 0$. Since all of the factors in the expression for $\overline{\beta}_{\frac{p(p-1)}{2}}$ are coprime, it suffices to prove that A divides $\overline{\beta}_t$ if $0 \in J$, that B divides $\overline{\beta}_t$ if $1728 \in J$ and that $\overline{\beta}_t$ is divisible by $B^2 - f(j)A^3$ for every $j \in J\setminus\{0,1728\}$. Recall that the p–th division polynomial of a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ is a constant because it has no roots. So $\overline{\beta}_t(A_0,B_0) = 0$ for all $A_0, B_0 \in \overline{\mathbb{F}}_p$ for which

$$j(A_0,B_0) := 1728 \cdot \frac{4A_0^3}{4A_0^3 + 27B_0^2} \in J.$$

Since $\overline{\beta}_t \neq 0$ is homogeneous if we assign A and B degrees 2 and 3 respectively, it can be written as a product $\gamma A^{d_A}B^{d_B}(B^2 - x_1A^3)\cdots(B^2 - x_kA^3)$, for some $\gamma, x_1, \ldots, x_k \in \overline{\mathbb{F}}_p^{\times}$. (Indeed, up to powers of A and B, $\overline{\beta}_t$ is a univariate polynomial in the variable B^2A^{-3}.)

If A does not divide $\overline{\beta}_t$, then $d_A = 0$, so $\overline{\beta}_t = \gamma B^{d_B}(B^2 - x_1A^3)\cdots(B^2 - x_kA^3)$. Hence $\overline{\beta}_t(0,1) = \gamma \neq 0$ and therefore $0 = j(0,1) \notin J$. This shows that A divides $\overline{\beta}_t$ if $0 \in J$ and a similar argument proves that B divides $\overline{\beta}_t$

if $1728 \in J$. Now let $j \in J \setminus \{0, 1728\}$ be arbitrary and take a Weierstrass model $y^2 = x^3 + A_0x + B_0$ of a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ with j–invariant j. Since $j(A_0, B_0) = j \in J$, we have $\overline{\beta}_t(A_0, B_0) = 0$ and $B_0^2 = f(j)A_0^3$. Since $j \notin \{0, 1728\}$, we have $A_0 \neq 0 \neq B_0$ and hence $\overline{\beta}_t(A_0, B_0) = 0$ implies that $B_0^2 = x_i A_0^3$ for some i and hence $x_i = f(j)$ for that i. It follows that $B^2 - f(j)A^3 = B^2 - x_i A^3$ divides $\overline{\beta}_t$, as desired. □

References

[1] J. W. S. Cassels, *A note on the division values of $\wp(u)$*, Mathematical Proceedings of the Cambridge Philosophical Society **45**, (1949), 167–172.

[2] W. Castryck, A. Folsom, H. Hubrechts, A.V. Sutherland, *The probability that the number of points on the Jacobian of a genus 2 curve is prime*, Proceedings of the London Mathematical Society **104**, (2012), 1235–1270.

[3] J. Cheon, S. Hahn, *Division polynomials of elliptic curves over finite fields*, Proc. Japan Acad. Ser. A Math. Sci. **72**, 10, (1996), 226–227.

[4] M. Deuring, *Die Typen der Multiplikatorringe Elliptischer Funktionenkörper*, Abh. Math., Sem. Univ. Hamburg **14**, (1941), 197–272.

[5] A. Enge, *Elliptic curves and their applications to cryptography: An introduction*, Kluwer Academic Publishers, (1999).

[6] H. Gunji, *The Hasse invariant and p–division points of an elliptic curve*, Arch. Math. **27**, (1976), 148–158.

[7] J. McKee, *Computing division polynomials*, J. Math. Comp. **63**, (1994), 767–771.

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer–Verlag, New York, (2009).

Christophe Debry
KU Leuven and Universiteit van Amsterdam
Departement Wiskunde, Celestijnenlaan 200B
3001 Leuven, Belgium
E-mail: christophe.debry@wis.kuleuven.be