AN ELEMENTARY PROOF FOR THE NUMBER OF SUPERSINGULAR ELLIPTIC CURVES

LUÍS R. A. FINOTTI

Abstract. Building on [Fin09], we give an elementary proof for the well known result that there exactly $\lceil (p-1)/4 \rceil - \lfloor (p-1)/6 \rfloor$ supersingular elliptic curves in characteristic p. We use a related polynomial instead of the supersingular polynomial itself to simplify the proof and this idea might be helpful to prove other results related to the supersingular polynomial.

Last revised: June 6, 2020.

1. Introduction

An elliptic curve over a field of characteristic $p > 0$ is *ordinary* if its p-torsion is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Otherwise, its p-torsion is trivial and we say that the elliptic curve is *supersingular*. It's a well known result that there are only finitely many supsersingular elliptic curves up to isomorphism, and in fact there are exactly $\lceil (p-1)/4 \rceil - \lfloor (p-1)/6 \rfloor$ supersingular elliptic curves in characteristic $p \geq 5$. More precisely, if k is an algebraically closed field of characteristic $p > 0$, or, more generally, if k contains $\mathbb{F}_{p^2}$, then there are exactly $\lceil (p-1)/4 \rceil - \lfloor (p-1)/6 \rfloor$ supersingular elliptic curves over k. (See for instance Chapter V of [Sil85].)

Hence, for a fixed characteristic $p > 0$, we define the *supersingular polynomial (in characteristic p)*, denoted by $\mathrm{ss}_p(X)$, as the monic polynomial that has simple roots exactly at the j-invariants of all supersingular elliptic curves, i.e.,

$$\mathrm{ss}_p(X) \stackrel{\text{def}}{=} \prod_{j \text{ supersig.}} (X - j). \tag{1.1}$$

In [Fin09], it was proved that the supersingular polynomial can be explicitly written as

$$\mathrm{ss}_p(X) = \left(-\frac{2}{9}\right)^r \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(-\frac{27}{4}\right)^i X^{i-r_1'} (X-1728)^{r_2'-i}, \tag{1.2}$$

where $r \stackrel{\text{def}}{=} (p-1)/2$, $r_1 \stackrel{\text{def}}{=} \lceil r/3 \rceil$, $r_2 \stackrel{\text{def}}{=} \lfloor r/2 \rfloor$, $r_1' \stackrel{\text{def}}{=} \lfloor r/3 \rfloor$, and $r_2' \stackrel{\text{def}}{=} \lceil r/2 \rceil$. Note, in particular, that $\mathrm{ss}_p(X) \in \mathbb{F}_p[X]$. More on the supersingular polynomial, including different

2000 *Mathematics Subject Classification.* Primary 11G20; Secondary 11G07.

Key words and phrases. arithmetic geometry, elliptic curves, supersingular polynomial.

formulas, can be found in Kaneko and Zagier's [KZ98], Brillhart and Morton's [BM04], and Morton's [Mor06]. We also note that the published formula in [Fin09] has a typo, but Eq. (1.2) is correct.

Note that in principle we are working over an algebraically closed field k of characteristic $p > 0$, so the supersingular j-invariants in Eq. (1.1) are taken to be in k. On the other hand, since $\mathrm{ss}_p \in \mathbb{F}_p[x]$, the polynomial itself does not depend on k, but simply on its characteristic.

Formula (1.2) above, which was nearly deduced by Deuring in [Deu41], was fully derived in [Fin09] by using the fact the an elliptic curve is supersingular if, and only if, its Hasse invariant is zero. (This result is due to Deuring and Hasse.) This was enough to obtain an expression quite close to the one above, where only a factor of X or $(X - 1728)$ would be missing. On the other hand, to show that this polynomial only has simple roots, we quoted the well-know result that there are exactly $(r_2' - r_1')$ supersingular j-invariants (up to isomorphism). (See, for instance, Theorem V.4.1(c) from [Sil85].)

At the end of [Fin09] an alternative proof is given, which is completely elementary. We first observe that $\mathrm{ss}_p(X)$ has simple roots if, and only if,

$$G(X) \overset{\mathrm{def}}{=} \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(-\frac{27}{4}\right)^i X^{i-r_1} (X-1728)^{r_2-i} \tag{1.3}$$

has simple roots, as it differs from $\mathrm{ss}_p(X)$ only by a constant multiple and possible factors of X or $(X - 1728)$. This second proof is then given by means of the differential equation

$$X(X-1728)G'' + ((-2r_2 + 2r_1 + 1)X - 1728(2r_1 + 1))G' + (r_2 - r_1)^2 G = 0, \tag{1.4}$$

which is deduced in that same paper. (Note that this differential equation is much simpler than the one for the actual supersingular polynomial $\mathrm{ss}_p(X)$, which can be found as Corollary 4.5 from [Fin09].)

(As a side note: the proof of expression (1.2) in [Fin09] is done by first showing the the right-hand side of this expression is monic and has all the supersingular j-invariants as roots, and then either quoting the known result on the number of supersingular elliptic curves or, equivalently, by proving that G above has simple roots.)

Although this latter proof is completely elementary, the deduction of Eq. (1.4) is not completely natural. It was motivated by similar proofs, and its deduction involved educated guesses and variation of parameters. Although this is perfectly valid, and give a nice and short proof of the statement without having to rely on any previous knowledge, as with the first proof given, we here would like to give a more direct proof of it, without using the differential equation. This proof is longer, but more direct and completely elementary.

More importantly, together with [Fin09], it illustrate a technique that can be helpful in proving results about the supersingular polynomial.

Our goal is then to prove, in a direct and elementary way, the following result:

Proposition 1.1. *The polynomial $G(X)$ (as in (1.3)) has only simple roots.*

Again, this was the last step in the proof of the formula given by Eq. (1.2), and with that we get the exact number of supersingular elliptic curves is its degree, i.e., $r_2' - r_1'$.

The original idea to attempt this new proof was to see if the techniques used in [Fin09] (and here) could be applied to a question of Kaneko and Zagier in [KZ98], where they ask for an elementary proof for the fact that if $p \equiv -1 \pmod{12}$ and $\mathrm{ss}_p(j) = 0$, then $\mathrm{ss}_p'(j) \in \mathbb{F}_p$. The idea was to rephrase the problem in terms of $G(X)$ instead of $\mathrm{ss}_p(X)$ (in fact, in terms of $\tilde{F}(X)$, as defined in Eq. (2.3) below). In that situation we have, for instance, that Eq. (2.7) below would relate $\tilde{F}$ and $\tilde{F}'$, which are related to ss_p and ss_p'.

Unfortunately we could not produce the elementary proof that was asked, but the work did yield this elementary proof for the number of supersingular elliptic curves.

On the other hand, together with [Fin09], these notes illustrate the overarching point that sometimes information about $\mathrm{ss}_p(X)$ can be more easily obtained by studying $\tilde{F}(X)$ instead, which is in fact the main point we try to make here.

2. The Proof

We start by restating Lemma 2.2 from [Fin09], which will be used here.

Lemma 2.1. *Let n and t be positive integers with $t \leq 3n$, and $n_1 \stackrel{\text{def}}{=} \max\{0, \lceil (3n-t)/3 \rceil\}$ and $n_2 \stackrel{\text{def}}{=} \min\{n, \lfloor (3n-t)/2 \rfloor\}$. Then, if $a, b \neq 0$, the coefficient of x^t in $(x^3+ax+b)^n$ is*

$$\left(\frac{b}{a}\right)^{3n-t} \sum_{i=n_1}^{n_2} \binom{n}{i} \binom{i}{3i-(3n-t)} \left(\frac{a^3}{b^2}\right)^i. \tag{2.1}$$

Remember that an elliptic curve in characteristic $p \geq 5$, given by an equation $y^2 = x^2 + ax + b$ is supersingular if, and only if, its *Hasse invariant*, which is given by that coefficient of x^{p-1} of $(x^3+ax+b)^{(p-1)/2}$, is zero. (Again, see [Sil85].) Then, Lemma 2.1 has a trivial consequence the following corollary:

Corollary 2.2. *If k is a field of characteristic $p \geq 5$ and E is an elliptic curve given by*

$$E/k \ : \ y^2 = f(x) \stackrel{\text{def}}{=} x^3 + ax + b, \tag{2.2}$$

with $a, b \neq 0$, then the Hasse invariant of E is

$$\left(\frac{b}{a}\right)^r \tilde{F}\left(\frac{a^3}{b^2}\right),$$

where

$$\tilde{F}(X) \overset{\text{def}}{=} \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} X^i. \tag{2.3}$$

So, if $a, b \neq 0$, then E is supersingular if, and only if, $\tilde{F}(a^3/b^2) = 0$.

Observe that if indeed $a, b \neq 0$, then a^3/b^2 is an invariant (under isomorphism) of E. In fact, as done in [Fin09], we have that if

$$F(X) \overset{\text{def}}{=} \frac{\tilde{F}(X)}{X^{r_1}} = \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} X^{i-r_1}, \tag{2.4}$$

then

$$G(X) = \left(-\frac{27}{4}\right)^{r_1} (X-1728)^{r_2-r_1} F\left(-\frac{27}{4} \cdot \frac{X}{X-1728}\right). \tag{2.5}$$

So, by construction, we have that $X = 1728$ is not a root of $G(X)$. Also, if $T(X) = -27X/4(X-1728)$, then

$$G'(X) = \left(-\frac{27}{4}\right)^{r_1} (X-1728)^{r_2-r_1-2} \left[(r_2-r_1)(X-1728)F(T(X)) + 1164F'(T(X))\right].$$

Thus, if $X = x_0$ is a root of $G(X)$ (and so $x_0 \neq 1728$), then $T(x_0)$ is a root of $F(X)$, and if x_0 is a double root of $G(X)$, then $T(x_0)$ is a also a double root of $F(X)$. Therefore, if $F(X)$ has no double roots, then neither does $G(X)$. Moreover, observe that $T(x_0) \neq -27/4$, so it suffices that $F(X)$ has no double roots different from $X = -27/4$. (In fact, $X = -27/4$ is not a root of $F(X)$, as seen at the end of Section 3 of[Fin09].)

To make our computations a bit more straight forward, we deal with $\tilde{F}(X)$ instead of $F(X)$ itself. So, our goal now is to prove the following proposition, which, from our previous remarks, is enough to prove Proposition 1.1.

Proposition 2.3. *If λ is a double (or higher order) root of $\tilde{F}(X)$, then λ is either 0 or $-27/4$.*

The rest of these notes is devoted to the proof of the proposition above. We proceed by contradiction. Assume then that we have a double root. If this root is non-zero and different from $-27/4$, we can assume that it has the form a^3/b^2 with $a, b \neq 0$, with a and b defining an elliptic curve as in Eq. (2.2). So, assume that $\tilde{F}(a^3/b^2) = 0$ and $\tilde{F}'(a^3/b^2) = 0$.

Reminding that $f(x) \overset{\text{def}}{=} x^3 + ax + b$, let a_i and b_i be such that

$$f(x)^r = \sum_{i=0}^{3r} a_i x^i \qquad \text{and} \qquad f(x)^{r-1} = \sum_{i=0}^{3r-3} b_i x^i. \tag{2.6}$$

By Lemma 2.1,

$$\begin{aligned} b_{p-4} &= \left(\frac{b}{a}\right)^r \sum_{i=r_1}^{r_2} \binom{r-1}{i}\binom{i}{3i-r}\left(\frac{a^3}{b^2}\right)^i \\ &= \left(\frac{b}{a}\right)^r \sum_{i=r_1}^{r_2} \left(1-\frac{i}{r}\right)\binom{r}{i}\binom{i}{3i-r}\left(\frac{a^3}{b^2}\right)^i \\ &= \left(\frac{b}{a}\right)^r \left(\tilde{F}\left(\frac{a^3}{b^2}\right) - \frac{1}{r}\frac{a^3}{b^2}\tilde{F}'\left(\frac{a^3}{b^2}\right)\right). \end{aligned} \tag{2.7}$$

So, if $\tilde{F}(a^3/b^2) = \tilde{F}'(a^3/b^2) = 0$, then $a_{p-1} = b_{p-4} = 0$.

Let

$$\begin{aligned} f^r &= f_1 x^p + f_2, \quad \text{with} \quad \deg f_1 = r-1, \ \deg f_2 \le p-2; \\ f^{r-1} &= g_1 x^p + g_2, \quad \text{with} \quad \deg g_1 = r-4, \ \deg g_2 \le p-1. \end{aligned}$$

(Note that $a_{p-1} = 0$.)

The proof of the proposition will be broken in smaller steps:

Step 1. $\deg g_2 \le p-5$, and hence $f_i = f\, g_i$ for $i = 1, 2$.

Proof. Observing that

$$\frac{\mathrm{d}}{\mathrm{d}x}(f^r) = \sum_{i=0}^{3r-1} (i+1) a_{i+1} x^i,$$

but also

$$\frac{\mathrm{d}}{\mathrm{d}x}(f^r) = -\frac{1}{2}(3x^2 + a) \sum_{i=0}^{3r-3} b_i x^i,$$

comparing the terms x^{p-2} in these equations, we obtain $b_{p-2} = 0$ (since $b_{p-4} = 0$), and comparing the terms x^{p-2}, we obtain $b_{p-3} = -a\, b_{p-1}/3$. Also, since

$$\sum_{i=0}^{3r} a_i x^i = (x^3 + ax + b) \sum_{i=0}^{3r-3} b_i x^i,$$

comparing the terms in x^{p-1} gives that $b_{p-1} = 0$, and hence also $b_{p-3} = 0$.

□

Step 2.

$$f\, g_2' = -\frac{3}{2} f' g_2. \tag{2.8}$$

Proof. We have,

$$\frac{\mathrm{d}}{\mathrm{d}x}(f^r) = -\frac{1}{2} f^{r-1} f' = -\frac{1}{2}(f' g_1 x^p + f' g_2).$$

On the other hand, also

$$\frac{\mathrm{d}}{\mathrm{d}x}(f^r) = f_1' x^p + f_2'.$$

So, by Step 1, we have

$$f_2' = (-1/2) f' g_2. \tag{2.9}$$

Again by Step 1, $f_i = f\, g_i$, for $i = 1, 2$, and so,

$$f_2' = \frac{\mathrm{d}}{\mathrm{d}x}(f\, g_2) = f' g_2 + f g_2',$$

which, together with equation (2.9), gives

$$f\, g_2' = -\frac{3}{2} f' g_2.$$

□

Step 3. $\deg g_2 = (p-9)/2$.

Proof. By Step 1, we have

$$g_2 = \sum_{i=0}^{k} b_i x^i,$$

for some $k \leq (p-5)$. Comparing coefficients of x^{k+2} in equation (2.8), we have $k\, b_k = -(9/2) b_k$. Hence, if p does not divide $(2k+9)$, then $\deg g_2 \leq (k-1)$.

Since $k \leq (p-5)$, we have that $2k + 9 \leq 2p - 1$, and therefore, if p divides $2k+9$, then $p = 2k + 9$.

If $b_{(p-9)/2} = 0$, then we can proceed as above for all $k \geq 0$, thus obtaining that $g_2 = 0$. Otherwise, $\deg g_2 = (p-9)/2$.

If $g_2 = 0$, then $f_2 = 0$, but $f_2(0) = b^r \neq 0$. Therefore, $\deg g_2 = (p-9)/2$. □

Step 4. $a_{r-1} \neq 0$ and

$$f_1 = \frac{1}{a_{r-1}} f_2.$$

Proof. By the previous step, and since $f_2 = f\, g_2$, we have that $\deg f_2 = (p-3)/2 = (r-1)$, and hence $a_{r-1} \neq 0$. Now,

$$(x^{3p} + a^p x^p + b^p) = f^p = f (f^r)^2 = f\, (f_1^2 x^{2p} + 2 f_1 f_2 x^p + f_2^2).$$

Thus, since $\deg f_1^2 = \deg f_2^2 = \deg f_1\, f_2 = (p-3)$ (observe that f_1 is monic),

$$f \left(\frac{1}{a_{r-1}} f_2 \right)^2 = x^p + C_1,$$
$$f\, f_1^2 = x^p + C_2,$$

with $C_1, C_2 \in k$. It follows, by the uniqueness of the quotient of the division of x^p by f, that $f_1^2 = (1/a_{r-1}\, f_2)^2$. Hence, since f_1 and $(1/a_{r-1}) f_2$ are monic, $f_1 = (1/a_{r-1}) f_2$.

□

This last step gives us:

$$(x^3+ax+b)(f_1^2x^{2p}+2a_{r-1}f_1^2x^p+a_{r-1}^2f_1^2)=(x^{3p}+a^px^p+b^p). \tag{2.10}$$

Comparing the terms in x^{2p}, x^p and constant term, we have

$$\begin{aligned} bf_1(0)^2+2a_{r-1}&=0,\\ b2a_{r-1}f_1(0)^2+a_{r-1}^2&=a^p,\\ ba_{r-1}^2f_1(0)^2&=b^p. \end{aligned}$$

It follows that

$$\begin{aligned} bf_1(0)^2&=-2a_{r-1},\\ b^p&=-2a_{r-1}^3,\\ a^p&=-3a_{r-1}^2. \end{aligned}$$

Hence, $(a^3/b^2)^p=-27/4$, and so $a^3/b^2=-27/4$, which contradicts our assumptions and concludes the proof of Proposition 2.3.

3. Conflict of Interests

The author states that there is no conflict of interests.

References

[BM04] J. Brillhart and P. Morton. Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial. *J. Number Theory*, 106(1):79–111, 2004.

[Deu41] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenköper. *Abh. Math. Sem. Univ. Hamburg*, 14:197–272, 1941.

[Fin09] L. R. A. Finotti. A formula for the supersingular polynomial. *Acta Arith.*, 139(3):265–273, 2009.

[KZ98] M. Kaneko and D. Zagier. Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 97–126. Amer. Math. Soc., Providence, RI, 1998.

[Mor06] P. Morton. Explicit identities for invariants of elliptic curves. *J. Number Theory*, 120(2):234–271, 2006.

[Sil85] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1985.

Department of Mathematics, University of Tennessee, Knoxville, TN – 37996
Email address: lfinotti@utk.edu