A FORMULA FOR THE SUPERSINGULAR POLYNOMIAL: ADDENDUM

LUÍS R. A. FINOTTI

ABSTRACT. In these notes we prove give a (different) elementary proof that the the equation given for the supersingular polynomial in [Fin08] has simple roots.

Last revised: September 10, 2008.

1. INTRODUCTION

In [Fin08], it was proved that the supersingular polynomial

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

can be explicitly written as

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

where, if p is the characteristic of the field of definition of the curve, then $r \stackrel{\text{def}}{=} (p-1)/2$, $r_1 \stackrel{\text{def}}{=} \lceil r/3 \rceil$, $r_2 \stackrel{\text{def}}{=} \lfloor r/2 \rfloor$, $r_1' \stackrel{\text{def}}{=} \lfloor r/3 \rfloor$, and $r_2' \stackrel{\text{def}}{=} \lceil r/2 \rceil$.

This formula was deduced by using the fact the an elliptic curve is supersingular if, and only if, its Hasse invariant is zero. 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 invariants j-invariants.

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

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

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

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

1991 *Mathematics Subject Classification.* Primary 11G20; Secondary 11T71.

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

which is deduced in that same paper.

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 quite fine, 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 hopefully can be of some interest.

Our goal is then to prove the following:

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

2. The Proof

As a trivial consequence of the Lemma 2.2 from [Fin08], we have:

Proposition 2.1. *If E is given by*

$$E/k \ : \ y^2 = f(x) \stackrel{\text{def}}{=} x^3 + ax + b \tag{2.1}$$

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

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

where

$$\tilde{F}(X) \stackrel{\text{def}}{=} \sum_{i=r_1}^{r_2} \binom{r}{i}\binom{i}{3i-r} X^i. \tag{2.2}$$

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

Proof. Just remember that an elliptic curve is supersingular if, and only if, the Hasse invariant is zero, and that the Hasse invariant a of curve as in (2.1) is the coefficient of x^{p-1} in $f(x)^r$. (Remember, $r \stackrel{\text{def}}{=} (p-1)/2$.) □

Observe that if indeed $a, b \neq 0$, then a^3/b^2 is an invariant (under isomorphisms) of E. In fact, as done in [Fin08], we have that if

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

then

$$G(X) = \left(-\frac{27}{4}\right)^{r_1} (X-1728)^{r_2-r_1} F\left(-\frac{27}{4}\cdot\frac{X}{X-1728}\right). \tag{2.4}$$

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 in [Fin08].)

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 2.2. *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. (2.1). So, assume that $\tilde{F}(a^3/b^2) = 0$ and $\tilde{F}'(a^3/b^2) = 0$.

Let a_i and b_i be such that

$$f(x)^r = \sum_{i=0}^{3r} a_i x^i \qquad \text{and} \qquad f(x)^{r-1} = \sum_{i=0}^{3r-3} b_i x^i. \tag{2.5}$$

By Lemma 2.2 from [Fin08],

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

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

Let

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

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

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

Step 1. $\deg g_2 \leq p-5$.

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.

$$f\, g_2' = -\frac{3}{2}f' g_2. \tag{2.6}$$

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

$$f_2' = (-1/2) f' g_2. \tag{2.7}$$

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 (2.7), 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 (2.6), 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.

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

Proof. By the previous step, and since $f_2 = f\, g_2$, we have that $\deg f_2 = (p-3)/2 = (r-1)$. 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:

$$(x^3 + ax + b)(f_1^2 x^{2p} + 2a_{r-1} f_1^2 x^p + a_{r-1}^2 f_1^2) = (x^{3p} + a^p x^p + b^p). \tag{2.8}$$

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

$$b f_1(0)^2 + 2a_{r-1} = 0,$$
$$b 2a_{r-1} f_1(0)^2 + a_{r-1}^2 = a^p,$$
$$b a_{r-1}^2 f_1(0)^2 = b^p.$$

It follows that

$$b f_1(0)^2 = -2a_{r-1},$$
$$b^p = -2a_{r-1}^3,$$
$$a^p = -3a_{r-1}^2.$$

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 2.2.

References

[Fin08] L. R. A. Finotti. A new formula for the supersingular polynomial. Available at `http://www.math.utk.edu/~finotti/`, 2008.

Department of Mathematics, University of Tennessee, Knoxville, TN – 37996
E-mail address: `finotti@math.utk.edu`