ACTA ARITHMETICA
139.3 (2009)

A formula for the supersingular polynomial

by

LUÍS R. A. FINOTTI (Knoxville, TN)

1. Introduction. Let k be a perfect field of characteristic $p > 0$ and E/k an elliptic curve over k. If $\bar{k}$ denotes the algebraic closure of k, then $E(\bar{k})$ is an Abelian group and its p-torsion, denoted by $E[p]$, is either 0 or $\mathbb{Z}/p\mathbb{Z}$. (See, for instance, Theorem V.3.1 in [7].) E is then called *supersingular* if $E[p] = 0$, and *ordinary* otherwise. (As observed by Silverman in Remark V.3.2.2 of [7], there are other characterizations of supersingular elliptic curves relevant to various applications.)

It is a known fact that, for a fixed characteristic $p > 0$, there are (up to isomorphism) finitely many supersingular elliptic curves. (See, for instance, Theorem V.4.1(c) of [7].) Let s be the number of supersingular elliptic curves (for the fixed characteristic p) and $j_1, \ldots, j_s$ be the j-invariants of these curves. The *supersingular polynomial* is defined as

$$\mathrm{ss}_p(X) := \prod_{i=1}^{s} (X - j_i). \tag{1.1}$$

In these notes we deduce an explicit formula for ss_p.

Deuring (in [2]) gave a characterization of supersingular elliptic curves for $p > 2$ based on the *Legendre form*: if E is given by

$$E/k \ : \ y^2 = x(x-1)(x-\lambda), \tag{1.2}$$

then E is supersingular if, and only if, λ is a root of

$$L_p(X) := \sum_{i=0}^{r} \binom{r}{i}^2 X^i, \quad \text{where} \quad r := \frac{p-1}{2}. \tag{1.3}$$

It turns out that this polynomial has distinct roots in $\bar{k}$, which allows us to deduce that there are exactly $\lceil r/2 \rceil - \lfloor r/3 \rfloor$ supersingular elliptic curves (up to isomorphism) in characteristic p.

2000 *Mathematics Subject Classification*: Primary 11G20; Secondary 11G07.
Key words and phrases: arithmetic geometry, elliptic curves, supersingular polynomial.

DOI: 10.4064/aa139-3-5

On the other hand, the supersingular polynomial, as previously defined, seems to yield a more natural criterion for supersingularity, since it depends on the j-invariant directly, which would be more appropriate in most situations than the λ for the curve's Legendre form. Deuring, also in [2], found formulas for the *Hasse invariant* (see Section 2) of an elliptic curve in terms of the j-invariant, from which one can deduce a formula for ss_p. In fact, we will follow a similar approach and the formula deduced here could be derived from Deuring's formulas without too much difficulty. Hence, the formula presented in these notes is not necessarily new, but as far as the author knows, it has not appeared explicitly in other publications. Also, the formula as presented here is not broken into cases depending on the congruence class of p modulo 12, as are the formulas presented by Deuring.

Several papers have dealt with the supersingular polynomial in the past, notably [5], [1], and [6]. In [1], J. Brillhart and P. Morton give an explicit formula for the supersingular polynomial, which depends on the *Jacobi polynomials* $P_n^{(\alpha,\beta)}$. In [5], which is partially expository, a few different polynomials in $\mathbb{Q}[X]$ are given that reduce to the supersingular polynomial and, in particular, the *Atkin's polynomials* are quite explicit. Also, Morton's [6] has a few formulas, and in fact mentions that a formula can also be deduced from Deuring's [2]. The formula given here is simpler than most previous formulas, except the one given by equations (1.2) and (1.6) of [6], which is equally simple.

We have:

Theorem 1.1. *Let $p \geq 5$. Then*

$$\mathrm{ss}_p(X) = (-2)^r \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(-\frac{27}{4}\right)^i X^{i-r_1'} (X-1728)^{r_2'-i}, \tag{1.4}$$

where $r := (p-1)/2$, $r_1 := \lceil r/3 \rceil$, $r_2 := \lfloor r/2 \rfloor$, $r_1' := \lfloor r/3 \rfloor$ and $r_2' := \lceil r/2 \rceil$.

In Section 4, we give an application of the approach taken here, giving a direct and elementary proof of the known and complex differential equation satisfied by the supersingular polynomial.

2. Deduction of the formula. Let k be a perfect field of characteristic $p \geq 5$ and E/k an elliptic curve over k:

$$E/k \, : \, y^2 = x^3 + ax + b. \tag{2.1}$$

Then the *Hasse invariant* of E is the coefficient x^{p-1} in $(x^3+ax+b)^{(p-1)/2}$. The following theorem, which is the only non-elementary result that we need here, gives a simple criterion for supersingularity, and is the crucial step of our deduction.

THEOREM 2.1 (Deuring, Hasse). *An elliptic curve E given by* (2.1) *is supersingular if, and only if, its Hasse invariant is zero.*

To find an explicit formula for the Hasse invariant, we provide the following simple lemma:

LEMMA 2.2. *Let n and t be positive integers with $t \leq 3n$, and $n_1 := \max\{0, \lceil (3n-t)/3 \rceil\}$ and $n_2 := \min\{n, \lfloor (3n-t)/2 \rfloor\}$. Then, if $a, b \neq 0$, the coefficient of x^t in $(x^3+ax+b)^n$ is*

$$\left(\frac{b}{a}\right)^{3n-t} \sum_{i=n_1}^{n_2} \binom{n}{i} \binom{i}{3i-(3n-t)} \left(\frac{a^3}{b^2}\right)^i. \tag{2.2}$$

Proof. One has

$$\begin{aligned}(x^3+ax+b)^n &= \sum_{i=0}^{n} \binom{n}{i} x^{3(n-i)}(ax+b)^i \\ &= \sum_{i=0}^{n}\sum_{l=0}^{i} \binom{n}{i}\binom{i}{l} a^l b^{i-l} x^{3n+l-3i}.\end{aligned}$$

Hence, the terms in x^t are obtained when $3n+l-3i = t$, i.e., $l = 3i-(3n-t)$. Since $l \geq 0$, we must have $i \geq \lceil (3n-t)/3 \rceil$, and since $l \leq i \leq n$, we must have $i \leq \lfloor (3n-t)/2 \rfloor$. ∎

Thus, if E is as in (2.1), then the Hasse invariant is given by

$$\left(\frac{b}{a}\right)^{r} \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(\frac{a^3}{b^2}\right)^i, \tag{2.3}$$

where $r := (p-1)/2$, $r_1 := \lceil r/3 \rceil$, and $r_2 := \lfloor r/2 \rfloor$. (We shall keep this notation throughout these notes.) Note that the use of floor and ceiling above prevents the need of dealing with different cases for the congruence class of p modulo 12.

So, if $a \neq 0$ (i.e., $j \neq 0$) and $b \neq 0$ (i.e., $j \neq 1728$), then E is supersingular if, and only if, a^3/b^2 is a root of

$$F(X) := \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} X^{i-r_1}. \tag{2.4}$$

The j-invariant of E is given by

$$j := 1728\,\frac{4a^3}{4a^3+27b^2}.$$

So, if $a \neq 0$ and $b \neq 0$, then

$$\frac{a^3}{b^2} = -\frac{27}{4} \cdot \frac{j}{j-1728}.$$

Thus, if $j \neq 0$ and $j \neq 1728$, E is supersingular if, and only if, j is a root of

$$F\left(-\frac{27}{4} \cdot \frac{X}{X-1728}\right).$$

Clearing denominators, we obtain

$$G(X) := \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(-\frac{27}{4}\right)^i X^{i-r_1} (X-1728)^{r_2-i}. \tag{2.5}$$

So, E is supersingular, with $j \neq 0, 1728$, if, and only if, its j-invariant is a root of $G(X)$.

We now deal with the cases when $j = 0$ or $j = 1728$. (It is well known when those values are supersingular, but we present a proof here, since this can be easily deduced from the Hasse invariant.) If $j = 1728$ (i.e., $b = 0$), then the Hasse invariant of E, which we shall denote by A, is given by the coefficient of x^{p-1} in

$$(x^3 + ax)^r = \sum_{i=0}^{r} \binom{r}{i} a^i x^{3r-2i}.$$

So,

$$A = \begin{cases} 0 & \text{if } r \equiv 1 \pmod 2, \\ \binom{r}{r/2} a^{r/2} & \text{if } r \equiv 0 \pmod 2. \end{cases}$$

Therefore, if $r \equiv 1 \pmod 2$, we should multiply $G(X)$ by $X - 1728$, and leave it unchanged otherwise. Hence, if we let $r_2' := \lceil r/2 \rceil$, this can be accomplished by changing $(X-1728)^{r_2-i}$ in G ((2.5)) to $(X-1728)^{r_2'-i}$.

If $j = 0$ (i.e., $a = 0$), then the Hasse invariant of E is given by the coefficient of x^{p-1} in

$$(x^3 + b)^r = \sum_{i=0}^{r} \binom{r}{i} b^i x^{3(r-i)}.$$

So,

$$A = \begin{cases} 0 & \text{if } r \not\equiv 0 \pmod 3, \\ \binom{r}{r/3} b^{r/3} & \text{if } r \equiv 0 \pmod 3. \end{cases}$$

Therefore, if $r \not\equiv 0 \pmod 3$, we should multiply $G(X)$ by X, and leave it unchanged otherwise. Hence, if we let $r_1' := \lfloor r/3 \rfloor$, this can be accomplished by changing X^{i-r_1} in G ((2.5)) to $X^{i-r_1'}$.

So, the roots of the polynomial

$$H(X) := \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(-\frac{27}{4}\right)^i X^{i-r_1'} (X-1728)^{r_2'-i} \tag{2.6}$$

are exactly the j-invariants of the supersingular polynomial. Since we know (see Theorem V.4.1(c) of [7]) that there are exactly $r_2' - r_1'$ such j-invariants,

$H(X)$ has no multiple roots and therefore is, up to a constant multiple, the supersingular polynomial. (An alternative proof of this fact will be given in Section 4. See also [3].)

3. The leading coefficient. In this section we finish the construction of the supersingular polynomial by adjusting the leading coefficient of $H(X)$. This coefficient is given by

$$\sum_{i=r_1}^{r_2} \binom{r}{i}\binom{i}{3i-r}\left(-\frac{27}{4}\right)^i. \tag{3.1}$$

Also, by (2.3), the coefficient of x^{p-1} in the polynomial $(x^3-3x+2)^r = (x-1)^{p-1}(x+2)^{(p-1)/2}$ is

$$\left(-\frac{2}{3}\right)^r \sum_{i=r_1}^{r_2} \binom{r}{i}\binom{i}{3i-r}\left(-\frac{27}{4}\right)^i.$$

We will now simplify the expression for this coefficient.

We need the following simple lemma:

Lemma 3.1. *If $h(x) := (x-1)^{p-1}(x+2)^r$ (in characteristic p), then*

$$h^{(n)}(0) = \begin{cases} n!\displaystyle\sum_{i=0}^{n}\binom{r}{i}2^{r-i} & \text{if } 0 \le n \le r, \\ n!\,3^r & \text{if } n \ge r. \end{cases}$$

Proof. We prove the lemma by induction. For $n=0$, the statement is trivially true. So, assume it is true for $n-1$, with $n \le r$. We have

$$\frac{d^n}{dx^n}((x-1)h(x)) = (x-1)^p\,\frac{d^n}{dx^n}(x+2)^r = (x-1)^p\,\frac{r!}{(r-n)!}\,(x+2)^{r-n}.$$

On the other hand, Leibniz rule gives us

$$\frac{d^n}{dx^n}((x-1)h(x)) = nh^{(n-1)}(x) + (x-1)h^{(n)}(x). \tag{3.2}$$

Comparing these two equations and evaluating at $x=0$, the induction hypothesis gives us

$$\begin{aligned} h^{(n)}(0) &= \frac{r!}{(r-n)!}\,2^{r-n} + nh^{(n-1)}(0) = \frac{r!}{(r-n)!}\,2^{r-n} + n!\sum_{i=0}^{n-1}\binom{r}{i}2^{r-i} \\ &= n!\sum_{i=0}^{n}\binom{r}{i}2^{r-i}. \end{aligned}$$

Hence, the lemma holds for all $n \le r$.

Observing that

$$\sum_{i=0}^{r} \binom{r}{i} 2^{r-i} = (1+2)^r,$$

we can proceed by assuming that the statement holds for some $n-1$ with $n \geq r+1$. Then, since

$$\frac{d^n}{dx^n}((x-1)h(x)) = (x-1)^p \, \frac{d^n}{dx^n}((x+2)^r) = 0$$

by (3.2), and using the induction hypothesis, we obtain

$$h^{(n)}(0) = nh^{(n-1)}(0) = n!\, 3^r,$$

which concludes the proof. ∎

Thus, the coefficient of x^{p-1} in $h(x) = (x-3x+2)^r$ is 3^r. (Note that this also implies that $F(-27/4) \neq 0$.) So, the leading coefficient of $H(X)$ is

$$\left(-\frac{3}{2}\right)^r 3^r = \frac{1}{(-2)^r},$$

which gives us the following formulas for the supersingular polynomial (still with $p \geq 5$):

$$\begin{aligned} \mathrm{ss}_p(X) &= (-2)^r \sum_{i=r_1}^{r_2} \binom{r}{i}\binom{i}{3i-r}\left(-\frac{27}{4}\right)^i X^{i-r_1'}(X-1728)^{r_2'-i} \\ &= \sum_{l=r_1-r_1'}^{r_2'-r_1'} \left[(-2)^r(-1728)^{r_2'-r_1'-l} \sum_{i=r_1}^{r_1'+l} \left(-\frac{27}{4}\right)^i \binom{r}{i}\binom{i}{3i-r}\binom{r_2'-i}{r_1'+l-i}\right] X^l. \end{aligned}$$

4. Differential equations. Finally, we give differential equations satisfied by the polynomials F, G, and ss_p, which can sometimes be useful. In fact, Igusa proved in [4] that $L_p(X)$ (given by (1.3)) has simple roots by using the fact that L_p satisfies the following differential equation:

$$4X(1-X)L_p'' + 4(1-2X)L_p' - L_p = 0.$$

(One should observe that this equation comes up naturally in a proper context, which we shall not describe here.) In the same spirit, we shall give a proof, at the end of this section, that H has simple roots, which was crucial to proving that it gives the supersingular polynomial up to a constant multiple. This would avoid quoting the known result on the number of supersingular elliptic curves for a given characteristic, as we have done in Section 2.

One should note that the differential equations given for G and ss_p are certainly not new, but the proofs given here are elementary and do not depend on any previous result, as the simplicity of the formulas allows us to check them directly. We start with a differential equation for

$$\tilde{F}(X) := X^{r_1} \cdot F(X) = \sum_{i=r_1}^{r_2} \binom{r}{i}\binom{i}{3i-r} X^i. \tag{4.1}$$

This has a quite simple differential equation, from which we deduce all others. Note that by (2.3), we have

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

Proposition 4.1. *We have*

$$4X^2(4X+27)\tilde{F}'' + 4X(8X+27)\tilde{F}' + 3(X-1)\tilde{F} = 0. \tag{4.2}$$

Proof. Expanding the left-hand side of (4.2) using (4.1), we find that the term in X^{i+1} has coefficient

$$\binom{r}{i}\binom{i}{3i-r}(16i(i-1)+32i+3) + \binom{r}{i+1}\binom{i+1}{3i+3-r}(108(i+1)i+108i-2).$$

We can then factor out $r!/((r-i)!(3i+3-r)!(r-2i)!)$ from this expression, leaving

$$(16i^2+16i+3)(3i+3-r)(3i+2-r)(3i+1-r) \\ + (108i^2+216i+105)(r-i)(r-2i)(r-2i-1).$$

Since we are in characteristic p and $r=(p-1)/2$, a simple calculation shows that the expression above is zero. ∎

We now proceed to deduce the other equations. Their proofs are simple and tedious, so we shall only give a brief description of the necessary steps.

Proposition 4.2. *The polynomial* $F(X)$ (*defined by* (2.4)) *satisfies the following differential equation*:

$$X(4X+27)F'' + (8(r_1+1)X + 27(2r_1+1))F' + \left(4r_1 + \frac{31}{36}\right)F = 0. \tag{4.3}$$

Proof. We just use (4.1) to replace $\tilde{F}$ (and its derivatives) by F (and its derivatives) in (4.2). After that, we can divide the resulting expression by X^{r_1}.

Then, observing that in characteristic p we always have $r_1^2 = 1/36$, one obtains (4.3). ∎

Proposition 4.3. *The polynomial* $G(X)$ (*defined by* (2.5)) *satisfies the following differential equation*:

$$X(X-1728)G'' + ((-2r_2+2r_1+1)X - 1728(2r_1+1))G' \\ + (r_2-r_1)^2G = 0. \tag{4.4}$$

Proof. The idea is the same as before. We just use

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

to replace F (and its derivatives) by G (and its derivatives) in (4.3). We multiply by $432(X - 1728)^{r_2 - r_1}$ to clear denominators.

Observing that

$$(2r_1 + 1)(r_2 - r_1) + \frac{31}{144} + r_1 = (r_2 - r_1)^2,$$

which can be easily done, for instance by checking the possible congruences of p modulo 12 (which gives specific values for r_1 and r_2 in characteristic p), one can then divide the resulting expression by $X - 1728$, obtaining (4.4). ■

We observe that (4.4) is the same as (1.6) in [1].

Finally, we find a differential equation for the supersingular polynomial itself.

Proposition 4.4. *Let* $B(X) := X^{r_1 - r_1'}(X - 1728)^{r_2' - r_2}$ *and* $C_0(X)$, $C_1(X)$, *and* $C_2(X)$ *be the coefficients of* G, G', *and* G'' *in* (4.4) *respectively. Also, let*

$$\begin{aligned} D_2(X) &:= C_2 B, \\ D_1(X) &:= C_1 B - 2C_2 B', \\ D_0(X) &:= C_0 B - C_1 B' + 2((B')^2 - (r_1 - r_1')(r_2' - r_2)B)C_2/B. \end{aligned}$$

Then

$$D_2\,\mathrm{ss}_p'' + D_1 \mathrm{ss}_p' + D_0\,\mathrm{ss}_p = 0. \tag{4.5}$$

Proof. As before, just use $\mathrm{ss}_p(X) = B(X)G(X)$ to obtain (4.5) from (4.4). (Note that the term C_2/B in D_0 is in fact a polynomial.) ■

Although (4.5) does not depend on the possible congruences of p modulo 12, making it somewhat more direct, we can give clearer equations if we break it into cases.

Corollary 4.5. *Let* $p \geq 5$ *be prime. If* $p \equiv 1 \pmod{12}$, *then*

$$X(X - 1728)\,\mathrm{ss}_p'' + \frac{1}{6}\,(7X - 6912)\,\mathrm{ss}_p' + \frac{1}{144}\,\mathrm{ss}_p = 0.$$

If $p \equiv 5 \pmod{12}$, *then*

$$X^2(X - 1728)\,\mathrm{ss}_p'' - \frac{1}{6}\,X(X - 6912)\,\mathrm{ss}_p' + \frac{1}{144}\,(49X - 165888)\,\mathrm{ss}_p = 0.$$

If $p \equiv 7 \pmod{12}$, *then*

$$X(X - 1728)^2\,\mathrm{ss}_p'' + \frac{1}{6}\,(X - 1728)(X - 6912)\,\mathrm{ss}_p' + \frac{1}{144}\,(25X + 81216)\,\mathrm{ss}_p = 0.$$

If $p \equiv 11 \pmod{12}$, *then*

$$X^2(X-1728)^2\,\mathrm{ss}_p'' - \frac{1}{6}\,(X-1728)(7X-6912)\,\mathrm{ss}_p' + \frac{1}{144}\,(169X^2 - 333504X + 286654464)\,\mathrm{ss}_p = 0.$$

We now use the differential equation (4.4) to prove that $H(X)$ has only simple roots. Indeed, if $H(x_0) = H'(x_0) = 0$, with $x_0 \neq 0, 1728$, we also have $H''(x_0) = 0$. Then successive differentiation would give that x_0 is a zero of $H(X)$ of infinite order, which is a contradiction. But also note that neither $X = 0$ nor $X = 1728$ can be a root of $H(X)$, as one can clearly see from the definition (remembering that $r_1 \leq r_2 \leq r = (p-1)/2 < p$), and hence $H(X)$ has no multiple roots at all.

Acknowledgements. The author would like to thank P. Morton and J. Cogdell for their useful comments.

References

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

[2] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14 (1941), 197–272.

[3] L. R. A. Finotti, *A formula for the supersingular polynomial: Addendum*, http://www.math.utk.edu/~finotti/, 2008.

[4] J.-I. Igusa, *Class number of a definite quaternion with prime discriminant*, Proc. Nat. Acad. Sci. U.S.A. 44 (1958), 312–314.

[5] M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, in: Computational Perspectives on Number Theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math. 7, Amer. Math. Soc., Providence, RI, 1998, 97–126.

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

[7] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1985.

Department of Mathematics
University of Tennessee
Knoxville, TN 37996, U.S.A.
E-mail: finotti@math.utk.edu

Received on 13.9.2008
and in revised form on 28.1.2009 (5798)