Pacific Journal of Mathematics

FORMAL GROUPS OF ELLIPTIC CURVES WITH POTENTIAL GOOD SUPERSINGULAR REDUCTION

Álvaro Lozano-Robledo

Volume 261 No. 1 January 2013

PACIFIC JOURNAL OF MATHEMATICS
Vol. 261, No. 1, 2013
dx.doi.org/10.2140/pjm.2013.261.145

FORMAL GROUPS OF ELLIPTIC CURVES WITH POTENTIAL GOOD SUPERSINGULAR REDUCTION

ÁLVARO LOZANO-ROBLEDO

Let L be a number field and let E/L be an elliptic curve with potentially supersingular reduction at a prime ideal $\wp$ of L above a rational prime p. In this article we describe a formula for the slopes of the Newton polygon associated to the multiplication-by-p map in the formal group of E, depending only on the congruence class of p mod 12, the $\wp$-adic valuation of the discriminant of a model for E over L, and the valuation of the j-invariant of E. The formula is applied to prove a divisibility formula for the ramification indices in the field of definition of a p-torsion point.

1. Introduction

Let L be a number field with ring of integers $\mathcal{O}_L$, let $p \geq 2$ be a prime, let $\wp$ be a prime ideal of $\mathcal{O}_L$ lying above p, and let $L_\wp$ be the completion of L at $\wp$. Let E be an elliptic curve defined over L with potential good (supersingular) reduction at $\wp$. Let us fix an embedding $\iota : \overline{L} \hookrightarrow \overline{L}_\wp$. Via ι, we may regard E as defined over $L_\wp$. Let $L_\wp^{\mathrm{nr}}$ be the maximal unramified extension of $L_\wp$, and let K_E be the extension of $L_\wp^{\mathrm{nr}}$ of minimal degree such that E has good reduction over K_E (see Section 3 for more details). Let $K = K_E$, and let ν_K be a valuation on K such that $\nu_K(p) = e$ and $\nu_K(\pi) = 1$, where π is a uniformizer for K. Let A be the ring of elements of K with nonnegative valuation. We fix a minimal model of E over A with good reduction, given by

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

with $a_i \in A$. In particular, the discriminant Δ is a unit in A. Let $\hat{E}/A$ be the formal group associated to E/A, with formal group law given by a power series $F(X, Y) \in A[[X, Y]]$, as defined in [Silverman 2009, Chapter IV]. Let

$$[p](Z) = \sum_{i=1}^{\infty} s_i Z^i$$

MSC2010: primary 11G05, 11G07; secondary 14H52, 14L05.
Keywords: elliptic curves, supersingular, formal group, torsion points.

be the multiplication-by-p homomorphism in $\hat{E}$, for some $s_i \in A$ for all $i \geq 1$. Since E/K has good supersingular reduction, the formal group $\hat{E}/A$ associated to E has height 2; see [Silverman 2009, Chapter V, Theorem 3.1]. Thus, $s_1 = p$ and the coefficients s_i satisfy $\nu_K(s_i) \geq 1$ if $i < p^2$ and $\nu_K(s_{p^2}) = 0$. Let $q_0 = 1$, $q_1 = p$ and $q_2 = p^2$, and put $e_i = \nu_K(s_{q_i})$. In particular $e_0 = \nu_K(s_1) = \nu_K(p) = e$ and $e_2 = \nu_K(s_{p^2}) = 0$. Let $e_1 = \nu_K(s_p)$. Then, the multiplication-by-p map can be expressed as

$$[p](Z) = pf(Z) + \pi^{e_1} g(Z^p) + h(Z^{p^2}),$$

where $f(Z)$, $g(Z)$ and $h(Z)$ are power series in $Z \cdot A[[Z]]$, with

$$f'(0) = g'(0) = h'(0) \in A^\times.$$

In this article, we are interested in determining the value of e_1. In the next section we discuss three examples that will be used during the rest of the paper to fix ideas. In Section 3, we prove consecutive refinements of a formula for e_1 that culminate in Theorem 3.9 and Corollary 3.12, where we show a formula that only depends on the congruence class of p mod 12, the $\wp$-adic valuation of the discriminant of a model for E over L, and the valuation of the j-invariant of E. In Section 4 we use the formula to calculate the value of e_1 for several interesting examples, and we show that if $p > 3$, the ramification index of $\wp$ in $L/\mathbb{Q}$ is $e(\wp, L) = 1$, and $e_1 < e$, then the numbers e_1 and $e - e_1$ can only take the values 1, 2, or 4 (see Corollary 4.7). Finally, in Section 5, we apply our formula to prove the following divisibility formulas for the ramification indices in the field of definition of a p-torsion point (see Theorem 5.2 and Corollary 5.4):

Theorem 1.1. *Let E/L be an elliptic curve with potential good supersingular reduction at a prime $\wp$ above a prime $p > 3$, and let e and e_1 be defined as above. Let $P \in E[p]$ be a nontrivial p-torsion point.*

(1) *Suppose $e_1 \geq pe/(p+1)$. Then the ramification index of any prime over $\wp$ in the extension $L(P)/L$ is divisible by $(p^2-1)/\gcd(p^2-1, e)$.*

(2) *Suppose $e_1 < pe/(p+1)$.*
   - *There are $p^2 - p$ points P in $E[p]$ such that the ramification index of a prime above $\wp$ in $L(P)/L$ is divisible by $(p-1)p/\gcd(p(p-1), e_1)$.*
   - *There are $p-1$ points P in $E[p]$ such that the ramification index of any prime above $\wp$ in $L(P)/L$ is divisible by $(p-1)/\gcd(p-1, e-e_1)$.*

In particular, suppose that $e(\wp, L) = 1$.

- *If $e_1 < e$, then $e_1 < pe/(p+1)$ and the ramification index of any prime over $\wp$ in $L(P)/L$ is divisible by $(p-1)/\gcd(p-1, 4)$.*
- *If $p \equiv 1 \bmod 12$, then $e_1 \geq e$ and the ramification index of any prime over $\wp$ in $L(P)/L$ is divisible by $(p^2-1)/\gcd(p^2-1, e)$.*

2. First examples

Before we dive deeper into the theory, let us exhibit two examples of elliptic curves over $L = \mathbb{Q}$ and one curve defined over a quadratic field $L = \mathbb{Q}(\sqrt{13})$, together with their minimal fields of good reduction (over $L_{\wp}^{\mathrm{nr}}$), and the values of e and e_1. The calculations have been completed with the aid of Sage [Stein et al. 2012] and Magma [Bosma et al. 2010].

Example 2.1. Let $E/\mathbb{Q}$ be the elliptic curve with Cremona label 121c2, with $j(E) = -11 \cdot 131^3$, given by a Weierstrass equation

$$y^2 + xy = x^3 + x^2 - 3632x + 82757.$$

The elliptic curve E has bad additive reduction at $p = 11$, but potentially good supersingular reduction at the same prime. The extension $K = K_E$ of $\mathbb{Q}_{11}^{\mathrm{nr}}$ is given by adjoining $\pi = \sqrt[3]{11}$, thus $e = 3$. The curve E has a minimal model with good supersingular reduction of the form

$$y^2 + \sqrt[3]{11}xy = x^3 + \sqrt[3]{11^2}x^2 + 3\sqrt[3]{11}x + 2$$

over $\mathbb{Q}_{11}^{\mathrm{nr}}(\pi)$, where $\pi = \sqrt[3]{11}$, and the discriminant of this model is $\Delta = -1$. The multiplication-by-11 map on the associated formal group $\hat{E}$ is given by a power series:

$$\begin{aligned}[11](Z) = 11Z - 55\pi Z^2 - 275\pi^2 Z^3 + 42350Z^4 - 181148\pi Z^5 - 659417\pi^2 Z^6 \\ +96265708Z^7 - 341161040\pi Z^8 - 1521191342\pi^2 Z^9 \\ +183261837077Z^{10} - 497606935519\pi Z^{11} + O(Z^{12}).\end{aligned}$$

Since $497606935519 = 17 \cdot 23 \cdot 151 \cdot 8428159$ is relatively prime to 11, we conclude that $e_1 = \nu_K(s_{11}) = \nu_K(-497606935519\pi) = 1$.

Example 2.2. Let $E/\mathbb{Q}$ be the elliptic curve with Cremona label 27a4, with $j(E) = -2^{15} \cdot 3 \cdot 5^3$, given by a Weierstrass equation

$$y^2 + y = x^3 - 30x + 63.$$

The elliptic curve E has bad additive reduction at $p = 3$, but potentially good supersingular reduction at the same prime. The extension $K = K_E$ of $\mathbb{Q}_3^{\mathrm{nr}}$ is given by adjoining $\alpha = \sqrt[4]{3}$ and a root β of $x^3 - 120x + 506 = 0$. The result is an extension $K = \mathbb{Q}_3^{\mathrm{nr}}(\alpha, \beta)$ of degree $e = 12$. For convenience we write $K = \mathbb{Q}_3^{\mathrm{nr}}(\gamma)$ where γ is a root of $p(x) = 0$, with

$$\begin{aligned}p(x) = x^{12} - 480x^{10} - 2024x^9 + 86391x^8 + 728640x^7 - 5378664x^6 \\ -87509664x^5 - 161677413x^4 + 2979983776x^3 \\ +22119216120x^2 + 62098532232x + 65301304309.\end{aligned}$$

The curve E has a minimal model with good supersingular reduction (which we will not write here, because the coefficients are unwieldy expressions in γ). The multiplication-by-3 map on the associated formal group $\hat{E}$ is given by a power series

$$[3](Z) = 3Z + s_3 Z^3 + O(Z^4),$$

where

$$s_3 = \tfrac{91366247104560778}{113527481110579959}\gamma^{11} - \tfrac{1556952329592412502}{340582443331739877}\gamma^{10} + \tfrac{3943076616393619924}{340582443331739877}\gamma^{9} + \cdots + \tfrac{495013631117553848}{340582443331739877}\gamma^{2} - \tfrac{544095024526171682}{113527481110579959}\gamma - \tfrac{3353034524919522230}{340582443331739877}.$$

The valuation we sought (computed with Sage) is $\nu_K(s_3) = 2$. Hence, $e_1 = 2$ in this case.

Example 2.3. Let j_0 be a root of the polynomial

$$x^2 - 6896880000x - 567663552000000,$$

and let $L = \mathbb{Q}(j_0) = \mathbb{Q}(\sqrt{13})$. Let $p = 13$ and let $\wp = (\sqrt{13})$ be the ideal above p in $\mathcal{O}_L$. Let E/L be the elliptic curve with j-invariant equal to j_0. The curve E has complex multiplication by $\mathbb{Z}[\sqrt{-13}]$, that is, $\operatorname{End}(E/\mathbb{C}) \cong \mathbb{Z}[\sqrt{-13}]$ and, in fact, all the endomorphisms are defined over $\mathbb{Q}(\sqrt{13}, i)$; see [Silverman 1994, Chapter 2, Theorem 2.2(b)]. Since 13 ramifies in L, it follows from Deuring's criterion (see [Lang 1987, Chapter 13, §4, Theorem 12]) that the reduction of E at $\wp$ is potentially supersingular. We choose a model for E/L given by

$$y^2 = x^3 + \frac{5231 j_0 - 50692880808000}{3825792}x + \frac{-550711 j_0 + 4485396184200000}{239112}.$$

The discriminant of this model is

$$\Delta_L = \frac{135464951768900000 j_0 - 934296399000452924640000000}{29889}$$

and $\nu_\wp(\Delta_L) = 0$. Hence, E/L has good supersingular reduction at $\wp$. In particular $K_E = L_\wp^{\mathrm{nr}}$ and $e = 2$. The multiplication-by-13 map on the associated formal group $\hat{E}$ is given by a power series:

$$[13](Z) = 13Z + \frac{-8092357 j_0 + 78421886609976000}{39852}Z^5 + \cdots + s_{13}Z^{13} + O(Z^{15}),$$

where

$$s_{13} = (-193923815261040770875476640000 j_0 + 1370109961997431363496278036289664000000)/29889.$$

Since $\nu_K(s_{13}) = \nu_\wp(s_{13}) = 1$, we conclude that $e_1 = 1$. The formal group and the valuation of s_{13} were calculated using Magma. Thanks to Harris Daniels for providing the polynomial that defines j_0.

Remark 2.4. Let N be the part of the Newton polygon of $[p](Z)$ that describes the roots of valuation > 0. Let $P_0 = (1, e)$, $P_1 = (p, e_1)$, and $P_2 = (p^2, 0)$. The slope of the segment P_0P_1 is $-(e-e_1)/(p-1)$, while the slope of the segment P_0P_2 is $-e/(p^2-1)$. It follows from the theory of Newton polygons (see [Serre 1972, p. 272]) that:

(1) If $pe/(p+1) < e_1$, then N is given by a single segment P_0P_2.

(2) Otherwise, if $pe/(p+1) \geq e_1$, then N is given by two segments P_0P_1 and P_1P_2.

In particular, if $e_1 \geq e$, then N has one single segment. We will frequently focus on the case $e_1 < e$, in which case the Newton polygon may have two segments. In this case, we shall show later (Corollary 3.2) that e_1 is independent of the chosen minimal model for E/K.

3. A formula for e_1

In this section we prove a formula for e_1 in terms of the valuations of the constants c_4 and c_6 of a minimal model for E/A. We need a number of preliminary results before we state and prove our formulas in Theorem 3.9 and Corollary 3.12. Let us begin with some further details about the extension $K_E/L_\wp^{\mathrm{nr}}$ that was mentioned in the introduction. We follow [Serre and Tate 1968] (see in particular p. 498, Corollary 3 there) to define an extension K_E of $L_\wp^{\mathrm{nr}}$ of minimal degree such that E has good reduction over K_E. Let ℓ be any prime such that $\ell \neq p$, and let $T_\ell(E)$ be the ℓ-adic Tate module. Let $\rho_{E,\ell} : \mathrm{Gal}(\overline{L_\wp^{\mathrm{nr}}}/L_\wp^{\mathrm{nr}}) \to \mathrm{Aut}(T_\ell(E))$ be the usual representation induced by the action of Galois on $T_\ell(E)$. We define the field K_E as the extension of $L_\wp^{\mathrm{nr}}$ such that

$$\mathrm{Ker}(\rho_{E,\ell}) = \mathrm{Gal}(\overline{L_\wp^{\mathrm{nr}}}/K_E).$$

In particular, the field K_E enjoys the following properties:

(1) E/K_E has good (supersingular) reduction.

(2) K_E is the smallest extension of $L_\wp^{\mathrm{nr}}$ such that E/K_E has good reduction, that is, if $K'/L_\wp^{\mathrm{nr}}$ is another extension such that E/K' has good reduction, then $K_E \subseteq K'$.

(3) $K_E/L_\wp^{\mathrm{nr}}$ is finite and Galois. Moreover (see [Serre 1972, §5.6, p. 312] when $L = \mathbb{Q}$, but the same reasoning holds over number fields, as the work of Néron [1964, p. 124–125] is valid for any local field):
   - If $p > 3$, then $K_E/L_\wp^{\mathrm{nr}}$ is cyclic of degree 1, 2, 3, 4, or 6.
   - If $p = 3$, the degree of $K_E/L_\wp^{\mathrm{nr}}$ is a divisor of 12.
   - If $p = 2$, the degree of $K_E/L_\wp^{\mathrm{nr}}$ is 2, 3, 4, 6, 8, or 24.

As before, we will write $K = K_E$. Let ν_K be a valuation on K such that $\nu_K(p) = e$ and $\nu_K(\pi) = 1$, where π is a uniformizer for K. Let A be the ring of elements of K with valuation ≥ 0.

Proposition 3.1. *Let $\omega(Z) = \left(1 + \sum_{i=1}^{\infty} w_i Z^i\right) dZ$ be the unique normalized invariant differential associated to $\hat{E}$ (as in [Silverman 2009, IV, §4]), with $w_i \in A$ for all $i \geq 1$. Then,*

$$[p](Z) = \sum_{i=1}^{\infty} s_i Z^i \equiv w_{p-1} Z^p + O(Z^{p+1}) \bmod pA.$$

In particular, $s_p \equiv w_{p-1} \bmod pA$. Thus, if $\nu_K(w_{p-1}) < e$, then

$$e_1 = \nu_K(s_p) = \nu_K(w_{p-1}).$$

Otherwise, if $\nu_K(w_{p-1}) \geq e$, then $e_1 \geq e$.

Proof. The congruence is shown in [Katz 1973, Lemma 3.6.5], so here we just give the key ingredients in the proof. Let $\varphi(Z) = Z + \sum_{k=2}^{\infty} (w_{k-1}/k) Z^k$ so that $\omega = d(\varphi(Z))$, and let $\psi(Z)$ be the inverse series to $\varphi(Z)$, so that $\psi(\varphi(Z)) = Z$. Since ω is the normalized invariant differential for $\hat{E}$, it follows that $p\omega(Z) = (\omega \circ [p])(Z)$ (see [Silverman 2009, Chapter IV, Corollary 4.3]), therefore, $[p](Z) = \psi(p\varphi(Z))$. The desired congruence falls out from this and the equality $\psi(\varphi(Z)) = Z$.

The congruence implies that $s_p = w_{p-1} + p\alpha$, for some $\alpha \in A$. In particular,

$$\nu_K(s_p) \geq \min\{\nu_K(w_{p-1}), \nu_K(p\alpha)\} = \min\{\nu_K(w_{p-1}), e + \nu_K(\alpha)\}.$$

If we assume that $\nu_K(w_{p-1}) < e$, then $\nu_K(w_{p-1}) < e + \nu_K(\alpha)$, and the inequality is in fact an equality and $\nu_K(s_p) = \nu_K(w_{p-1})$. Otherwise, if $\nu_K(w_{p-1}) \geq e$, then $e_1 = \nu_K(s_p) \geq e$, as claimed. □

Corollary 3.2. *Let*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad \text{and} \quad y^2 + a_1' xy + a_3' y = x^3 + a_2' x^2 + a_4' x + a_6'$$

be two minimal models for an elliptic curve E/A and let $[p](Z) = \sum s_i Z$ and $[p]'(Z) = \sum s_i'(Z)$ be the multiplication-by-p maps for their respective formal groups. Then, there is a constant $u \in A^\times$ such that $s_p \equiv u^{p-1} s_p' \bmod pA$. In particular, if $e_1 < e$, then the number $e_1 = \nu_K(s_p)$ as defined above is independent of the chosen minimal model for the elliptic curve E/A.

Proof. Let

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \text{ and } y^2 + a_1' xy + a_3' y = x^3 + a_2' x^2 + a_4' x + a_6'$$

be two minimal models, with $a_i, a_i' \in A$, for the same elliptic curve E/A, and let $\hat{E}/A$ and $\hat{E}'/A$ be the formal groups associated to each model, with formal group laws given by $F(X, Y)$ and $F'(X, Y)$, respectively. Since these are minimal models for the same curve E/A, it follows that $(\hat{E}, F)$ and $(\hat{E}', F')$ are isomorphic formal groups; see [Silverman 2009, Chapter VII, Proposition 2.2]. Thus, there is a power series $f(Z) = uZ + O(Z^2)$, for some $u \in A^\times$, such that

$$f(F(X, Y)) = F'(f(X), f(Y)).$$

Let $\omega(Z) = \sum w_n Z^n$, $[p](Z) = \sum s_i Z$ and $\omega'(Z) = \sum w'_n Z^n$, $[p]'(Z) = \sum s'_i(Z)$ be the invariant differentials, and multiplication-by-p maps, for $\hat{E}$ and $\hat{E}'$, respectively. Then, by Proposition 3.1,

$$\begin{aligned} f([p](Z)) &= [p]'(f(Z)) \\ &= \sum s'_i(f(Z)) \equiv w'_{p-1}(f(Z))^p + \cdots \equiv u^p \cdot w'_{p-1} Z^p + O(Z^{p+1}), \\ f([p](Z)) &= u([p](Z)) + \cdots \equiv u(w_{p-1}Z^p + \cdots) + \cdots \equiv u \cdot w_{p-1} Z^p + O(Z^{p+1}). \end{aligned}$$

Therefore, $u^p \cdot w'_{p-1} \equiv u \cdot w_{p-1} \bmod pA$, or $w_{p-1} \equiv u^{p-1} w'_{p-1} \bmod pA$. Hence $s_p \equiv u^{p-1} s'_p \bmod pA$, as claimed.

In particular, if $e_1 < e$, and $e_1 = \nu_K(s_p)$ and $e'_1 = \nu_K(s'_p)$, then there is some $\alpha \in A$ such that $s_p = u^{p-1} s'_p + p\alpha$. Hence,

$$e_1 = \nu_K(s_p) = \nu_K(u^{p-1}s'_p + p\alpha) = \min\{\nu_K(s'_p), e + \nu_K(\alpha)\} = \nu_K(s'_p) = e'_1.$$

Thus, the valuation of s_p is independent of the chosen minimal model for E/A. □

Remark 3.3. Here is an alternative proof of Corollary 3.2 using the Hasse invariant $\mathscr{H}(E, \omega)$ as defined in [Katz 1973, Section 2.0]. Let E/A be given by a minimal model

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

with $a_i \in A$, and let $\omega = dx/(2y + a_1x + a_3)$ be an invariant differential for E/A. Let $\mathscr{H}(E, \omega)$ be the Hasse invariant. Moreover, let $\hat{E}/A$ be the associated formal group, let

$$\omega(Z) = \left(1 + \sum_{n=1}^{\infty} w_n Z^n\right) dZ = (1 + a_1 Z + (a_1^2 + a_2)Z^2 + \cdots)\, dZ,$$

be the unique normalized invariant differential associated to $\hat{E}$ and write

$$[p](Z) = \sum_{i=1}^{\infty} s_i Z^i,$$

as before. Then, Lemmas 3.6.1 and 3.6.5 of [Katz 1973] imply that $a_p \equiv \mathscr{H}(E, \omega) \bmod pA$.

Now, if

$$y^2+a_1'xy+a_3'y=x^3+a_2'x^2+a_4'x+a_6'$$

is another minimal model for E/A, then there is a constant $u\in A^\times$ such that the new invariant differential ω' and ω are related by $\omega'=u\omega$, and $\mathscr{H}(E,\omega)=u^{p-1}\mathscr{H}(E,u\omega)$; see [Katz 1973, p. Ka-29]. If $\hat{E}'/A$ is the formal group associated to this new minimal model, and $[p]'(Z)=\sum_{i=1}^{\infty}s_i'Z^i$, then

$$s_p\equiv\mathscr{H}(E,\omega)\equiv u^{p-1}\mathscr{H}(E,u\omega)\equiv u^{p-1}s_p' \bmod pA.$$

Since we have assumed that $e'=\nu(a_p)<e$, the coefficients s_p and s_p' have the same valuation.

Lemma 3.4. *Let E/A be given by a model $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$, with $a_i\in A$, and let $\omega(Z)=(1+\sum_{i=1}^{\infty}w_iZ^i)\,dZ$ be the unique normalized invariant differential associated to $\hat{E}$. Then, $w(Z)\in\mathbb{Z}[a_1,a_2,a_3,a_4,a_6][\![Z]\!]$. Moreover, if $\mathbb{Z}[a_1,a_2,a_3,a_4,a_6]$ is made into a graded ring by assigning weights $\mathrm{wt}(a_i)=i$, then $w_n\in\mathbb{Z}[a_1,a_2,a_3,a_4,a_6]$ is homogeneous of weight n.*

Proof. Let $f(x,y)=y^2+a_1xy+a_3y-(x^3+a_2x^2+a_4x+a_6)$ and let $v(Z)\in A[\![Z]\!]$ be the unique power series such that $v(Z)=f(Z,v(Z))$. The existence of $v(Z)$ is shown in [Silverman 2009, Chapter IV, Proposition 1.1], and, moreover, it is also shown that $v(Z)=Z^3(1+\sum_{k=1}^{\infty}A_kZ^k)\in\mathbb{Z}[a_1,\dots,a_6][\![Z]\!]$. When we assign weights $\mathrm{wt}(a_i)=i$, then A_n is homogeneous of weight n.

Now define $x(Z)=Z/v(Z)$ and $y(Z)=-1/v(Z)$. It follows that the coefficients of Z^n in $Z^2x(Z)$, $Z^3\frac{d}{dZ}(x(Z))$, and $Z^3y(Z)$ are homogeneous of weight n. Since

$$\omega(Z)=\left(\frac{\frac{d}{dZ}(x(Z))}{2y(Z)+a_1X(Z)+a_3}\right)dZ=\left(\frac{Z^3\frac{d}{dZ}(x(Z))}{2Z^3y(Z)+(a_1Z)(Z^2x(Z))+a_3Z^3}\right)dZ,$$

it follows that w_n, the coefficient of Z^n in $\omega(Z)$, must be homogeneous of degree n, as claimed. □

Lemma 3.5. *Let E/A be given by a model $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$, with $a_i\in A$, with discriminant $\Delta(E)$ and j-invariant $j(E)$, and let $\omega(Z)=\sum w_nZ^n$ be the normalized invariant differential on $\hat{E}/A$. Define the constants b_2,b_4,b_6,b_8, c_4, and $c_6\in A$ as usual, such that $y^2=x^3-27c_4x-54c_6$ is an alternative model for E/A (which is also minimal as long as $p\neq 2$ or 3), and such that*

$$1728\Delta(E)=c_4^3-c_6^2\quad\textit{and}\quad j(E)=\frac{c_4^3}{\Delta}.$$

(1) *With the grading $\mathrm{wt}(a_k)=k$, the constants $b_{2k},c_4,c_6\in\mathbb{Z}[a_1,a_2,a_3,a_4,a_6]$ have weights $2k$, 4 and 6, respectively.*

(2) *We have $w_1^4\equiv a_1^4\equiv c_4 \bmod 2A$, and $w_2^2\equiv(a_1^2+a_2)^2\equiv c_4 \bmod 3A$.*

(3) *Let $p > 3$ and let $R = \mathbb{Z}[X, Y]$ be a graded ring with* $\mathrm{wt}(X) = 4$ *and* $\mathrm{wt}(Y) = 6$. *Then, there is a constant $u \in A^\times$ and a homogeneous polynomial $P_p(X, Y) \in R$ of degree $p-1$ such that $w_{p-1} \equiv u^{p-1} P_p(c_4, c_6) \bmod pA$.*

Proof. Part (1) follows by inspection of the formulas that define $b_2, \ldots, b_8, c_4, c_6$ (see for instance [Silverman 2009, Chapter III.1], but notice that there is a typo in the formula for b_2: the correct formula is $b_2 = a_1^2 + 4a_2$).

Part (2) follows from the expression of $\omega(Z)$ in terms of $a_1, \ldots, a_6$,

$$\omega(Z) = (1 + a_1 Z + (a_1^2 + a_2)Z^2 + (a_1^3 + 2a_1a_2 + 2a_3)Z^3 + \cdots)\, dZ,$$

together with the fact that from the formulas one can easily check that $c_4 \equiv b_2^2 \bmod 6$, $b_2 = a_1^2 + 4a_2 \equiv a_1^2 \bmod 2$, and $b_2 \equiv a_1^2 + a_2 \bmod 3$.

To show part (3), let us assume that $p > 3$. Thus, E/A has a minimal model of the form $y^2 = x^3 - 27c_4x - 54c_6$. Let $\hat{E}'/A$ be the formal group associated to this model, and let $\omega'(Z) = \sum w'_n Z^n$ be its normalized invariant differential. By Lemma 3.4, w_{p-1} may be expressed as a homogeneous polynomial in $\mathbb{Z}[a'_4, a'_6]$, where $a'_4 = -27c_4$ and $a'_6 = -54c_6$. Hence, there is a polynomial $P_p \in R = \mathbb{Z}[X, Y]$ such that $w_{p-1} = P_p(c_4, c_6)$. Now, if E/A is given by any other minimal model, Proposition 3.1 and Corollary 3.2 combined say that there exists some $u \in A^\times$ such that, as claimed,

$$w_{p-1} \equiv s_p \equiv u^{p-1} s'_p \equiv u^{p-1} w'_{p-1} \equiv u^{p-1} P_p(c_4, c_6) \bmod pA. \qquad \square$$

Before we state the next result, we define quantities $r(p)$ and $s(p)$ for each prime $p > 3$, by

$$r(p) = \begin{cases} 1, & \text{if } p \equiv 5 \text{ or } 11 \bmod 12, \\ 0, & \text{if } p \equiv 1 \text{ or } 7 \bmod 12, \end{cases} \quad \text{and} \quad s(p) = \begin{cases} 1, & \text{if } p \equiv 3 \bmod 4, \\ 0, & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

Equivalently, $r(p) = \frac{1}{2}\bigl(1 - \bigl(\frac{-3}{p}\bigr)\bigr)$ and $s(p) = \frac{1}{2}\bigl(1 - \bigl(\frac{-4}{p}\bigr)\bigr)$, where $\bigl(\frac{\cdot}{p}\bigr)$ is the Legendre symbol.

Lemma 3.6. *Let $p > 3$ be a prime, and let $R = \mathbb{Z}[X, Y]$ be a graded ring with* $\mathrm{wt}(X) = 4$ *and* $\mathrm{wt}(Y) = 6$. *Suppose $P(X, Y) \in R$ is homogeneous of degree $p-1$, and let Δ and j be two extra variables such that $1728\Delta = X^3 - Y^2$ and $\Delta \cdot j = X^3$. Then, there is some polynomial $Q(T) \in \mathbb{Z}[T]$ such that*

$$P(X, Y) = X^{r(p)} Y^{s(p)} \Delta^{\frac{p-\alpha}{12}} Q(j),$$

where $\alpha = 1, 5, 7$ or 11, and such that $p \equiv \alpha \bmod 12$.

Proof. Suppose that $p > 3$ is a prime with $p \equiv \alpha \bmod 12$, with $\alpha = 1, 5, 7$ or 11. Since $P(X, Y)$ is homogeneous of degree $p-1$, we can write

$$P(X, Y) = \sum c_{a,b} X^a Y^b$$

such that $a, b \geq 0$, $4a + 6b = p - 1$, and $c_{a,b} \in \mathbb{Z}$. Since $p \equiv \alpha \mod 12$, there is some integer $t \geq 0$ such that $p = \alpha + 12t$. In particular, $4a + 6b = (\alpha - 1) + 12t$, or $2a + 3b = (\alpha - 1)/2 + 6t$. Notice that $2r(p) + 3s(p) = (\alpha - 1)/2$. It follows that $a, b > 0$, and we may write

$$P(X, Y) = \sum c_{a,b} X^a Y^b = X^{r(p)} Y^{s(p)} \sum c_{a,b} X^{a-r(p)} Y^{b-s(p)}$$

and $2(a - r(p)) + 3(b - s(p)) = 6t$. We conclude that $a - r(p) \equiv 0 \mod 3$, and $b - s(p) \equiv 0 \mod 2$. Let us write $a - r(p) = 3f$ and $b - s(p) = 2g$, so that

$$P(X, Y) = X^{r(p)} Y^{s(p)} \sum c_{3f+r(p),2g+s(p)} (X^3)^f (Y^2)^g,$$

where $f, g \geq 0$ and $f + g = t = (p - \alpha)/12$. Put $d_{f,g} = c_{3f+r(p),2g+s(p)}$. Then,

$$\begin{aligned} P(X, Y) &= X^{r(p)} Y^{s(p)} \sum d_{f,g} (X^3)^f (Y^2)^g \\ &= X^{r(p)} Y^{s(p)} \sum d_{f,g} (X^3)^f (X^3 - 1728\Delta)^{\frac{p-\alpha}{12} - f} \\ &= X^{r(p)} Y^{s(p)} \Delta^{\frac{p-\alpha}{12}} \sum d_{f,g} \left(\frac{X^3}{\Delta}\right)^f \left(\frac{X^3 - 1728\Delta}{\Delta}\right)^{\frac{p-\alpha}{12} - f} \\ &= X^{r(p)} Y^{s(p)} \Delta^{\frac{p-\alpha}{12}} \sum d_{f,g} j^f (j - 1728)^{\frac{p-\alpha}{12} - f}. \end{aligned}$$

Hence, if we define a polynomial

$$Q(T) = \sum d_{f,g} T^f (T - 1728)^{\frac{p-\alpha}{12} - f} \in \mathbb{Z}[T],$$

then $P(X, Y) = X^{r(p)} Y^{s(p)} \Delta^{\frac{p-\alpha}{12}} Q(j)$, as desired. □

Definition 3.7. Let $p > 3$ be a prime and let $P_p(X, Y)$ be the polynomial whose existence was shown in Lemma 3.5. We define $Q_p(T) \in \mathbb{Z}[T]$ as the unique polynomial with integer coefficients such that

$$P_p(X, Y) = X^{r(p)} Y^{s(p)} \Delta^{\frac{p-\alpha}{12}} Q_p(j),$$

where, as usual, $1728\Delta = X^3 - Y^2$ and $\Delta \cdot j = X^3$, and $\alpha = 1, 5, 7$ or 11 such that $p \equiv \alpha \mod 12$.

Remark 3.8. Let $p > 3$. The polynomial $P_p(c_4, c_6)$ of Lemma 3.5 can be explicitly calculated (mod pA) as follows. Let E/A be given by

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

with $a_i \in A$, and let $\omega = dx/(2y + a_1 x + a_3)$ be an invariant differential for E/A. Let $\mathcal{H}(E, \omega)$ be the Hasse invariant (as in Remark 3.3). Then $w_{p-1} \equiv \mathcal{H}(E, \omega) \mod pA$. The curve E/A is also given by a minimal model $E'/A : y^2 = x^3 - 27c_4 x - 54c_6$ and it is well known that the Hasse invariant $\mathcal{H}(E', \omega')$ of a curve given by $y^2 = f(x)$

is congruent to the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ modulo pA; see, for instance, [Silverman 2009, Chapter V, Theorem 4.1(a)]. Thus,

$$P_p(c_4,c_6) \equiv \sum_{\frac{p-1}{6}\le k\le \frac{p-1}{4}} (-1)^k \binom{\frac{p-1}{2}}{k}\binom{k}{3k-\frac{p-1}{2}}(27c_4)^{3k-\frac{p-1}{2}}(54c_6)^{\frac{p-1}{2}-2k}$$

$$\equiv \sum_{\substack{m,n\ge 0\\ 4m+6n=p-1}} (-1)^{m+n}\binom{\frac{p-1}{2}}{m+n}\binom{m+n}{m}(27c_4)^m(54c_6)^n \mod pA.$$

For instance, $P_5=-54c_4$, $P_7=-162c_6$, $P_{11}=29160c_4c_6$, and

$$P_{13}=-393660c_4^3+43740c_6^2=\Delta(E)(-349920j(E)-75582720).$$

Notice these polynomials satisfy the conclusions of Lemma 3.6, with $Q_5(T)=-54$, $Q_7(T)=-162$, $Q_{11}(T)=29160$, $Q_{13}(T)=-349920T-75582720$.

Theorem 3.9. *Let E/L be an elliptic curve with potential good supersingular reduction at a prime $\wp$ above a prime p. Let $K=K_E$ be the extension of $L_\wp^{\mathrm{nr}}$ defined above, let A, $e=\nu_K(p)$, and e_1 be as before, and let $e(\wp,L)$ be the ramification index of $\wp$ in $L/\mathbb{Q}$. Let $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ be a minimal model for E/A with good reduction, and let $c_4,c_6\in A$ be the usual quantities associated to this model.*

(1) *If $p=2$, and $(\nu_K(c_4))/4<e$, then*

$$e_1=\frac{\nu_K(c_4)}{4}=\frac{\nu_K(j(E))}{12}=\frac{e\cdot\nu_\wp(j(E))}{12e(\wp,L)}.$$

(2) *If $p=3$, and $(\nu_K(c_4))/2<e$, then*

$$e_1=\frac{\nu_K(c_4)}{2}=\frac{\nu_K(j(E))}{6}=\frac{e\cdot\nu_\wp(j(E))}{6e(\wp,L)}.$$

(3) *If $p>3$, and $\lambda=r(p)\nu_K(c_4)+s(p)\nu_K(c_6)+\nu_K(Q_p(j(E)))<e$, then*

$$e_1=\lambda=r(p)\frac{\nu_K(j(E))}{3}+s(p)\frac{\nu_K(j(E)-1728)}{2}+\nu_K(Q_p(j(E)))$$
$$=\frac{e}{e(\wp,L)}\cdot\Big(r(p)\frac{\nu_\wp(j(E))}{3}+s(p)\frac{\nu_\wp(j(E)-1728)}{2}+\nu_\wp(Q_p(j(E)))\Big).$$

Otherwise, $e_1\ge e$.

Proof. Let $\hat{E}/A$ be the formal group associated to E and let $[p](Z)=\sum_{i=1}^\infty s_iZ^i$ be the multiplication-by-p map on $\hat{E}$. By definition, $e=\nu_K(p)$ and $e_1=\nu_K(s_p)$. Moreover, by Proposition 3.1, we know that if $\nu_K(w_{p-1})<e$, then $e_1=\nu_K(w_{p-1})$ where $\omega(Z)=\big(1+\sum_{i=1}^\infty w_iZ^i\big)\,dZ$ is the normalized invariant differential for $\hat{E}$, and $e_1\ge e$ otherwise. Let us assume that $\nu_K(w_{p-1})<e$. Now we can use Lemma 3.5:

(1) If $p = 2$, then $w_1^4 \equiv c_4 \bmod 2A$. Since we are assuming $\nu_K(2) = e > \nu_K(w_1)$, we must have $4\nu_K(w_1) = \nu_K(w_1^4) = \nu_K(c_4)$, and it follows that $e_1 = \nu_K(c_4)/4$.

(2) Similarly, if $p = 3$, then $w_2^2 \equiv c_4 \bmod 3A$. Hence, $e_1 = \nu_K(c_4)/2$.

(3) Suppose $p > 3$. Then, there is a constant $u \in A^\times$ and a homogeneous polynomial $P_p(X, Y) \in R$ of degree $p - 1$ (where $\mathrm{wt}(X) = 4$ and $\mathrm{wt}(Y) = 6$) such that $w_{p-1} \equiv u^{p-1} P_p(c_4, c_6) \bmod pA$. Let $\alpha = 1, 5, 7$, or 11, such that $p \equiv \alpha \bmod 12$. Then, by Lemma 3.6, there is a polynomial $Q_p(T) \in \mathbb{Z}[T]$ such that

$$w_{p-1} \equiv u^{p-1} c_4^{r(p)} c_6^{s(p)} \Delta(E)^{\frac{p-\alpha}{12}} Q_p(j(E)) \bmod pA.$$

Since E/L has potential good reduction, the j-invariant $j(E)$ is integral at $\wp$ (see [Silverman 2009, Chapter VII, Proposition 5.5]), thus via our fixed embedding ι, we have $j(E) \in A$. Since $j(E) \in A \cap L_\wp$, and $Q_p(T) \in \mathbb{Z}[T]$, it follows that $Q_p(j(E)) \in A \cap L_\wp$. Therefore, $\nu_K(Q_p(j(E))$ is a nonnegative multiple of $e/e(\wp, L)$. Define λ as in the statement of the theorem, so that λ equals $\nu_K(u^{p-1} c_4^{r(p)} c_6^{s(p)} \Delta(E)^{(p-\alpha)/12} Q_p(j(E)))$. Thus, if $\lambda < e$, it follows that $\nu_K(w_{p-1}) = \lambda$ and Proposition 3.1 implies that $e_1 = \lambda$, as desired. □

When $p \equiv 1 \bmod 12$, the quantities $r(p)$ and $s(p)$ vanish simultaneously and we obtain the following simpler formula.

Corollary 3.10. *Let E/L be an elliptic curve with potential good supersingular reduction at a prime $\wp$ above a prime $p \equiv 1 \bmod 12$. Let K_E, A, e and e_1 be as before, and let $e(\wp, L)$ be the ramification index of $\wp$ in $L/\mathbb{Q}$. Let $Q_p(T) \in \mathbb{Z}[T]$ be as in Definition 3.7, and define an integer λ by*

$$\lambda = \nu_K(Q_p(j(E))) = \frac{e}{e(\wp, L)} \cdot \nu_\wp(Q_p(j(E))).$$

If $\lambda < e$, then $e_1 = \lambda \geq 1$. Otherwise, if $\lambda \geq e$, then $e_1 \geq e$. In particular, if $e(\wp, L) = 1$ or $\nu_\wp(Q_p(j(E))) = 0$, then $e_1 \geq e$.

The value of $e/e(\wp, L)$, and therefore the value of e, can be obtained directly from a model of E/L, thanks to the classification of Néron models. As a reference for the following theorem, the reader can consult [Néron 1964, p. 124–125] or [Serre 1972, §5.6, p. 312], where $\mathrm{Gal}(K_E/L_\wp^{\mathrm{nr}})$ is denoted by Φ_p, and therefore $e/e(\wp, L) = \mathrm{Card}(\Phi_p)$. Notice, however, that the section we cite of [Serre 1972] restricts its attention to the case $L = \mathbb{Q}$.

Theorem 3.11. *Let $p > 3$, let E/L be an elliptic curve with potential good reduction, and let Δ_L be the discriminant of any model of E defined over L. Let K_E be the smallest extension of $L_\wp^{\mathrm{nr}}$ such that E/K_E has good reduction. Then $e/e(\wp, L) = [K_E : L_\wp^{\mathrm{nr}}] = 1, 2, 3, 4,$ or 6. Moreover:*

- *$e/e(\wp, L) = 2$ if and only if $\nu_\wp(\Delta_L) \equiv 6 \bmod 12$,*

- $e/e(\wp, L) = 3$ *if and only if* $\nu_\wp(\Delta_L) \equiv 4$ *or* $8 \bmod 12$,
- $e/e(\wp, L) = 4$ *if and only if* $\nu_\wp(\Delta_L) \equiv 3$ *or* $9 \bmod 12$,
- $e/e(\wp, L) = 6$ *if and only if* $\nu_\wp(\Delta_L) \equiv 2$ *or* $10 \bmod 12$.

Therefore, our formula for e_1 only depends on the $\wp$-adic valuation of $j(E)$, $j(E) - 1728$, and Δ_L.

Corollary 3.12. *Let $p > 3$ be a prime and let E/L be an elliptic curve with potentially supersingular good reduction at a prime $\wp$ above p. Let $e(\wp, L)$ be the ramification index of $\wp$ in $L/\mathbb{Q}$. Let $j(E) \in L$ be its j-invariant, let Δ_L be the discriminant of a model for E over L, and define an integer λ as follows*:

- *If* $\nu_\wp(\Delta_L) \equiv 6 \bmod 12$, *then* $e/e(\wp, L) = 2$. *Let*
$$\lambda = \tfrac{2}{3} r(p)\nu_\wp(j(E)) + s(p)\nu_\wp(j(E) - 1728) + 2\nu_\wp(Q_p(j(E))).$$
- *If* $\nu_\wp(\Delta_L) \equiv 4$ *or* $8 \bmod 12$, *then* $e/e(\wp, L) = 3$. *Let*
$$\lambda = r(p)\nu_\wp(j(E)) + \tfrac{3}{2} s(p)\nu_\wp(j(E) - 1728) + 3\nu_\wp(Q_p(j(E))).$$
- *If* $\nu_\wp(\Delta_L) \equiv 3$ *or* $9 \bmod 12$, *then* $e/e(\wp, L) = 4$. *Let*
$$\lambda = \tfrac{4}{3} r(p)\nu_\wp(j(E)) + 2s(p)\nu_\wp(j(E) - 1728) + 4\nu_\wp(Q_p(j(E))).$$
- *If* $\nu_\wp(\Delta_L) \equiv 2$ *or* $10 \bmod 12$, *then* $e/e(\wp, L) = 6$. *Let*
$$\lambda = 2r(p)\nu_\wp(j(E)) + 3s(p)\nu_\wp(j(E) - 1728) + 6\nu_\wp(Q_p(j(E))).$$

If $\lambda < e$, then $e_1 = \lambda$. Otherwise, if $\lambda \geq e$, then $e_1 \geq e$.

4. More examples

In this section we provide a few examples of usage of the formula for e_1 developed in Theorem 3.9.

Example 4.1. Let us return to the curve $E/\mathbb{Q}$ with label 121c2. In Example 2.1 we showed a minimal model over $\mathbb{Q}_{11}^{\mathrm{nr}}(\sqrt[3]{11})$ and we proved that $e_1 = 1$. We can verify the value $e_1 = 1$ using the formula of Theorem 3.9. Here $p = 11$, so $r(11) = s(11) = 1$, and $L = \mathbb{Q}$, so $e(\wp, L) = 1$. Moreover, for the chosen minimal model we have quantities

$$c_4 = 131\sqrt[3]{11}, \quad \text{and} \quad c_6 = -4973.$$

Moreover, we saw in Remark 3.8 that $Q_{11}(T) = 29160 = 2^3 \cdot 3^6 \cdot 5$. Thus,

$$\begin{aligned} \lambda &= \nu_K(c_4) + \nu_K(c_6) + \nu_K(Q_p(j)) \\ &= \nu_K(131\sqrt[3]{11}) + \nu_K(-4973) + \nu_K(29160) = 1 + 0 + 0 = 1. \end{aligned}$$

Since $\lambda < e = 3$, we conclude that $e_1 = \lambda = 1$. We may also verify this value using the formula in Corollary 3.12. The discriminant of the model for $E/\mathbb{Q}$ given in Example 2.1 is $\Delta_{\mathbb{Q}} = -11^8$; we have $j(E) = -11 \cdot 131^3$ and $j(E) - 1728 = -4973^2$. Hence,

$$\lambda = r(p)\nu_p(j(E)) + \tfrac{3}{2}s(p)\nu_p(j(E) - 1728) + 3\nu_p(Q_p(j(E))) \\ = 1 \cdot 1 + \tfrac{3}{2} \cdot 1 \cdot 0 + 3 \cdot 0 = 1,$$

and so $e_1 = \lambda = 1$.

Example 4.2. Let $E'/\mathbb{Q}$ be the curve with label 121a1, given by a Weierstrass equation

$$y^2 + xy + y = x^3 + x^2 - 30x - 76.$$

The j-invariant of E' is $j(E') = -11 \cdot 131^3$, equal to $j(E)$, where E is curve 121c2 as in Examples 2.1 and 4.1. Thus, E' is a quadratic twist of E. Indeed, E' is the quadratic twist of E by -11. In particular, E and E' are isomorphic over $\mathbb{Q}(\sqrt{-11})$. Since $K_E = \mathbb{Q}_{11}^{\mathrm{nr}}(\sqrt[3]{11})$, it follows that

$$K_{E'} = \mathbb{Q}_{11}^{\mathrm{nr}}(\sqrt[3]{11}, \sqrt{-11}) = \mathbb{Q}_{11}^{\mathrm{nr}}(\sqrt[6]{-11}).$$

Thus, $e = e(E') = 6$, while $e = e(E) = 3$, and $\nu_{K_{E'}}(\kappa) = 2\nu_{K_E}(\kappa)$ for any $\kappa \in K_E \subseteq K_{E'}$. Moreover, since $K_E \subseteq K_{E'}$, the minimal model for E over K_E,

$$y^2 + \sqrt[3]{11}xy = x^3 + \sqrt[3]{11^2}x^2 + 3\sqrt[3]{11}x + 2,$$

is also a minimal model for E' over $K_{E'}$. It follows that

$$\lambda(E') = \nu_{K_{E'}}(c_4) + \nu_{K_{E'}}(c_6) + \nu_{K_{E'}}(Q_{11}(j)) \\ = 2\nu_{K_E}(c_4) + 2\nu_{K_E}(c_6) + 2\nu_{K_E}(Q_{11}(j)) = 2 \cdot 1 + 0 + 0 = 2,$$

where we have used the fact that $c_4, c_6 \in K_E$. Since $\lambda(E') < e(E') = 6$, we conclude that $e_1(E') = 2$.

Alternatively, we can verify $e_1(E') = 2$ using the formula of Corollary 3.12. The discriminant of the rational model for $E'/\mathbb{Q}$ listed above is $\Delta_{\mathbb{Q}} = -11^2$. Moreover, $j(E') = -11 \cdot 131^3$, and $j(E') - 1728 = -4973^2$. Hence

$$\lambda = 2r(p)\nu_p(j) + 3s(p)\nu_p(j - 1728) + 6\nu_p(Q_p(j)) = 2 \cdot 1 \cdot 1 + 3 \cdot 1 \cdot 0 + 6 \cdot 0 = 2,$$

and so $e_1 = \lambda = 2$.

Example 4.3. In Example 2.2 we looked at the elliptic curve $E/\mathbb{Q}$ with label 27a4, for $p = 3$, and concluded that $e_1 = 2$. The constant c_4 (which we will not write explicitly here due again to its unwieldy form in terms of γ) for the minimal model we used to compute e_1 has valuation $\nu_K(c_4) = 4$, in agreement with the formula

$e_1 = \nu_K(c_4)/2$ given by Theorem 3.9. Alternatively, and much easier to compute,

$$\lambda = \frac{e \cdot \nu_3(j(E))}{6} = \frac{12 \cdot \nu_3(-2^{15} \cdot 3 \cdot 5^3))}{6} = 2.$$

Since $2 = \lambda < e = 12$, we conclude that $e_1 = \lambda = 2$.

Example 4.4. Let $L = \mathbb{Q}(\sqrt{13})$, put $p = 13$ and $\wp = (\sqrt{13})$, and let E/L be the elliptic curve with j-invariant j_0 as described in Example 2.3. There we found that $K = L_\wp^{\mathrm{nr}}$. Thus, $e = e(\wp, L) = 2$, and we calculated directly that $e_1 = 1$. Since $p \equiv 1 \bmod 12$, we may use Corollary 3.10 to verify that indeed $e_1 = 1$. Here $e(\wp, L) = 2$, and we know from Remark 3.8 that $Q_{13}(T) = -349920T - 75582720$. One can verify (using Sage or Magma) that

$$\nu_\wp(Q_{13}(j_0)) = \nu_\wp(-349920 j_0 - 75582720) = 1.$$

Thus,

$$\lambda = \nu_K(Q_{13}(j(E)) = \frac{e}{e(\wp, L)} \nu_\wp(Q_{13}(j_0)) = \nu_\wp(Q_{13}(j_0)) = 1.$$

Since $1 = \lambda < 2 = e$, it follows from Corollary 3.10 that $e_1 = \lambda = 1$, as desired.

Example 4.5. In this example (see Table 1) we provide the values of e and e_1, calculated using our formula, and verified using the multiplication-by-p map on the formal group, for all those elliptic curves with potentially supersingular reduction that appear as rational points on modular curves $X_0(p)$ of genus > 0 (if the curve $X_0(p)$ has genus 0, then $p = 2$, 3, 5, 7, or 13, and there are infinitely many rational points given by a 1-parameter family; see [Maier 2009]). These points are well-known, but seem to be spread out across the literature. Our main references are [Birch and Kuyk 1975, pp. 78–80; Mazur 1978; Kenku 1982].

The reader may notice that in Table 1 the difference $e - e_1$, and the value e_1, are always 1 or 2, for all $p > 3$. In addition, in Example 4.2 we have seen an example of a curve with $e - e_1 = 6 - 2 = 4$. A priori, we know that $e = 1, 2, 3, 4$ or 6 for elliptic curves over $\mathbb{Q}$ (see [Serre 1972, §5.6, p. 312]), so if we assume $e_1 < e$, then e_1 and $e - e_1$ may take the values $1, 2, 3, 4$, or 5. In fact, we will show next that the difference $e - e_1$ and e_1 may only take the values 1, 2, or 4, when $L = \mathbb{Q}$ and more generally whenever $e(\wp, L) = 1$.

Corollary 4.6. *Let E/L be an elliptic curve with potentially supersingular reduction at a prime $\wp$ lying above a prime $p > 3$, and let e and e_1 be defined as in Section 1. Assume that $e_1 < e$, and also assume that $e(\wp, L) = 1$. Then e_1 and $e - e_1$ can only take the values* 1, 2, *or* 4. *Moreover, $j(E) \equiv 0$ or $1728 \bmod \wp$, and*

(1) *If $j(E) \equiv 0 \bmod \wp$, then $e = 3$ or 6, and $e_1 = ek/3$, where $k = \nu_\wp(j(E)) = 1$ or 2.*

(2) *If $j(E) \equiv 1728 \bmod \wp$, then $e = 2$ or 4, and $e_1 = e/2$.*

j-invariant	p	Cremona label(s)	Good reduction over	e	e_1
$-2^{15}\,3\cdot 5^3$	3	27A2, 27A4	L (see caption)	12	2
$-11\cdot 131^3$	11	121C2	$\mathbb{Q}(\sqrt[3]{11})$	3	1
-2^{15}		121B1, 121B2	$\mathbb{Q}(\sqrt[4]{11})$	4	2
-11^2		121C1	$\mathbb{Q}(\sqrt[3]{11})$	3	2
$-17^2\,101^3/2$	17	14450P1	$\mathbb{Q}(\sqrt[3]{17})$	3	2
$-17\cdot 373^3/2^{17}$		14450P2	$\mathbb{Q}(\sqrt[3]{17})$	3	1
$-2^{15}\,3^3$	19	361A1, 361A2	$\mathbb{Q}(\sqrt[4]{19})$	4	2
$-2^{18}\,3^3\,5^3$	43	1849A1, 1849A2	$\mathbb{Q}(\sqrt[4]{43})$	4	2
$-2^{15}\,3^3\,5^3\,11^3$	67	4489A1, 4489A2	$\mathbb{Q}(\sqrt[4]{67})$	4	2
$-2^{18}\,3^3\,5^3\,23^3\,29^3$	163	26569A1, 26569A2	$\mathbb{Q}(\sqrt[4]{163})$	4	2

Table 1. j-invariants with potentially supersingular reduction in $X_0(p)$. In the first row, $L = \mathbb{Q}(\sqrt[4]{3}, \beta)$, where $\beta^3 - 120\beta + 506 = 0$.

Proof. Let $p > 3$ be a prime, assume that $e_1 < e$, let K_E be the extension of degree e of $L_{\wp}^{\mathrm{nr}}$ defined above, and fix a minimal model of E over K_E with good supersingular reduction. Let Δ be its discriminant, and let c_4 and c_6 be the usual quantities. Let $\lambda = r(p)\nu_K(c_4) + s(p)\nu_K(c_6) + \nu_K(Q_p(j(E)))$ as in Theorem 3.9. If $\lambda \geq e$ then $e_1 \geq e$, but we have assumed that $e_1 < e$, and hence $e_1 = \lambda$. Notice that we have assumed $e(\wp, L) = 1$. In this case, $\nu_K(Q_p(j(E))) = e \cdot \nu_{\wp}(Q_p(j(E)))$ is a multiple of e. Since $e_1 = \lambda < e$, it follows that $\nu_K(Q_p(j(E))) = 0$, and under our assumptions

$$e_1 = r(p)\nu_K(c_4) + s(p)\nu_K(c_6). \tag{4-1}$$

Since $\nu_K(\Delta) = 0$ and $p \neq 2, 3$, the equality $1728\Delta = c_4^3 - c_6^2$ implies that $\nu_K(c_4)$ and $\nu_K(c_6)$ cannot be simultaneously positive. If both were zero, then our formula (4-1) would say $1 \leq e_1 = 0$, a contradiction, so one of the valuations must be positive and the other one must vanish.

If $\nu_K(c_4) > 0$ and $\nu_K(c_6) = 0$, then $\nu_K(j(E)) = \nu_K(c_4^3/\Delta) = 3\nu_K(c_4) > 0$. Since $j(E) \in L$, it follows that $j(E) \equiv 0 \bmod \wp$. In particular, $\nu_K(j)$ is a multiple of $e/e(\wp, L) = e$, say $\nu_K(j) = ek$, for some $k \geq 1$. Theorem 3.9 says that $e_1 = r(p)\nu_K(c_4) + s(p)\nu_K(c_6) = r(p)\nu_K(c_4)$. Thus, we must have $r(p) = 1$ (in particular, $p \equiv 5 \bmod 6$ in this case) and $e_1 = \nu_K(c_4)$, otherwise $0 = e_1 \geq 1$, a contradiction. Hence,

$$e_1 = \nu_K(c_4) = \frac{\nu_K(j)}{3} = \frac{ek}{3}.$$

Since $e_1 < e$ by assumption, it follows that $1 \le k < 3$. In addition, e_1 is a positive integer, so $ek \equiv 0 \bmod 3$, hence $e \equiv 0 \bmod 3$. Finally, $e = 1, 2, 3, 4$, or 6, so $e = 3$ or 6 in this case, and $e_1 = 1, 2$, or 4, as claimed.

If instead we have $\nu_K(c_4) = 0$ and $\nu_K(c_6) > 0$, we have $e_1 = \nu_K(c_6)$ (we must have $p \equiv 3 \bmod 4$ in this case). The equality $c_6^2 = \Delta \cdot (j(E) - 1728)$ implies that

$$e_1 = \nu_K(c_6) = \frac{\nu_K(j-1728)}{2} > 0.$$

It follows that $j \equiv 1728 \bmod \wp$ and $\nu_K(j - 1728) = eh$ for some $h \ge 1$. Since $e_1 < e$, we have $h < 2$ so $h = 1$, and since e_1 is an integer, we have $e \equiv 0 \bmod 2$. Thus, $e = 2, 4$, or 6, and therefore, $e_1 = 1, 2$, or 3. However, we shall show next that $j \equiv 1728 \bmod \wp$ and $e = 6$ is not possible. Thus, $e_1 = 1$, or 2, and the proof of the corollary would be finished.

Indeed, suppose $j \equiv 1728 \bmod \wp$ and $e = 6$. Let Δ_L, $c_{4,L}$ and $c_{6,L}$ be the discriminant and the usual constants associated to the original model of E over L. By the work of Néron on minimal models (Theorem 3.11), the degree $e = 6$ if and only if $\nu_\wp(\Delta_L) \equiv 2$ or $10 \bmod 12$. Since $\Delta_L \cdot j(E) = (c_{4,L})^3$, and $j \equiv 1728 \bmod \wp$, with $p > 3$, it follows that $\nu_\wp(\Delta_L) = 3\nu_\wp(c_{4,L})$ and therefore $\nu_\wp(\Delta_L) \equiv 0 \bmod 3$, and we cannot have $\nu_\wp(\Delta_L) \equiv 2$ or $10 \bmod 12$. This is a contradiction, and therefore $e = 6$ and $j \equiv 1728 \bmod \wp$ are incompatible. This ends the proof of the corollary. □

Corollary 4.7. *Under the notation and assumptions of Corollary 4.6, if $p > 3$ and $e_1 < e$, then $e_1 \le 2e/3$. In particular, $pe/(p + 1) > e_1$.*

Proof. Let $p \ge 5$ and $e_1 < e$. It follows from Corollary 4.6 that, in all cases, we have $e_1 = e/3$, or $e_1 = 2e/3$ or $e_1 = e/2$. Thus, $e_1 \le 2e/3$. In particular,

$$\frac{pe}{p+1} \ge \frac{5e}{6} > \frac{2e}{3} \ge e_1. \qquad \square$$

5. Torsion points

Lemma 5.1 (Serre). *Let E/L be an elliptic curve with potential good supersingular reduction at a prime $\wp$ above p. Let $K = K_E$ be the smallest extension of $L_\wp^{\mathrm{nr}}$ such that E/K has good (supersingular) reduction at $\wp$, and let $e = \nu_K(p)$ be its ramification index. Let A, $e_1 = \nu(s_p)$ and π be as above, so that $[p](Z) = pf(Z) + \pi^{e_1} g(Z^p) + h(Z^{p^2})$, where $f(Z)$, $g(Z)$ and $h(Z)$ are power series in $Z \cdot A[[Z]]$, with $f'(0) = g'(0) = h'(0) \in A^\times$.*

(1) *If $pe/(p + 1) \le e_1$, then $[p](Z) = 0$ has $p^2 - 1$ roots of valuation $e/(p^2 - 1)$.*

(2) *If $pe/(p+1) > e_1$, then $[p](Z) = 0$ has $p-1$ roots of valuation $(e-e_1)/(p-1)$ and $p^2 - p$ roots with valuation $e_1/(p(p - 1))$.*

Proof. This is shown in [Serre 1972, §1.10, pp. 271–272]. If $pe/(p+1) < e_1$, the Newton polygon for $[p](Z)$ has only one segment and if $pe/(p+1) \geq e_1$, then the polygon has two segments (see Remark 2.4). □

Theorem 5.2. *Let E/L be an elliptic curve with potential good supersingular reduction at a prime $\wp$ above a prime $p > 3$, and let e and e_1 be defined as above. Let $P \in E[p]$ be a nontrivial p-torsion point.*

(1) *Suppose $e_1 \geq pe/(p+1)$. Then the ramification index of any prime over $\wp$ in the extension $L(P)/L$ is divisible by $(p^2-1)/\gcd(p^2-1, e)$.*

(2) *Suppose $e_1 < pe/(p+1)$.*
   - *There are p^2-p points P in $E[p]$ such that the ramification index of a prime above $\wp$ in $L(P)/L$ is divisible by $(p-1)p/\gcd(p(p-1), e_1)$.*
   - *There are $p-1$ points P in $E[p]$ such that the ramification index of any prime above $\wp$ in $L(P)/L$ is divisible by $(p-1)/\gcd(p-1, e-e_1)$.*

In particular, if $e(\wp, L) = 1$ and $e_1 < e$, then $e_1 < pe/(p+1)$ and the ramification index of any prime over $\wp$ in $L(P)/L$ is divisible by $(p-1)/\gcd(p-1, 4)$.

Proof. Let E/L be an elliptic curve with potentially supersingular reduction at $\wp$ above $p > 3$, and let $P \in E(\overline{L})[p]$ be a point of exact order p. Let $\iota : \overline{L} \hookrightarrow \overline{L}_\wp$ be a fixed embedding. Let $F = L(P)$ and let $\mathfrak{P}$ be the prime of F above $\wp$ associated to the embedding ι. Let K be the smallest extension of $L_\wp^{\mathrm{nr}}$ such that E/K has good (supersingular) reduction at $\wp$. Choose a model E'/K with good reduction and isomorphic to E over K, and let $T \in E'(K)[p]$ be the point that corresponds to $\iota(P)$ on $E(\overline{L}_\wp)$. Suppose that the degree of the extension $K(T)/K$ is g. Since $K/L_\wp^{\mathrm{nr}}$ is of degree $e/e(\wp, L)$, it follows that the degree of $K(T)/L_\wp^{\mathrm{nr}}$ is $eg/e(\wp, L)$.

Let $\mathcal{F} = \iota(F) \subseteq \overline{L}_\wp$. Since E and E' are isomorphic over K, it follows that $K(T) = K\mathcal{F}$ and, therefore, the degree of the extension $K\mathcal{F}/L_\wp^{\mathrm{nr}}$ is $eg/e(\wp, L)$. Since $K/L_\wp^{\mathrm{nr}}$ is Galois (see Section 1), $g = [K(T) : K] = [\mathcal{F}L_\wp^{\mathrm{nr}} : K \cap \mathcal{F}L_\wp^{\mathrm{nr}}]$, so the degree of $[\mathcal{F}L_\wp^{\mathrm{nr}} : L_\wp^{\mathrm{nr}}]$ equals $g \cdot k$ where $k = [K \cap \mathcal{F}L_\wp^{\mathrm{nr}} : L_\wp^{\mathrm{nr}}]$. Hence, the degree of $\mathcal{F}/L_\wp$ is divisible by gk and, in particular, the ramification index of the prime ideal $\mathfrak{P}$ over $\wp$ in the extension $L(P)/L$ is divisible by gk, where $g = [K(T) : K]$. Thus, we just need to show that $[K(T) : K]$ satisfies the divisibility properties that are claimed in the statement of the theorem.

Let $T \in E'[p]$ be an arbitrary point on $E'(\overline{K})$ of exact order p, and write t for the corresponding torsion point in the formal group, that is, $t = -x(T)/y(T) \in \hat{E}'(\mathcal{M}_p)$.

(1) Let us first assume that $e_1 \geq pe/(p+1)$. By Lemma 5.1, the valuation of $t \in \hat{E}'[p]$ is $e/(p^2-1)$. Hence, the ramification index in the extension $K(T)/K$ is divisible by the quantity $(p^2-1)/\gcd(p^2-1, e)$, as claimed.

(2) Now let us suppose that $e_1 < pe/(p+1)$. By Lemma 5.1, there are $p-1$ points in $\hat{E}'[p]$ with valuation $(e-e_1)/(p-1)$ and p^2-p points with valuation

$e_1/(p(p-1))$, respectively. Thus, the ramification index of $K(T)/K$ is divisible by $(p-1)/\gcd(p-1, e-e_1)$ or $p(p-1)/\gcd(p(p-1), e_1)$, respectively.

Finally, suppose that $e(\wp, L) = 1$ and $e_1 < e$. Then, Corollary 4.7 shows that $pe/(p+1) > e_1$. Moreover, we showed in Corollary 4.6 that, when $p > 3$ and $e_1 < e$, the numbers e_1 and $e-e_1$ can only take the values 1, 2, or 4. Thus, the ramification index in $K(T)/K$ is divisible by at least $(p-1)/\gcd(p-1, 4)$, as claimed. This concludes the proof of the theorem. □

Example 5.3. Let $E/\mathbb{Q}$ be the elliptic curve with Cremona label "121c2", which we already studied in Examples 2.1 and 4.1, and we calculated $e = 3$ and $e_1 = 1$. Hence, if P is any nontrivial 11-torsion point on $E(\overline{\mathbb{Q}})$, then the ramification of any prime above $p = 11$ in the extension $\mathbb{Q}(P)/\mathbb{Q}$ must be divisible by, at least, $(p-1)/\gcd(p-1, 4) = 10/2 = 5$. Let us show that there is a 11-torsion point where the ramification index is exactly 5.

Indeed, let $F = \mathbb{Q}(\zeta)$, where $\zeta = \zeta_{11}$ is a primitive 11-th root of unity. Then, $E(F)_{\text{tors}} \cong \mathbb{Z}/11\mathbb{Z}$ and there is a point $P \in E(F)$ of order 11 with coordinates

$$x(P) = 11\zeta^9 + 11\zeta^8 + 22\zeta^7 + 22\zeta^6 + 22\zeta^5 + 22\zeta^4 + 11\zeta^3 + 11\zeta^2 + 39,$$
$$y(P) = 44\zeta^9 - 55\zeta^8 - 66\zeta^7 - 99\zeta^6 - 99\zeta^5 - 66\zeta^4 - 55\zeta^3 + 44\zeta^2 + 85.$$

Notice, however, that $x(P)$ and $y(P)$ are stable under complex conjugation. Hence, $P \in E(\mathbb{Q}(\zeta)^+)$, and in fact $\mathbb{Q}(P) = \mathbb{Q}(x(P), y(P)) = \mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta+\zeta^{-1})$. Thus, $\mathbb{Q}(P)/\mathbb{Q}$ is totally ramified at 11 and the ramification index is 5.

Corollary 3.10 implies that if $p \equiv 1 \bmod 12$, and $e(\wp, L) = 1$, then $e_1 \geq e$. When we combine this with Theorem 5.2 we obtain:

Corollary 5.4. *Let E/L be an elliptic curve with potential good supersingular reduction at a prime $\wp$ above a rational prime $p \equiv 1 \bmod 12$, let e be as above, and suppose $e(\wp, L) = 1$. Let $P \in E[p]$ be a nontrivial p-torsion point. Then the ramification index of any prime over $\wp$ in $L(P)/L$ is divisible by $(p^2-1)/\gcd(p^2-1, e)$.*

However, the conclusion of the previous corollary is not valid when $e(\wp, L) > 1$.

Example 5.5. Let $L = \mathbb{Q}(\sqrt{13})$, and let E/L be the elliptic curve with j-invariant j_0 as described in Example 2.3 and 4.4. There is a point $P \in E(\overline{L})$ such that $L(P)$ is given by $L(\alpha)$, where α is a root of a polynomial $q(x) \in L[x] = \mathbb{Q}(j_0)[x]$,

$$q(x) = x^{12} + \frac{34960589\,j_0 - 2813426633070000000}{478224}x^{10} + \cdots$$

of degree 12, and such that $L(P)/L$ is totally ramified above $\wp$. Recall that we have calculated $e = 2$ and $e_1 = 1$ for this curve, so the ramification in this extension agrees with the conclusion of Theorem 5.2 which predicts the existence of 12 points in $E[p]$ such that the ramification index of any prime above $\wp$ in $L(P)/L$ is divisible by $12/\gcd(12, e-e_1) = 12/\gcd(12, 2-1) = 12$.

Acknowledgments

I would like to thank Kevin Buzzard, Brian Conrad, and Felipe Voloch for several useful references and suggestions. I am also thankful to the anonymous referee for numerous suggestions, and a very thorough report.

References

[Birch and Kuyk 1975] B. J. Birch and W. Kuyk (editors), *Modular functions of one variable, IV*, Lecture Notes in Mathematics **476**, Springer, Berlin, 1975. MR 51 #12708 Zbl 0315.14014

[Bosma et al. 2010] W. Bosma and J. J. Cannon and C. Fieker and A. Steel (editors), *Handbook of Magma functions,* edition 2.16, 2010.

[Katz 1973] N. M. Katz, "p-adic properties of modular schemes and modular forms", pp. 69–190 in *Modular functions of one variable, III* (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), edited by W. Kuyk and J.-P. Serre, Lecture Notes in Mathematics **350**, Springer, Berlin, 1973. MR 56 #5434 Zbl 0271.10033

[Kenku 1982] M. A. Kenku, "On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class", *J. Number Theory* **15**:2 (1982), 199–202. MR 84c:14036 Zbl 0493.14017

[Lang 1987] S. Lang, *Elliptic functions*, 2nd ed., Graduate Texts in Mathematics **112**, Springer, New York, 1987. MR 88c:11028 Zbl 0615.14018

[Maier 2009] R. S. Maier, "On rationally parametrized modular equations", *J. Ramanujan Math. Soc.* **24**:1 (2009), 1–73. MR 2010f:11060 Zbl 1214.11049

[Mazur 1978] B. Mazur, "Rational isogenies of prime degree", *Invent. Math.* **44**:2 (1978), 129–162. MR 80h:14022 Zbl 0386.14009

[Néron 1964] A. Néron, "Modèles minimaux des variétés abéliennes sur les corps locaux et globaux", *Inst. Hautes Études Sci. Publ.Math. No.* **21** (1964), 128. MR 31 #3423 Zbl 0132.41403

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR 52 #8126 Zbl 0235.14012

[Serre and Tate 1968] J.-P. Serre and J. Tate, "Good reduction of abelian varieties", *Ann. of Math.* (2) **88** (1968), 492–517. MR 38 #4488 Zbl 0172.46101

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994. MR 96b:11074 Zbl 0911.14015

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009. MR 2010i:11005 Zbl 1194.11005

[Stein et al. 2012] W. A. Stein and the Sage development team, *Sage* (mathematics software), version 5.0, 2012, Available at http://www.sagemath.org.

Received May 23, 2012. Revised August 9, 2012.

ÁLVARO LOZANO-ROBLEDO
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CONNECTICUT
196 AUDITORIUM ROAD, UNIT 3009
STORRS CT 06269
UNITED STATES

alvaro.lozano-robledo@uconn.edu

PACIFIC JOURNAL OF MATHEMATICS

msp.org/pjm

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2013 is US $400/year for the electronic version, and $485/year for print and electronic.
Subscriptions, requests for back issues and changes of subscribers address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and the Science Citation Index.

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published monthly except July and August. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS

Volume 261 No. 1 January 2013