Compositio Mathematica **107:** 125–141, 1997.

Effective p-descent[*]

A. BROUMAS
Department of Mathematics, The University of Arizona, Tucson, AZ 85721, USA;
e-mail address: antonios@math.arizona. edu

Received 26 March 1996; accepted in revised form 26 March 1996

Abstract. Given E, an elliptic curve defined over K, a field of positive characteristic, provided that j, the Weierstrass j-invariant, is not an element of K^p, we construct explicitly, that is, we give by a closed form formula, a non-trivial homomorphism, $\mu\colon E(K)\to K^+$, from the group of K-rational points of E to K^+, the additive group of K. In the course of our analysis we discover a canonical differential, $\omega_q\in\Omega_{K|\mathbb{F}_p}$, associated to E and we relate it to the differential $\mathrm{d}q/q$ associated to the Tate curve. If the transcendence degree of K over $\mathbb{F}_p$ is equal to one, as for example is the case for function fields in one variable, then μ is a p-descent map, that is, its kernel is equal to $pE(K)$ and the explicit formula for μ can be used to provide effective proofs of analogues of classical theorems on elliptic curves. For example, in the author's thesis at The University of Texas at Austin the analogue of Siegel's Theorem on the finiteness of integral points of $E(K)$ is proved effectively.

Mathematics Subject Classifications (1991): Primary: 11G05; Secondary: 11G07, 14K99.

Key words: elliptic curves, descent, effective, derivation, characteristic p

1. Introduction

Here we extend work of Kramer [Kra], Voloch [Vol] and Ulmer [Ulm] and we present the p-descent map concretely in closed form. Our method works for general prime p and quite general field K, see Subsections (2.1), (4.1) and (4.6), but it is simpler to state the main result uniformly for all $p\geqslant 5$ and restrict ourselves in the function field case with $[K\colon\mathbb{F}_p]_{\mathrm{tr}}=1$.

MAIN THEOREM. *Let K be a function field in one variable, of characteristic $p\geqslant 5$, and let $E\colon y^2=x^3+a_4x+a_6$, $a_4,a_6\in K$, be an elliptic curve with origin $\mathcal{O}$. Assume that the Hasse invariant A is nonzero and $dj\neq 0$ for d the canonical derivation which maps K to $\Omega_{K|\mathbb{F}_p}$. Let $\mathcal{D}=18(a_6/a_4)j(d/dj)$. Then we have a homomorphism $\mu\colon E(K_s)\to K_s^+$ which is Galois equivariant with respect to $G=\mathrm{Gal}(K_s\,|\,K)$, defined by $\mu(E[2])=\{0\}$ and*

$$\mu(x,y)=\pi\left(\frac{\mathcal{D}x}{2y}\right)+yM(x)+\pi\left(\frac{-2x^2-\frac{1}{6}\frac{\mathcal{D}\Delta}{\Delta}x-\frac{4}{3}a_4}{2y}\right)\quad \textit{if } y\neq 0,$$

where all quantities above can be computed directly from a_4 and a_6. That is: j is the j-invariant, Δ the discriminant, A the Hasse invariant, π is defined by

[*] This is part of the author's dissertation at The University of Texas at Austin

$\pi(z) = z^p - Az$ and M is defined by: $(x^3 + a_4x + a_6)^{(p-1)/2} = x^pM(x)+$ *lower order terms*.

All our work is based on two different descriptions of the Galois group G of the field extension $K_s(E^{(p)}) \mid K_s(E)$ where $E^{(p)}$ is the Frobenius curve associated to E and $K_s(E^{(p)})$ is viewed as an extension of $K_s(E)$ via the Verschiebung, the dual isogeny to the Frobenius map. See Section (3). Then in Section (4) a generalized Manin map, see [M], of order 1, that is a homomorphism involving only first order differentiation is constructed from $E^{(p)}(K_s)$ to K_s^+ and normalized in accordance with the Galois action of G. This map has a very simple expression in coordinates and this allows us to produce a formula for the Manin map μ from $E(K_s)$ to K_s^+.

The expositions of Voloch [Vol] and Ulmer [Ulm] are naturally the origins of this work and only after reading through them everything presented here can be seen via the right historical perspective.

Having μ explicitly given, certain applications become accessible. For example, in [B], one finds an effective proof of Siegel's Theorem on the finiteness of integral points on a non-isotrivial elliptic curve defined over a function field finitely generated over $\mathbb{F}_p$, of transcendence degree one. There, a careful local investigation, facilitating the formula for μ, compares height with local distance from the origin, and passing to global, the height of the integral points is bounded, which amounts to effectively identifying them.

We have tried to avoid computations and justify as many results as possible using only general theory. However, all our intuition was developed via explicit calculations for $p = 5, a_4 = 3t^4, a_6 = 4$ and $p = 7, a_4 = 1, a_6 = 5t^6$ and $p = 11$, $a_4 = 5t^2, a_6 = t^8$.

2. Conventions and notation

2.1. *Our field*. Let K be a field of characteristic $p > 0$. By K_s we denote the separable closure of K. It is crucial for our analysis that $\mathrm{Der}_{\mathbb{F}_p}K$ is nonzero. Hence, we need $K \neq K^p$. As it will turn out, see Section (6), we may assume without loss of generality that $K = K_s$, that is that K is separably closed.

2.2. *Elliptic curves*. Our object of study will be an elliptic curve, E, defined over K. The case of characteristic $p = 2$ will be studied in Appendix (A) and for $p \neq 2$ the Weierstrass Equation for E can be taken to be: of its plane projective embedding given by a Weierstrass Equation

$$E: y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

2.3. *Frobenius*. For simplicity of notation we denote $E^{(p)}$, the image of the relative – with respect to K - Frobenius map, by E'

$$E^{(p)} \equiv E': y'^2 = x'^3 + a_2^p x'^2 + a_4^p x' + a_6^p \tag{2}$$

and the Frobenius map is given by: $F: E \to E': (x,y) \mapsto (x^p, y^p)$ and for V, its dual isogeny, the Verschiebung: $V: E' \to E: (x', y') \mapsto (x_{\text{ver}}(x',y'), y_{\text{ver}}(x',y'))$ we have: $V \circ F \equiv [p]_E$ and $F \circ V \equiv [p]_{E'}$.

The Frobenius map, F, is always inseparable but its dual isogeny, the Verschiebung, V, is separable unless the Hasse invariant of E is zero.

2.4. *Calculating the Hasse invariant*. We will introduce A via one of its explicit calculations. The algorithm goes back to Deuring [Deur] 8.2, p. 253. We present here the case $p \geqslant 3$ with $a_1 = a_3 = 0$. Hence (1) is the equation of the elliptic curve and one calculates A as the coefficient of x^{p-1} in the polynomial $(f(x))^{(p-1)/2}$. In addition define L, and M, L and M polynomials, $\deg L \leqslant (p-2)$, by

$$\begin{aligned} f(x)^{(p-1)/2} &= (x^3 + a_2 x^2 + a_4 x + a_6)^{(p-1)/2} \\ &= L(x) + Ax^{p-1} + x^p M(x). \end{aligned} \tag{3}$$

Hasse, in [Ha], proves the following theorem: Let K be a separably closed field of positive characteristic p. Then there exists a unique separable, Galois, cyclic of order p, unramified extension of the elliptic field $K(E) = K(x,y)$, if and only if the Hasse invariant A is nonzero.

2.5. *Some properties of* A. Given the standard choices for invariant under the group law differentials on E and E',

$$\omega = \frac{\mathbf{d}x}{2y} \quad \text{and} \quad \omega' = \frac{\mathbf{d}x'}{2y'},$$

the Hasse invariant, A, can be defined equivalently via:

LEMMA 2.1. *Let V denote the Verschiebung and let $V^\star$ be the induced* (*pull back*) *map on differentials. That is: $V^\star: \Omega_{K(E)|K} \to \Omega_{K(E')|K}$. Then*

$$V^\star(\omega) = A\omega'. \tag{4}$$

Proof. This is the dual statement to 12.4.1.3 in [KM] p. 354. Since in [KM] the Hasse invariant, A, is defined via the map $tg(V)$: Lie$(E^{(p)}, K) \to$ Lie(E, K), using autoduality of elliptic curves we identify Lie(E,K) with $H^1(E, \mathcal{O}_E)$, where $\mathcal{O}_E$ is the structure sheaf of E, and the connection with our calculation in (3) is provided by [Hart] IV.4. Proposition 4.21, p. 332–333. □

See that $A \neq 0$ if and only if the Verschiebung is separable and in that case the field extension $K(E')$ over $V^*(K(E)))$ is the unique extension of Hasse's Theorem.

LEMMA 2.2. *For V as above and with $a_1 = 0 = a_3$ we have*

$$y_{\text{ver}} = \frac{1}{A}\, y' \frac{\mathbf{d}x_{\text{ver}}}{\mathbf{d}x'}. \tag{5}$$

Proof. By the lemma above

$$V^\star\left(\frac{\mathbf{d}x}{2y}\right)=A\frac{\mathbf{d}x'}{2y'}\quad\text{and}\quad V^\star\left(\frac{\mathbf{d}x}{2y}\right)=\frac{\mathbf{d}x_{\text{ver}}}{2y_{\text{ver}}}.$$

[Silv] II.4.1., p. 35. □

2.6. *Denoting derivations.* At this point allow us to introduce some additional notation. We use d and $\mathbf{d}$ to denote the canonical derivations: $d\colon K\to\Omega_{K|\mathbb{F}_p}$ and $d\colon K_s\to\Omega_{K_s|\mathbb{F}_p}$ and $\mathbf{d}\colon K_s(E)\to\Omega_{K_s(E)|K_s}$ and $\mathbf{d}\colon K_s(E')\to\Omega_{K_s(E')|K_s}$. We use $\mathcal{D}$ and δ to denote field derivations, that is, elements of $\mathrm{Der}_{\mathbb{F}_p}K$ or $\mathrm{Der}_{\mathbb{F}_p}K_s$.

Let $\mathcal{D}$ be a derivation of K. Then we define $(\ )^{\mathcal{D}}$ to denote the derivation of $K(E')$ that extends $\mathcal{D}$ on K and it is trivial on x'. Since E' is defined over K^p we also have that $(y')^{\mathcal{D}}=0$ and so $(\ )^{\mathcal{D}}$ on $K[x',y']$ is simply differentiation of the coefficients of the polynomials in x' and y' and extends naturally as a derivation on $K(x',y')$.

Finally, for f in $K_s(E)$, a rational function on E defined over K_s, by $\mathcal{D}f$ we denote the composition $\mathcal{D}\circ f\ |_{\mathrm{reg}(f,K_s)}$ where $\mathrm{reg}(f,K_s)=\{$'points' of $E(K_s)$ where f is regular$\}$. Similarly we define $\mathcal{D}g'$ for g' in $K_s(E')$.

3. Preliminaries

3.1. *Restrictions.* Later on we will require that, $E'[p]$, the p-torsion of E', is not defined over K^p. This condition has various reformulations:

LEMMA 3.1. *For E an elliptic curve defined over K a field separably closed of characteristic $p>0$ the following are equivalent*:

(1) *E can be defined over K^p.*
(2) *The p-torsion of E is defined over K. That is $E[p]\subset E(K)$.*
(3) *The p-torsion of E' is defined over K^p. That is $E'[p]\subset E'(K^p)$.*

Proof. The only inference that needs justification is $(2)\Rightarrow(1)$. One may argue as follows: if $E[p]$ is defined over K then the quotient curve, $E/E[p]$, see [Silv] Proposition 4.12, p. 78, is also defined over K and the map, $E\to E/E[p]$, is a separable isogeny of degree p, defined over K. But then, its dual isogeny has to be purely inseparable because their composition gives the multiplication by $[p]$ map, which is not separable. See [Silv] Theorem III.6.1., p. 84. Hence, E is the image of a purely inseparable map of degree p, defined over K, that is, E is defined over K^p. □

Hence, we simply require that, j, the j-invariant of E, is not in K^p. Note that $j\notin K^p$ implies $j\notin\overline{\mathbb{F}_p}$, which implies $A\neq 0$, since all supersingular j-invariants are in $\mathbb{F}_{p^2}$. Hence, $E'[p]$ is cyclic of order p. See [Huse] Table 2 in 13.7, p. 258. Given that K is assumed to be separably closed we get that $E'[p]$ is defined over K.

3.2. *Descriptions of* $G = \mathrm{Gal}(K(E') \mid K(E))$. Cassels, [C] p.40 Equation (1.5), attributes to Deuring, an alternative description of $K(E')$. We have $K(x', y') \approx K(x, y, z)$, for z algebraic over $K(x, y)$, satisfying $\pi(z) = z^p - Az = yM(x)$ where M was defined in (3). Voloch in [Vol] Lemma 1.1 calculates z explicitly as

$$z = -2\frac{y'}{A}\sum_{i=1}^{(p-1)/2} \frac{1}{x' - x'_i},$$

where x'_i are the x' coordinates of the points of E' of exact order p. In fact there are p possible choices for z and the one presented above is uniquely characterized by $(z - (y/x))(\mathcal{O}') = 0$. Note that, due to symmetry, z is in $K(x, y)$ even if x_i's are not in K.

Define $G = \mathrm{Gal}(K(E') \mid K(E))$. To be precise, $G = \mathrm{Gal}(K(E') \mid V^*(K(E)))$. There are two canonical descriptions of G. First we may think of it as consisting of translations of the functions in $K(E')$ by the points of order p on E'. That is

$$G = \{\tau_{P'} \colon P' \in E'[p]\} \quad \text{where} \quad (\tau_{P'}g')(Q') = g'(P' \oplus Q') \tag{6}$$

and second since $K(E') = K(E)(z)$ one may think of G as translations of the special function z by $(p-1)$-st roots of A. Observe that, since we have assumed K to be separably closed, z is essentially the Artin–Schreier generator of $K(E')$ and employing it we get

$$G = \langle\sigma\rangle \quad \text{for} \ \sigma \colon z \to z + c \quad \text{for} \ c \colon c^{p-1} = A. \tag{7}$$

The two descriptions of G force a canonical isomorphism between the points of order p on E' and the additive subgroup of K^+ generated by the $(p-1)$-st roots of A. We call the isomorphism cgal and it is defined by

$$\mathrm{cgal}(P'_i) \overset{\mathrm{def}}{=} z(Q' \oplus P'_i) - z(Q'). \tag{8}$$

The isomorphism cgal does not depend on the choice of Q'. However, Q' needs be chosen so that no poles occur in Equation (8), above.

The definition of cgal forces an isomorphism

$$\mathrm{cgal} \colon E'[p] \overset{\sim}{\to} \langle c\rangle \tag{9}$$

and employing it we can index the points in $E'[p]$ by their corresponding Galois constants – their images under cgal – and have

$$E'[p] = \{P'_c \colon c^p - Ac = 0\}, \quad \text{where} \ \mathrm{cgal}(P'_c) = c. \tag{10}$$

4. Proof of the main theorem

Our goal is to construct a nontrivial homomorphism μ: $E(K) \to K^+$ and calculate $\mu(P)$ explicitly in terms of $x(P)$ and $y(P)$. The origins of our work are in [Vol] Theorem 3.1. and [Ulm] Proposition 5.3. diagram p. 249. As Voloch and Ulmer do, our first step is the construction of a homomorphism β: $E'(K) \to K^+$. It turns out that one may construct β directly and then obtain a closed form formula for μ based on formal manipulations of the formula for β. For the most part we restrict ourselves to $p \geqslant 3$ and later on to $p > 3$. See Appendix (A) for $p = 2$ and Appendix (B) for $p = 3$.

THEOREM 4.1. *Let E' be an elliptic curve defined over $(K)^p$. Then for any $\delta \in \mathrm{Der}_{\mathbb{F}_p} K$ the following map is a homomorphism*

$$\beta\colon E'(K) \to K^+\colon \begin{cases} \beta(P') = 0 & \text{for } P' \in E'[2], \\ \beta(x', y') = A\dfrac{\delta x'}{2y'} & \text{else.} \end{cases} \tag{11}$$

Equivalently $\beta(x', y') = A(\delta x'/2y')$ or

$$= A\frac{\delta y'}{3(x')^2 + 2a_2^p(x') + a_4^p},$$

whichever is well defined.

Proof. The proof is a straightforward calculation. One should use the addition formulae for elliptic curves in Weierstrass form; see [Ta] or [Silv], p. 58. Observe that since E' is defined over K^p we have

$$\delta y' = \frac{3(x')^2 + 2a_2^p(x') + a_4^p}{2y'}\delta x'$$

and the rest is trivial. That is, for $(x', y') = (x'_1, y'_1) \oplus (x'_2, y'_2)$, we have explicitly $x' = x'(x'_1, y'_1, x'_2, y'_2)$ and $y' = y'(x'_1, y'_1, x'_2, y'_2)$ and it is a formal identity that

$$\frac{\delta x'}{y'} = \frac{\delta x'_1}{y'_1} + \frac{\delta x'_2}{y'_2}.$$

To verify it, a symbolic calculator may be used; we used Mathematica. □

4.1. *Canonical choice of δ. Admissible derivations.* Normalize β as follows: choose δ, say $\mathcal{D}$, requiring that: $\beta(P') = \mathrm{cgal}(P')$ for $P' \in E'[p]$ and call such derivations, $\mathcal{D}$, admissible. Remember cgal was defined by Equation (8) in Subsection (3.2) and the points of order p, for each given fixed characteristic p, are explicitly calculated in [G]. Clearly the set of admissible derivations can be described by

$$\mathcal{D} \text{ admissible} \Leftrightarrow \langle \mathcal{D}, \omega_q \rangle = 1 \quad \text{for } \omega_q = \frac{A\, \mathrm{d}x'_c}{c2y'_c}, \tag{12}$$

where $P'_c \equiv (x'_c, y'_c)$ is any particular non-trivial point of order p on E'.*

See that ω_q is well defined and nonzero because: (1) the Hasse invariant, A is nonzero and so we have p points of order p on E' and cgal is well defined and $c = \mathrm{cgal}(P'_c)$ is nonzero as a $(p-1)$-st root of A and (2) since $E'[p]$ is in $E(K)$ but not in $E(K^p)$ we have $\mathrm{d}x'_c \neq 0$; see Lemma (3.1) in Subsection (3.1).

Hence, the set of admissible derivations is nonempty and the suggested normalization of β is feasible. As an illustration, consider the case when K is the separable closure of $\mathbb{F}_p[t]$ and E is an elliptic curve not defined over K^p. Then not only there exists an admissible derivation, $\mathcal{D}$, but in addition, since all derivations of K are multiples of each other, it is unique and it is determined as follows

$$\frac{A\mathcal{D}(x'(P'_c))}{(2y'(P'_c))} = \mathrm{cgal}(P'_c) = c \Leftrightarrow \mathcal{D} = \frac{c}{A} 2y'_c \frac{\mathrm{d}}{\mathrm{d}x'_c}. \tag{13}$$

4.2. *Transforming* β. The steps in this subsection are presented in reverse order of discovery. Reading [Kra], [Vol] and [Ulm] and experimenting with the computer we guessed that

$$\mu(x, y) = \pi\left(\frac{\mathcal{D}x}{2y}\right) + \pi(\text{function in } K(E)) + yM(x).$$

Following this belief, we were led to the normalization of β using cgal and then we worked backwards rewriting the formula for β.

For $g' \in K(E')$ and $\mathcal{D}$ a derivation of K and for $\mathcal{D}g'$ and $\mathcal{D}x'$ and $(\ )^{\mathcal{D}}$ defined in Subsection (2.6), we have

$$\mathcal{D}g' = \left(\frac{\mathbf{d}g'}{\mathbf{d}x'}\right)\mathcal{D}x' + ((g')^{\mathcal{D}})|_{\mathrm{reg}((g')^{\mathcal{D}}, K)}. \tag{14}$$

In particular

$$\mathcal{D}x_{\mathrm{ver}} = \frac{\mathbf{d}x_{\mathrm{ver}}}{\mathbf{d}x'}\mathcal{D}x' + x^{\mathcal{D}}_{\mathrm{ver}}. \tag{15}$$

Now let $P \in E(K)$ denote a generic K rational point of E. Let $P' = (x', y')$ be any point in $V^{-1}(P)$ so that $P = V(P') = (x_{\mathrm{ver}}(P'), y_{\mathrm{ver}}(P')) = (x_{\mathrm{ver}}, y_{\mathrm{ver}})$. Then invoking (15) above and Lemma (2.2) that gives $y_{\mathrm{ver}} = (1/A)y'(\mathbf{d}x_{\mathrm{ver}}/\mathbf{d}x')$, β becomes:

* The choice of notation, ω_q, will be explained in Section (5).

$$\begin{aligned}
\beta(x',y') &= A\frac{\mathcal{D}x'}{2y'}\\
&= A\frac{\mathcal{D}x'}{2y'} - \frac{1}{2y_{\text{ver}}}\mathcal{D}x_{\text{ver}} + \frac{\mathcal{D}x_{\text{ver}}}{2y_{\text{ver}}}\\
&= A\frac{1}{2y'}\mathcal{D}x' - \frac{1}{2y_{\text{ver}}}\left(\frac{\mathbf{d}x_{\text{ver}}}{\mathbf{d}x'}\mathcal{D}x' + x_{\text{ver}}^{\mathcal{D}}\right) + \frac{\mathcal{D}x_{\text{ver}}}{2y_{\text{ver}}}\\
&= \left(A\frac{1}{2y'}\mathcal{D}x' - \frac{1}{2y_{\text{ver}}}\frac{\mathbf{d}x_{\text{ver}}}{\mathbf{d}x'}\mathcal{D}x'\right) + \left(-\frac{x_{\text{ver}}^{\mathcal{D}}}{2y_{\text{ver}}} + \frac{\mathcal{D}x_{\text{ver}}}{2y_{\text{ver}}}\right)\\
&= \frac{\mathcal{D}x_{\text{ver}}}{2y_{\text{ver}}} - \frac{x_{\text{ver}}^{\mathcal{D}}}{2y_{\text{ver}}}. \qquad (16)
\end{aligned}$$

Now adding and subtracting z and defining g' by: $g'(x',y') = -z - (x_{\text{ver}}^{\mathcal{D}}/2y_{\text{ver}})$ we obtain

$$\begin{aligned}
\beta(x',y') &= \frac{\mathcal{D}x_{\text{ver}}}{2y_{\text{ver}}} + z - z - \frac{x_{\text{ver}}^{\mathcal{D}}}{2y_{\text{ver}}}\\
&= \frac{\mathcal{D}x_{\text{ver}}}{2y_{\text{ver}}} + z + g'(x',y'). \qquad (17)
\end{aligned}$$

Observe that $g'(x',y') = (\beta(x',y') - z) - (\mathcal{D}x_{\text{ver}}/2y_{\text{ver}})$ and viewing the Verschiebung as $V\colon E' \to E\colon (x,y,z) \mapsto (x,y)$ we have that the functions x_{ver} and y_{ver} are invariant under the action of the Galois group $G = \text{Gal}(K(E') \mid K(E)) = \text{Gal}(K(E') \mid V^*(K(E)))$. The same holds true for the difference $(\beta(x',y') - z)$ due to the normalization of β. Therefore g' is a function in $K(x',y')$ which is Galois invariant with respect to G and so $g' \in V^*(K(x,y))$. Define g and Q functions in $K(x,y)$ by $g \circ V \equiv g'$ and by $(Q(x,y)/2y) = g(x,y)$ where Q is a mnemonic for quadratic and was introduced anticipating the determination of g. Then for $(x,y) = (x_{\text{ver}}(x',y'), y_{\text{ver}}(x',y'))$ we have

$$\frac{Q(x,y)}{2y} = g(x,y) = g'(x',y') = \left(-z - \frac{x_{\text{ver}}^{\mathcal{D}}}{2y_{\text{ver}}}\right)(x',y'). \qquad (18)$$

4.3. *Passing to μ.* We construct μ exactly as Voloch and Ulmer do. Let π be defined by: $\pi(z) = z^p - Az$ and introduce μ requiring that the following diagram commutes

$$\begin{tikzcd}
E'(K) \arrow[r, "V"] \arrow[d, "\beta"'] & E(K) \arrow[d, "\mu"'] \\
K^+ \arrow[r, "\pi"] & K^+
\end{tikzcd} \qquad (19)$$

It is a rather trivial matter but let's make sure that μ is well defined. We have

$$\mu(P) \overset{\text{def}}{=} \pi(\beta(P')) = \pi\left(A\frac{\mathcal{D}x'}{2y'}\right) \quad \text{for any } P' \in V^{-1}(P). \tag{20}$$

The points P', mentioned above, are defined over K because V, the Verschiebung, is assumed to be separable and the choice of P' leads to no indeterminacy because π annihilates $\beta(E'[p])$ and $E'[p] = \ker V$. In addition V and β and π are group homomorphisms and all together we have:

THEOREM 4.2. *The map μ, defined via* (19) *and* (20)*, is a homomorphism*

$$\mu: E(K) \to K^+.$$

Formulae (17) and (18) that give β and Q respectively and the fact that the function z, see Subsection (3.2), satisfies: $\pi(z) = yM(x)$, for M defined by (3), result to a closed form formula for μ that has as follows: $\mu(E[2]) = \{0\}$ and for $(x, y) \in E(K)$ with $y \neq 0$ and for (x', y') any point in $E'(K)$ so that $V(x', y') = (x, y)$ we have

$$\begin{aligned}
\mu(x,y) &\overset{\text{def}}{=} \pi(\beta(x',y')) \\
&\overset{(16)}{=} \pi\left(\frac{\mathcal{D}x_{\text{ver}}(x',y')}{2y_{\text{ver}}(x',y')}\right) + \pi\left(-\frac{x_{\text{ver}}^{\mathcal{D}}(x',y')}{2y_{\text{ver}}(x',y')}\right) \\
&\overset{(17),(18)}{=} \pi\left(\frac{\mathcal{D}x}{2y}\right) + \pi\left(z + \frac{Q(x,y)}{2y}\right) \\
&\overset{(3.2),(3)}{=} \pi\left(\frac{\mathcal{D}x}{2y}\right) + yM(x) + \pi\left(\frac{Q(x,y)}{2y}\right).
\end{aligned} \tag{21}$$

See that neither a formula giving $x = x_{\text{ver}}(x', y')$ as a function of x' and y' nor the explicit knowledge of (x', y') are required for the determination of $\mu(x, y)$. There may be more than one admissible derivations, $\mathcal{D}$. Each one gives rise to a different map, μ. In what follows we will determine the set of admissible derivations and the unknown function, Q.

4.4. *Identifying* $Q(x)$. Inspecting Formula (21) that gives μ above and (18) that defines Q, we realize that Q may have poles only at $\mathcal{O}$. See that $Q = -2zy_{\text{ver}} - x_{\text{ver}}^{\mathcal{D}}$ and z, y_{ver} and x_{ver} have poles only above $\mathcal{O}$ and for $(\ )^{\mathcal{D}}$, the differentiation defined in Subsection (4.2), we have: the set of polar places of $x_{\text{ver}}^{\mathcal{D}}$ is included in the set of polar places of x_{ver}. Hence Q is a polynomial in x and y.

Let's try to determine $Q(x, y)$. Remember μ is a homomorphism. Hence μ is an odd function. So Q is even, that is, a polynomial only in x (see [Silv] III.2.3.1. p. 59). Finally, since $\pi(-(x_{\text{ver}}^{\mathcal{D}}/2y)) = yM(x) + \pi(Q(x)/2y)$ and $x_{\text{ver}}^{\mathcal{D}}/2y$ has no poles above $\mathcal{O}$, Q has to be of degree exactly 2 so that $\pi(Q/2y)$ cancels the pole due to $yM(x)$ and μ is given as

$$\mu(x,y) = \pi\left(\frac{\mathcal{D}x}{2y}\right) + yM(x) + \pi\left(\frac{ax^2+bx+c}{2y}\right). \tag{22}$$

To be exact we need $a = -2$ because $M(x)$ is monic (see Equation (3)).

Now let's repeat the process of transforming β as we did in Equation (16) but this time starting from

$$\beta(x',y') = A\frac{\mathcal{D}y'}{3x'^2 + 2a_2^p x' + a_4^p}$$

and invoking

$$V^\star\left(\frac{\mathbf{d}y}{3x^2+2a_2x+a_4}\right) = A\frac{\mathbf{d}y'}{3x'^2+2a_2^p x' + a_4^p}.$$

This way we arrive at

$$\beta(x',y') = \frac{\mathcal{D}y_{\text{ver}}}{3x_{\text{ver}}^2 + 2a_2x_{\text{ver}} + a_4} - \frac{y_{\text{ver}}^{\mathcal{D}}}{3x_{\text{ver}}^2 + 2a_2x_{\text{ver}} + a_4}, \tag{23}$$

and using (20) which defines μ and our previous calculation of β in (16) we can express μ in two different ways

$$\begin{aligned}\mu(x,y) &= \pi\left(\frac{\mathcal{D}x_{\text{ver}}}{2y_{\text{ver}}}\right) + \pi\left(-\frac{x_{\text{ver}}^{\mathcal{D}}}{2y_{\text{ver}}}\right)\\ &= \pi\left(\frac{\mathcal{D}y_{\text{ver}}}{3x_{\text{ver}}^2 + 2a_2x_{\text{ver}} + a_4}\right) + \pi\left(-\frac{y_{\text{ver}}^{\mathcal{D}}}{3x_{\text{ver}}^2 + 2a_2x_{\text{ver}} + a_4}\right).\end{aligned} \tag{24}$$

Starting from the equation for $E\colon y^2 = x^3 + a_2x^2 + a_4x + a_6$ and using $\mathcal{D}$-differentiation we can relate $\mathcal{D}x$ and $\mathcal{D}y$ via

$$2y\mathcal{D}y = (3x^2+2a_2x+a_4)\mathcal{D}x + ((\mathcal{D}a_2)x^2 + (\mathcal{D}a_4)x + (\mathcal{D}a_6)).$$

Then (24), the equation above, invoking for one more time $\pi(-(x_{\text{ver}}^{\mathcal{D}}/2y_{\text{ver}})) = \pi(Q(x)/2y) + yM(x)$, yields

$$\pi\left(-\frac{y_{\text{ver}}^{\mathcal{D}}}{3x_{\text{ver}}^2 + 2a_2x_{\text{ver}} + a_4}\right) \tag{25}$$

$$= \pi\left(\frac{Q(x)}{2y}\right) + \pi\left(\frac{\mathcal{D}x}{2y} - \frac{\mathcal{D}y}{3x^2+2a_2x+a_4}\right) + yM(x) \tag{26}$$

$$= \pi\left(\frac{1}{2y}\left(Q(x) - \frac{(\mathcal{D}a_2)x^2 + (\mathcal{D}a_4)x + (\mathcal{D}a_6)}{(3x^2+2a_2x+a_4)}\right)\right) + yM(x). \tag{27}$$

Observe now that $y^{\mathcal{D}}_{\text{ver}}/(3x^2_{\text{ver}} + 2a_2x_{\text{ver}} + a_4)$ has no poles above the points of E with $y = 0$ and so Q is determined by

$$Q(e_i) = \frac{(\mathcal{D}a_2)e_i^2 + (\mathcal{D}a_4)e_i + (\mathcal{D}a_6)}{3e_i^2 + 2a_2e_i + a_4}$$

which also reads $Q(e_i) = -\mathcal{D}e_i$ for e_i the roots of f: $f(x) = x^3 + a_2x^2 + a_4x + a_6$ and $(e_i, 0)$ are the points of order 2.

4.5. *Solving* $Q(e_i) = -\mathcal{D}e_i$, $i = 1, 2, 3$. So we have to solve a linear system of three equations and three unknowns a, b and c. The determinant of the system is the Vandermode determinant of the quantities $e_i, i = 1, 2, 3$; hence nonzero because its square equals to $\frac{1}{16}\Delta$ and Δ, the discriminant of the elliptic curve, is nonzero. Since we already know $a = -2$ we can also obtain an equation binding $\mathcal{D}$, the canonical derivation.

Note that due to symmetry the solutions involve only symmetric functions of e_1, e_2 and e_3. Hence explicit knowledge of the coordinates e_i is not required and we can proceed employing any form of the elementary symmetric functions theorem and the fact that $e_i, i = 1, 2, 3$, are the roots of f: $f(x) = x^3 + a_2x^2 + a_4x + a_6$. Alternatively, instead of solving the system above, we can pinpoint Q as the unique quadratic in x so that

$$Q(x) = \frac{(\mathcal{D}a_2)x^2 + (\mathcal{D}a_4)x + (\mathcal{D}a_6)}{3x^2 + 2a_2x + a_4} \text{ modulo } f.$$

One way or another we obtain

$$\begin{aligned}
a &= \tfrac{16}{\Delta}((2a_4^2 - 6a_2a_6)\mathcal{D}a_2 + (-a_2a_4 + 9a_6)\mathcal{D}a_4 + (2a_2^2 - 6a_4)\mathcal{D}a_6),\\
b &= \tfrac{16}{\Delta}((a_2a_4^2 - 3a_4a_6 - 2a_2^2a_6)\mathcal{D}a_2 + (-a_2^2a_4 + 2a_4^2 + 3a_2a_6)\mathcal{D}a_4\\
&\qquad + (2a_2^3 - 7a_2a_4 + 9a_6)\mathcal{D}a_6),\\
c &= \tfrac{16}{\Delta}((a_2a_4a_6 - 9a_6^2)\mathcal{D}a_2 + (-2a_2^2a_6 + 6a_4a_6)\mathcal{D}a_4\\
&\qquad + (a_2^2a_4 - 4a_4^2 + 3a_2a_6)\mathcal{D}a_6),
\end{aligned} \tag{28}$$

where Δ is the discriminant of the elliptic curve given in [Ta], p. 180 or [Silv], p. 46 as a polynomial in a_2, a_4 and a_6.

To simplify the presentation we will treat the case $p = 3$ in Appendix (B).

4.6. *Calculation for* $p > 3$. In this case a linear change of variables allows us to assume without loss of generality that a_2 in (1) is equal to zero. Then we obtain

$$\begin{aligned}
a &= \frac{3(2a_4\mathcal{D}a_6 - 3a_6\mathcal{D}a_4)}{4a_4^3 + 27a_6^2},\\
b &= -\frac{1}{6}\frac{\mathcal{D}\Delta}{\Delta} \quad \text{where } \Delta = -16(4a_4^3 + 27a_6^2),\\
c &= \tfrac{2}{3}a_4a = -\tfrac{4}{3}a_4.
\end{aligned} \tag{29}$$

In order to have $a = -2$ we realize that admissible derivations, $\mathcal{D}$, are the ones that satisfy

$$\left\langle \mathcal{D}, \frac{9a_6(\mathrm{d}a_4) - 6a_4(\mathrm{d}a_6)}{2(4a_4^3 + 27a_6^2)} \right\rangle = 1$$

and so we obtain an alternative description of ω_q. That is, comparing with (12) in Subsection (4.1), we have

$$\omega_q = \frac{A\,\mathrm{d}x'_c}{c2y'_c} = \frac{a_4\,\mathrm{d}j}{18a_6 j}, \tag{30}$$

where j is the Weierstrass j invariant given by $j = (-48a_4)^3/\Delta$.

Note that our restriction $j \notin K^p$, see Subsection (3.1), guarantees: $j \neq 0, a_6 \neq 0$, $a_4 \neq 0$ and $\mathrm{d}j \neq 0$. Hence, once more we see that ω_q is well defined and nonzero; cf. Subsection (4.1).

Under a change of variables $x_u = u^2x, y_u = u^3y$, ω_q changes to $(\omega_q)_u = u^{-2}\omega_q$. When we started working in this problem this was one of our first observations and at that time it helped us guess

$$\omega_q = r\frac{a_4\,\mathrm{d}j}{a_6} \quad \text{for } r \in K(j).$$

See that even if K is not separably closed, still ω_q is in $\Omega_{K|\mathbb{F}_p}$. In particular, if we work over $\mathbb{F}_p(j)$ or any function field in one variable then the unique choice for $\mathcal{D}$ is

$$\mathcal{D} = \frac{2(4a_4^3 + 27a_6^2)\,\mathrm{d}}{9a_6(\mathrm{d}a_4) - 6a_4(\mathrm{d}a_6)} = 18\frac{a_6}{a_4}j\frac{\mathrm{d}}{\mathrm{d}j}.$$

Overall, provided that some admissible derivation, $\mathcal{D}$, does exist, (21), the formula for μ becomes: $\mu(E[2]) = \{0\}$ and for $y \neq 0$

$$\mu(x,y) = \pi\left(\frac{\mathcal{D}x}{2y}\right) + yM(x) + \pi\left(\frac{-2x^2 - \frac{1}{6}\frac{\mathcal{D}\Delta}{\Delta}x - \frac{4}{3}a_4}{2y}\right) \tag{31}$$

and this concludes the proof of our main theorem.

5. Tate's curve and Serre's derivation

In order to justify the notation ω_q, we need refer to the connection between ω_q and $\mathrm{d}q/q$, the canonical differential of the ground field, $\mathbb{F}_p((q))$, of the Tate curve, dual to Serre's derivation, $\partial = q(\mathrm{d}/\mathrm{d}q)$. The canonical differential, $\mathrm{d}q/q$, which also appears in Ulmer's work, see [Ulm], p. 254, is given by

$$\frac{\mathrm{d}q}{q} = \frac{3E_6\,\mathrm{d}E_4 - 2E_4\,\mathrm{d}E_6}{E_4^3 - E_6^2},$$

where E_{2k} are the Eisenstein series normalized so that their q expansion starts with 1. To compare the two expressions

$$\omega_q = \frac{a_4\,\mathrm{d}j}{18a_6 j} \quad \text{and} \quad \omega_q = \frac{\mathrm{d}q}{q},$$

note that our curve $E\colon y^2 = x^3 + a_4x + a_6$ is isomorphic to the Tate curve

$$E_q\colon \tilde{y}^2 + \tilde{x}\tilde{y} = \tilde{x}^3 + h_4\tilde{x} + h_6 \quad \text{for}$$

$$h_4 = \tfrac{1}{48} + a_4, \;\; h_6 = \tfrac{1}{1728} + a_6 + \tfrac{a_4}{12},$$

$$\tilde{x} = x - \tfrac{1}{12} \quad \text{and } \tilde{y} = y - \tfrac{1}{2}(x - \tfrac{1}{12}).$$

Given the classical q-expansions for h_4 and h_6 (see [Silv], p. 356 Sect. 14) we get the following q-expansions for a_4 and a_6

$$a_4 = -\tfrac{1}{48} - 5\sum_{n\geqslant 1} \frac{n^3q^n}{1-q^n} \quad \text{and} \quad a_6 = \tfrac{1}{864} - \tfrac{7}{12}\sum_{n\geqslant 1} \frac{n^5q^n}{1-q^n}, \tag{32}$$

and employing them, for

$$j = \frac{6912a_4^3}{4a_4^3 + 27a_6^2}, \quad \text{we obtain} \quad \frac{a_4\,\mathrm{d}j}{18a_6 j} = \frac{\mathrm{d}q}{q}.$$

Alternatively, following Tate's suggestion, we can use the correspondences $E_4 \leftrightarrow c_4$ and $E_6 \leftrightarrow -c_6$, where c_4 and c_6 are the parameters introduced by Tate in [Ta] and which for $a_1 = a_3 = a_2 = 0$ become $c_4 = -48a_4$ and $c_6 = -864a_6$. Then ω_q becomes

$$\frac{c_4}{c_6}\frac{\mathrm{d}j}{j} = -\frac{E_4}{E_6}\frac{\mathrm{d}j}{j} = \frac{\mathrm{d}q}{q}$$

and from a theorem of Ramanujan, see [SD], p. 78, $(q(\mathrm{d}/\mathrm{d}q)\Delta)/\Delta = E_2$ and the formula for μ reads

$$\mu(x,y) = \pi\left(\frac{q\frac{\mathrm{d}}{\mathrm{d}q}x}{2y}\right) + yM(x) + \pi\left(\frac{-2x^2 - \frac{1}{6}E_2x + \frac{1}{36}E_4}{2y}\right). \tag{33}$$

6. Working over K not separably closed

In fact, the only place, where we used that K is separably closed, is when we claimed that the extension $K(E')\,|\,K(E)$ is Galois, with Galois group $G =$

Gal$(K(E') \mid K(E))$. According to Hasse, see [Ha], we need A, the Hasse invariant, to be nonzero and a $(p-1)$-st power. Hence, the extension from K to K_1, for $K_1 = K(A^{1/(p-1)}$ would be sufficient. Note that, since K contains $\mathbb{F}_p$, if it contains one $(p-1)$-st root of A then it contains them all.

Arguing from general principles one may be able to prove that the maps β and μ, defined in (11) and (19), can be chosen to be Galois equivariant with respect to $G_s = \text{Gal}(K_s \mid K)$. However, in our case, see Section (4) and Appendix (A), we have produced explicit expressions for β and μ and have specified the set of admissible derivations via the explicit calculation of ω_q.

Hence, we need only observe that ω_q is defined over the field of definition, $K = \mathbb{F}_p(a_1, a_3, a_2, a_4, a_6)$, of our elliptic curve, E, even if K is not separably closed. Hence, provided that $j \notin K^p$ a derivation $\mathcal{D}$ of K_s defined over K can be chosen so that $\langle \mathcal{D}, \omega_q \rangle \neq 0$ resulting to β and μ also defined over K. In particular, for E defined over $\mathbb{F}_p(j)$, for j the Weierstrass j-invariant of E, then β and μ can be defined over $\mathbb{F}_p(j)$ too.

7. Applications

We attempt here a brief synopsis of the relevant contents of [Vol], [Ulm] and [B].

7.1. *The kernel of* μ. First observe that $pE(K) \subset \ker(\mu)$. We have $\mu(pP) = p\mu(P)$ because μ is a group homomorphism and $p\mu(P) = 0$ because we work in characteristic p. Now remember that μ was defined via the commutative diagram, (19), and $\mu \circ V = \pi \circ \beta$. Hence, $\mu(P) = 0 \Leftrightarrow \pi(\beta(P')) = 0$ for all P' in $V^{-1}(P)$. Since the kernel of π equals to $\{c : c^p - Ac = 0\}$ we get $\beta(P') \in \langle c \rangle$, the additive group generated by any nonzero such c. In fact, since $V^{-1}(P) = P' \oplus E'[p]$ and $\beta(E'[p]) = \langle c \rangle$, we may choose $P' = (x', y')$, P' in $V^{-1}(P)$, so that $\beta(P') = 0$ and since

$$\beta(P') = \beta(x', y') = \frac{\mathcal{D}x'}{2y'},$$

(points of order 2 can be treated separately), we get that P' can be chosen so that $\mathcal{D}x' = 0$.

In general, $\mathcal{D}$ is not fully determined and the condition $\mathcal{D}x' = 0$ is not that informative. So, let's restrict ourselves to the case $[K : \mathbb{F}_p]_{\text{tr}} = 1$. In this case $\mathcal{D} = 18(a_6/a_4)j(\mathrm{d}/\mathrm{d}j)$ and $\mathcal{D}x' = 0$ gives $x' \in K^p$. By inspection of the equation defining E', (2), we get $y' \in K^p$ also. Hence, $(x', y') = F(Q)$ for some Q in $E(K)$. As we have seen, in Subsection (2.3), $V \circ F = [p]_E$ and so $P = V(P') = (V \circ F)(Q) = pQ$. Hence, if the transcendence degree of K over $\mathbb{F}_p$ is equal to one, $\ker(\mu) \subset pE(K)$, resulting to $\ker(\mu) = pE(K)$. For an alterative proof see also [Vol] Theorem 3.1.

7.2. μ *as a descent map*. For K a function field in one variable and K_v its completion with respect to v, one of its valuations, Ulmer in [Ulm], p. 248 and 249 proves that $\mathrm{Sel}(K_v, [p])$, the local Selmer group for the multiplication by p map, equals to $\mu(E(K_v))$. Ulmer calculates $\mathrm{Sel}(K_v, [p])$ in Theorem 5.5. Having μ explicitly given an alternative calculation can be based on the fact that μ is continuous and $E(K_v)$ is compact for all local topologies. Then a continuity argument results to the identification of $\mu(E(K_v))$. In [B] such a calculation is undertaken and the integral points of $E(K)$ with respect to any chosen set of valuations of K are effectively computed.

7.3. *Further research.* The method presented here has been recently generalized by the author to at least an algorithm for doing p^n descent for elliptic curves in positive characteristic. The key idea is the generalization of the Hasse invariant A to an infinite Witt vector with effectively computable components. For a generalization to the case of Abelian varieties see [BuVo].

Appendix A. Calculation for $p = 2$

The case $p = 2$ has already been treated by Kramer in [Kra]. See also [Vol] Remark 3.3. Let E be given by: $y^2 + a_1xy = x^3 + a_2x^2 + a_6$. Then $\Delta = a_1^6a_6$ and $j = a_1^6/a_6$ and the map μ is given by

$$\mu \colon E(K) \to K^+ \colon \mu(x, y) = \frac{a_6}{a_1^2x^2} + \pi\left(\frac{a_6\frac{\mathrm{d}x}{\mathrm{d}a_6}}{x}\right), \tag{34}$$

where $\pi(z) = z^2 + a_1z$.

We would like to present here a direct calculation of the canonical differential ω_q. Remember that β is normalized by: $\beta(P') = \mathrm{cgal}(P')$ for P' a non-trivial point of order p on E' and $\mathrm{cgal}(P')$ is a $(p-1)$-st root of the Hasse invariant, A. But presently $p - 1 = 1$ and we have a unique choice for the point P', $P' = (0, a_6)$ and $\mathrm{cgal}(P') = A = a_1$. Since the invariant differential ω' on E' is given by

$$\omega' = \frac{\mathbf{d}x'}{x'} \quad \text{and} \quad \beta(x', y') = a_1\frac{\mathcal{D}x'}{x'},$$

then $\mathcal{D}$ is restricted by

$$\left\langle \mathcal{D}, \frac{\mathrm{d}a_6}{a_6} \right\rangle = 1,$$

and the canonical differential ω_q in $\Omega_{K|\mathbb{F}_p}$, that corresponds to E is

$$\omega_q = \frac{\mathrm{d}a_6}{a_6}.$$

A routine calculation, using the formulae in [Ta], p. 181, also in [Silv], p. 46, verifies again that

$$\omega_q = \frac{c_4}{c_6}\frac{\mathrm{d}j}{j}.$$

Appendix B. Calculation for $p = 3$

In this case by a linear change of variables we can assume $a_4 = 0$ in Equation (1). The discriminant Δ is given as $\Delta = 2a_2^3 a_6$ and the invariant j equals a_2^6/Δ. Substituting in (28) we obtain

$$\begin{aligned} a &= \frac{2a_2^2\mathcal{D}a_6}{2a_2^3 a_6} = \frac{\mathcal{D}a_6}{a_2 a_6} = 1, \\ b &= \frac{a_2^2 a_6 \mathcal{D}a_2 + 2a_2^3\mathcal{D}a_6}{2a_2^3 a_6}, \\ c &= 0. \end{aligned} \tag{35}$$

Hence, (21), the formula for μ in characteristic 3 becomes

$$\mu(x,y) = \pi\left(\frac{\mathcal{D}x}{2y}\right) + y + \pi\left(\frac{x^2 + 2\frac{\mathcal{D}a_2}{a_2} + \frac{\mathcal{D}a_6}{a_6}}{2y}\right). \tag{36}$$

Note. One verifies that again we have

$$\omega_q = \frac{\mathrm{d}a_6}{a_2 a_6} = \frac{c_4}{c_6}\frac{\mathrm{d}j}{j} \leftrightarrow \frac{\mathrm{d}q}{q}.$$

Acknowledgements

I would like to thank Dr. Jeffrey Vaaler and Dr. John Tate for all their help and guidance during my graduate school years and my advisor Dr. Felipe Voloch for all his support and patience and for giving me an excellent thesis problem to work on.

References

[B] Broumas, A.: Effective p-descent, Ph.D. Thesis, The University of Texas at Austin (1995).

[BuVo] Buium, A., and Voloch, J. F.: Reduction of the Manin map in characteristic p, *J. reine angew. Math.* 460 (1995) 117–126.

[C] Cassels, J. W. S.: Some elliptic function identities, *Acta Arith.* XXVIII (1971) 37–52.

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

[G] Gunji, H.: The Hasse invariant and p-division points of an elliptic curve, *Arch. Math.* (Basel) XXVII (1976) 148–158.

[Ha] Hasse, H.: Existenz separabler zyklischer unverzweigter Erweiterungs-körper vom Primzahlgrade p über elliptischen Funktionenkörper der Charakteristik p, *J. Reine Angew. Math.* 172 (1934) p. 77–85.

[Hart] Hartshorne, R.: Algebraic Geometry, *Graduate Texts in Math.* (52) Springer-Verlag (1977).

[Huse] Husemöller, D.: Elliptic curves, *Graduate Texts in Math.* Springer-Verlag (1987).

[KM] Katz, N., and Mazur, B.: Arithmetic Moduli of Elliptic Curves, Princeton University Press (1985).

[Kra] Kramer, K.: Two descent for elliptic curves in characteristic two, *Trans. Amer. Math. Soc.* 232 (1977) 279–295.

[M] Manin, Y. I.: Rational points of algebraic curves over function fields, *Izv. Akad. Nauk SSSR Ser. Mat.* 27 (1963) 1395–1440. *Amer. Math. Soc. Transl. Ser.* 2 Vol. 50 189–234.

[SD] Serre, J. P.: Congruences et forms modulaires (d'apres H.P.F. Swinnerton–Dyer) Seminaire Bourbaki no. 416 (1971/72). Also in *Collected Papers* III 74–88, Springer-Verlag (1986) Vol. I–III.

[Silv] Silverman, J. H.: The arithmetic of elliptic curves, *Graduate Texts in Math.* (106) Springer-Verlag (1986).

[Ta] Tate, J.: The arithmetic of elliptic curves, *Invent. Math.* 23 (1974) 179–206.

[Ulm] Ulmer, D. L.: p-descent in characteristic p, *Duke Math. J.* 62 (1991) 237–265.

[Vol] Voloch, J. F.: Explicit p-descent for elliptic curves in characteristic p, *Compositio Math.* 74 (1990) 247–258.