J. F. VOLOCH

Explicit p-descent for elliptic curves in characteristic p

Compositio Mathematica, tome 74, nº 3 (1990), p. 247-258
<http://www.numdam.org/item?id=CM_1990__74_3_247_0>

Compositio Mathematica **74**: 247–258, 1990.

Explicit p-descent for elliptic curves in characteristic p

J.F. VOLOCH
IMPA, Est. D. Castorina 110, Rio de Janeiro 22460, Brasil

Received 18 April 1989; accepted in revised form 9 October 1989

Introduction

The purpose of this paper is to define the analogue in characteristic $p > 0$ of a map defined by Manin [5] for elliptic curves over function fields of characteristic zero.

Manin's map is a homomorphism $\mu: E(K) \to K^+$, where K is a function field in one variable over $\mathbf{C}$ and E/K is an elliptic curve. Manin used this map to obtain the function field analogue of Siegel's finiteness theorem for integral point on elliptic curves (and a generalization of this map to prove Mordell's conjecture over function fields, this proof actually contained a gap which was filled by Coleman [0].) Then Stiller [9] (see also [10]) used Manin's map to bound the rank of $E(K)$, when the j-invariant of E is non-constant.

In this paper we will be concerned with elliptic curves E/K where K is a function field in one variable over a finite field of characteristic p. Under a mild restriction on E (see §3) we will define a homomorphism $\mu: E(K) \to K^+$ with kernel $pE(K)$. This map will furnish an explicit way of doing p-descent on E. As a consequence, we shall show that the Selmer group for the p-descent is finite. The finiteness of the Selmer group is a result of Milne ([6], for abelian varieties of any dimension).

We shall also give a proof of the function field analogue of Siegel's theorem in positive characteristic along the same lines as Manin's proof in characteristic zero.

Finally we will relate our map with the reduction modulo p of Manin's map.

Conventions and notation

Throughout this paper, K will denote a field of characteristic $p > 0$ and E will be an elliptic curve defined over K with Weierstrass equation (with $a_i \in K$):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

The invariant differential associated with equation (1) will be $\omega = \mathrm{d}x/2y + a_1x + a_3$ and the Hasse invariant of equation (1) will be the element $A \in K$ for which $C(\omega) = A^{1/p}\omega$, where C is the Cartier operator (see [4]). When E is supersingular then $A = 0$ for any Weierstrass equation for E. When E is ordinary, a change of variables $x = u^2x_1 + r, y = u^3y_1 + u^2sx_1 + t, u \neq 0$, changes A to $u^{1-p}A$. Hence if E is ordinary, we can talk unambiguously of the Hasse invariant of E/K as a well-defined element of $K^x/(K^x)^{p-1}$.

We shall assume throughout this paper that E/K is an ordinary elliptic curve with Hasse invariant $1 \in K^x/(K^x)^{p-1}$. Any ordinary elliptic curve will satisfy this condition after a separable extension of the ground field.

Let E' be the elliptic curve with Weierstrass equation

$$(y')^2 + a_1^px'y' + a_3^py' = (x')^3 + a_2^p(x')^2 + a_4^px' + a_6^p \tag{2}$$

From our assumption that E/K has Hasse invariant 1 it will follow (see §1) that the p-torsion points of E' are defined over K.

Finally, let $F: E \to E'$ be the isogeny given by $F(x, y) = (x^p, y^p)$ and $\phi: E' \to E$ be the isogeny dual to F. Both F and ϕ have degree p, F is purely inseparable and ϕ is separable since E is ordinary.

1. Descent via ϕ

Before giving an explicit ϕ-descent procedure we will give another equation for E' (following Deuring [1]) that will be suitable for our purposes. Suppose $p \neq 2$ (for $p = 2$, see Remark 1.4) and that E has a Weierstrass equation (1) with $a_1 = a_3 = 0$. Let

$$(x^3 + a_2x^2 + a_4x + a_6)^{(p-1)/2} = U(x) + Ax^{p-1} + x^pV(x).$$

$U(x), V(x) \in K[x]$, $\deg U \leqslant p-2$. Note that A is the Hasse invariant of (1).

LEMMA 1.1. *The cover of E defined by $z^p - Az = yV(x)$ is an étale cover of degree p and is isomorphic to E' over K.*

Proof. Since $A \neq 0$, the cover is certainly separable and of degree p and is unramified, except possibly above the origin O of E. But

$$yV(x) = (y/x)^p - Ay/x - yU(x)/x^p$$

and $yU(x)/x^p$ is regular at O, so the cover is also unramified above O.

As any ordinary elliptic curve has an unique étale cover of degree p, the above cover must be isomorphic to E' over some finite extension of K. We now prove that there is an isomorphism over K. First note that $yU(x)/x^p$ vanishes at O, so there is a point O' above O where $z - y/x$ vanishes and O' is obviously defined over K. Note also that the p-torsion points of the cover are the points above O.

We have the E' is given by equation (2) and so x, y are the coordinates of $\phi(x', y')$. Hence to give the isomorphism over K promised above, it suffices to show that $z \in K(x', y')$. Let P_i, $i = 1, \ldots, p - 1$, be the non-trivial p-torsion points on E' and x_i, $i = 1, \ldots, (p - 1)/2$ be their x'-coordinates. Then $x_i \in K$, by Gunji's formula [2].

It is easy to check that z has poles only at O' and P_i, $1 \leqslant i \leqslant p - 1$, $\mathrm{res}_{P_i} z\phi^*\omega = -1$ and, by above, $(z - y/x)(O') = 0$. Clearly these conditions uniquely determine z. Since the Hasse invariant of (2) is A^p, we have that the invariant differential ω' of (2) satisfies $A\omega' = \phi^*\omega$. Using this it is easy to check that the function

$$-y'/A \sum_{1}^{(p-1)/2} (x' - x_i)^{-1}$$

has the same properties of z noticed above, so it is equal to z. This completes the proof.

REMARK 1.2. If $c \in K$ satisfies $c^{p-1} = A$ then $z - y/x - c$ vanishes at a point above O, that is, a p-torsion point of E'. This shows that the p-torsion points of E' are defined over K.

Now we are ready to give the explicit ϕ-descent. Let $\pi(z) = z^p - z$ and choose a $(p - 1)st$ root c of A. Note that $c \in K$ since we assumed that the Hasse invariant of E/K is in $(K^\times)^{p-1}$.

PROPOSITION 1.3. *The map* $\alpha: E(K) \to K^+/\pi(K^+)$ *given by* $\alpha(O) = 0$ *and* $\alpha(x, y) = yV(x)/c^p$ *is a homomorphism with kernel* $\phi(E'(K))$.

Proof. Let $\bar{K}$ be a separable closure of K and G to Galois group of $\bar{K}/K$.

We have a homomorphism $\bar{\alpha}: E(K) \to H^1(G, \ker \phi)$ obtained by taking Galois cohomology of the exact sequence

$$O \to \ker \phi \to E'(\bar{K}) \to E(\bar{K}) \to O.$$

Explicitly, $\bar{\alpha}(P)(\sigma) = Q^\sigma - Q$ for $\sigma \in G$, where $Q \in E'$ satisfies $\phi(Q) = P$.

The function $(z - y/x)/c$ identifies $\ker \phi$ with $\mathbf{Z}/p\mathbf{Z}$ (see Remark 1.2), inducing an isomorphism $H^1(G, \ker \phi) \to H^1(G, \mathbf{Z}/p\mathbf{Z})$. On the other hand, $H^1(G, \mathbf{Z}/p\mathbf{Z})$ is isomorphic to $K^+/\pi(K^+)$ by $u \to (\sigma \to v^\sigma - v)$, for some v satisfying $\pi(v) = u$. Composing all these isomorphisms, $\bar{\alpha}$ identifies with α as in the statement of the proposition.

REMARK 1.4. In characteristic 2 we take a Weierstrass equation (1) for E with $a_3 = a_4 = 0$. The étale cover giving E' is then $z^2 + a_1 z = x + a_2$, as is easily checked. The analogue of α is $\alpha(x, y) = (x + a_2)/a_1^2 \pmod{\pi(K^+)}$. (See [3] Prop. 1.1(a)).

2. Descent via F

Suppose $p \neq 2$. In the proof of Proposition 1.3 it was remarked that the function $(z - y/x)/c$ (where c is a fixed $(p-1)st$ root of A) identifies ker ϕ with $\mathbf{Z}/p\mathbf{Z}$. Let P_i be the point corresponding to $i \in \mathbf{Z}/p\mathbf{Z}$.

Gunji has shown that the function on E' given by

$$f_i = A^p \sum_{j=1}^{p-1} (ic)^{-pj} D^j x' \tag{3}$$

where $D = y' \mathrm{d}/\mathrm{d}x'$, has divisor $p(P_i - O')$. We shall use $f = f_1$ to give an explicit F-descent.

PROPOSITION 2.1. *The map* β: $E'(K) \to K^x/(K^x)^p$ *given by*

$$\beta(P) = \begin{cases} 1, & P = O' \\ f(P_{-1})^{-1}, & P = P_1 \\ f(P), & P \neq O', P_1 \end{cases}$$

is a homomorphism with kernel $F(E(K))$.

Proof. We first prove that β is a homomorphism. Let $Q \in E'(K)$ be fixed and consider the function $g(P) = f(P + Q)$. The divisor of g is $p((P_1 - Q) - (-Q))$, so the divisor of g/f is

$$p[(P_1 - Q) + O' - P_1 - (-Q)]$$

The divisor in square brackets is principal and defined over K, so is the divisor of a function $r \in K(E')$. Hence there exists $\lambda \in K^x, g = \lambda f r^p$, that is, $f(P + Q) \equiv \lambda f(P) \bmod (K^x)^p$ for all $P \in E'(K)$. We now show that $\lambda \equiv f(Q) \bmod (K^x)^p$. We have that

$$f(2Q) = \lambda f(Q) r(Q)^p$$
$$f(3Q) = \lambda f(2Q) r(2Q)^p = \lambda^2 f(Q)(r(Q)r(2Q))^p$$

and, generally,

$$f(pQ) = \lambda^{p-1} f(Q)(r(Q)r(2Q)\ldots r((p-1)Q))^p.$$

Hence, $\lambda \equiv f(Q)f(pQ)\,\mathrm{mod}(K^\times)^p$. Note now that $f \circ F$ is the pth power of a function on E defined over K, as follows from (3). Hence $f(pQ) = f \circ F(\phi(Q)) \in (K^\times)^p$. It follows that $\lambda \equiv f(Q)\,\mathrm{mod}(K^\times)^p$, proving that β is a homomorphism.

As $f \circ F$ is a pth power in $K(E)$, it follows that $\ker \beta$ contains $F(E(K))$. We now prove the reverse inclusion.

Gunji [3] showed that $y'\, \mathrm{d}f/\mathrm{d}x' = cf$ and, from (3), $f \in K^p[x, y]$. Let now δ be a derivation of K. We have that

$$\delta f(P) = \mathrm{d}f/\mathrm{d}x'(P)\delta x' = cf(P)\delta x'(P)/y'(P). \tag{4}$$

If $\beta(P) = 1$, then $f(P) \in (K^\times)^p$, so $\delta f(P) = 0$. We conclude that $\delta x'(P) = 0$ and, since δ was arbitrary, that $x'(P) \in K^p$. It follows from (2) that $y'(P) \in K^p$ so $P \in F(E(K))$, as desired.

REMARK 2.2. As F is inseparable, F-descent cannot be done using Galois cohomology. One has to use flat cohomology of group-schemes [7]. As a group-scheme, $\ker F$ is isomorphic to μ_p, so H^1 $(K, \ker F)$ is isomorphic to $K^\times/(K^\times)^p$ and β is the map coming from the cohomology sequence of the exact sequence

$$0 \to \ker F \to E \to E' \to 0$$

On the other hand, F-descent behaves just like the prime-to-p cases (see, e.g., [8] ex. 10.1), the Kummer pairing being

$$\langle P, P_i \rangle = \beta(P)^i \equiv f_i(P)\,\mathrm{mod}(K^\times)^p.$$

The proof in the prime-to-p case does not work in this context because of inseparability.

REMARK 2.3. In characteristic 2, if E has a Weierstrass equation (1) with $a_3 = a_4 = 0$, the analogue of f is simply x' and the analogue of β is

$$\beta(P) = \begin{cases} 1, & P = O' \\ a_6 & P = P_1 \\ x'(P), & P \neq O', P_1 \end{cases}$$

3. The complete P-descent

Let k be a perfect field of characteristic $p > 0$ and K either a function field or a power series field in one variable over k. Assume that the p-torsion points of

E are not defined over K. Then $t = f(P_{-1})^{-1}$ does not belong to K^p. Let $\delta = \mathrm{d}/\mathrm{d}t$ and define $\beta_1: E'(K) \to K^+$ by $\beta_1(P) = t\delta\beta(P)/\beta(P)$. Since β is defined modulo pth powers, β_1 is a well-defined homomorphism with kernel $F(E(K))$. Recall that $\pi(z) = z^p - z$.

THEOREM 3.1. *Define* $\mu: E(K) \to K^+$ *by* $\mu(P) = \pi(\beta_1(Q))$ *for some* Q *with* $\phi(Q) = P$. *Then* μ *is a well-defined homomorphism with kernel* $pE(K)$.

Proof. Assume $p \neq 2$ (for $p = 2$ see Remark 3.3). Choose a Weierstrass equation (1) for E with $a_1 = a_3 = 0$. Note that changing the Weierstrass equation for E changes f by a pth power, so β and β_1 are unchanged. We can further change the Weierstrass equation so that $A = 1$.

We first show that μ is independent of the choice of Q. Let $Q, Q' \in \phi^{-1}(P)$. Then $Q - Q' \in \ker\phi$ and we can write $Q - Q' = iP_1$, for some $i \in \mathbf{Z}/p\mathbf{Z}$. It follows, by our choice of t that $\beta_1(Q) = \beta_1(Q') + i$. Hence $\pi(\beta_1(Q)) = \pi(\beta_1(Q'))$, as desired.

Now we show that $\mu(P) \in K$. Let $\bar{K}$ be a separable closure of K and G the Galois group of $\bar{K}/K$. Obviously $\mu(P) \in \bar{K}$. Let $\sigma \in G$ then $\mu(P)^\sigma = \pi(\beta_1(Q^\sigma))$. On the other hand, $Q^\sigma - Q \in \ker\phi$ since $\phi(Q^\sigma - Q) = P^\sigma - P = 0$. As above, we conclude that $\pi(\beta_1(Q^\sigma)) = \pi(\beta_1(Q))$, that is, $\mu(P)^\sigma = \mu(P)$. Since $\sigma \in G$ was arbitrary we conclude that $\mu(P) \in K$.

As μ is obviously a homomorphism, it only remains to be shown that $\ker\mu = pE(K)$. Consider the following diagram with exact rows:

$$\begin{array}{ccccccccc}
0 \longrightarrow & \ker\phi & \longrightarrow & E'(K)/F(E(K)) & \xrightarrow{\phi} & E(K)/pE(K) & \longrightarrow & E(K)/\phi(E'(K)) & \longrightarrow 0 \\
 & \downarrow & & \downarrow{\scriptstyle \beta_1} & & \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \alpha} & \\
0 \longrightarrow & \mathbf{Z}/p\mathbf{Z} & \longrightarrow & K^+ & \xrightarrow{\pi} & K^+ & \longrightarrow & K^+/\pi(K^+) & \longrightarrow 0.
\end{array}$$

We will show that this diagram commutes. By the choice of t, β_1 identifies $\ker\phi$ with $\mathbf{Z}/p\mathbf{Z}$. Also, by definition, $\mu \circ \phi = \pi \circ \beta_1$. It remains to be shown that $\mu(P) \equiv \alpha(P) \bmod \pi(K^+)$. This is clear from looking at α as a map to $H^1(G, \ker\phi)$ and identifying $\ker\phi$ with $\mathbf{Z}/p\mathbf{Z}$ via β_1.

It is obvious that $pE(K)$ is contained in $\ker\mu$ since K has characteristic p. Conversely, if $\mu(P) = 0$, then $\alpha(P) = 0$, so $P = \phi(Q)$, $Q \in E(K)$. Hence $\pi(\beta_1(Q)) = \mu(P) = 0$, so $\beta_1(Q) = i \in \mathbf{Z}/p\mathbf{Z}$. Then $\beta_1(Q - iP_1) = 0$, that is, $Q = F(R) + iP_1$ $R \in E(K)$ and, finally, $pR = \phi(Q - iP_1) = \phi(Q) = P$. This completes the proof.

REMARK 3.2. For completeness it is worth mentioning that the p-descent for E' (or for any elliptic curve with K-rational p-torsion) is straightforward. If α' is the map (for E') given by Proposition 1.3, then it is easy to check that the map $\beta \oplus \alpha': E'(K) \to K^\times/(K^\times)^p \oplus K^+/\pi(K^+)$ is a homomorphism with kernel $pE'(K)$ (see, e.g., [12]).

REMARK 3.3. In characteristic 2, take a Weierstrass equation (1) for E with

$a_3 = a_4 = 0$. One can further take $A(= a_1) = 1$ and the proof of Theorem 3.1 applies in this case with minor changes.

A procedure for doing 2-descent in characteristic 2 was given by Kramer [3], in a somewhat different fashion. He defined a homomorphism $\gamma: E(K) \to H$, where H is a certain quotient of $K^x \oplus a_6(K^+)^2$, with $\ker\gamma = 2E(K)$. When a_6 is not a square in K, which is the case we are in (otherwise see Remark 3.2 and [3] Prop. 1.3(b)), it is easy to show that H is the quotient of $K^x \oplus a_6(K^+)^2$ by $\ker\lambda$, where $\lambda(u, v) = v + \pi(a_6\delta u/u) \in K^+$, where $\delta = \mathrm{d}/\mathrm{d}a_6$. Hence H is isomorphic to K^+ and, under this isomorphism, γ becomes $(x, y) \to a_6/(a_1x)^2 + \pi(a_6\delta x/x)$ (see [3]). On the other hand a simple calculation shows that this map is precisely μ.

REMARK 3.4. It is fairly obvious that $\mu(x, y)$ is a rational function of $x, y, \delta x, \delta y$ with coefficients in $\mathbf{F}_p(a_1, a_2, a_3, a_4, a_6)$, but, apparently, there is no simple formula for μ for arbitrary p. In characteristic 3, taking $a_1 = a_3 = a_4 = 0, a_2 = 1$, then $t = a_6$ and $\mu(x, y) = a_6y/x^3 - \pi(a_6\delta x/y)$.

REMARK 3.5. Without the hypothesis that the p-torsion of E is not defined over K one could still take $\beta' = t/\beta\cdot\mathrm{d}\beta/\mathrm{d}t$, for some $t \in K^x\backslash(K^x)^p$, as an analogue of Manin's map. We have $\beta':(E'(K)) \to K^+$ with kernel $F(E(K))$. For the relation of these maps with the reduction modulo p of Manin's map in characteristic zero see Section 6.

REMARK 3.6. Ulmer (personal communication) has shown that the flat cohomology group $H^1(K, \ker[p])$ is naturally isomorphic to $t\delta K$ and that the map defined in Theorem 3.1 coincides with the coboundary map of the cohomology sequence of the exact sequence

$$0 \to \ker[p] \to E \xrightarrow{p} E \to 0.$$

4. Local analysis

In order to prove the finiteness results below we need to take a local analysis of μ. Throughout this section k is a perfect field of characteristic $p > 0$ and $K = k((s))$, for a variable s. Let v denote the valuation on $K, R = k[[s]], M = sR$.

Let E/K be an elliptic curve satisfying the hypotheses of Section 3. Let $\bar{E}/k$ be the reduction modulo v of E and denote, as usual, by $E_0(K)$ and set of points on $E(K)$ reducing, modulo v, to a non-singular point on $\bar{E}$ and by $E_1(K)$ the set of points on $E(K)$ reducing to the origin $\bar{O}$ of $\bar{E}$. Recall that $E_1(K) = \hat{E}(M)$, where $\hat{E}$ is the formal group of E and let $E_r(K) = \hat{E}(M^r)$, $r \geqslant 1$. Finally, let T be the parameter in the formal group $\hat{E}$. We will use similar notation for E' and $\bar{E}$. (See [8] Chs. IV and VII).

THEOREM 4.1. (*a*) *The maps μ and β_1, defined in Section* 3, *are continuous in the*

v-adic topology. (*b*) *If E has good, ordinary, reduction and $v(dt) = 0$ then $\mu(E(K))$ and $\beta_1(E'(K))$ are contained in R.*

Proof. In characteristic 2 this follows from [3], Proposition 2.2, 2.4. We will assume that $p \neq 2$ and take a minimal Weierstrass equation (1) for E with $a_1 = a_3 = 0$.

(a) The isogeny ϕ induces a homomorphism $\hat{\phi}: \hat{E}' \to \hat{E}$ given by a power series $\hat{\phi}(T) \in TR[[T]]$. As ϕ is separable, $\hat{\phi}'(0) \neq 0$ so there exists $\lambda \in TK[[T]]$ which is a formal inverse of $\hat{\phi}$. It is easy to see that λ converges in M^r, for r sufficiently large.

Since μ and β_1 are homomorphisms between topological groups, it is sufficient to check their continuity at any particular point. Near O, $\mu = \pi(\beta_1 \circ \lambda)$, hence the continuity of μ follows from that of β_1. Finally, away from O' and P_1, $\beta_1 = t\delta f/f$, hence is continuous.

(b) Assume, without loss of generality, that k is algebraically closed. Since E has good, ordinary, reduction $\phi(E'(K)) = E(K)$. Thus, it suffices to prove the result for β_1. Recall that $\beta_1(P) = (t/\mathrm{d}t)(\mathrm{d}\beta(P)/\beta(P))$.

We first show that $t \in R^\times$. In fact, the reduction $\bar{f}$, of f modulo v, is a function on $\bar{E}'$ with divisor $p(\bar{P}_1 - \bar{O}')$, so it does not have a pole or a zero at $\bar{P}_{-1}$, as desired. All there is to be shown now is that $v(\mathrm{d}\beta(P)) \geqslant v(\beta(P))$ for all $P \in E'(K)$. Suppose first that $\bar{P} \neq \bar{P}_1, \bar{O}'$. Then $\beta(P) = f(P)$ and $\bar{f}(\bar{P}) \neq 0, \infty$, that is, $f(P) \in R^\times$ and the result follows. If $P = P_1 + Q$, $Q \in E'_1(K)$ then $\beta(P) = t\beta(Q)$ and the result for P follows from the result for Q. We now prove the result in $E'_1(K)$.

Now f can be expressed in $E'_1(K)$ as $f(T) = T^{-p}g(T)$, $g(T) \in R[[T]]$, by (3). Reducing modulo v, $\bar{f}$ has a pole of order p at $\bar{O}'$, so $\bar{g}(0) \neq 0$, that is, $g(0) \in R^\times$. As β is defined modulo $(K^\times)^p$ we can take $\beta = g(T)$ in $E'_1(K)$ and, for $T \in M$, $v(g(T)) = 0$, $v(dg(T)) \geqslant 0$, as desired.

REMARK 4.2. It is clear that the proof of Theorem 4.1(a) applies to show that the function β', defined in Remark 3.5, is continuous. This result was also shown by Milne [6].

REMARK 4.3. Ulmer has obtained precise results on the images of the maps μ and β_1 (for the case of β_1 see [11]) and applied these results to compute the Selmer group for the p-descent (see his forthcoming publications).

Assume that K is a function field in one variable over the finite field k of characteristic p and let E/K be an elliptic curve satisfying the hypotheses of Section 3. Denote by V the set of places of K and let $S = \{u \in K \mid u \in \mu(E(K_v)), v \in V\}$. We shall show now that S is finite.

THEOREM 4.4. *There exists a divisor D of K for which S is contained in $L(D)$. Hence, S is finite.*

Proof. Given $v \in V$, as μ is continuous and $E(K_v)$ is compact, there exists c_v with $v(\mu(P)) \geqslant c_v$, for all $P \in E(K_v)$. Further, $c_v = 0$ for almost all v, specifically for those v satisfying the hypotheses of Theorem 4.1(b). Hence $\Sigma c_v v = D$ is a divisor of K and S is contained in $L(D)$. Since $L(D)$ is finite, S is finite.

Clearly, $\mu(E(K))$ is contained in S, so we get an injection of $E(K)/pE(K)$ into S which, by the way, proves the (weak) Mordell-Weil theorem.

5. Integral points

In this section we shall prove the function field analogue in positive characteristic of Siegel's finiteness theorem for integral points on elliptic curves. Our proof will be very similar to Manin's proof in characteristic zero. In fact, the proof of Lemma 5.1 below is identical to the outline in [5], pg. 194. The added complication of positive characteristic is dealt with by Lemma 5.2.

LEMMA 5.1. *Let K be a function field in one variable over a finite field and S a finite set of places of K.*

(*a*) *Let E/K be an ordinary elliptic curve whose p-torsion points are not defined over K. If* (1) *is a Weierstrass equation for E then the set* $\{P \in E(K)\backslash pE(K) \mid v(x(P)) \geqslant 0$ *for all v not in S*$\}$ *is finite.*

(*b*) *Let A/K be an ordinary elliptic curve and assume that its p-torsion subgroup Γ is defined over K. Let $F: A/\Gamma \to A$ be the isogeny dual to the natural isogeny $A \to A/\Gamma$. If* (1) *is a Weierstrass equation for A then the set* $\{P \in A(K)\backslash F(A/\Gamma(K)) \mid v(x(P)) \geqslant 0,$ *for all v not in S*$\}$ *is finite.*

Proof. (a) Without loss of generality, we can take a finite separable extension of K and assume that the Hasse invariant of E/K is 1.

If the conclusion is false, there exists $v \in S$ and a sequence $P_n \in E(K)\backslash pE(K)$, with $v(x(P_n)) \to -\infty$ as $n \to \infty$. Hence $P_n \to O$ in the v-adic topology, so $\mu(P_n) \to 0$, by Theorem 4.1(a). As $\mu(P_n) \in L(D)$, by Theorem 4.1, this can only happen if $\mu(P_n) = 0$ for all n sufficiently large. This implies that $P_n \in pE(K)$ for n large, which is a contradiction, proving (a).

(b) As above, we may assume that the Hasse invariant of A/K is 1. We can then use the function β' defined in Remark 3.5 as μ was used in the proof of (a) (see Remark 4.2).

LEMMA 5.2. *Notation and hypotheses as in Lemma* 5.1(*a*). *The set* $\{P \in E(K) \mid v(x(P)), v(x(pP)) \geqslant 0,$ *for all v not in S*$\}$ *is finite.*

Proof. Assume first that $p \neq 2$. By changing the y-coordinate of (1), we can assume that $a_1 = a_3 = 0$. Let $b \in K$ be the x-coordinate of a non-trivial p-torsion point P_1 in $E'(K)$. Note that b is not a pth power for, otherwise, $P_1 \in F(E(K))$, contradicting the hypothesis that the p-torsion of E is not defined over K.

Enlarge S, if necessary, so that $v(b) = 0$ and (1) is minimal and has good, ordinary, reduction for all v not in S.

Let $P \in E(K)$ satisfy $v(x(P)), v(x(pP)) \geqslant 0$ for all v not in S. Then $v(x(P)^p - b) \geqslant 0$ for all such v. Suppose that for some such v, $v(x(P)^p - b) > 0$. Then $F(P) \equiv \pm P_1 \mod E_1'(K_v)$. Hence $pP \equiv \phi(\pm P_1) = 0 \mod E_1(K_v)$. This implies that $v(x(pP)) < 0$ contrary to hypothesis. It follows that $v(x(P)^p - b) = 0$ for all v not in S. On the other hand, the multiplicities of the zeroes of $x(P)^p - b$ are bounded since $db \neq 0$, so

$$v(db) + 1 = v(d(x(P)^p - b)) + 1 \geqslant v(x(P)^p - b).$$

It follows that there are only finitely many possibilities for $x(P)^p - b$, hence only finitely many possibilities for P, as desired.

For $p = 2$, take a Weierstrass equation (1) for E with $a_3 = a_4 = 0$ and work with the y-coordinate instead of the x-coordinate. We leave the details to the reader.

THEOREM 5.3. *Let K be a function field in one variable over a finite field and S a finite set of places of K. If A/K is an elliptic curve with non-constant j-invariant and $f \in K(A)$ is a non-constant function then the set $\{P \in A(K) \mid v(f(P)) \geqslant 0$, for all v not in $S\}$ is finite.*

Proof. It is well-known that it is sufficient to prove the theorem when f is the x-coordinate of a Weierstrass equation (1) for A (see, e.g., [8] Cor. IX.3.2.2). Let $j(A)$ be the j-invariant of A and note that A is ordinary since $j(A)$ is non-constant.

As in the proof of Lemma 5.1, we may assume that the Hasse invariant of A/K is 1. Suppose that the p-torsion points of A are defined over K. By Lemma 5.1(b) it is sufficient to prove the theorem for A/Γ. Note now that $j(A/\Gamma) = j(A)^{1/p}$, hence repeating this finitely many times we arrive, since $j(A)$ is non-constant, at an elliptic curve E satisfying the hypotheses of Lemma 5.1(a) and we only have to prove the theorem for E. By Lemma 5.1(a) it is enough to show that the set $\{P \in pE(K) \mid v(x(P)) \geqslant 0$, for all v not in $S\}$ is finite.

Enlarge S, if necessary, as in the proof of Lemma 5.2. Let $P = pQ$, $Q \in E(K)$, satisfy $v(x(P)) \geqslant 0$ for some v not in S. Then $v(x(Q)) \geqslant 0$ for, otherwise, $Q \in E_1(K_v)$ and, since this is a subgroup of $E(K_v)$, $P \in E_1(K_v)$, absurd. Now the result follows from Lemma 5.2.

REMARK 5.4. Theorem 5.3 is false without the assumption that the j-invariant is non-constant. The best possible result when the j-invariant is constant is Lemma 5.1(b).

REMARK 5.5. With a bit more effort the proof of Theorem 5.3 can be made effective. We leave the details to the reader.

6. Manin's map

Manin's map is characteristic zero is defined as follows. Let E/K be on elliptic curve defined over the field K of characteristic zero possessing a derivation δ. Let $P(\delta)$ be the polynomial of degree 2 in δ annihilating the periods of E, that is, the Picard-Fuchs operator. Define $M: E(K) \to K^+$ as $M(P) = P(\delta)\int_0^P \omega$, where ω is a regular differential on E. For example, if E_q is the Tate curve ([8]) defined over $\mathbf{C}((q)) = K$ and, under the isomorphism $E_q \simeq K^x/q^{\mathbf{Z}}$, $\omega = \mathrm{d}u/u$ (u = parameter in K^x), $P(\mathrm{d}/\mathrm{d}q) = (q\mathrm{d}/\mathrm{d}q)^2$ (since the periods are 1, $\log q$) and finally:

$$M(u) = (q\mathrm{d}/\mathrm{d}q)^2 \int \mathrm{d}u/u = q\frac{\mathrm{d}}{\mathrm{d}q}\left(\frac{q}{u}\cdot\frac{\mathrm{d}u}{\mathrm{d}q}\right).$$

THEOREM 6.1. *Let K be a function field in on variable over a perfect field k of characteristic $p > 0$, E/K the elliptic curve of equation* (1) *and δ the derivation of K/k defined in Section* 3. *If $\tilde{E}/\tilde{K}$ is a lifting of E/K to characteristic zero with Manin map M, then there exists $a \in K^x$ such that*

$$M \equiv a\delta\mu \pmod p.$$

Proof. By choosing a place v of K for which E/K has multiplicative reduction and taking a lifting $\tilde{v}$ of v to a place of $\tilde{K}$ we are reduced, by the above, to computing μ for the Tate curve over $k((q)) = K$.

From equation (4) of Section 2 we have

$$\beta(P) = ct\delta x'(P)/y'(P)$$

As $x'(P) = x(u, q^p)$ and similarly for y', we get immediately that $c\delta x'/y' = \delta u/u$ hence $\beta(u) = t\delta u/u$. As P_1 corresponds to $u = q$ we have $\beta(q) = 1$ so $\beta(u) = q/u\cdot \mathrm{d}u/\mathrm{d}q$. As $\varphi: E' \to E$ is given by $u (\mathrm{mod}\, q^{p\mathbf{Z}}) \mapsto u (\mathrm{mod}\, q^{\mathbf{z}})$ it follows that

$$\mu(u) = \pi\left(\frac{q}{u}\cdot\frac{\mathrm{d}u}{\mathrm{d}q}\right).$$

Finally $-q\mathrm{d}\mu/\mathrm{d}q = q/\mathrm{d}q(q/u\cdot \mathrm{d}u/\mathrm{d}q) \equiv M \pmod p$, and $-q\mathrm{d}/\mathrm{d}q = a\delta$ for some $a \in K^x$.

Acknowledgments

Part of this work was done during a visit to Australasia. The author would like to thank MacQuarie University and the University of Sydney in Australia and

Victoria University of Wellington, in New Zealand for their hospitality. The author would also like to thank D. Ulmer for various comments and suggestions on an earlier draft of this paper.

References

0. Coleman, R.F., "Manin's proof of the Mordell conjecture over function fields", preprint.
1. Deuring, M., "Die Typen der Multiplicatorenringe elliptischer Fünktionenkörper". *Hamb. Abhandlungen* 14 (1941) 197–272.
2. Gunji, H. "The Hasse invariant and p-division points of an elliptic curve". *Arch. Math.* (Basel) XXVII (1976) 148–158.
3. Kramer, K., "Two-descent for elliptic curves in characteristic two". *Trans. Amer. Math. Soc.* 232 (1977) 279–295.
4. Lang, S., "Elliptic functions", Addison-Wesley, Reading, MA 1973.
5. Manin, Yu.I., "Rational points of algebraic curves over function fields". *AMS Transl.* (2) 50 (1966) 189–234.
6. Milne, J.S., "Elements of order p in the Tate-Shafarevich group". *Bull. Lon. Math. Soc.* 2 (1970) 293–296.
7. Milne, J.S., "Arithmetic Duality Theorems", Academic Press, Orlando, 1986.
8. Silverman, J.H., "The Arithmetic of Elliptic Curves", Springer, New York, 1986.
9. Stiller, P.F., "Elliptic curves over function fields and the Picard number". *Amer. J. of Math.* 102 (1980).
10. Stiller, P.F., "Automorphic forms and the Picard number of an elliptic surface", Vieweg, Braunschweig, 1984.
11. Ulmer, D.L., "The arithmetic of Universal elliptic modular curves", Ph.D. Thesis, Brown University, 1987.
12. Vvedenskii, O.N., "The Artin effect on elliptic curves I". *Math. USSR Izvestija* 15 (1980) 277–288.