LMS J. Comput. Math. 17 (Special issue A) (2014) 1–13
doi:10.1112/S1461157014000175

Computation of Mordell–Weil bases for ordinary elliptic curves in characteristic two

G. Moehlmann

Abstract

In this paper we consider ordinary elliptic curves over global function fields of characteristic 2. We present a method for performing a descent by using powers of the Frobenius and the Verschiebung. An examination of the local images of the descent maps together with a duality theorem yields information about the global Selmer groups. Explicit models for the homogeneous spaces representing the elements of the Selmer groups are given and used to construct independent points on the elliptic curve. As an application we use descent maps to prove an upper bound for the naive height of an S-integral point on A. To illustrate our methods, a detailed example is presented.

1. *Introduction*

Let A be an elliptic curve defined over a global field K. Then $\hat{A}(K) := A(K)/(A(K))_{\mathrm{tor}}$ is a free abelian group of finite rank. For K a number field or a rational function field of characteristic greater than or equal to 5, there are algorithms, which may not always succeed, to compute generators for $\hat{A}(K)$ by doing a two-descent. These generators are called a Mordell–Weil basis. See the documentation of [**1**] for references for the algorithms that are used in Magma. These algorithms make use of the separability of the multiplication by two isogeny. Our main goal in this paper is to describe how similar techniques can be applied to compute Mordell–Weil bases for ordinary elliptic curves over global function fields of characteristic 2. By using flat cohomology we first construct descent maps as described in [**7**, **16**, **17**] and utilize them to compute Selmer groups. Then we represent the elements of the Selmer groups as homogeneous spaces as in [**4**], utilize them to construct independent points, and enlarge the group generated by these points as in [**10**]. At the end we use our descent maps to compute an upper bound for the naive height of an S-integral point on A.

This paper is based on the author's PhD thesis at Carl-von-Ossietzky University Oldenburg.

2. *Descent via Frobenius and Verschiebung*

Let A be an ordinary elliptic curve defined over a field K of characteristic 2. Then we can assume that A is given by a Weierstrass equation of the form

$$A : y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0.$$

We denote the zero of A by $\mathcal{O}_A$. Let $\phi : A \to B$ be an isogeny of degree n and $\phi^\vee$ its dual isogeny. As a result of the snake lemma, the sequence of kernels and cokernels

$$\begin{aligned} 0 \to A(K)[\phi] \to A(K)[n] \to B(K)[\phi^\vee] \to B(K)/\phi(A(K)) \\ \to A(K)/nA(K) \to A(K)/\phi^\vee(B(K)) \to 0 \end{aligned}$$

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 11G05 (primary), 11G07, 14G25, 14G17 (secondary).

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.

is exact. For an elliptic curve over a global function field K the computation of the torsion points is comparatively easy, so we assume that they are known. Consequently generators for $A(K)/\phi^\vee(B(K))$ and for $B(K)/\phi(A(K))$ yield generators for $A(K)/nA(K)$, which also generate a subgroup of finite index of $A(K)$. In the following we make use of specific isogenies to construct $\mathbb{Z}$-linear independent points on $A(K)$: the ith power Frobenius is a purely inseparable isogeny $F^i : A \to A^{(2^i)}$ of degree 2^i given by $F^i(x,y) = (x^{2^i}, y^{2^i})$. The Weierstrass equation of $A^{(2^i)}$ is

$$A^{(2^i)} : y^2 + a_1^{2^i} xy + x^3 + a_2^{2^i} x^2 + a_6^{2^i} = 0. \tag{2.1}$$

The dual isogeny of F^i is called the ith power Verschiebung. We denote it by $V^i : A^{(2^i)} \to A$. As we require A to be ordinary, the Verschiebung is separable. If the 2^i-torsion of $A^{(2^i)}$ is K-rational, the kernel of the Verschiebung, $\ker V^i$, is isomorphic to $\mathbb{Z}/2^i\mathbb{Z}$ as a finite flat group scheme over K. In the following, let T denote a generator of $\ker V^i$. An isomorphism Ξ is given by mapping T to 1. For an arbitrary isogeny Φ, the kernel of the dual isogeny $\Phi^\vee$ is isomorphic to the Cartier dual $(\ker \Phi)^\vee$ of the kernel of Φ. The Cartier dual of $\mathbb{Z}/2^i\mathbb{Z}$ is isomorphic to the K-group scheme of 2^ith roots of unity $\boldsymbol{\mu}_{2^i}$. Hence for the Frobenius there is an isomorphism $\psi : \ker F^i \to \boldsymbol{\mu}_{2^i}$ such that the diagram

$$\begin{array}{ccc} \ker F^i \times \ker V^i & \longrightarrow & \mathbb{G}_m \\ \downarrow{\scriptstyle \psi} \quad \downarrow{\scriptstyle \Xi} & & \downarrow{\scriptstyle \mathrm{id}} \\ \boldsymbol{\mu}_{2^i} \times \mathbb{Z}/2^i\mathbb{Z} & \longrightarrow & \mathbb{G}_m \end{array}$$

commutes. Here the rows are given by the Weil pairing e_i or the Cartier duality pairing. Let R be a finite K-algebra, then due to the commutativity of the diagram we have $\psi(P') = e_i(P', T)$ for every $\operatorname{Spec} R$-rational point P' on $\ker F^i$. The short exact sequences

$$0 \to \ker V^i \to A^{(2^i)} \xrightarrow{V^i} A \to 0$$
$$0 \to \ker F^i \to A \xrightarrow{F^i} A^{(2^i)} \to 0$$

induce the long exact sequences

$$0 \to \ker V^i(K) \to A^{(2^i)}(K) \xrightarrow{V^i} A(K) \to H^1(K, \ker V^i)$$
$$0 \to \ker F^i(K) \to A(K) \xrightarrow{F^i} A^{(2^i)}(K) \to H^1(K, \ker F^i)$$

in flat cohomology. Thus we get homomorphisms

$$\hat{\alpha}_i : A(K) \to H^1(K, \ker V^i)$$
$$\hat{\beta}_i : A^{(2^i)}(K) \to H^1(K, \ker F^i)$$

for which $\ker \hat{\alpha}_i = V^i(A^{(2^i)}(K))$ and $\ker \hat{\beta}_i = F^i(A(K))$. As a result of the Kummer sequence or the Artin–Schreier–Witt sequence together with Hilbert 90, which states that $H^1(K, \mathbb{G}_m)$ and $H^1(K, W_i)$ are trivial, we have $H^1(K, \mathbb{Z}/2^i\mathbb{Z}) \simeq W_i(K)/\wp(W_i(K))$ and $H^1(K, \boldsymbol{\mu}_{2^i}) \simeq K^\times/(K^\times)^{2^i}$. Here W_i denotes the truncated Witt vectors of length i, and $\wp$ is the Artin–Schreier map given by mapping a truncated Witt vector v to $Fv - v$. The composition of $\hat{\alpha}_i$ or $\hat{\beta}_i$ and both the isomorphisms induced by Ξ or ψ and by the Artin–Schreier–Witt or Kummer sequence yields homomorphisms

$$\alpha_i : A(K) \to W_i(K)/\wp(W_i(K))$$
$$\beta_i : A^{(2^i)}(K) \to K^\times/(K^\times)^{2^i}$$

under the assumption that the 2^i-torsion of $A^{(2^i)}$ is defined over K. The following propositions demonstrate how α_i and β_i can be evaluated in this situation.

https://doi.org/10.1112/S1461157014000175 Published online by Cambridge University Press

PROPOSITION 2.1. *Let Q be in $A^{(2^i)}$ with $V^i(Q) = P$, and let σ be a generator of the cyclic Galois group of $K(Q)/K$. Then $\alpha_i(P) = v + \wp(W_i(K))$ where $v \in W_i(K)$ is determined by the equation $\Xi(Q - \sigma(Q)) = w - \sigma(w)$ for $w \in W_i(\bar{K})$ with $K(w) = K(Q)$ and $\wp(w) = v$.*

Proof. This proposition follows from tracing through the various morphisms. As V^i is separable, $\ker V^i$ is an étale group scheme. Hence Galois cohomology can be used for computations in $H^1(K, \ker V^i)$. Consequently $\hat{\alpha}_i$ maps a point P to the cocycle $\sigma \mapsto Q - \sigma(Q)$, and, on the other hand, when we identify $\mathbb{Z}/2^i\mathbb{Z}$ and $W_i(\mathbb{F}_2)$ via $1 \mapsto (1, \dots, 1)$, the isomorphism $W_i(K)/\wp(W_i(K)) \to H^1(K, \mathbb{Z}/2^i\mathbb{Z})$ is given by mapping v to $\sigma \mapsto w - \sigma(w)$. Patching things together proves the statement. □

PROPOSITION 2.2. *Let f be a function in the function field of $A^{(2^i)}$ with principal divisor $(f) = (2^i T - 2^i \mathcal{O}_{A^{(2^i)}})$ such that $f \circ F^i = g^{2^i}$ holds for a function g on A. Then for P in $A^{(2^i)}(K)$ we have*

$$\beta_i(P) = \begin{cases} 1 & \text{if } P = \mathcal{O}_{A^{(2^i)}}, \\ f(-P)^{-1} & \text{if } P = T, \\ f(P) & \text{otherwise.} \end{cases}$$

Proof. If we use Čech cocycles to represent elements in the cohomology groups, the isomorphism $K^\times/(K^\times)^{2^i} \to H^1(K, \boldsymbol{\mu}_{2^i})$ is given by $a \mapsto (1 \otimes b)/(b \otimes 1)$ with $b^{2^i} = a$. We denote it by δ_K. Moreover, $\hat{\beta}_i$ maps a point $P \in A^{(2^i)}(K)$ to the cocycle $(1 \otimes x_Q, 1 \otimes y_Q) - (x_Q \otimes 1, y_Q \otimes 1)$ representing an element in $H^1(K, \ker F^i)$. Here $F^i(x_Q, y_Q) = P$ holds. Composing $\hat{\beta}_i$ and the isomorphism that is induced by ψ, we get

$$\begin{aligned} e_i(\delta_F(P), T) &= e_i((1 \otimes x_Q, 1 \otimes y_Q) - (x_Q \otimes 1, y_Q \otimes 1), T) \\ &= \frac{g((1 \otimes x_Q, 1 \otimes y_Q))}{g((x_Q \otimes 1, y_Q \otimes 1))} \\ &= \frac{1 \otimes g((x_Q, y_Q))}{g((x_Q, y_Q)) \otimes 1}. \end{aligned}$$

This follows from the formula for the Weil pairing given in [11, p. 313]. On the other hand, we have

$$\delta_K(f(P)) = \delta_K(g(x_Q, y_Q)^{2^i}) = \frac{1 \otimes g((x_Q, y_Q))}{g((x_Q, y_Q)) \otimes 1}.$$ □

For $i = 1$ this construction yields

$$\alpha_1 : A(K) \to W_1(K)/\wp(W_1(K)), (x, y) \mapsto \frac{x + a_2}{a_1^2} \equiv \frac{a_6}{a_1^2 x^2}$$

and

$$\beta_1 : A^{(2)}(K) \to K^\times/(K^\times)^2, (x, y) \mapsto \begin{cases} x & \text{for } x \neq 0, \\ a_6 & \text{for } x = 0, \\ 1 & \text{for } (x, y) = \mathcal{O}_{\mathcal{A}^{(\in)}}. \end{cases}$$

These are the same maps as constructed in [7]. An easy computation shows that, for an ordinary elliptic curve A given by $A : y^2 + a_1 xy + x^3 + a_2 x^2 + a_6 = 0$, the curve $A^{(4)}$ has K-rational 4-torsion if and only if a_2 is of the form $a_2 = a_1^2(s^2 + s)$ for an element $s \in K$. The

https://doi.org/10.1112/S1461157014000175 Published online by Cambridge University Press

point $T = (a_1^2 a_6, a_1^6 s^4 a_6 + a_6^2)$ on $A^{(4)}(K)$ is of order 4. An examination of the Galois group operation on the preimages of the Witt vector

$$\left(\frac{a_6}{a_1^2 x^2}, \frac{a_6 y}{a_1^3 x^3} + \frac{a_6}{a_1^4 x} + \frac{s a_6 + a_6}{a_1^2 x^2} + \frac{a_6^2}{a_1^4 x^4}\right)$$

and the computation of the principal divisor of $(y + (1/a_1^4)x^2 + a_1^4 s^4 x)$ demonstrates that α_2 and β_2 are given by

$$\alpha_2 : A(K) \to W_2(K)/\wp(W_2(K)),\ (x,y) \mapsto \left(\frac{a_6}{a_1^2 x^2}, \frac{a_6 y}{a_1^3 x^3} + \frac{a_6}{a_1^4 x} + \frac{s a_6 + a_6}{a_1^2 x^2} + \frac{a_6^2}{a_1^4 x^4}\right)$$

and

$$\beta_2 : A^{(4)}(K) \to K^\times/(K^\times)^4,\ (x,y) \mapsto \begin{cases} a_1^2 a_6^3 & \text{if } (x,y) = T, \\ 1 & \text{if } (x,y) = \mathcal{O}', \\ \left(y + \dfrac{1}{a_1^4} x^2 + a_1^4 s^4 x\right) & \text{otherwise.} \end{cases}$$

Remark. Similar techniques can be used to construct descent maps for supersingular elliptic curves in characteristic 2. These will be presented in a subsequent publication.

Remark. Let $A^{(2^i)}$ be given by a Weierstrass equation of the form (2.1). Then for $i = 1$ the 2^i-torsion is always K-rational. But for $i \geqslant 2$ this is not the case. By working over L, the field of definition of $A^{(2^i)}[2^i]$, we can still construct descent maps. This time they are mapping points on $A(K)$ or $A^{(2^i)}(K)$ to subsets of $W_i(L)/\wp(W_i(L))$ or $L^\times/(L^\times)^{2^i}$, respectively. With an inflation-restriction argument we can describe these subsets. When it comes to calculating the global image of these descent maps for $i = 1, 2$ as described in § 5, it is possible to construct models for the relevant homogeneous spaces that are defined over K. The techniques to complete this task are basically the same as in § 5.

3. *Local duality*

Throughout this section let K_v be the completion of K with respect to a valuation v. For an arbitrary isogeny $\phi : A \to B$ of elliptic curves over K_v and dual isogeny $\phi^\vee$ we denote the connection homomorphisms in cohomology by

$$\alpha : A(K_v) \to H^1(K_v, \ker \phi^\vee) \quad \text{and} \quad \beta : B(K_v) \to H^1(K_v, \ker \phi).$$

The Weil pairing induces a cup product pairing

$$\cup : H^1(K_v, \ker \phi) \times H^1(K_v, \ker \phi^\vee) \to H^2(K_v, \mathbb{G}_m). \tag{3.2}$$

Theorem 3.1. *The images $\alpha(A(K_v))$ and $\beta(B(K_v))$ are exact orthogonal complements under the cup product pairing.*

Proof. The diagram

$$\begin{array}{ccc} H^0(K_v, A^\vee) \times H^1(K_v, A) & \longrightarrow & H^2(K_v, \mathbb{G}_m) \\ \downarrow{\scriptstyle \alpha} & \nearrow{\scriptstyle \iota} & \\ H^1(K_v, \ker \phi^\vee) \times H^1(K_v, \ker \phi) & & \end{array}$$

https://doi.org/10.1112/S1461157014000175 Published online by Cambridge University Press

commutes (compare [8, C.5]). The upper pairing is given by [8, Theorem 7.8], and the vertical morphisms are the suitable homomorphisms in the long exact cohomology sequences of

$$0 \to \ker\phi \to A \to B \to 0$$

and its dual sequence. Let $b \in \operatorname{Im}\beta \subseteq H^1(K_v, \ker\phi)$ and $a \in \operatorname{Im}\alpha \subseteq H^1(K_v, \ker\phi^\vee)$ be elements in the images. This means there are K_v-rational points $P \in H^0(K_v, B) = B(K_v)$ and $Q \in H^0(K_v, A^\vee) \cong H^0(K_v, A) = A(K_v)$ such that $\alpha(Q) = a$ and $\beta(P) = b$. If we denote the upper pairing by $(.,.)_1$, the lower by $(.,.)_2$, and by ι the induced homomorphism $\iota : H^1(K_v, \ker\phi) \to H^1(K_v, A)$, then we have $(a,b)_2 = (Q, \iota(b))_1 = (Q,0)_1 = 0$ due to the exactness of the cohomology sequence. Hence the images are orthogonal. For $b' \in H^1(K_v, \ker\phi)$ such that $(a,b')_2 = 0$ holds for all $a \in \operatorname{Im}\alpha$, we have $(Q, \iota(b'))_1 = 0$ for all $Q \in H^0(K_v, A^\vee)$. As $(.,.)_1$ yields an exact duality, we have $\iota(b') = 0$ and consequently $b' \in \operatorname{Im}\beta$. □

PROPOSITION 3.2. *For the previously mentioned isogenies F^i and V^i and descent maps $\alpha_i^v : A(K_v) \to W_i(K_v)/\wp(W_i(K_v))$ and $\beta_i^v : A^{(2^i)}(K_v) \to K_v^\times/(K_v^\times)^{2^i}$, the cup product pairing*

$$\cup : H^1(K_v, \ker V^i) \times H^1(K_v, \ker F^i) \to H^2(K_v, \mathbb{G}_m)$$

is nothing other than the Artin–Schreier–Witt pairing

$$[.,.) : W_i(K_v)/\wp W_i(K_v) \times K_v^\times/(K_v^\times)^{2^i} \to \mathbb{Q}/\mathbb{Z}.$$

Proof. Because of the commutativity of diagram (2), this statement follows from the explicit formula for the cup product pairing on $\mathbb{Z}/2^i\mathbb{Z}$ and $\boldsymbol{\mu}_{2^i}$ as given in [9, proof of Theorem 4]. □

REMARK. The Artin–Schreier–Witt pairing can be evaluated efficiently as described in [14].

4. *Local images*

For $i = 1, 2$, statements about the images of α_i^v and β_i^v can be proven.

PROPOSITION 4.1. *Let k be the residue class field of K_v, R_v the valuation ring, and U_n the set $U_n := \{u \in R_v^\times \mid v(u-1) \geqslant n\}$. Assuming that the coefficients of the Weierstrass equation for A are in R_v, the following equations hold:*

$$\begin{aligned}
[\operatorname{Im}\beta_1^v : U_{2v(a_1)}(K_v^\times)^2/(K_v^\times)^2] &= [A^{(2)}(K_v) : A_1^{(2)}(K_v)]/[A(K_v) : A_1(K_v)],\\
[K_v^\times/(K_v^\times)^2 : \operatorname{Im}\beta_1^v] &= 2(\#k)^{v(a_1)}[A(K_v) : A_1(K_v)]/[A^{(2)}(K_v) : A_1^{(2)}(K_v)],\\
[\operatorname{Im}\beta_2^v : U_{4v(a_1)}(K_v^\times)^4/(K_v^\times)^4] &= [A^{(4)}(K_v) : A_1^{(4)}(K_v)]/[A(K_v) : A_1(K_v)],\\
[K_v^\times/(K_v^\times)^4 : \operatorname{Im}\beta_2^v] &= 4(\#k)^{v(a_1)}[A(K_v) : A_1(K_v)]/[A^{(4)}(K_v) : A_1^{(4)}(K_v)].
\end{aligned}$$

Proof. The first two equalities can be found in [7]. For the other two, we can adapt the proof. The rows of the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_1(K_v) & \xrightarrow{F^2} & A_1^{(4)}(K_v) & \xrightarrow{\beta_2^v} & U_{4v(a_1)}(K_v^\times)^4/(K_v^\times)^4 & \longrightarrow & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A(K_v) & \xrightarrow{F^2} & A^{(4)}(K_v) & \xrightarrow{\beta_2^v} & \operatorname{Im}\beta_2 & \longrightarrow & 0
\end{array}$$

https://doi.org/10.1112/S1461157014000175 Published online by Cambridge University Press

are exact. Here A_1 or $A_1^{(4)}$ denotes the kernel of reduction. As in [7], the surjectivity of the upper right map is the only part that is not obvious. It can be proven by a short calculation:

$$\begin{aligned}\left(y+\frac{x^2}{a_1^4}+a_1^4s^4x\right)\frac{a_1^4x^4}{y^4} &= \frac{x^3}{y^2}\frac{a_1^4xy+x^3+a_1^8s^4x^2}{y^2}\\ &= \frac{y^2+a_1^4xy+a_1^8(s^8+s^4)x^2+a_6^4}{y^2}\frac{y^2+a_1^8s^8x^2+a_6^4}{y^2}\\ &= 1+a_1^4u^{-4}\left(z+a_1^4s^4z^2+a_1^8s^8z^3+a_6^4\frac{z}{y^2}+a_1^4a_6^4s^4\frac{z^2}{y^2}\right)\end{aligned}$$

where u is a unit in the valuation ring and $z := x/y$. As (x,y) is in $A_1^{(4)}(K_v)$, the valuation of z is positive. Hence the image is in $U_{4v(a_1)}$. The map $(x,y)\mapsto x/y$ is an isomorphism between $A_1^{(4)}(K_v)$ and the valuation ideal of R_v. This proves the surjectivity. □

COROLLARY 4.2. *If the valuation $v(\Delta(A))$ of the discriminant is equal to 0 then the local images are given by*

$$\operatorname{Im}\beta_i^v = U_0(K_v^\times)^{2^i}/(K_v^\times)^{2^i}$$

and

$$\operatorname{Im}\alpha_i^v = W_i(k)+\wp(W_i(K_v))/\wp(W_i(K_v)).$$

REMARK. If A does not have good reduction at v, we can still compute $\operatorname{Im}\alpha_i^v$. In order to do so, we calculate random points on $A(K_v)$ and their images. To generate the points, we apply Hensel's lemma and approximate their coordinates to a prescribed precision. Using Tate's algorithm and the second or fourth equation of Proposition 4.1 we can determine the cardinality

$$\#\operatorname{Im}\alpha_i^v = [K_v^\times/(K_v^\times)^{2^i} : \operatorname{Im}\beta_i^v],$$

and consequently we know when to stop our algorithm. For small examples this is really fast. But for increasing valuation of a_1, this step may cause trouble, as it gets more difficult to generate the random points in a way that the probability of their images generating $\operatorname{Im}\alpha_i^v$ is reasonable. The image of β_i^v is an infinite group. But it only takes finitely many computations to decide if a given element $b\in K_v^\times/(K_v^\times)^{2^i}$ is in $\operatorname{Im}\beta_i^v$ or not. All we have to do is to test if b is orthogonal to $\operatorname{Im}\alpha_i^v$. Moreover, evaluating the Artin–Schreier–Witt pairing as described in [14] requires the arguments to be given only up to a finite precision.

5. *Global images*

Let K be a global function field and v a valuation of K. Let $A^{(2^i)}$ have K-rational 2^i-torsion. The embedding $K\to K_v$ induces homomorphisms

$$\operatorname{res}_{V^i}^v : W_i(K)/\wp W_i(K)\to W_i(K_v)/\wp W_i(K_v)\quad\text{and}\quad \operatorname{res}_{F^i}^v : K^\times/(K^\times)^{2^i}\to K_v^\times/(K_v^\times)^{2^i}.$$

The V^i- and F^i-Selmer group are respectively defined as

$$\operatorname{Sel}(K,V^i) := \{w\in W_i(K)/\wp W_i(K)\mid \operatorname{res}_{V^i}^v(w)\in\operatorname{Im}\alpha_i^v \text{ for all valuations } v\}$$

and

$$\begin{aligned}\operatorname{Sel}(K,F^i) &:= \{a\in K^\times/(K^\times)^{2^i}\mid \operatorname{res}_{F^i}^v(a)\in\operatorname{Im}\beta_i^v \text{ for all valuations } v\}\\ &= \{a\in K^\times/(K^\times)^{2^i}\mid \left[\operatorname{Im}\alpha_i^v,\operatorname{res}_{F^i}^v(a)\right)=0 \text{ for all valuations } v\}\end{aligned}$$

https://doi.org/10.1112/S1461157014000175 Published online by Cambridge University Press

PROPOSITION 5.1. *For $i = 1, 2$, there are effective divisors D_j of* $\mathrm{Div}(K)$ *such that every element in* $\mathrm{Sel}(K, V^i)$ *has a representative $b = (b_0, \ldots, b_{i-1}) \in W_i(K)$ where b_j is in the Riemann–Roch space $\mathcal{L}(D_j)$. At most one place where A has good reduction appears in the support of the D_j.*

Proof. We choose one place v_0 of K and arbitrary representatives in $W_i(K)$ for the elements in $\mathrm{Sel}(K, V^i)$. To deal with the places $v \neq v_0$ where A has good reduction, we apply Artin–Schreier–Witt reduction to get new representatives for which the valuation of the components at v is either not negative or odd. Due to Corollary 4.2 the second case does not occur. As a result of the strong approximation theorem, the components of the new representatives will not have any new poles except at v_0. Afterwards we apply the same reduction to the remaining places different from v_0. This time it is possible for the components to have an odd, negative valuation. But, as the local image is finite, the valuation is bounded below. Finally, we reduce the valuation at v_0. Again we get a lower bound, but this time it depends not only on the finite image of $\alpha_i^{v_0}$ but also on the degree of v_0 and the genus of K. □

REMARK. In order to calculate the divisors D_j, one only has to compute the poles and zeros of the coefficients and the genus of K. As a result we get representatives for a finite subset of $W_i(K)/\wp(W_i(K))$ that contains $\mathrm{Sel}(K, V^i)$. To compute the elements that actually are in $\mathrm{Sel}(K, V^i)$ we have to find those that are contained in the local images $\mathrm{Im}\,\alpha_i^v$ for the finitely many places v of bad reduction. This task requires elements in K to be represented as Laurent series in K_v to a prescribed precision and Artin–Schreier polynomials to be factorized over K_v.

For $\mathrm{Sel}(K, F^i)$ we can proceed in a similar fashion.

PROPOSITION 5.2. *For $i = 1, 2$, there is a finite set S of places of K such that* $\mathrm{Sel}(K, F^i)$ *is a subset of*

$$K(S, 2^i) := \{a \in K^\times/(K^\times)^{2^i} \mid v(a) \equiv 0 \bmod 2^i \text{ for all } v \notin S\}.$$

If $A^{(2^i)}$ has good reduction at v, then v is not in S.

Proof. This is a consequence of Corollary 4.2. □

REMARK. The calculation of generators for $K(S, 2^i)$ amounts to calculating generators for the S-class and the S-unit group of K (see, for example, [**13**]). In order to determine if an element $a \in K(S, 2^i)$ is in $\mathrm{Sel}(K, F^i)$, we examine whether it is orthogonal to $\mathrm{Im}\,\alpha_i^v$ for the places of bad reduction. This requires a finite amount of evaluations of the Artin–Schreier–Witt pairing.

Finally, we want to compute the elements $w = (w_0, \ldots, w_{i-1})$ that are in $\mathrm{Sel}(K, V^i)$ (or $a \in \mathrm{Sel}(K, F^i)$) that are in the image of α_i (or β_i). Therefore we have to decide if there is a point $P_w \in A(K)$ (or $P_a \in A^{(2^i)}(K)$) for which $\alpha_i(P_w) = w$ (or $\beta_i(P_a) = a$) holds or not. For α_i this results in the equations

$$\begin{aligned}
i = 1 &: y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0 \\
&\qquad \frac{x + a_2}{a_1^2} = w_0 + z_0^2 + z_0, \\
i = 2 &: y^2 + a_1xy + x^3 + a_1^2(s^2 + s)x^2 + a_6 = 0 \\
&\qquad \left(\frac{a_6}{a_1^2x^2}, \frac{a_6y}{a_1^3x^3} + \frac{a_6}{a_1^4x} + \frac{sa_6 + a_6}{a_1^2x^2} + \frac{a_6^2}{a_1^4x^4}\right) = (w_0, w_1) + \wp(z_0, z_1),
\end{aligned}$$

https://doi.org/10.1112/S1461157014000175 Published online by Cambridge University Press

in the variables $x, y, z_0, \ldots, z_{i-1}$. Their homogenizations define a projective curve C_w over K which is a covering of A. Artin–Schreier–Witt theory shows that this covering is unramified, thus has genus 1 and is cyclic of exponent 2^i. Moreover, it is flat, hence étale and smooth. The points over $\mathcal{O} \in A(K)$ define a K-rational divisor of degree 2^i on C_w. For β_i we get similar results. This time the equations are

$$\begin{aligned} i = 1 : y^2 + a_1^2 xy + x^3 + a_2^2 x^2 + a_6^2 &= 0 \\ x &= az^2, \\ i = 2 : y^2 + a_1^4 xy + x^3 + a_1^8 (s^2 + s)^4 x^2 + a_6^4 &= 0 \\ y + \frac{1}{a_1^4} x^2 + a_1^4 s^4 x &= az^4, \end{aligned}$$

in the variables x, y, z. Their homogenizations define a projective covering C_a of the elliptic curve $A^{(2^i)}$. This covering is defined over K and purely inseparable. A short computation using Tate's genus formula shows that C_a has genus 1 and is smooth. The preimage of $\mathcal{O} \in A^{(2^i)}(K)$ under $C_a \to A^{(2^i)}$ is a K-rational divisor of degree 2^i on C_a. In [4] it is shown that smooth projective curves of genus 1 having a K-rational divisor of a specific degree, in our case 2 or 4, possess special models. As these models are advantageous for the computation of rational points we have to compute rational transformations from the aforementioned models to those presented in [4]. For $i = 1$ this amounts to using the second equation to eliminate x in the first, followed by some obvious transformations. As a result, for $i = 1$ we get the models given by

$$\begin{aligned} C_w : y^2 + (a_1 z^2 + a_1^2 z + (a_1^3 w_0 + a_1 a_2))y + a_1^2 w_0 z^4 + (a_1^3 w_0 + a_1^3 + a_1 a_2) z^3 \\ + (a_1^4 w_0^2 + a_1^4 w_0 + a_2^2) z^2 + (a_1^5 w_0^2 + a_1 a_2^2) z + a_1^6 w_0^3 + a_1^2 a_2^2 w_0 + a_6 = 0 \end{aligned}$$

and

$$C_a : y^2 + a_1^2 axy + a_1^2 a_6 a x^4 + a_2^2 a^2 x^2 z^2 + a^3 z^4 = 0$$

in a weighted projective space. For $i = 2$ we can represent C_w and C_a as the intersection of two quadrics. This time it is too hard to find a transformation to such a model by hand. We can do it by using Magma for the computation of bases for some Riemann–Roch spaces. This results in formulas for the defining equations, but as they are rather lengthy we omit them. Deciding whether an element $w \in \mathrm{Sel}(K, V^i)$ or $a \in \mathrm{Sel}(K, F^i)$ is in the image of α_i or β_i is equivalent to deciding if C_w or C_a possesses a K-rational point, and such a K-rational point yields a preimage on $A(K)$ or $A^{(2^i)}(K)$. The element w (or a) is by construction in the local image of α_i^v (or β_i^v). Consequently, there is a K_v-rational point on C_w (or C_a) for every valuation v of K. Due to the failure of the Hasse principal for curves of genus 1, this does not imply the existence of a K-rational point. As described in [4], when performing a search for K-rational points on such a curve it is advantageous if the curve is given by a model with small coefficients. In [4] techniques to minimize and reduce the coefficients of the models we are dealing with are presented. The minimization algorithms can be applied to our situation without any modifications. A straightforward algorithm based on Groebner base computations over the constant field of K can be used to reduce the coefficients. Sieving techniques as described in [18] prove to be useful for the computation of points on the minimized and reduced model. For the computation of Mordell–Weil bases, this calculation of rational points on the homogeneous spaces is a major bottleneck. Here the models given by the α_2- and β_2-descent are often advantageous. Assuming a point P on $A(K)$ can be computed as a preimage of a point on a homogeneous space C_1 for α_1 (or β_1) and as a preimage of a point C_2 for α_2 (or β_2), and assuming the models both for $i = 1$ and for $i = 2$ are minimized and reduced, then in general $C_2(K)$ will have a point that has roughly one half of the height of the smallest

https://doi.org/10.1112/S1461157014000175 Published online by Cambridge University Press

point on $C_1(K)$. The rank of the elliptic curve A given by

$$y^2 + (t^4 + t^3 + t^2 + 1)xy + x^3 + (t^4 + t^3 + t^2) = 0$$

over $\mathbb{F}_2(t)$ is 1. But even though the coefficients of the Weierstrass equation are small, finding a point of infinite order on $A(K)$ using a V- and F-descent is very time-consuming. Using a V^2- and F^2-descent instead, it only takes a few minutes.

6. *Heights and infinite descent*

Siksek [10] presents an algorithm to compute a Mordell–Weil basis for an elliptic curve over a number field given the generators of a subgroup of finite index. With minor modifications, this algorithm can also be applied over global function fields of characteristic 2. All we need is an estimate of the difference between the naive height h and the canonical height $\hat{h}$. Such an estimate can be achieved by the same means as described in [12]. As a result we get the following proposition.

PROPOSITION 6.1. *Let A be an elliptic curve over a global function field K given by a Weierstrass equation. Denote the j-invariant of A by j. Then for every $P = (x, y) \in A(K)$ the inequality*

$$h(P) - \hat{h}(P) \leqslant \tfrac{1}{12}h(j) + C$$

holds. Here C is a constant that depends only on the poles of the coefficients of a Weierstrass equation of A. It can be calculated explicitly.

Proof. Silverman's method for elliptic curves over number fields can also be applied over global function fields. The term $\frac{1}{12}h(j)$ is due to the difference of the local height function and the valuation of the x-coordinate for points on an elliptic curve with integral coefficients. For the poles of the coefficients of A we have to transform the model. In this way the constant C comes into existence. □

Another way to obtain an upper bound for the difference of the naive and the canonical height is described in [10] and [5]. Their techniques can also be applied in our situation.

7. *S-integral points*

Let S be a finite set of valuations of K, and let A be an ordinary elliptic curve given by the Weierstrass equation

$$y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0,$$

where the coefficients a_i do not have any poles outside of S. We call a point $P = (x_0, y_0) \in K^2$ that satisfies the Weierstrass equation *S-integral* if and only if x_0 hence also y_0 do not have poles outside of S. As shown by Voloch in [17], an ordinary elliptic curve whose j-invariant is transcendental over the constant field of K has finitely many S-integral points (see also [2] and [3]). We use Voloch's methods to compute an upper bound for their naive height. Combining α_1 and β_1, we get a homomorphism

$$\mu : A(K) \to K,\ (x, y) \mapsto \frac{a_6}{a_1^2x^2} + \wp\left(\frac{a_6\delta x}{x}\right).$$

Here δ is given by $\delta = d/da_6$ assuming a_6 is not a square in K and $\wp(z) = z^2 + z$. See [17] for details and proofs. The kernel of μ is $2A(K)$, hence its image is finite. Given generators for a subgroup of odd finite index of $A(K)$ (e.g. a Mordell–Weil basis), one can easily compute $\operatorname{Im}\mu$ because it is generated by the images.

https://doi.org/10.1112/S1461157014000175 Published online by Cambridge University Press

PROPOSITION 7.1. *Let $(x_0, y_0) \in A(K)$ be an S-integral point, $v \in S$ and $n \in \mathbb{N}$ sufficiently large. If $v(x_0) \leqslant -n$, then $v(\mu(x_0, y_0)) \geqslant n/2 - C_v$, where C_v is an explicit constant that depends only on the Weierstrass equation of A.*

Proof. We use the notation $v(x_0) =: -n$, $v(y_0) =: -m$, $v(a_i) =: -d_i$. Now n is sufficiently large if $3n > \max\{d_1 + m + n, d_2 + 2n, d_6\}$ holds. In that case we have $2m = 3n$. This means y_0^2 and x_0^3 have the same valuation at v, and the valuation of the other terms is greater. Setting $d := \max\{2d_1, d_2, d_6/3\}$, then we have $n > d$. For $c := n - d$ the valuation of x_0^3 and y_0^2 at v is $v(x^3) = v(y^2) = 3d + 3c$, but the valuation of the other terms in the Weierstrass equation is greater than or equal to $3d + \frac{5}{2}c$. When writing the terms as Laurent series in a local uniformizer π at v, we have that x_0^3 and y_0^2 are non-zero first at $\pi^{-(3d+3c)}$ while the others are zero before $\pi^{-(3d+5/2c)}$, hence the first $\frac{1}{2}c$ coefficients of the series of x_0^3 and y_0^2 are equal. Consequently for x_0 the leading $\frac{1}{2}c$ coefficients at the odd powers of π are zero. Therefore we have $v(dx/xd\pi) \geqslant c/2 - 1$. Set $c_2 := v(a_6 d\pi/da_6)$; then $v(a_6 dx/xda_6) \geqslant c/2 + c_2 - 1 = (n-d)/2 + c_2 - 1$. The valuations of $(a_6 dx/xda_6)^2$ and $a_6/a_1^2 x^2$ are greater than or equal to $(n-d)/2 + c_2 - 1$, and this proves the statement. □

In order to calculate the constants C_v, one only has to compute the valuation of the a_i and of $a_6 d\pi/da_6$ at v. By combining C_v and the valuation of the finitely many elements in $\operatorname{Im}\mu$ at v, we get lower bounds for the valuations of the x-coordinate of points on $A(K) \setminus 2A(K)$ at the places in S. But the naive height of S-integral points in $2A(K)$ is also bounded.

PROPOSITION 7.2. *Let $P = (x_0, y_0)$ be an S-integral point in $2A(K)$. Then $h(P) \leqslant C$. The constant C only depends on the coefficients of the Weierstrass equation of A and can be computed explicitly.*

Proof. Let $Q = (x_1, y_1)$ be in $A(K)$ with $2Q = P$, and let w be a valuation outside of S. Due to the addition law, we have $x_0 = (x_1^4 + a_1^2 a_6)/a_1^2 x_1^2$. If $w(x_1) < 0$, then $w(x_0)$ is also less than zero because we have $w(a_i) \geqslant 0$. Hence Q is an S-integral point, and we have $w(x_1) \geqslant 0$ and $w((x_1^4 + a_1^2 a_6)/a_1^2 x_1^2) \geqslant 0$. Using the triangle inequality, we see that for the valuation of the numerator of $(x_1^4 + a_1^2 a_6)/a_1^2 x_1^2$ at w there are two possibilities. Either $w(x_1^4) \leqslant w(a_1^2 a_6)$ or $w(x_1^4 + a_1^2 a_6) = w(a_1^2 a_6)$. Looking at the denominator, the latter implies $w(x_1) \leqslant \frac{1}{2} w(a_6)$. Therefore x_1 may have zeros only at finitely many valuations, and those zeros are bounded. This yields bounds for the naive height of S-integral points in $2A(K)$. □

REMARK. If a_6 is a square, the same proof can be applied after a minor modification of μ. Using the results about the Selmer groups, it is possible to compute bounds for the valuations of the elements in the image of μ without having explicit points on $A(K)$.

8. *Examples*

In this section we apply our algorithm to different examples. The computations are carried out by our Magma implementation.

8.1. *Example 1*

First we consider the elliptic curve A given by

$$A : y^2 + xy + x^3 + t^{12} + t^{10} + t^8 + t^5 + t^4 + t^3 + t^2 + t + 1 = 0$$

over the rational function field $\mathbb{F}_2(t)$. We compute the V- and the F-Selmer group. This takes less than a second. The places of bad reduction are $(t^2 + t + 1), (t^6 + t^5 + t^3 + t^2 + 1)$

https://doi.org/10.1112/S1461157014000175 Published online by Cambridge University Press

and $(1/t)$. Following Proposition 5.1, we see that the Riemann–Roch space $\mathcal{L}(3(1/t))$ contains representatives for the image of α_1. The local image of α_1 at (t^2+t+1) and $(t^6+t^5+t^3+t^2+1)$ is trivial. Hence the elements in the V-Selmer group possess representatives that vanish at (t^2+t+1) and $(t^6+t^5+t^3+t^2+1)$. The cardinality of the local image of α_1 at $(1/t)$ is 4. We compute it by randomly generating sufficiently many points on A defined over $\mathbb{F}_2((1/t))$. Combining the local information proves that the V-Selmer group is generated by the classes of 1 and t^3. The F-Selmer group is generated by the class of t^8+t+1 and t^2+t+1. The non-trivial 2-torsion point on $A^{(2)}$ is a preimage of t^8+t+1 under β_1. Therefore the rank of $A(\mathbb{F}_2(t))$ is at most 3 and the preimages of 1 and t^3 under α_1 plus the image of Q under the Verschiebung, where Q is a preimage of t^2+t+1, generate a subgroup of finite index. The preimages of 1 correspond to $\mathbb{F}_2(t)$-rational points on the curve of genus 1 given by

$$y^2+(x^2+xz+z^2)y = x^4+xz^3+(t^{12}+t^{10}+t^8+t^5+t^4+t^3+t^2+t)z^4.$$

We minimize it, reduce it and transform it into the intersection of two quadrics. This takes about a minute and yields the model given by the equations

$$\begin{aligned}
&(t+1)x_1^2+tx_1x_2+(t^3+t+1)x_1x_3+(t^2+1)x_1x_4+(t^2+t)x_2^2+(t^4+t^3+t)x_2x_3\\
&\quad+(t^2+1)x_2x_4+t^3x_3^2+(t^3+t)x_3x_4+(t^2+t+1)x_4^2=0,\\
&(t^3+t^2+t)x1^2+(t^3+t^2+1)x_1x_2+(t^3+1)x_1x_3+(t^3+t^2+t+1)x_2x_3\\
&\quad+(t^3+t^2+1)x_2x_4+t^2x_3^2+(t^3+1)x_3x_4+(t^3+t^2+t)x_4^2=0.
\end{aligned}$$

A sieving algorithm computes the point

$$(t+1,\, t^4+t^2,\, t^2+1,\, 1)$$

in a few seconds. This point yields the point

$$(t^2+t+1,\, t^6+t^5+t^3+t+1)$$

on $A(\mathbb{F}_2(t))$. In the same manner we calculate

$$\left(\frac{t^9+t^7+t^5+t^4+t^3+t^2+t}{t^6+t^4+1}, \frac{t^{15}+t^8+t^6+t^5+t^4+1}{t^9+t^8+t^7+t^4+t^3+t^2+1}\right),$$

which is a preimage of t^3. Calculating a preimage for t^2+t+1 yields the point

$$(t^6+t^5+t^4+t^2+t+1,\, t^{12}+t^{10}+t^8+t^6+t^5+t^4+t^3+t^2+t)$$

on $A^{(2)}(\mathbb{F}_2(t))$. Its image under the Verschiebung is

$$\left(\frac{t^3+t^2+t}{t^4+1}, \frac{t^{12}+t^{11}+t^9+t^8+t^2+t+1}{t^6+t^4+t^2+1}\right)$$

on $A(\mathbb{F}_2(t))$. These points could also be calculated using a V^2- and F^2-descent. We compute the V^2- and F^2-Selmer groups. The former is generated by the classes of the Witt vectors $(0,t^3)$, $(1,t^5+t^3)$, and (t^3,t^5+t^3+1), the latter by $1/(t^4+t^2+1)$ and $1/(t^8+t+1)$. Calculating explicit models for the corresponding homogeneous spaces and $\mathbb{F}_2(t)$-rational points on them yields the same points on $A(\mathbb{F}_2(t))$. These three points are $\mathbb{Z}$-linearly independent and generate a subgroup G of finite index of $\hat{A}(K)$. Their regulator is 30. The estimate of the difference between the naive and the canonical height together with a brute force search for small points shows that there are no points of canonical height less than $\frac{7}{6}$. Hence the index $[\hat{A}(\mathbb{F}_2(t)) : G]$

https://doi.org/10.1112/S1461157014000175 Published online by Cambridge University Press

is at most 12. See [10] for more information. A short computation reveals that the index is equal to 9, and a Mordell–Weil basis is given by

$$\left(\frac{t^9+t^7+t^5+t^4+t^3+t^2+t}{t^6+t^4+1}, \frac{t^{15}+t^8+t^6+t^5+t^4+1}{t^9+t^8+t^7+t^4+t^3+t^2+1}\right),$$
$$(t^2+t+1, t^6+t^5+t^3+t+1), \quad (t^3+t^2+t, t^6+t^5+t^2+1).$$

Set $S := \{(1/t)\}$. Then the Weierstrass equation for A has coefficients that are S-integral. With the method mentioned in § 7, it can be seen that 12 is an upper bound for the naive height of an S-integral point. Iterating over the possible x-coordinates, we compute 20 different S-integral points. In [6] the authors describe a method to transform a bound for the naive height into a bound for the absolute value of the coefficients of a representation of an S-integral point as a linear combination in the Mordell–Weil basis. In our case the bound for the Mordell–Weil coefficients is 8. Iterating over the possible coefficients yields the same 20 points.

8.2. *Example 2*

Ulmer [15] constructs the family A_n of elliptic curves over $\mathbb{F}_q(t)$ defined by the Weierstrass equations

$$A_n : y^2 + xy = x^3 + t^{2^n+1}.$$

Without constructing any points, he proves that the rank of $A_n(\mathbb{F}_q(t))$ is greater than or equal to $(2^n-1)/2n$. We use our implementation to compute the rank and independent points on $A_n(\mathbb{F}_q(t))$ for $q = 2$ and $n = 1, \ldots, 5$. As a result we get

$n = 1 : \operatorname{rank}\big(A_1(\mathbb{F}_2(t))\big) = 1$
points: $(t, 0)$;
$n = 2 : \operatorname{rank}\big(A_2(\mathbb{F}_2(t))\big) = 1$
points: (t^2, t^3);
$n = 3 : \operatorname{rank}\big(A_3(\mathbb{F}_2(t))\big) = 2$
points: $(t^3, 0)$, (t^4, t^6+t^5);
$n = 4 : \operatorname{rank}\big(A_4(\mathbb{F}_2(t))\big) = 2$
points: $(t^6+t^5+t^4+t^2, t^9+t^5+t^2)$, $(t^8, t^{12}+t^{10}+t^9)$;
$n = 5 : \operatorname{rank}\big(A_5(\mathbb{F}_2(t))\big) = 4$
points: $(t^{12}+t^9, t^{18}+t^{12}+t^9)$, $(t^{11}, 0)$, $(t^{16}, t^{24}+t^{20}+t^{18}+t^{17})$,
$$\left(\frac{t^{22}+t^{20}+t^{16}+t^{15}+t^{11}+t^{10}+t^6}{t^8+t^6+1}, \frac{t^{33}+t^{32}+t^{31}+t^{26}+t^{24}+t^{23}+t^{16}+t^{15}+t^{12}}{(t^{12}+t^{11}+t^{10}+t^9+t^8+t^6+t^4+t^3+1}\right).$$

For these five curves, the rank of $A_n(\mathbb{F}_2(t))$ is equal to $\lceil (2^n-1)/2n \rceil$.

References

1. W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system I: the user language', *J. Symbolic Comput.* 24 (1997) no. 3/4, 235–265.
2. A. Broumas, 'Effective p-descent', PhD Thesis, University of Texas, 1995.
3. A. Broumas, 'Effective p-descent', *Compos. Math.* 107 (1997) 125–141.
4. J. E. Cremona, T. A. Fisher and M. Stoll, 'Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves', *Algebra Number Theory* 4 (2010) 763–820.
5. J. E. Cremona, M. Prickett and S. Siksek, 'Height difference bounds for elliptic curves over number fields', *J. Number Theory* 116 (2006) no. 1, 42–68.

https://doi.org/10.1112/S1461157014000175 Published online by Cambridge University Press

6. J. Gebel, A. Pethő and H. Zimmer, 'Computing integral points on elliptic curves', *Acta Arith.* 68 (1994) no. 2, 171–192.
7. K. Kramer, 'Two-descent for elliptic curves in characteristic two', *Trans. Amer. Math. Soc.* 232 (1977) 279–295.
8. J. S. Milne, *Arithmetic duality theorems*, 2nd edn (BookSurge, 2006).
9. S. Shatz, 'Cohomology of Artinian group schemes over local fields', *Ann. of Math.* (2) 79 (1963) no. 3, 411–449.
10. S. Siksek, 'Descent on curves of genus 1', PhD Thesis, University of Exeter, 1995.
11. J. H. Silverman, *The arithmetic of elliptic curves* (Springer, 1986).
12. J. H. Silverman, 'The difference between the Weil height and the canonical height on elliptic curves', *Math. Comp.* 55 (1990) 723–743.
13. D. Simon, Equations dans les corps de nombres et discriminants minimaux', PhD Thesis, Université Bordeaux, 1998.
14. L. Thomas, 'Ramification groups in Artin–Schreier–Witt extensions', *J. Théor. Nombres Bordeaux* 17 (2005) 689–720.
15. D. Ulmer, 'Elliptic curves with large rank over function fields', *Ann. of Math.* (2) 155 (2002) 295–315.
16. D. Ulmer, 'p-descent in characteristic p', *Duke Math. J.* 62 (1991) 237–265.
17. J. F. Voloch, 'Explicit p-descent for elliptic curves in characteristic p', *Compos. Math.* 74 (1990) 247–258.
18. T. Womack, 'Explicit descent on elliptic curves', PhD Thesis, University of Nottingham, 2003.

G. Moehlmann
Institut für Mathematik
Technische Universität Berlin
Straße des 17. Juni 136
D-10623 Berlin
Germany

moehlman@math.tu-berlin.de