Canad. Math. Bull. Vol. **53** (1), 2010 pp. 87–94
doi:10.4153/CMB-2010-019-9

Elliptic Curves over the Perfect Closure of a Function Field

Dragos Ghioca

Abstract. We prove that the group of rational points of a non-isotrivial elliptic curve defined over the perfect closure of a function field in positive characteristic is finitely generated.

1 Introduction

For this paper we fix a prime number p and denote by $\mathbb{F}_p$ the finite field with p elements. The perfect closure K^{per} of a field K of characteristic p is defined to be $\bigcup_{n\geq 1} K^{1/p^n}$.

The classical Lehmer conjecture (see [12, p. 476]) asserts that there is an absolute constant $C > 0$ so that any algebraic number α that is not a root of unity satisfies the following inequality for its logarithmic height:

$$h(\alpha) \geq \frac{C}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}.$$

A partial result towards this conjecture is obtained in [3]. The analog of Lehmer's conjecture for elliptic curves and abelian varieties asks for a good lower bound for the canonical height of a non-torsion point of the abelian variety. This question has also been much studied (see [1, 2, 7, 11, 14, 20]). In Section 3, using a Lehmer-type result for elliptic curves from [5], we prove the following.

Theorem 1.1 *Let K be a function field of transcendence degree* 1 *over $\mathbb{F}_p$ (*i.e., *K is a finite extension of $\mathbb{F}_p(t)$). Let E be a non-isotrivial elliptic curve defined over K. Then $E(K^{\mathrm{per}})$ is finitely generated.*

Using specializations we are able to extend the conclusion of Theorem 1.1 to the perfect closure of any finitely generated field extension K of $\mathbb{F}_p$ (see Theorem 3.3).

Using completely different methods, Minhyong Kim studied the set of rational points of non-isotrivial curves of genus at least two over the perfect closure of a function field in one variable over a finite field (see [8]).

Combining the result of Theorem 3.3 with the results obtained by the author and Rahim Moosa in [4], one can prove the full Mordell–Lang conjecture for abelian varieties A which are isogenous with a direct product of non-isotrivial elliptic curves (where the *full* Mordell–Lang conjecture refers to the intersection of a subvariety of A with the divisible hull of a finitely generated subgroup of A; see also the remark of Thomas Scanlon at the end of [16]).

Received by the editors November 6, 2006; revised December 3, 2006.
Published electronically December 4, 2009.
AMS subject classification: **11G50**, 11G05.
Keywords: elliptic curves, heights.

2 Tame Modules

In this section we prove a technical result about tame modules which will be used in the proof of Theorem 1.1.

Definition 2.1 Let R be an integral domain and let K be its field of fractions. If M is an R-module, then by the *rank* of M, denoted $\mathrm{rk}(M)$, we mean the dimension of the K-vector space $M \otimes_R K$. We call M a *tame* module if every finite rank submodule of M is finitely generated.

If R is a ring and M is an R-module, we denote by M_{tor} the set of torsion elements of M.

Lemma 2.2 *Let R be a Dedekind domain and let M be an R-module with M_{tor} finite. Assume there exists a function $h\colon M \to \mathbb{R}_{\geq 0}$ satisfying the following properties:*

(i) *(quasi-triangle inequality) $h(x \pm y) \leq 2(h(x) + h(y))$, for every $x, y \in M$.*
(ii) *if $x \in M_{\mathrm{tor}}$, then $h(x) = 0$.*
(iii) *there exists $c > 0$ such that for each $x \notin M_{\mathrm{tor}}$, $h(x) > c$.*
(iv) *there exists $a \in R \setminus \{0\}$ such that R/aR is finite and for all $x \in M$, $h(ax) \geq 8h(x)$.*

Then M is a tame R-module.

Proof By the definition of a tame module, it suffices to assume that M is a finite rank R-module and conclude that it is finitely generated.

Let $a \in R$ as in (iv) of Lemma 2.2. By [15, Lemma 3], M/aM is finite. The following result is the key to the proof of Lemma 2.2.

Sublemma 2.3 *For every $D > 0$, there exist only finitely many $x \in M$ such that $h(x) \leq D$.*

Proof of Sublemma 2.3 If we suppose Sublemma 2.3 is not true, then we can define

$$C = \inf\{D \mid \text{ there exists infinitely many } x \in M \text{ such that } h(x) \leq D\}.$$

Properties (ii) and (iii) and the finiteness of M_{tor} yield $C \geq c > 0$. By the definition of C, it must be that there exists an infinite sequence of elements z_n of M such that for every n, $h(z_n) < \frac{3C}{2}$.

Because M/aM is finite, there exists a coset of aM in M containing infinitely many z_n from the above sequence.

But if $k_1 \neq k_2$ and z_{k_1} and z_{k_2} are in the same coset of aM in M, then let $y \in M$ be such that $ay = z_{k_1} - z_{k_2}$. Using properties (iv) and (i), we get

$$h(y) \leq \frac{h(z_{k_1} - z_{k_2})}{8} \leq \frac{h(z_{k_1}) + h(z_{k_2})}{4} < \frac{3C}{4}.$$

We can do this for any two elements of the sequence that lie in the same coset of aM in M. Because there are infinitely many of them lying in the same coset, we can construct infinitely many elements $z \in M$ such that $h(z) < \frac{3C}{4}$, contradicting the minimality of C. ∎

https://doi.org/10.4153/CMB-2010-019-9 Published online by Cambridge University Press

From this point on, our proof of Lemma 2.2 follows the classical descent argument in the Mordell–Weil theorem (see [17]).

Take coset representatives $y_1, \ldots, y_k$ for aM in M. Define then

$$B = \max_{i \in \{1,\ldots,k\}} h(y_i).$$

Consider the set $Z = \{x \in M \mid h(x) \leq B\}$, which is finite according to Sublemma 2.3. Let N be the finitely generated R-submodule of M which is spanned by Z.

We claim that $M = N$. If we suppose this is not the case, then by Sublemma 2.3 we can pick $y \in M - N$ which minimizes $h(y)$. Because N contains all the coset representatives of aM in M, we can find $i \in \{1, \ldots, k\}$ such that $y - y_i \in aM$. Let $x \in M$ be such that $y - y_i = ax$. Then $x \notin N$ because otherwise it would follow that $y \in N$ (we already know $y_i \in N$). By our choice of y and by properties (iv) and (i), we have

$$h(y) \leq h(x) \leq \frac{h(y - y_i)}{8} \leq \frac{h(y) + h(y_i)}{4} \leq \frac{h(y) + B}{4}.$$

This means that $h(y) \leq \frac{B}{3} < B$. This contradicts the fact that $y \notin N$ because N contains all the elements $z \in M$ such that $h(z) \leq B$. This contradiction shows that indeed $M = N$ and so, M is finitely generated. ■

3 Elliptic Curves

Unless otherwise stated, the setting is the following: K is a finitely generated field of transcendence degree 1 over $\mathbb{F}_p$ where p is a prime as always. We fix an algebraic closure K^{alg} of K. We denote by $\mathbb{F}_p^{\text{alg}}$ the algebraic closure of $\mathbb{F}_p$ inside K^{alg}.

Let E be a non-isotrivial elliptic curve (*i.e.* , $j(E) \notin \mathbb{F}_p^{\text{alg}}$) defined over K. Let K^{per} be the perfect closure of K inside K^{alg}. Theorem 1.1, which we are going to prove in this section, says that $E(K^{\text{per}})$ is finitely generated.

For every finite extension L of K we denote by M_L the set of discrete valuations v on L, normalized so that the value group of v is $\mathbb{Z}$. For each $v \in M_L$ we denote by f_v the degree of the residue field of v over $\mathbb{F}_p$. If $P \in E(L)$ and $m \in \mathbb{Z}$, mP represents the point on the elliptic curve obtained using the group law on E. We define a notion of height for the point $P \in E(L)$ with respect to the field K

$$h_K(P) = \frac{-1}{[L:K]} \sum_{v \in M_L} f_v \min\{0, v(x(P))\}$$

(see [18, Chapter VIII] and [19, Chapter III]). Then we define the canonical height of P with respect to K as

$$\widehat{\mathrm{h}}_{E/K}(P) = \frac{1}{2} \lim_{n \to \infty} \frac{h_K(2^n P)}{4^n}.$$

We also denote by $\Delta_{E/K}$ the divisor which is the minimal discriminant of E with respect to the field K (see [18, Chapter VIII]). By $\deg(\Delta_{E/K})$ we denote the degree of the divisor $\Delta_{E/K}$ (computed with respect to $\mathbb{F}_p$). We denote by g_K the genus of the function field K.

The following result is proved in [5] (see their Theorem 7, which extends a similar result of Hindry and Silverman [6] valid for function fields of characteristic 0).

***Theorem 3.1* (Goldfeld–Szpiro)** *Let E be an elliptic curve over a function field K of one variable over a field in any characteristic. Let $\widehat{\mathrm{h}}_{E/K}$ denote the canonical height on E and let $\Delta_{E/K}$ be the minimal discriminant of E, both computed with respect to K. Then for every point $P \in E(K)$ that is not a torsion point:*

$$\widehat{\mathrm{h}}_{E/K}(P) \geq 10^{-13} \deg(\Delta_{E/K}) \text{ if } \deg(\Delta_{E/K}) \geq 24(g_K - 1)\,,$$

and

$$\widehat{\mathrm{h}}_{E/K}(P) \geq 10^{-13-23g} \deg(\Delta_{E/K}) \text{ if } \deg(\Delta_{E/K}) < 24(g_K - 1).$$

We are ready to prove our first result.

Proof of Theorem 1.1. We first observe that replacing K by a finite extension does not affect the conclusion of the theorem. Thus, at the expense of replacing K by a finite extension, we may assume E is semi-stable over K (the existence of such a finite extension is guaranteed by [18, Chapter VII, Proposition 5.4(c)]; see also Corollary 1.4 from [18, Appendix A, Corollary 1.4]).

As before, we let $\widehat{\mathrm{h}}_{E/K}$ and $\Delta_{E/K}$ be the canonical height on E and the minimal discriminant of E, respectively, computed with respect to K.

We let F be the usual Frobenius. For every $n \geq 1$, we denote by $E^{(p^n)}$ the elliptic curve obtained by raising to power p^n the coefficients of a Weierstrass equation for E. Thus

$$F^n \colon E(K^{1/p^n}) \to E^{(p^n)}(K) \tag{3.1}$$

is a bijection. Moreover, for every $P \in E\left(K^{1/p}\right)$,

$$pP = (VF)(P) \in V\left(E^{(p)}(K)\right) \subset E(K)$$

where V is the Verschiebung. Similarly, we get that

$$p^n E\left(K^{1/p^n}\right) \subset E(K) \text{ for every } n \geq 1. \tag{3.2}$$

Thus $E(K^{\mathrm{per}})$ lies in the p-division hull of the $\mathbb{Z}$-module $E(K)$. Because $E(K)$ is finitely generated (by the Mordell–Weil theorem), we conclude that $E(K^{\mathrm{per}})$, as a $\mathbb{Z}$-module, has finite rank.

We will show next that the height function $\widehat{\mathrm{h}}_{E/K}$ and $p^2 \in \mathbb{Z}$ satisfy the properties (i)–(iv) of Lemma 2.2 corresponding to the $\mathbb{Z}$-module $E(K^{\mathrm{per}})$.

Property (ii) is well known for $\widehat{\mathrm{h}}_{E/K}$. Property (i) follows from the quadraticity of $\widehat{\mathrm{h}}$: $\widehat{\mathrm{h}}(P+Q) + \widehat{\mathrm{h}}(P-Q) = 2\,\widehat{\mathrm{h}}(P) + 2\,\widehat{\mathrm{h}}(Q)$ (see [17, p. 40, Section 3.6]) for all points $P, Q \in E$. Hence $\widehat{\mathrm{h}}(P \pm Q) \leq 2(\widehat{\mathrm{h}}(P) + \widehat{\mathrm{h}}(Q))$. We also have the formula

$$\widehat{\mathrm{h}}_{E/K}(p^2P) = p^4\,\widehat{\mathrm{h}}_{E/K}(P) \geq 8\,\widehat{\mathrm{h}}(P) \text{ for every } P \in E(K^{\mathrm{alg}}),$$

https://doi.org/10.4153/CMB-2010-019-9 Published online by Cambridge University Press

(see [18, Chapter VIII]), which proves that property (iv) of Lemma 2.2 holds. Now we prove that property (iii) also holds (here we will use Theorem 3.1). Let P be a non-torsion point of $E(K^{\mathrm{per}})$. Then $P \in E(K^{1/p^n})$ for some $n \geq 0$. Because K^{1/p^n} is isomorphic to K, they have the same genus, which we call g. We denote by $\widehat{\mathrm{h}}_{E/K^{1/p^n}}$ and $\Delta_{E/K^{1/p^n}}$ the canonical height on E and the minimal discriminant of E, respectively, computed with respect to K^{1/p^n}. Using Theorem 3.1, we conclude

$$\widehat{\mathrm{h}}_{E/K^{1/p^n}}(P) \geq 10^{-13-23g} \deg(\Delta_{E/K^{1/p^n}}).$$

We have $\widehat{\mathrm{h}}_{E/K^{1/p^n}}(P) = [K^{1/p^n} : K]\, \widehat{\mathrm{h}}_{E/K}(P) = p^n\, \widehat{\mathrm{h}}_{E/K}(P)$. Now, using the proof of Proposition 5.4(b) from Chapter VII of [18], and the fact that E has semi-stable reduction over K, we conclude that $E/K^{1/p^n}$ has the same minimal discriminant as E/K. However, the degree of the minimal discriminant changes by a factor of p^n, because each place of K^{1/p^n} is ramified of degree p^n over K. Thus

$$\deg(\Delta_{E/K^{1/p^n}}) = p^n \deg(\Delta_{E/K}).$$

We conclude that for every non-torsion $P \in E(K^{\mathrm{per}})$,

$$\widehat{\mathrm{h}}_{E/K}(P) \geq 10^{-13-23g} \deg(\Delta_{E/K}).$$

Because E is non-isotrivial, $\Delta_{E/K} \neq 0$ and so, $\deg(\Delta_{E/K}) \geq 1$. We conclude

$$\widehat{\mathrm{h}}_{E/K}(P) \geq 10^{-13-23g}. \tag{3.3}$$

Inequality (3.3) shows that property (iii) of Lemma 2.2 holds for $\widehat{\mathrm{h}}_{E/K}$. Thus properties (i)-(iv) of Lemma 2.2 hold for $\widehat{\mathrm{h}}_{E/K}$ and $p^2 \in \mathbb{Z}$ relative to the $\mathbb{Z}$-module $E(K^{\mathrm{per}})$.

We show that $E_{\mathrm{tor}}(K^{\mathrm{per}})$ is finite. Equation (3.2) shows that the prime-to-p-torsion of $E(K^{\mathrm{per}})$ equals the prime-to-p-torsion of $E(K)$; thus the prime-to-p-torsion of $E(K^{\mathrm{per}})$ is finite. If there exists infinite p-power torsion in $E(K^{\mathrm{per}})$, equation (3.1) yields that we have arbitrarily large p-power torsion in the family of elliptic curves $E^{(p^n)}$ over K. But this contradicts standard results on uniform boundedness for the torsion of elliptic curves over function fields, as established in [13] (actually, [13] proves a uniform boundedness of the entire torsion of elliptic curves over a fixed function field; thus including the prime-to-p-torsion). Hence $E_{\mathrm{tor}}(K^{\mathrm{per}})$ is finite.

Because all the hypotheses of Lemma 2.2 hold, we conclude that $E(K^{\mathrm{per}})$ is tame. Because $\mathrm{rk}\,(E(K^{\mathrm{per}}))$ is finite, we conclude that $E(K^{\mathrm{per}})$ is finitely generated. ■

Remark 3.2. It is absolutely crucial in Theorem 1.1 that E is non-isotrivial. Theorem 1.1 fails in the isotrivial case, *i.e.,* there exists no $n \geq 0$ such that $E(K^{\mathrm{per}}) = E(K^{1/p^n})$. Indeed, if E is defined by $y^2 = x^3 + x$ $(p > 2)$, $K = \mathbb{F}_p(t, (t^3+t)^{\frac{1}{2}})$ and $P = (t, (t^3+t)^{\frac{1}{2}})$, then $F^{-n}P \in E(K^{1/p^n}) \setminus E(K^{1/p^{n-1}})$, for every $n \geq 1$. So, $E(K^{\mathrm{per}})$ is not finitely generated in this case (and we can get a similar example also for the case $p = 2$).

https://doi.org/10.4153/CMB-2010-019-9 Published online by Cambridge University Press

We extend now the result of Theorem 1.1 to elliptic curves defined over arbitrary function fields in characteristic p.

Theorem 3.3 *Let K be a finitely generated field extension of $\mathbb{F}_p$. Let E be a non-isotrivial elliptic curve defined over K. Then $E(K^{\mathrm{per}})$ is a finitely generated group.*

Proof At the expense of replacing K by a finite extension we may assume $E[p] \subset E(K)$. Clearly, if we prove Theorem 3.3 for a finite extension of K, then our result holds also for K. Therefore we assume from now on that $E[p] \subset E(K)$.

Let $j(E)$ be the j-invariant of E. Because E is non-isotrivial, then $j(E)$ is transcendental over $\mathbb{F}_p$. Also, because E is defined over K, then $j(E) \in K$. Let $F_0 := \mathbb{F}_p(j(E))$. We denote by F_0^{alg} the algebraic closure of F_0 inside a fixed algebraic closure K^{alg} of K.

Let $d := \operatorname{trdeg}_{F_0} K$. If $d = 0$, then Theorem 1.1 yields the conclusion of Theorem 3.3. Therefore, we assume from now on that $d \geq 1$. Because $d \geq 1$, we view K as the function field of a parameter variety V defined over F_0. Then we may view E as the generic fiber of a family of elliptic curves $\pi\colon \mathsf{E} \to V$ such that if η is the generic point of V, then $\pi^{-1}(\eta) = \mathsf{E}_\eta = E$. The residue field of the generic fiber of π is K, while for every closed point $y \in V$, the corresponding residue field is denoted by $F_0(y)$. Note that for each closed point y, $F_0(y)$ is a function field of transcendence degree 1 over F_p. Because the generic fiber of π is smooth (E is an elliptic curve), there exists a non-empty Zariski dense set $V_0 \subset V$, such that π is smooth over V_0. For each $y \in V_0(F_0^{\mathrm{alg}})$, we get the fiber E_y called the *specialization* of E_η over y. A rational point $P \in \mathsf{E}_\eta(K)$ corresponds to a rational section $s_P\colon V \to \mathsf{E}$ and for $y \in V_0$, we obtain a point $s_P(y) \in \mathsf{E}_y(F_0(y))$. The map $P \to s_P(y)$ induces the *specialization (group) homomorphism* $\mathsf{E}_\eta(K) \to \mathsf{E}_y(F_0(y))$. Because $\dim V_0 = d$, then there exists a non-empty Zariski open subset $V_1 \subset V_0$ which has a finite morphism into affine space $\psi\colon V_1 \to \mathbb{A}^d$. Moreover, the image of ψ contains a non-empty Zariski open subset of $\mathbb{A}^d$. We obtain the morphism $\psi \circ \pi\colon \mathsf{E} \to \mathbb{A}^d$ whose generic fiber is again E. Thus we may view our family of elliptic curves $\{\mathsf{E}_y\}$ as parametrized by $\mathbb{A}^d$. By [10, Theorem 7.2], there exists a Hilbert subset $S \subset \mathbb{A}^d(F_0)$ such that for $t \in S$ and $y \in V_1(F_0^{\mathrm{alg}})$ with $\psi(y) = t$, the specialization morphism

$$\mathsf{E}_\eta(K) \to \mathsf{E}_y(F_0(y)) \tag{3.4}$$

is injective. In particular, because $E[p] \subset E(K)$:

(3.5) $E[p]$ injects through the specialization morphism.

By [9, Chapter 9, Theorem 4.2], F_0 is a Hilbertian field. Hence, S is infinite (in particular, it is non-empty). Let $y \in \psi^{-1}(S)$ be fixed. The above specialization morphism extends to a morphism $E(K^{1/p^n}) \to \mathsf{E}_y(F_0(y)^{1/p^n})$ for every $n \geq 1$. We are using the fact that the valuation v on K corresponding to the specialization (3.4) has a unique extension on K^{1/p^n}, which we also call v. In addition, the residue field of v on K^{1/p^n} is contained in $F_0(y)^{1/p^n}$, because $F_0(y)$ is the residue field of v on K. In particular, we have a group homomorphism

$$E(K^{\mathrm{per}}) \to \mathsf{E}_y(F_0(y)^{\mathrm{per}}), \tag{3.6}$$

where $F_0(y)^{\mathrm{per}}$ is the perfect closure of $F_0(y)$ inside F_0^{alg}. Using (3.5) in (3.6) we conclude that

(3.7) $E[p^\infty](K^{\mathrm{per}})$ injects through the specialization morphism.

We showed in (3.2) that $E(K^{\mathrm{per}})$ is contained in the p-division hull of $E(K)$. Therefore (3.4) and (3.7) yield that (3.6) is also injective. Hence $E(K^{\mathrm{per}})$ embeds into $\mathsf{E}_y(F_0(y)^{\mathrm{per}})$. By construction, E_y is an elliptic curve of j-invariant equal to $j(E)$ (note that $j(E) \in F_0$ and F_0 is the constant field in our specialization). Thus E_y is a non-isotrivial elliptic curve and $F_0(y)$ is a function field of transcendence degree 1 over $\mathbb{F}_p$. By Theorem 1.1, $\mathsf{E}_y(F_0(y)^{\mathrm{per}})$ is finitely generated. Hence $E(K^{\mathrm{per}})$ is also finitely generated, as desired. ■

Acknowledgments I would like to thank Thomas Scanlon for asking me the analogue of Theorem 3.3 for ordinary abelian varieties. His question motivated me to obtain the results presented in this paper. I also thank the referee for his or her very useful comments.

References

[1] M. H. Baker and J. H. Silverman, *A lower bound for the canonical height on abelian varieties over abelian extensions.* Math. Res. Lett. **11**(2004), no. 2-3, 377–396.

[2] S. David and M. Hindry, *Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C. M.* J. Reine Angew. Math. **529**(2000), 1–74.

[3] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial.* Acta Arith. **34**(1979), no. 4, 391–401.

[4] D. Ghioca and R. Moosa, *Division points of subvarieties of isotrivial semi-abelian varieties.* Int. Math. Res. Not. **2006**, Art. ID 65437.

[5] D. Goldfeld and L. Szpiro, *Bounds for the order of the Tate-Shafarevich group.* Compositio Math. **97**(1995), no. 1-2, 71–87

[6] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves.* Invent. Math. **93**(1988), no. 2, 419–450. doi:10.1007/BF01394340

[7] ———, *On Lehmer's conjecture for elliptic curves.* In: Séminaire de Théorie des Nombres, Paris 1988-1989, Progr. Math. 91, Birkhäuser Boston, Boston, MA, 1990, pp. 103–116.

[8] M. Kim, *Purely inseparable points on curves of higher genus.* Math. Res. Lett. **4**(1997), no. 5, 663–666.

[9] S. Lang, *Fundamentals of Diophantine geometry.* Springer-Verlag, New York, 1983.

[10] ———, *Number theory. III. Diophantine geometry.* In: Encyclopaedia of Mathematical Sciences 60, Springer-Verlag, Berlin, 1991.

[11] M. Laurent, *Minoration de la hauteur de Néron-Tate.* In: Séminaire de théorie des nombres, Paris 1981–82, Progr. Math. 38, Birkhäuser Boston, Boston, MA, 1983, pp. 137–151.

[12] D. H. Lehmer, *Factorization of certain cyclotomic functions.* Ann. of Math. (2) **34**(1933), no. 3, 461–479. doi:10.2307/1968172

[13] M. Levin, *On the group of rational points on elliptic curves over function fields.* Amer. J. Math. **90**(1968), 456–462. doi:10.2307/2373538

[14] D. W. Masser, *Counting points of small height on elliptic curves.* Bull. Soc. Math. France **117**(1989), no. 2, 247–265.

[15] B. Poonen, *Local height functions and the Mordell-Weil theorem for Drinfeld modules.* Compositio Math. **97**(1995), no. 3, 349–368.

[16] T. Scanlon, *A positive characteristic Manin-Mumford theorem.* Compositio Math. **141**(2005), no. 6, 1351–1364. doi:10.1112/S0010437X05001879

[17] J.-P. Serre, *Lectures on the Mordell-Weil theorem.* Aspects of Mathematics E15, Friedr. Vieweg & Sohn, Braunschweig, 1989.

[18] J. H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

[19] ———, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics 151, Springer-Verlag, New York, 1994.

[20] ———, *A lower bound for the canonical height on elliptic curves over abelian extensions.* J. Number Theory **104**(2004), no. 2, 353–372. doi:10.1016/j.jnt.2003.07.001

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4
e-mail: dragos.ghioca@uleth.ca