ARITHMETIC ELLIPTIC CURVES IN GENERAL POSITION

Shinichi Mochizuki

February 2009

Abstract. We combine various well-known techniques from the theory of heights, the theory of "noncritical Belyi maps", and classical analytic number theory to conclude that the *"ABC Conjecture"*, or, equivalently, the so-called *"Effective Mordell Conjecture"*, holds for *arbitrary* rational points of the projective line minus three points if and only if it holds for rational points which are in *"sufficiently general position"* in the sense that the following properties are satisfied: (a) the rational point under consideration is *bounded away* from the three points at infinity at a given finite set of primes; (b) the Galois action on the l-power torsion points of the corresponding elliptic curve determines a *surjection* onto $GL_2(\mathbb{Z}_l)$, for some prime number l which is roughly of the order of the sum of the height of the elliptic curve and the logarithm of the discriminant of the minimal field of definition of the elliptic curve, but does *not divide* the conductor of the elliptic curve, the rational primes that are absolutely ramified in the minimal field of definition of the elliptic curve, or the local heights [i.e., the orders of the q-parameter at primes of [bad] multiplicative reduction] of the elliptic curve.

Introduction

In the classical intersection theory of subvarieties, or cycles, on algebraic varieties, various versions of the *"moving lemma"* allow one to replace a given cycle by another cycle which is *equivalent*, from the point of view of intersection theory, to the given cycle, but is supported on subvarieties which are in a *"more convenient"* position — i.e., typically, a *"more general"* position, which is *free of inessential, exceptional pathologies* — within the ambient variety.

In the present paper, after reviewing, partly for the purpose of establishing notation and terminology, the *general theory of heights* in §1, we proceed in §2 to apply the theory of *"noncritical Belyi maps"* of [Mzk1], together with a technique developed by Elkies [cf. [Elkies]; [vF]] — which, in fact, may be traced back to the work of Moret-Bailly and Szpiro [cf. the discussion at the top of [Elkies], p. 106] — for relating Belyi maps to the ABC Conjecture, to show that the ABC, Effective Mordell, and Vojta Conjectures for *arbitrary* rational points of hyperbolic curves over number fields are *equivalent* to the ABC Conjecture for rational points over a number field of the projective line minus three points which lie in some *"compactly bounded subset"* of the set of all rational points [cf. Theorem 2.1]. Here, "compactly bounded" means that at some finite collection S of primes of the number field that

Typeset by $\mathcal{AMS}$-TEX

includes the archimedean primes, the rational points lie in some given *compact subset* of the set of rational points of the projective line minus three points over the *completion* of the number field at the given prime [cf. Example 1.3, (ii)]. Such compactly bounded subsets of the set of rational points are of interest since the *height* of a rational point that lies in such a compactly bounded subset may be computed, up to a bounded discrepancy, by considering the *distance* of the rational point from the divisor at infinity *solely at the primes that do not lie over primes of* S.

Thus, in summary, we use the noncritical Belyi maps of [Mzk1] to *"***move** *the rational points over number fields of interest* **away** *from the divisor at infinity at the primes lying over [typically* **archimedean***!] primes of* S*"*. This use of Belyi maps is interesting in that it is reminiscent of the use of Belyi maps in the technique of *"Belyi cuspidalization"* [cf. [Mzk2], §2, §3; [Mzk3], §2; [Mzk4], §3]. That is to say, in the technique of Belyi cuspidalization, "critical" [i.e., more precisely, "not necessarily noncritical"!] Belyi maps are used to *"***move** *rational points* **closer** *to the divisor at infinity at* **nonarchimedean** *primes"* [cf., especially, the theory of [Mzk2], §3].

Theorem 2.1	*Belyi cuspidalization*
uses *noncritical* Belyi maps	uses *critical* Belyi maps
moves rational points of interest *away* from divisor at infinity	*moves* rational points of interest *closer* to divisor at infinity
of interest primarily at *archimedean* primes of a number field	of interest at *nonarchimedean* primes of a number field

In particular, the use of Belyi maps in Theorem 2.1 of the present paper proceeds, so to speak, in the *"opposite direction"* to their use in the theory of Belyi cuspidalization.

Finally, in §3, §4, we examine another example of the notion of being *"arithmetically in general position"*, namely, the phenomenon of *"full Galois actions"* — i.e., Galois actions whose images are equal to either $SL_2(\mathbb{Z}_l)$ or $GL_2(\mathbb{Z}_l)$ — on the l-power torsion points of an elliptic curve over a number field for some prime number l. More precisely, we combine the techniques of [Serre], [Falt] relating *isogenies* and *heights* of elliptic curves over number fields [cf. §3] with some classical analytic number theory involving the *prime number theorem* [cf. §4] to show [cf. Corollaries 4.3, 4.4] that if one considers *elliptic curves* over number fields of bounded degree which are either *"degenerating"* [i.e., admit at least one prime of potentially multiplicative reduction] or *"compactly bounded away from infinity"* [cf. Theorem 2.1], then, with finitely many possible exceptions, one obtains a *"full Galois action"* for *some* prime number l which is roughly of the order of the sum of the *height* of the elliptic curve and *logarithm of the discriminant* of the minimal field of definition of the elliptic curve and, moreover, is *prime* to various numbers that are, in some

sense, *characteristic* to the elliptic curve, such as the *conductor* of the elliptic curve, the rational primes that are *absolutely ramified* in the minimal field of definition of the elliptic curve, and the *local heights* [i.e., the orders of the q-parameter at primes of multiplicative reduction] of the elliptic curve.

Section 1: Generalities on Heights

In the present §1, we review, partly for the purpose of establishing notation and terminology, various well-known facts concerning *arithmetic line bundles* and *heights*.

Let X be a *normal scheme* which is *proper* and *flat* over $\mathrm{Spec}(\mathbb{Z})$ [where $\mathbb{Z}$ denotes the ring of rational integers]. Write $X_{\mathbb{Q}} \stackrel{\text{def}}{=} X \times_{\mathbb{Z}} \mathbb{Q}$ for the *generic fiber* of X; X^{arc} for the *compact normal complex analytic space* determined by X. Thus, the underlying topological space of X^{arc} may be identified with the set of *complex points* $X(\mathbb{C})$, equipped with the topology induced by the topology of $\mathbb{C}$. Note, moreover, that the complex conjugation automorphism $\iota_{\mathbb{C}}$ of $\mathbb{C}$ induces a *complex conjugation automorphism* ι_X of X^{arc} which is compatible with $\iota_{\mathbb{C}}$.

Definition 1.1.

(i) We shall refer to as an *arithmetic line bundle* $\overline{\mathcal{L}} = (\mathcal{L}, |-|_{\mathcal{L}})$ on X any pair consisting of a line bundle $\mathcal{L}$ on X and a hermitian metric $|-|_{\mathcal{L}}$ on the line bundle $\mathcal{L}^{\mathrm{arc}}$ determined by $\mathcal{L}$ on X^{arc} that is compatible [in the evident sense] with the complex conjugation automorphism ι_X. If $\overline{\mathcal{L}} = (\mathcal{L}, |-|_{\mathcal{L}})$, $\overline{\mathcal{M}} = (\mathcal{M}, |-|_{\mathcal{M}})$ are arithmetic line bundles on X, then a *morphism* $\overline{\mathcal{L}} \to \overline{\mathcal{M}}$ is defined to be a morphism of line bundles $\mathcal{L} \to \mathcal{M}$ such that locally on X^{arc}, sections of $\mathcal{L}$ with $|-|_{\mathcal{L}} \leq 1$ map to sections of $\mathcal{M}$ with $|-|_{\mathcal{M}} \leq 1$. We define the set $\Gamma(\overline{\mathcal{L}})$ of *global sections of* $\overline{\mathcal{L}} = (\mathcal{L}, |-|_{\mathcal{L}})$ *over* X to be the set of morphisms $\overline{\mathcal{O}}_X \to \overline{\mathcal{L}}$, where we write $\overline{\mathcal{O}}_X$ for the trivial line bundle $\mathcal{O}_X$ equipped with the trivial hermitian metric. There is an evident notion of *tensor product* of arithmetic line bundles on X. The isomorphism classes of arithmetic line bundles on X, together with the operation of tensor product, thus determine a *group* $\mathrm{APic}(X)$.

(ii) Let $\phi : Y \to X$ be a morphism of normal, $\mathbb{Z}$-proper, $\mathbb{Z}$-flat schemes. Then there is an evident notion of *pull-back of arithmetic line bundles* by ϕ. If $\overline{\mathcal{L}}$ is an arithmetic line bundle on X, then we shall denote its pull-back to Y by the notation $\phi^*\overline{\mathcal{L}}$ or, when there is no fear of confusion, $\overline{\mathcal{L}}|_Y$.

Let F be a *number field* [i.e., a finite extension of the rational number field $\mathbb{Q}$], whose *ring of integers* we denote by $\mathcal{O}_F$, and whose *set of valuations* we denote by $\mathbb{V}(F)$. Thus, $\mathbb{V}(F)$ decomposes as a disjoint union $\mathbb{V}(F) = \mathbb{V}(F)^{\mathrm{non}} \bigcup \mathbb{V}(F)^{\mathrm{arc}}$ of *nonarchimedean* and *archimedean* valuations. If $v \in \mathbb{V}(F)$, then we shall write F_v for the *completion* of F at v and $|-|_v : F_v \to \mathbb{R}$ for the real-valued valuation map determined by v. If $v \in \mathbb{V}(F)^{\mathrm{non}}$, then we shall write $\mathrm{ord}_v(-) : F_v \to \mathbb{Z}$ for the order defined by v and q_v for the cardinality of the residue field of F_v.

An *arithmetic divisor* on F is defined to be a finite formal sum

$$\sum_{v \in \mathbb{V}(F)} c_v \cdot v$$

— where $c_v \in \mathbb{Z}$ if $v \in \mathbb{V}(F)^{\mathrm{non}}$ and $c_v \in \mathbb{R}$ if $v \in \mathbb{V}(F)^{\mathrm{arc}}$ [cf. [Szp], §1.1]. Here, if all of the c_v are ≥ 0, then we shall say that the arithmetic divisor is *effective*. Thus, the arithmetic divisors on F naturally form a group $\mathrm{ADiv}(F)$. If $f \in F$, then the assignment

$$f \mapsto \mathrm{ADiv}(f) \stackrel{\mathrm{def}}{=} \sum_{v \in \mathbb{V}(F)^{\mathrm{non}}} \mathrm{ord}_v(f) \cdot v - \sum_{v \in \mathbb{V}(F)^{\mathrm{arc}}} [F_v : \mathbb{R}] \cdot \log(|f|_v) \cdot v$$

[where log denotes the natural logarithm] determines an element $\in \mathrm{ADiv}(F)$, which we shall refer to as the *principal* arithmetic divisor associated to f. Thus, the principal arithmetic divisors determine a subgroup $\mathrm{APrc}(F) \subseteq \mathrm{ADiv}(F)$. Moreover, as is well-known, there is a *natural isomorphism*

$$\mathrm{ADiv}(F)/\mathrm{APrc}(F) \stackrel{\sim}{\to} \mathrm{APic}(\mathrm{Spec}(\mathcal{O}_F))$$

— cf. [Szp], Proposition 1.1. In particular, the *degree* map

$$\deg_F : \mathrm{ADiv}(F)/\mathrm{APrc}(F) \to \mathbb{R}$$

defined by sending

$$\mathbb{V}(F)^{\mathrm{non}} \ni v \mapsto \log(q_v); \quad \mathbb{V}(F)^{\mathrm{arc}} \ni v \mapsto 1$$

[cf. [Szp], §1.1] determines a homomorphism $\mathrm{APic}(\mathrm{Spec}(\mathcal{O}_F)) \to \mathbb{R}$, which we shall also denote by $\deg_F$. When there is no fear of confusion, we shall also regard [by abuse of notation] $\deg_F$ as a map defined on $\mathrm{ADiv}(F)$. Note that if we set $\underline{\deg}_F \stackrel{\mathrm{def}}{=} \frac{1}{[F:\mathbb{Q}]} \cdot \deg_F$, then for any finite extension K of F, it follows that

$$\underline{\deg}_K(\overline{\mathcal{L}}|_{\mathrm{Spec}(\mathcal{O}_K)}) = \underline{\deg}_F(\overline{\mathcal{L}})$$

for any arithmetic line bundle $\overline{\mathcal{L}}$ on $\mathrm{Spec}(\mathcal{O}_F)$. In particular, if $\overline{\mathbb{Q}}$ is an *algebraic closure* of $\mathbb{Q}$, then for any

$$x \in X(\overline{\mathbb{Q}}) = \bigcup_{\overline{\mathbb{Q}} \supseteq F,\ [F:\mathbb{Q}] < \infty} X(F)$$

and any arithmetic line bundle $\overline{\mathcal{M}}$ on X, it makes sense to define

$$\mathrm{ht}_{\overline{\mathcal{M}}}(x) \stackrel{\mathrm{def}}{=} \underline{\deg}_F(x_F^* \overline{\mathcal{M}}) \in \mathbb{R}$$

— where $x_F : \mathrm{Spec}(\mathcal{O}_F) \to X$ is any morphism that gives rise to x.

Definition 1.2.

(i) We shall refer to the function

$$\mathrm{ht}_{\overline{\mathcal{M}}} : X(\overline{\mathbb{Q}}) \to \mathbb{R}$$

as the *height function* associated to the arithmetic line bundle $\overline{\mathcal{M}}$.

(ii) Fix a subset $\mathcal{F} \subseteq X(\overline{\mathbb{Q}})$. If $\alpha, \beta : \mathcal{F} \to \mathbb{R}$ are *functions*, then we shall write

$$\alpha \lesssim_{\mathcal{F}} \beta \text{ (respectively, } \alpha \gtrsim_{\mathcal{F}} \beta;\ \alpha \approx_{\mathcal{F}} \beta)$$

if there exists a ["constant"] $C \in \mathbb{R}$ such that $\beta(x) - \alpha(x) \leq C$ (respectively, $\alpha(x) - \beta(x) \leq C$; $|\alpha(x) - \beta(x)| \leq C$) for all $x \in \mathcal{F}$; we shall omit the subscript $\mathcal{F}$ when there is no fear of confusion. [Thus, $\alpha \approx \beta$ if and only if $\alpha \lesssim \beta$ and $\alpha \gtrsim \beta$.] The relation "$\approx$" clearly defines an equivalence relation on the set of functions $\mathcal{F} \to \mathbb{R}$; we shall refer to an equivalence class relative to this equivalence relation as a(n) *[$\mathcal{F}$-]BD-class* [i.e., *"bounded discrepancy class"*]. The BD-class of α will be denoted by $[\alpha]_{\mathcal{F}}$, or simply $[\alpha]$, when there is no fear of confusion. Finally, we observe that it makes sense to apply the notation "$\gtrsim$", "$\lesssim$", "$\approx$" to BD-classes.

Example 1.3. Various Natural Subsets of the Set of Points. In the notation of the above discussion, we consider various natural examples of subsets "$\mathcal{F} \subseteq X(\overline{\mathbb{Q}})$" as in Definition 1.2, (ii).

(i) If $d \in \mathbb{N} \bigcup \{\infty\}$, then we shall denote by

$$X(\overline{\mathbb{Q}})^{\leq d} \subseteq X(\overline{\mathbb{Q}})$$

the union of the subsets $X(F) \subseteq X(\overline{\mathbb{Q}})$ as F ranges over the number fields such that $[F : \mathbb{Q}] \leq d$ [so $X(\overline{\mathbb{Q}})^{\leq \infty} = X(\overline{\mathbb{Q}})$];

$$X(\overline{\mathbb{Q}})^{=d} \stackrel{\text{def}}{=} X(\overline{\mathbb{Q}})^{\leq d} \backslash X(\overline{\mathbb{Q}})^{\leq d-1} \subseteq X(\overline{\mathbb{Q}})$$

[cf. the discussion in Definition 1.5, (i), below of *"minimal fields of definition"*]. More generally, if $\mathcal{E} \subseteq X(\overline{\mathbb{Q}})$ is any subset, then we shall write $\mathcal{E}^{\leq d} \stackrel{\text{def}}{=} \mathcal{E} \bigcap X(\overline{\mathbb{Q}})^{\leq d}$, $\mathcal{E}^{=d} \stackrel{\text{def}}{=} \mathcal{E} \bigcap X(\overline{\mathbb{Q}})^{=d}$. If $\mathcal{E} \subseteq X(\overline{\mathbb{Q}})$ is a subset such that each $\mathcal{E}^{\leq d}$ [where d ranges over the positive integers] is finite, then we shall say that $\mathcal{E}$ is *Galois-finite*.

(ii) Let us refer to a compact subset of a topological space which is equal to the closure of its interior as a *compact domain*. Let $V \subseteq \mathbb{V}(\mathbb{Q})$ be a *finite subset* that contains $\mathbb{V}(\mathbb{Q})^{\mathrm{arc}}$. For each $v \in V^{\mathrm{arc}} \stackrel{\text{def}}{=} V \bigcap \mathbb{V}(\mathbb{Q})^{\mathrm{arc}}$ (respectively, $v \in V^{\mathrm{non}} \stackrel{\text{def}}{=} V \bigcap \mathbb{V}(\mathbb{Q})^{\mathrm{non}}$), let

$$\mathcal{K}_v \subseteq X^{\mathrm{arc}} \text{ (respectively, } \mathcal{K}_v \subseteq X(\overline{\mathbb{Q}}_v))$$

be a nonempty ι_X-stable *compact domain* (respectively, a nonempty $\mathrm{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v)$-stable subset whose intersection with each $X(K) \subseteq X(\overline{\mathbb{Q}}_v)$, for $K \subseteq \overline{\mathbb{Q}}_v$ a finite

extension of $\mathbb{Q}_v$, is a *compact domain* in $X(K)$) such that $\mathcal{K}_v \neq X^{\mathrm{arc}}$ (respectively, $\mathcal{K}_v \neq X(\overline{\mathbb{Q}}_v)$). Then let us write

$$\mathcal{K}_V \subseteq X(\overline{\mathbb{Q}})$$

for the subset of points $x \in X(F) \subseteq X(\overline{\mathbb{Q}})$, where $[F : \mathbb{Q}] < \infty$, such that for each $v \in V^{\mathrm{arc}}$ (respectively, $v \in V^{\mathrm{non}}$), the set of $[F : \mathbb{Q}]$ points of X^{arc} (respectively, $X(\mathbb{Q}_v)$) determined by x is contained in $\mathcal{K}_v$. We shall refer to a subset $X(\overline{\mathbb{Q}})$ obtained [i.e., as a "$\mathcal{K}_V$"] in this fashion as a *compactly bounded subset*, to V as the *support* of the compactly bounded subset, and to the "$\mathcal{K}_v$" as the *bounding domains* of the compactly bounded subset. Note that by applying well-known *approximation* results in elementary number theory, it follows immediately [cf. the definition given above of the term "compact domain"!] that the bounding domains of a compactly bounded subset of $X(\overline{\mathbb{Q}})$, hence also the support of a compactly bounded subset of $X(\overline{\mathbb{Q}})$, are *completely determined* by the compactly bounded subset itself.

Proposition 1.4. (Basic Properties of Heights) *In the notation of the above discussion, let* $\overline{\mathcal{L}} = (\mathcal{L}, |-|_{\mathcal{L}})$, $\overline{\mathcal{M}} = (\mathcal{M}, |-|_{\mathcal{M}})$ *be* **arithmetic line bundles** *on* X. *Write* $\mathcal{L}_{\mathbb{Q}} \stackrel{\mathrm{def}}{=} \mathcal{L}|_{X_{\mathbb{Q}}}$, $\mathcal{M}_{\mathbb{Q}} \stackrel{\mathrm{def}}{=} \mathcal{M}|_{X_{\mathbb{Q}}}$. *Then:*

(i) We have

$$\mathrm{ht}_{\overline{\mathcal{L}}\otimes\overline{\mathcal{M}}}(x) = \mathrm{ht}_{\overline{\mathcal{L}}}(x) + \mathrm{ht}_{\overline{\mathcal{M}}}(x)$$

for $x \in X(\overline{\mathbb{Q}})$.

(ii) If some positive tensor power of the line bundle $\mathcal{L}_{\mathbb{Q}}$ *on* $X_{\mathbb{Q}}$ *is* **generated by global sections** *[for instance, if the line bundle* $\mathcal{L}_{\mathbb{Q}}$ *is* **ample***], then*

$$\mathrm{ht}_{\overline{\mathcal{L}}} \gtrsim 0$$

[i.e., where "$\gtrsim$*" denotes "*$\gtrsim_{X(\overline{\mathbb{Q}})}$*"].*

(iii) The **BD-class** *of* $\mathrm{ht}_{\overline{\mathcal{L}}}$ *depends only on the* **isomorphism class** *of the line bundle* $\mathcal{L}_{\mathbb{Q}}$ *on* $X_{\mathbb{Q}}$. *In particular, it makes sense to write* $[\mathrm{ht}_{\mathcal{L}}]$ *or* $[\mathrm{ht}_{\mathcal{L}_{\mathbb{Q}}}]$ *for the BD-class* $[\mathrm{ht}_{\overline{\mathcal{L}}}]$ *of* $\mathrm{ht}_{\overline{\mathcal{L}}}$.

(iv) Let d *be a positive integer,* $C \in \mathbb{R}$. *Suppose further that the line bundle* $\mathcal{L}_{\mathbb{Q}}$ *is* **ample** *on* $X_{\mathbb{Q}}$. *Then the set of points* $x \in X(\overline{\mathbb{Q}})^{\leq d}$ *[cf. Example 1.3, (i)] such that* $\mathrm{ht}_{\overline{\mathcal{L}}}(x) \leq C$ *is* **finite**.

Proof. Assertion (i) follows immediately from the definitions. Next, we consider assertion (ii). To verify assertion (ii), it suffices to show that if $s \in \Gamma(X_{\mathbb{Q}}, \mathcal{L}_{\mathbb{Q}})$, and we write $\mathcal{F} \subseteq X(\overline{\mathbb{Q}})$ for the subset of points at which s is *nonzero*, then $\mathrm{ht}_{\overline{\mathcal{L}}} \gtrsim_{\mathcal{F}} 0$. Now observe that if $\overline{\mathcal{M}}$ is an arithmetic line bundle that arises [by pull-back to X] from an arithmetic line bundle on $\mathrm{Spec}(\mathbb{Z})$, then

$$\mathrm{ht}_{\overline{\mathcal{L}}\otimes\overline{\mathcal{M}}} \approx_{X(\overline{\mathbb{Q}})} \mathrm{ht}_{\overline{\mathcal{L}}}$$

[cf. assertion (i)]. Moreover, for a suitable choice of $\overline{\mathcal{M}}$ arising from an arithmetic line bundle on $\mathrm{Spec}(\mathbb{Z})$, the section s determines a section t of $\mathcal{L}_{\mathbb{Q}} \otimes \mathcal{M}_{\mathbb{Q}}$ that extends to a section of $\mathcal{L} \otimes \mathcal{M}$ over X such that $|t|_{\mathcal{L}\otimes\mathcal{M}} \leq 1$ on X^{arc} [where we recall that X^{arc} is *compact*!]. Thus, by replacing $\overline{\mathcal{L}}$ by $\overline{\mathcal{L}} \otimes \overline{\mathcal{M}}$ and s by t, we may assume that s determines a section of $\mathcal{L}$ over X and that $|s|_{\mathcal{L}} \leq 1$ on X^{arc}. Now the fact that $\mathrm{ht}_{\overline{\mathcal{L}}}(x) \geq 0$ for all $x \in \mathcal{F}$ is immediate from the definitions. This completes the proof of assertion (ii). Next, to verify assertion (iii), it suffices to apply assertions (i), (ii) to the arithmetic line bundle $\overline{\mathcal{L}} \otimes \overline{\mathcal{M}}^{-1}$ in the situation where $\mathcal{L}_{\mathbb{Q}} \cong \mathcal{M}_{\mathbb{Q}}$.

Finally, we consider assertion (iv). A proof of this well-known fact may, essentially, be found in [Silv1] [cf. [Silv1], Theorem 2.1]. From the point of view of the present discussion, an argument may be given as follows: First, we observe that [some positive tensor power of] the ample line bundle $\mathcal{L}_{\mathbb{Q}}$ yields an embedding $\epsilon_{\mathbb{Q}} : X_{\mathbb{Q}} \subseteq P_{\mathbb{Q}}$, where $P = \mathbb{P}^n_{\mathbb{Z}}$ is a projective space over $\mathbb{Z}$. Next, by blowing up X in an appropriate fashion, we conclude that there exists a normal, $\mathbb{Z}$-proper, $\mathbb{Z}$-flat scheme Y, together with morphisms $\phi : Y \to X$, $\psi : Y \to P$ such that $\phi_{\mathbb{Q}}$ is an isomorphism, and $\psi_{\mathbb{Q}} = \epsilon_{\mathbb{Q}} \circ \phi_{\mathbb{Q}}$. Thus, to verify assertion (iv) for the pair $(X, \overline{\mathcal{L}})$, it suffices to verify assertion (iv) for the pair $(Y, \phi^*\overline{\mathcal{L}})$, which, by assertion (iii), is equivalent to assertion (iv) for the pair $(Y, \psi^*\overline{\mathcal{L}}_P)$, where we write $\overline{\mathcal{L}}_P$ for the line bundle $\mathcal{O}_P(1)$ equipped with the standard Fubini-Study metric. But assertion (iv) for the pair $(Y, \psi^*\overline{\mathcal{L}}_P)$ follows from assertion (iv) for the pair $(P, \overline{\mathcal{L}}_P)$. Thus, we may assume that $(X, \overline{\mathcal{L}}) = (P, \overline{\mathcal{L}}_P)$.

Next, observe that since any finite set of points of a fiber of $P \to \mathrm{Spec}(\mathbb{Z})$ is contained in the complement of a hypersurface, it follows immediately that, for any positive integer $e \leq d$, the product $P \times \ldots \times P$ of e copies of P [over $\mathbb{Z}$] admits a [necessarily normal, $\mathbb{Z}$-proper, and $\mathbb{Z}$-flat] *quotient* Q by the action of the symmetric group on e letters, and that some positive tensor power of the tensor product of the pull-backs of $\overline{\mathcal{L}}_P$ by the various projections $P \times \ldots \times P \to P$ descends to an arithmetic line bundle $\overline{\mathcal{L}}_Q = (\mathcal{L}_Q, |-|_{\mathcal{L}_Q})$ on Q such that $(\mathcal{L}_Q)_{\mathbb{Q}}$ is ample on $Q_{\mathbb{Q}}$. Since each point $x_P \in P(F)$ for F such that $[F : \mathbb{Q}] = e$ determines [by considering the various $\mathbb{Q}$-conjugates of x_P] a point $x_Q \in Q(\mathbb{Q})$ [which, in turn, determines x_P, up to a finite number of possibilities], we thus conclude [by varying e] that it suffices to verify that the set of points of $y \in Q(\mathbb{Q})$ such that $\mathrm{ht}_{\overline{\mathcal{L}}_Q}(y) \leq C$ is finite. Moreover, by embedding Q via $(\mathcal{L}_Q)_{\mathbb{Q}}$ into some projective space $Z = \mathbb{P}^m_{\mathbb{Z}}$ as in the argument of the preceding paragraph, we thus conclude that it suffices to verify that the set of points of $z \in Z(\mathbb{Q})$ such that $\mathrm{ht}_{\overline{\mathcal{L}}_Z}(z) \leq C$ is finite, where $\overline{\mathcal{L}}_Z$ is given by $\mathcal{O}_Z(1)$ equipped the standard Fubini-Study metric.

Next, let us observe that [as is easily verified] there exists a *unique* arithmetic line bundle $\overline{\mathcal{L}}_S$ on $S \stackrel{\mathrm{def}}{=} \mathrm{Spec}(\mathbb{Z})$, up to isomorphism, of degree [i.e., "$\deg_{\mathbb{Q}}$"] C; moreover, any arithmetic line bundle on S of degree $\leq C$ *embeds* into $\overline{\mathcal{L}}_S$. In particular, by applying such an embedding, we conclude that given any point $z \in Z(\mathbb{Q}) = Z(S)$ such that $\mathrm{ht}_{\overline{\mathcal{L}}_Z}(z) \leq C$, the $m+1$ standard generating sections of $\mathcal{L}_Z$ restrict, via the morphism $S \to Z$ determined by z, to sections $\in \Gamma(\overline{\mathcal{L}}_S)$. Since [as is easily verified] $\Gamma(\overline{\mathcal{L}}_S)$ is a *finite set*, it thus follows that there is only a *finite number of possibilities* for the projective coordinates of z. This completes the proof of assertion (iv). $\bigcirc$

Remark 1.4.1. Observe that it follows immediately from the definitions, together with Proposition 1.4, (iii), that the theory of *"BD-classes of height functions* $\mathrm{ht}_{\overline{\mathcal{L}}}(-)$ *on* $X(\overline{\mathbb{Q}})$*"* in fact depends *only on the scheme* $X_{\mathbb{Q}}$. In particular, this theory may be applied to any *normal, projective scheme* Y *over* $\mathbb{Q}$ [i.e., by regarding Y as the "$X_{\mathbb{Q}}$" determined by some $\mathbb{Z}$-flat, $\mathbb{Z}$-projective model "X" of Y that arises from a projective embedding of Y].

Definition 1.5.

(i) Note if $x \in X(F) \subseteq X(\overline{\mathbb{Q}})$, where $[F : \mathbb{Q}] < \infty$, then by considering the scheme-theoretic image of the corresponding morphism $\mathrm{Spec}(F) \to X$, one obtains a well-defined *minimal field of definition* $F_{\min} \subseteq F$ of x. In particular, it makes sense to say that F *"is a minimal field of definition of* x*"* [i.e., that $F = F_{\min}$].

(ii) Let $E \subseteq Z$ be an *effective Cartier divisor* contained in the regular locus of a normal noetherian scheme Z. Then observe that the closed subscheme $E_{\mathrm{red}} \subseteq Z$ is also an effective Cartier divisor. We shall say that E is *reduced* if $E = E_{\mathrm{red}}$.

(iii) Let $x \in X(F) \subseteq X(\overline{\mathbb{Q}})$, where F is a *minimal field of definition* of x. Then the *different ideal* of F determines an *effective arithmetic divisor*

$$\delta_x \in \mathrm{ADiv}(F)$$

which is supported in $\mathbb{V}(F)^{\mathrm{non}}$. In particular, the assignment

$$X(\overline{\mathbb{Q}}) \ni x \mapsto \text{log-diff}_X(x) \stackrel{\mathrm{def}}{=} \underline{\deg}_F(\delta_x) \in \mathbb{R}$$

determines a well-defined *log-different function* log-diff_X on $X(\overline{\mathbb{Q}})$.

(iv) Fix an *effective Cartier divisor* $D \subseteq X$; write $U_X \stackrel{\mathrm{def}}{=} X \backslash D$. Let $x \in U_X(F) \subseteq U_X(\overline{\mathbb{Q}})$, where F is a *minimal field of definition* of x [regarded as a point of $X(\overline{\mathbb{Q}})$]. Then the morphism $\mathrm{Spec}(\mathcal{O}_F) \to X$ determined by x [where we recall that X is *proper*!] allows one to pull-back the divisor D to $\mathrm{Spec}(\mathcal{O}_F)$ so as to obtain an *effective divisor* D_x on $\mathrm{Spec}(\mathcal{O}_F)$. Note that D_x, $(D_x)_{\mathrm{red}}$ may also be regarded as *arithmetic divisors* $\in \mathrm{ADiv}(F)$ that are supported in $\mathbb{V}(F)^{\mathrm{non}}$. We shall refer to

$$\mathfrak{f}_x^D \stackrel{\mathrm{def}}{=} (D_x)_{\mathrm{red}} \in \mathrm{ADiv}(F)$$

as the *conductor of* x. Thus, the assignment

$$X(\overline{\mathbb{Q}}) \ni x \mapsto \text{log-cond}_D(x) \stackrel{\mathrm{def}}{=} \underline{\deg}_F(\mathfrak{f}_x^D) \in \mathbb{R}$$

determines a well-defined *log-conductor function* log-cond_D on $U_X(\overline{\mathbb{Q}}) \subseteq X(\overline{\mathbb{Q}})$.

Remark 1.5.1. In the spirit of Remark 1.4.1, we observe that the *log-different function* log-diff_X on $X(\overline{\mathbb{Q}})$ [cf. Definition 1.5, (iii)] depends *only on the scheme* $X_{\mathbb{Q}}$. On the other hand, although the *log-conductor function* log-cond_D on $U_X(\overline{\mathbb{Q}})$

[cf. Definition 1.5, (iv)] may depend on the pair of $\mathbb{Z}$-schemes (X, D), one verifies immediately that the *BD-class* of log-cond_D on $U_X(\overline{\mathbb{Q}})$ depends *only on the pair of* $\mathbb{Q}$*-schemes* $(X_{\mathbb{Q}}, D_{\mathbb{Q}})$. Indeed, this follows immediately from the observation that if (X', D') is another pair [i.e., consisting of an effective Cartier divisor D' in a normal, $\mathbb{Z}$-proper, $\mathbb{Z}$-flat scheme X'], then any isomorphism $X'_{\mathbb{Q}} \xrightarrow{\sim} X_{\mathbb{Q}}$ that induces an isomorphism $D'_{\mathbb{Q}} \xrightarrow{\sim} D_{\mathbb{Q}}$ *extends*, for some *finite set of prime numbers* Σ, to an isomorphism $X' \times_{\mathbb{Z}} \mathbb{Z}[\Sigma^{-1}] \xrightarrow{\sim} X \times_{\mathbb{Z}} \mathbb{Z}[\Sigma^{-1}]$ that induces an isomorphism $D' \times_{\mathbb{Z}} \mathbb{Z}[\Sigma^{-1}] \xrightarrow{\sim} D \times_{\mathbb{Z}} \mathbb{Z}[\Sigma^{-1}]$ — where we write $\mathbb{Z}[\Sigma^{-1}] \stackrel{\text{def}}{=} \mathbb{Z}[\{p^{-1}\}_{p \in \Sigma}]$.

Proposition 1.6. (Conductor Bounded by the Height) *Let $D \subseteq X$ be an* **effective Cartier divisor**, *$\overline{\mathcal{L}} = (\mathcal{L}, |-|_{\mathcal{L}})$ an* **arithmetic line bundle** *on X such that $\mathcal{L} = \mathcal{O}_X(D)$. Write $U \stackrel{\text{def}}{=} X \backslash D$, $\text{ht}_D \stackrel{\text{def}}{=} \text{ht}_{\overline{\mathcal{L}}}$ [cf. Proposition 1.4, (iii)]. Then*

$$\text{log-cond}_D \lesssim \text{ht}_D$$

on $U(\overline{\mathbb{Q}})$.

Proof. Write $s \in \Gamma(X, \mathcal{L})$ for the section determined by the *tautological inclusion* $\mathcal{O}_X \hookrightarrow \mathcal{O}_X(D)$. Then the asserted inequality $\text{log-cond}_D \lesssim \text{ht}_{\overline{\mathcal{L}}}$ follows, for the contributions at the *nonarchimedean* primes, from the definition of log-cond_D [i.e., involving "$(-)_{\text{red}}$"] in Definition 1.5, (iv), and, for the contributions at the *archimedean* primes, from the fact that the continuous function $|s|_{\mathcal{L}}$ on the *compact* topological space X^{arc} is *bounded*. ◯

Proposition 1.7. (Conductors and Log Differents) *Let*

$$\phi : Y \to Z$$

be a generically finite morphism of normal, $\mathbb{Z}$-proper, $\mathbb{Z}$-flat schemes of dimension two. [Thus, the induced morphism on generic fibers $\phi_{\mathbb{Q}} : Y_{\mathbb{Q}} \to Z_{\mathbb{Q}}$ is a **finite** *[possibly]* **ramified covering of smooth, proper curves** *over finite extensions of $\mathbb{Q}$.] Let e be a positive integer;*

$$D \subseteq Y; \quad E \subseteq Z$$

effective, $\mathbb{Z}$-flat Cartier divisors such that the generic fibers $D_{\mathbb{Q}}$, $E_{\mathbb{Q}}$ satisfy the following conditions: (a) $D_{\mathbb{Q}}$, $E_{\mathbb{Q}}$ are **reduced***; (b) $D_{\mathbb{Q}} = \phi_{\mathbb{Q}}^{-1}(E_{\mathbb{Q}})_{\text{red}}$; (c) if we write $U_Y \stackrel{\text{def}}{=} Y \backslash D$, $U_Z \stackrel{\text{def}}{=} Z \backslash E$, then $\phi_{\mathbb{Q}}$ restricts to a finite* **étale** *morphism $(U_Y)_{\mathbb{Q}} \to (U_Z)_{\mathbb{Q}}$; (d) the* **ramification index** *of $\phi_{\mathbb{Q}}$ at each point of $D_{\mathbb{Q}}$* **divides** *e. Then:*

(i) If we restrict functions on $Z(\overline{\mathbb{Q}})$, $U_Z(\overline{\mathbb{Q}})$ to $U_Y(\overline{\mathbb{Q}})$ via ϕ, then

$$\text{log-cond}_E - \text{log-cond}_D \lesssim \text{log-diff}_Y - \text{log-diff}_Z \lesssim \left(1 - \frac{1}{e}\right) \cdot \text{log-cond}_E$$

on $U_Y(\overline{\mathbb{Q}})$.

(ii) Suppose that the **ramification index** *of* $\phi_{\mathbb{Q}}$ *at each point of* $D_{\mathbb{Q}}$ *is* **equal** *to* e. *Then the sheaves of differentials "*$\omega_{(-)}$*" on* $Y_{\mathbb{Q}}$, $Z_{\mathbb{Q}}$ *satisfy the relation*

$$\begin{aligned}\deg(\omega_{Y_{\mathbb{Q}}}) &= \deg(\omega_{Y_{\mathbb{Q}}}(D_{\mathbb{Q}})) - \deg(\mathcal{O}_{Y_{\mathbb{Q}}}(D_{\mathbb{Q}})) \\ &= \deg(\omega_{Z_{\mathbb{Q}}}(E_{\mathbb{Q}})|_{Y_{\mathbb{Q}}}) \cdot \left\{1 - \frac{\deg(\mathcal{O}_{Z_{\mathbb{Q}}}(E_{\mathbb{Q}}))}{e \cdot \deg(\omega_{Z_{\mathbb{Q}}}(E_{\mathbb{Q}}))}\right\}\end{aligned}$$

— where we use the notation "$\deg(-)$*" to denote the degree of a line bundle on* $Y_{\mathbb{Q}}$ *or* $Z_{\mathbb{Q}}$.

Proof. First, we consider assertion (i). We begin by observing that there exists a *finite set of prime numbers* Σ such that the *restriction* of $Y \to Z$ to the spectrum of $\mathbb{Z}[\Sigma^{-1}] \stackrel{\text{def}}{=} \mathbb{Z}[\{p^{-1}\}_{p\in\Sigma}]$ is a *finite tamely ramified morphism of smooth, proper families of curves* over finite étale coverings of $\mathrm{Spec}(\mathbb{Z}[\Sigma^{-1}])$. In particular, the *"prime-to-*Σ *portion"* of the inequality "$\text{log-cond}_E - \text{log-cond}_D = \text{log-diff}_Y - \text{log-diff}_Z \leq (1 - e^{-1}) \cdot \text{log-cond}_E$" [i.e., with "$=$" and "$\leq$", not "$\lesssim$"!] follows immediately from the *elementary theory of differents*. Note that the *"portion over* Σ*"* of log-cond_E, log-cond_D is ≈ 0 [cf. Remark 1.5.1], while [again by the elementary theory of differents] the *"portion over* Σ*"* of $\text{log-diff}_Y - \text{log-diff}_Z$ is ≥ 0 [i.e., with "$\geq$", not "$\gtrsim$"!]. Thus, to complete the proof of assertion (i), it suffices to show that the *"portion over* Σ*"* of the quantity $\text{log-diff}_Y - \text{log-diff}_Z$ is *bounded* in $U_Y(\overline{\mathbb{Q}})$. Moreover, by working locally, we reduce immediately to the following elementary *claim*:

> Fix a *prime number* p and a *positive integer* d. Then there exists a positive integer n such that for any *finite Galois extension* L/K of finite extensions of $\mathbb{Q}_p$ with $[L : K] \leq d$, the *different ideal* of L/K contains $p^n \cdot \mathcal{O}_L$ [where we write $\mathcal{O}_L$ for the ring of integers of L].

To verify this *claim*, we reason as follows: By separating the extension $L[\zeta]/K$, where ζ is a primitive p-th root of unity, into a *composite* of wildly ramified and tamely ramified extensions [and observing that if we restrict to *tamely ramified* L/K, then it suffices to take $n = 1$], we reduce immediately to the case of *wildly ramified* L/K such that K contains a *primitive* p*-th root of unity* ζ. Moreover, since $\mathrm{Gal}(L/K)$ is a [necessarily *solvable*!] *p-group* of order $\leq d$, it suffices to consider the case where $[L : K] = p$. Since $\zeta \in K$, it follows immediately from *elementary Kummer theory* that $L = K(\lambda)$ for some $\lambda \in L$ such that $\kappa \stackrel{\text{def}}{=} \lambda^p \in K$. Moreover, by multiplying κ by an element of $(K^\times)^p$, we may assume that κ is a unit multiple of π_K^a, where π_K is a uniformizer of K and a is a nonnegative integer $< p$. In particular, it follows that $\kappa \in \mathcal{O}_K$, but $\kappa \notin p^p \cdot \mathcal{O}_K$, hence that $\mathcal{O}_L \supseteq \lambda \cdot \mathcal{O}_L \supseteq p \cdot \mathcal{O}_L$. On the other hand, since in this case, we have an inclusion of $\mathcal{O}_K$-algebras $\mathcal{O}_K[X]/(X^p - \kappa) \hookrightarrow \mathcal{O}_L$, one computes easily that the different ideal of L/K contains $p \cdot \lambda^{p-1} \cdot \mathcal{O}_L \supseteq p^{1+(p-1)} \cdot \mathcal{O}_L = p^p \cdot \mathcal{O}_L$. This completes the proof of the *claim*, and hence of assertion (i). Assertion (ii) follows immediately from the *Riemann-Hurwitz formula* for ramified coverings of smooth, proper curves. ◯

Section 2: Bounds on Heights

In the present §2, we discuss our *first main result* [cf. Theorem 2.1], to the effect that the so-called Effective Mordell or ABC Conjectures are equivalent to the ABC Conjecture for rational points [over number fields of bounded degree] contained in a fixed *compactly bounded subset* of the set of all rational points [cf. Example 1.3, (ii)]. The technique used in Corollary 2.1 goes back to work of Elkies [cf. [Elkies]; [vF]] and Moret-Bailly and Szpiro [cf. the discussion at the top of [Elkies], p. 106], except that instead of using "arbitrary" Belyi maps, we use *noncritical Belyi maps*, as discussed in [Mzk1].

Theorem 2.1. (Compactly Bounded Subsets and the ABC Conjecture) *Let Σ be a finite set of prime numbers. Then in the terminology of §1 [cf., especially, Definitions 1.2, 1.5; Example 1.3; Remarks 1.4.1, 1.5.1], the following two statements are* **equivalent***:*

(i) **(Effective Mordell/ABC/Vojta Conjecture)** *Let X be a smooth, proper, geometrically connected curve over a number field; $D \subseteq X$ a reduced divisor; $U_X \stackrel{\text{def}}{=} X \backslash D$; d a positive integer; $\epsilon \in \mathbb{R}_{>0}$ a positive real number. Write ω_X for the canonical sheaf on X. Suppose that U_X is a* **hyperbolic curve** *— i.e., that the degree of the line bundle $\omega_X(D)$ is* **positive***. Then the inequality of BD-classes of functions*

$$\mathrm{ht}_{\omega_X(D)} \lesssim (1+\epsilon)(\text{log-diff}_X + \text{log-cond}_D)$$

holds on $U_X(\overline{\mathbb{Q}})^{\leq d}$.

(ii) **(ABC Conjecture for Σ-Supported Compactly Bounded Subsets)** *Let $P \stackrel{\text{def}}{=} \mathbb{P}^1_{\mathbb{Q}}$ be the* **projective line** *over $\mathbb{Q}$; $C \subseteq P$ the divisor consisting of the three points "0", "1", and "∞"; $U_P \stackrel{\text{def}}{=} P \backslash C$; d a positive integer; $\epsilon \in \mathbb{R}_{>0}$ a positive real number; $\mathcal{K}_V \subseteq U_P(\overline{\mathbb{Q}})$ a* **compactly bounded subset** *[i.e., regarded as a subset of $P(\overline{\mathbb{Q}})$ — cf. Example 1.3, (ii)] whose* **support contains** *Σ. Write ω_P for the canonical sheaf on P. Then the inequality of BD-classes of functions*

$$\mathrm{ht}_{\omega_P(C)} \lesssim (1+\epsilon)(\text{log-diff}_P + \text{log-cond}_C)$$

holds on $\mathcal{K}_V \bigcap U_P(\overline{\mathbb{Q}})^{\leq d}$.

Proof. The fact that (i) $\Longrightarrow$ (ii) is immediate from the definitions. Thus, it suffices to verify that (ii) $\Longrightarrow$ (i). Let X, D, U_X, d, ϵ be as in (i). Now it follows immediately from the well-known structure of étale fundamental groups of hyperbolic curves over algebraically closed fields of characteristic zero that for any positive integer e, there exists a *connected finite étale Galois covering $U_Y \to U_X$*, such that if we write Y for the normalization of X in U_Y and $E \stackrel{\text{def}}{=} (D \times_X Y)_{\text{red}} \subseteq Y$, then Y is a *hyperbolic curve*, and, moreover, $Y \to X$ is *ramified at each point of E with ramification index equal to e*. Here, we think of e as a *fixed* number that will be chosen below.

Write $d' \stackrel{\text{def}}{=} d \cdot \deg(Y/X)$. Then I *claim* that to complete the proof of the implication "(ii) $\Longrightarrow$ (i)", it suffices to verify the inequality

$$\text{ht}_{\omega_Y} \ \lesssim \ (1+\epsilon') \cdot \text{log-diff}_Y$$

on $U_Y(\overline{\mathbb{Q}})^{\leq d'}$ for arbitrary $\epsilon' \in \mathbb{R}_{>0}$. Indeed, suppose that this inequality is satisfied for some $\epsilon' \in \mathbb{R}_{>0}$ such that $(1+\epsilon')^2 \leq 1+\epsilon$. Then by choosing appropriate normal, $\mathbb{Z}$-proper, $\mathbb{Z}$-flat models for Y, X, we may apply Proposition 1.7, (i), to conclude that $\text{log-diff}_Y \ \lesssim \ \text{log-diff}_X + \text{log-cond}_D$ on $U_Y(\overline{\mathbb{Q}})^{\leq d'}$; moreover, by Proposition 1.7, (ii), it follows that by choosing e to be *sufficiently large*, we may assume that $\deg(\omega_X(D)|_Y) = \deg(\omega_Y(E)) \leq (1+\epsilon') \cdot \deg(\omega_Y)$. But, by Proposition 1.4, (i), (ii), (iii), this implies that $\text{ht}_{\omega_X(D)} \ \lesssim \ (1+\epsilon') \cdot \text{ht}_{\omega_Y}$ on $U_Y(\overline{\mathbb{Q}})^{\leq d'}$. Thus, we conclude that

$$\begin{aligned} \text{ht}_{\omega_X(D)} \ &\lesssim \ (1+\epsilon') \cdot \text{ht}_{\omega_Y} \ \lesssim \ (1+\epsilon')^2 \cdot \text{log-diff}_Y \\ &\lesssim \ (1+\epsilon')^2 (\text{log-diff}_X + \text{log-cond}_D) \\ &\lesssim \ (1+\epsilon)(\text{log-diff}_X + \text{log-cond}_D) \end{aligned}$$

on $U_Y(\overline{\mathbb{Q}})^{\leq d'}$. Since every point of $U_X(\overline{\mathbb{Q}})^{\leq d}$ clearly lifts to a point of $U_Y(\overline{\mathbb{Q}})^{\leq d'}$, this completes the verification of the *claim*.

Thus, in summary, to complete the proof of Theorem 2.1, it suffices to verify that (ii) implies (i) for data X, D, U_X, d, ϵ as in (i) such that $D = \emptyset$. To this end, let us suppose that the inequality

$$\text{ht}_{\omega_X} \ \lesssim \ (1+\epsilon) \cdot \text{log-diff}_X$$

is *false* on $X(\overline{\mathbb{Q}})^{=d}$. Let $V \subseteq \mathbb{V}(\mathbb{Q})$ be a finite subset that contains $\mathbb{V}(\mathbb{Q})^{\text{arc}}$ and [the subset of $V(\mathbb{Q})^{\text{non}}$ determined by] Σ. Then it follows immediately from the *compactness* of the set of rational points of X over any finite extension of $\mathbb{Q}_v$ for $v \in V$ that there exists a subset $\Xi \subseteq X(\overline{\mathbb{Q}})^{=d}$, together with a(n) [unordered] *d-tuple of points* Ξ_v of $X(\overline{\mathbb{Q}}_v)$ for each $v \in V$, such that the inequality $\text{ht}_{\omega_X} \ \lesssim \ (1+\epsilon) \cdot \text{log-diff}_X$ is *false* on Ξ, and, moreover, the [unordered] d-tuples of $\mathbb{Q}$-conjugates of points $\in \Xi$ *converge*, as [unordered] d-tuples of points of $X(\overline{\mathbb{Q}}_v)$, to Ξ_v. Moreover, by the *main result* of [Mzk1] [cf. [Mzk1], Theorem 2.5], there exists a *"noncritical Belyi map"*

$$\phi : X \to P$$

which is *unramified* over U_P, and, moreover, *"noncritical" at the points of each* Ξ_v [i.e., maps the points of each Ξ_v into $U_P(\overline{\mathbb{Q}}_v)$]. In particular, [after possibly eliminating finitely many elements from Ξ] it follows that there exists a *compactly bounded subset* $\mathcal{K}_V \subseteq U_P(\overline{\mathbb{Q}})$ [i.e., whose bounding domains are the unions of Galois-conjugates of images via ϕ of *sufficiently small compact neighborhoods* of the points of Ξ_v in $X(\overline{\mathbb{Q}}_v)$, for $v \in V$] such that $\phi(\Xi) \subseteq \mathcal{K}_V$.

Now set $E \stackrel{\text{def}}{=} \phi^{-1}(C)_{\text{red}} \subseteq X$ [so $\phi^* \omega_P(C) \cong \omega_X(E)$]. Let $\epsilon' \in \mathbb{R}_{>0}$ be such that the inequality

$$1 + \epsilon' \leq (1+\epsilon) \cdot \Big(1 - \epsilon' \cdot \deg(E)/\deg(\omega_X)\Big)$$

is satisfied. Then by (ii), it follows that $\mathrm{ht}_{\omega_P(C)} \lesssim (1+\epsilon')(\text{log-diff}_P + \text{log-cond}_C)$ on $\phi(\Xi)$. On the other hand, by choosing appropriate normal, $\mathbb{Z}$-proper, $\mathbb{Z}$-flat models for P, X, we may apply Proposition 1.7, (i) [where we take "e" to be 1], to conclude that $\text{log-diff}_P + \text{log-cond}_C \lesssim \text{log-diff}_X + \text{log-cond}_E$ on Ξ. Also, we recall from Proposition 1.6 that $\text{log-cond}_E \lesssim \mathrm{ht}_E \stackrel{\text{def}}{=} \mathrm{ht}_{\mathcal{O}_X(E)}$ on Ξ. Thus, by Proposition 1.4, (i), (iii), we compute to find that

$$\begin{aligned}
\mathrm{ht}_{\omega_X} &\approx \mathrm{ht}_{\omega_X(E)} - \mathrm{ht}_E \approx \mathrm{ht}_{\omega_P(C)} - \mathrm{ht}_E \\
&\lesssim (1+\epsilon')(\text{log-diff}_P + \text{log-cond}_C) - \mathrm{ht}_E \\
&\lesssim (1+\epsilon')(\text{log-diff}_X + \text{log-cond}_E) - \mathrm{ht}_E \\
&\lesssim (1+\epsilon')(\text{log-diff}_X + \mathrm{ht}_E) - \mathrm{ht}_E \approx (1+\epsilon') \cdot \text{log-diff}_X + \epsilon' \cdot \mathrm{ht}_E \\
&\approx (1+\epsilon') \cdot \text{log-diff}_X + \epsilon' \cdot (\deg(E)/\deg(\omega_X)) \cdot \mathrm{ht}_{\omega_X}
\end{aligned}$$

on Ξ, i.e., that $\mathrm{ht}_{\omega_X} \lesssim (1+\epsilon) \cdot \text{log-diff}_X$ on Ξ — in contradiction to our hypothesis on Ξ. This completes the proof of Theorem 2.1. ◯

Section 3: Full Special Linear Galois Actions on Torsion Points

In the present §3, we give *various conditions on a prime l* that ensure that *the image of the Galois representation* on the l-power torsion points of an elliptic curve over a number field is *"rather large"* [cf. Theorem 3.8]. In particular, we show that if one considers *elliptic curves over number fields of bounded degree* that have at least one [nonarchimedean] prime of *potentially* [bad] *multiplicative reduction*, then, if one excludes finitely many exceptional elliptic curves, it holds that *for any prime number l of the order of the height of the elliptic curve, the image of the associated Galois representation in $GL_2(\mathbb{Z}_l)$ contains $SL_2(\mathbb{Z}_l)$*. Here, the condition of having at least one prime of potentially multiplicative reduction *holds automatically*, with finitely many exceptions, if one restricts oneself to elliptic curves arising from points of the moduli stack of elliptic curves that are contained in some *compactly bounded subset* of the set of all points. In particular, for such a prime number l, *the elliptic curve will not have any rational torsion points of order l*. Thus, this result may be regarded as a sort of "poor man's uniform boundedness conjecture" — now Merel's theorem [cf. [Merel]] – although, in fact, it is not strictly implied by Merel's theorem. Alternatively, it may be regarded as an effective version of a theorem of Serre [cf. [Serre], Chapter IV, Theorem 3.2]. The proof is similar to that of Faltings' proof of the Tate Conjecture [cf. [Falt]], only technically much simpler. That is to say, the main technique is essentially the standard one, going back to Tate, for proving "Tate conjecture-type results".

We begin by reviewing various well-known facts concerning the structure of $SL_2(\mathbb{F}_l)$, $SL_2(\mathbb{Z}_l)$, for l a prime number ≥ 5.

Lemma 3.1. (The Structure of SL_2) *Let $l \geq 5$ be a prime number. Then:*

(i) Let $G \subseteq SL_2(\mathbb{F}_l)$ be the subgroup generated by the matrices $\alpha \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\beta \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Then $G = SL_2(\mathbb{F}_l)$.

(ii) The finite group $SL_2(\mathbb{F}_l)$ has no nontrivial abelian quotients.

(iii) Let $H \subseteq GL_2(\mathbb{F}_l)$ be a subgroup that contains the matrix $\alpha \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, as well as at least one matrix that is not upper triangular. Then $SL_2(\mathbb{F}_l) \subseteq H$.

(iv) Let $J \subseteq GL_2(\mathbb{Z}_l)$ be a closed subgroup whose image H_J in $GL_2(\mathbb{F}_l)$ contains the matrix $\alpha \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, as well as a matrix which is not upper triangular. Then $SL_2(\mathbb{Z}_l) \subseteq J$.

Proof. First, we consider assertion (i). Note that if $\mu, \lambda \in \mathbb{F}_l$, then $\beta^{\mu} \cdot \alpha^{\lambda}$ [where we observe that this expression makes sense since both α^l and β^l are equal to the identity matrix] takes the vector $v \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} \lambda \\ \mu \cdot \lambda + 1 \end{smallmatrix}\right)$. Thus, if we let $\gamma \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, then for any $\lambda \in \mathbb{F}_l^{\times}$, there exists a $g_{\lambda} \in G$ such that $\lambda \cdot \gamma \cdot v = \left(\begin{smallmatrix} \lambda \\ 0 \end{smallmatrix}\right) = g_{\lambda} \cdot v$. In particular, we have $\lambda \cdot g_1 \cdot v = \lambda \cdot \gamma \cdot v = g_{\lambda} \cdot v$, so $\lambda \cdot v \in G \cdot v$. Thus, in summary, we have proven that $(\mathbb{F}_l \times \mathbb{F}_l) - \{\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)\} \subseteq G \cdot v$. Now let us prove that an arbitrary element $\delta \in SL_2(\mathbb{F}_l)$ is contained in G. By the conclusion of the above argument, we may assume that $\delta \cdot v = v$. But this implies that δ is a lower triangular matrix all of whose diagonal entries are equal to 1. Thus, δ is a power of β, hence contained in G, as desired. This completes the proof of assertion (i).

Next, we consider assertion (ii). Let $\lambda \in \mathbb{F}_l^{\times}$ be such that $\lambda^2 \neq 1$. [Note that such a λ exists since $l \geq 5$.] Let $\epsilon \stackrel{\text{def}}{=} \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$. Then $\epsilon \cdot \alpha \cdot \epsilon^{-1} \cdot \alpha^{-1} = \alpha^{\lambda^2 - 1}$. Thus, α (and, similarly, β) is contained in the commutator subgroup of $SL_2(\mathbb{F}_l)$, so assertion (ii) follows from assertion (i). This completes the proof of assertion (ii).

Next, we consider assertion (iii). Note that α generates an l-Sylow subgroup S of $GL_2(\mathbb{F}_l)$, and that the number of l-Sylow subgroups of $GL_2(\mathbb{F}_l)$ is precisely $l + 1$. Since the normalizer of S in $GL_2(\mathbb{F}_l)$ is the set of upper triangular matrices, and we have assumed that H contains at least one non-upper triangular matrix, it follows that the number n_H of l-Sylow subgroups of H is ≥ 2. On the other hand, by the general theory of Sylow subgroups, it follows that n_H is congruent to 1 modulo l. Since $2 \leq n_H \leq l + 1$, we thus obtain that $n_H = l + 1$. In particular, in the notation of assertion (i), we conclude that $\alpha, \beta \in H$. Thus, by assertion (i), we have $SL_2(\mathbb{F}_l) \subseteq H$, as desired. This completes the proof of assertion (iii).

Finally, we consider assertion (iv). By assertion (iii), we have that $SL_2(\mathbb{F}_l) \subseteq H_J$. Let $J' \subseteq SL_2(\mathbb{Z}_l)$ be the closure of the commutator subgroup of J. Thus, by assertion (ii), J' surjects onto $SL_2(\mathbb{F}_l)$. Now by [Serre], Chapter IV, §3.4, Lemma 3, this implies that $SL_2(\mathbb{Z}_l) = J' \subseteq J$, as desired. This completes the proof of assertion (iv). $\bigcirc$

Next, we consider the *local theory at nonarchimedean primes*. Let K be a finite extension of $\mathbb{Q}_p$ [where p is a prime number] with residue field k, maximal ideal $\mathfrak{m}_K \subseteq \mathcal{O}_K$, and *valuation map* $v_K : K^{\times} \to \mathbb{Z}$ [which we normalize so that v_K

is *surjective*]; $\overline{K}$ an algebraic closure of K; $G_K \stackrel{\text{def}}{=} \mathrm{Gal}(\overline{K}/K)$; $E \to \mathrm{Spec}(\mathcal{O}_K)$ a *one-dimensional semi-abelian scheme* over $\mathcal{O}_K$ such that the generic fiber E_K of E is *proper*, while the special fiber E_k of E is isomorphic to $(\mathbb{G}_{\mathrm{m}})_k$, the multiplicative group over k.

Let l be a *prime number* [possibly equal to p]; write

$$M_l(E) \stackrel{\text{def}}{=} \mathrm{Hom}(\mathbb{Z}/l \cdot \mathbb{Z}, E(\overline{K}))$$

for the *"mod l" Tate module* of E_K. Thus, $M_l(E)$ is [noncanonically!] isomorphic as an $\mathbb{F}_l$-module to $\mathbb{F}_l \times \mathbb{F}_l$, and, moreover, is equipped with a continuous action by G_K [induced by the natural action of G_K on $\overline{K}$]. Also, it is well-known [cf., e.g., [FC], Chapter III, Corollary 7.3] that $M_l(E)$ fits into a natural exact sequence of G_K-modules

$$0 \to \mathbb{F}_l(1) \to M_l(E) \to \mathbb{F}_l \to 0$$

— where the "(1)" is a Tate twist, and "$\mathbb{F}_l$" is equipped with the trivial Galois action. Moreover, the extension class associated to this exact sequence is precisely that obtained by extracting an l-th root of the *Tate parameter* $q_E \in \mathfrak{m}_K$. The Tate parameter is an element of $\mathfrak{m}_K$ that is naturally associated to E and has the property that the subscheme $\mathcal{O}_K/(q_E)$ is equal to the pull-back via the classifying morphism $\mathrm{Spec}(\mathcal{O}_K) \to \overline{\mathcal{M}}_{\mathrm{ell}}$ — where we write $\overline{\mathcal{M}}_{\mathrm{ell}}$ for the *moduli stack of one-dimensional semi-abelian varieties* over $\mathbb{Z}$ — of the divisor at infinity $\infty_{\mathcal{M}} \subseteq \overline{\mathcal{M}}_{\mathrm{ell}}$. Thus, the above exact sequence splits if and only if q_E has an l-th root in K. Note that in order for this to happen, it is necessary that $v_K(q_E)$ be *divisible by l*. In particular, we have the following well-known result.

Lemma 3.2. (Local Rank One Subgroups of l-Torsion)

(i) Let

$$N \subseteq M_l(E)$$

be a one-dimensional $\mathbb{F}_l$-subspace which is **stabilized** *by G_K. Then* **either** $v_K(q_E) \in l \cdot \mathbb{Z}$, **or** N *is equal to the submodule $\mathbb{F}_l(1) \subseteq M_l(E)$ of the above exact sequence.*

(ii) The submodule $\mathbb{F}_l(1) \subseteq M_l(E)$ of the above exact sequence defines a finite, flat subgroup scheme $\boldsymbol{\mu}_l \subseteq E$ over $\mathcal{O}_K$, whose quotient we denote by $E' \stackrel{\text{def}}{=} E/\boldsymbol{\mu}_l$. [Thus, $E' \to \mathrm{Spec}(\mathcal{O}_K)$ is a one-dimensional semi-abelian scheme over $\mathcal{O}_K$ whose generic fiber is proper, and whose special fiber is isomorphic to $(\mathbb{G}_{\mathrm{m}})_k$.] The Tate parameter $q_{E'}$ of E' satisfies the relation $q_{E'} = q_E^l$; in particular, we have

$$\deg_\infty(E') = l \cdot \deg_\infty(E)$$

— where we write $\deg_\infty(E) \stackrel{\text{def}}{=} \log(\#(\mathcal{O}_K/(q_E))) \in \mathbb{R}$.

Definition 3.3. We shall refer to the positive integer $v_K(q_E) \in \mathbb{Z}_{>0}$ as the *local height of E* [or E_K].

Remark 3.3.1. Note that even if E_K only has *potentially multiplicative reduction*, one may define the *local height of* E_K as the element $\in \mathbb{Q}$ computed by *dividing* the local height of $E_K \times_K L$ for some finite extension L of K over which E_K has multiplicative reduction by the *ramification index* of L/K [so one verifies immediately that this definition is *independent* of the choice of L].

Next, let $F \subseteq \overline{\mathbb{Q}}$ be a *number field*, $E \to \mathrm{Spec}(\mathcal{O}_F)$ a *one-dimensional semi-abelian variety* whose generic fiber E_F is *proper*. Also, for simplicity, we assume that F is *totally imaginary*. Thus, E_F is an elliptic curve over F. Let us write ω_E for the finite, flat $\mathcal{O}_F$-module of rank one consisting of the *invariant differentials* on E. If $v \in \mathbb{V}(F)^{\mathrm{arc}}$, then we get a natural metric on $(\omega_E)_v \stackrel{\mathrm{def}}{=} (\omega_E) \otimes_F F_v$ by integration: if $\alpha \in (\omega_E)_v$, then

$$|\alpha|^2 \stackrel{\mathrm{def}}{=} \int_{E_v} \alpha \wedge \overline{\alpha}$$

— where $E_v \stackrel{\mathrm{def}}{=} E \times_F F_v$, and $\overline{\alpha}$ is the complex conjugate of α. Thus, by equipping ω_E with this metric at the archimedean places of F, we obtain an *arithmetic line bundle* $\overline{\omega}_E$ on $\mathrm{Spec}(\mathcal{O}_F)$. Let us write

$$\mathrm{ht}^{\mathrm{Falt}}(E) \stackrel{\mathrm{def}}{=} \underline{\deg}_F(\overline{\omega}_E) \in \mathbb{R}$$

for the so-called *Faltings height of the elliptic curve* E.

Next, let us observe that $E \to \mathrm{Spec}(\mathcal{O}_F)$ defines a classifying morphism

$$\phi : \mathrm{Spec}(\mathcal{O}_F) \to \overline{\mathcal{M}}_{\mathrm{ell}}$$

— where we write $\overline{\mathcal{M}}_{\mathrm{ell}}$ for the *moduli stack of one-dimensional semi-abelian varieties* over $\mathbb{Z}$. As is well-known, this stack has a *"divisor at infinity"* $\infty_{\mathcal{M}} \subseteq \overline{\mathcal{M}}_{\mathrm{ell}}$, whose complement $\mathcal{M}_{\mathrm{ell}} \subseteq \overline{\mathcal{M}}_{\mathrm{ell}}$ is the *moduli stack of elliptic curves* over $\mathbb{Z}$. Set

$$\underline{\deg}_\infty(E) \stackrel{\mathrm{def}}{=} \underline{\deg}_F(\infty_E) \in \mathbb{R}$$

— where we write $\infty_E \stackrel{\mathrm{def}}{=} \phi^{-1}(\infty_{\mathcal{M}}) \subseteq \mathrm{Spec}(\mathcal{O}_F)$.

Although the algebraic stack $\overline{\mathcal{M}}_{\mathrm{ell}}$ is *not a scheme*, it is nevertheless normal, $\mathbb{Z}$-proper, and $\mathbb{Z}$-flat. Thus, one verifies immediately that the theory of §1 extends immediately to the case of $\overline{\mathcal{M}}_{\mathrm{ell}}$; in particular, one may consider *functions on subsets of* $\overline{\mathcal{M}}_{\mathrm{ell}}(\overline{\mathbb{Q}})$, *BD-classes of such functions*, and *height functions on* $\overline{\mathcal{M}}_{\mathrm{ell}}(\overline{\mathbb{Q}})$ *associated to arithmetic line bundles on* $\overline{\mathcal{M}}_{\mathrm{ell}}$. Write

$$\mathrm{ht}_\infty$$

for the *BD-class* of height functions determined by the line bundle $\mathcal{O}_{\overline{\mathcal{M}}_{\mathrm{ell}}}(\infty_{\mathcal{M}})$. Also, we observe that if we write $[E] \in \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$ for the isomorphism class determined by E, then we may regard $[E] \mapsto \mathrm{ht}^{\mathrm{Falt}}([E]) \stackrel{\mathrm{def}}{=} \mathrm{ht}^{\mathrm{Falt}}(E)$, $[E] \mapsto \underline{\deg}_\infty([E]) \stackrel{\mathrm{def}}{=} \underline{\deg}_\infty(E)$ as *functions* on $\mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$. Now we have the following well-known result.

Proposition 3.4. (Faltings Heights and the Divisor at Infinity) *For any* $\epsilon \in \mathbb{R}_{>0}$*, we have*

$$\underline{\deg}_\infty \lesssim \mathrm{ht}_\infty \lesssim 12(1+\epsilon)\cdot \mathrm{ht}^{\mathrm{Falt}} \lesssim (1+\epsilon)\cdot \mathrm{ht}_\infty$$

on $\mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$*. In particular, if* $C \in \mathbb{R}$*, then the set of points* $[E] \in \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})^{\leq d}$ *such that* $\mathrm{ht}^{\mathrm{Falt}}([E]) \leq C$ *is* **finite**.

Proof. The first "$\lesssim$" follows immediately from the definitions [cf. the proof of Proposition 1.6]. The remaining "$\lesssim$'s" follows from [Silv2], Proposition 2.1 [cf. also the discussion in the proof of [FC], Chapter V, Proposition 4.5, of the *logarithmic singularities* at infinity of the metric defined on "$\overline{\omega}_E$", as one allows "E" to vary in $\mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$; the proof of [Silv1], Proposition 8.2]. Finally, the *finiteness* assertion follows immediately from the inequalities already shown, together with Proposition 1.4, (iv). ◯

Lemma 3.5. (Global Rank One Subgroups of l-Torsion) *Let* $\epsilon \in \mathbb{R}_{>0}$*;* l *a* **prime number***;* $H_F \subseteq E_F$ *a subgroup scheme such that* $H_F \times_F \overline{\mathbb{Q}}$ *is isomorphic to the constant group scheme determined by* $\mathbb{Z}/l\cdot\mathbb{Z}$*. We shall call such a subgroup scheme* H_F ***l*-cyclic**. *Write* $(E_H)_F \stackrel{\mathrm{def}}{=} E_F/H_F$*. [Thus,* $(E_H)_F$ *is* **isogenous** *to* E_F*, hence has* **semi-stable reduction** *at all the finite primes of* F *and extends to a one-dimensional semi-abelian scheme* $E_H \to \mathrm{Spec}(\mathcal{O}_F)$*.] Suppose further that* l *is* **prime** *to the* **local heights** *of* E *at all of its primes of [bad] multiplicative reduction [a condition that is satisfied, for instance, if* l *is* $>$ *these local heights]. Then we have*

$$\frac{1}{12(1+\epsilon)}\ l\cdot \underline{\deg}_\infty(E) \leq \mathrm{ht}^{\mathrm{Falt}}(E) + 2\ \log(l) + C$$

for some **constant** $C \in \mathbb{R}$ *which [may depend on* ϵ *but] is* **independent** *of* E*,* F*,* H_F*, and* l*.*

Proof. Note that the assumption on l implies, by Lemma 3.2, (i), that at all the primes of multiplicative reduction, H_F corresponds to the subspace $\mathbb{F}_l(1)$ of Lemma 3.2, (i). Thus, at primes of multiplicative reduction, E_H may be identified with the elliptic curve "E'" of Lemma 3.2, (ii). In particular, it follows that $\underline{\deg}_\infty(E_H) = l\cdot \underline{\deg}_\infty(E)$. On the other hand, the degree l covering morphism $E_F \to (E_H)_F$ extends [cf., e.g., [FC], Chapter I, Proposition 2.7] to a morphism $E \to E_H$. Thus, we have a natural inclusion $\omega_{E_H} \subseteq \omega_E$ whose cokernel is annihilated by l. Moreover, since integrating a $(1,1)$-form over E_v differs from integrating over $(E_H)_v$ by a factor of l, we conclude that $\mathrm{ht}^{\mathrm{Falt}}(E_H) = \underline{\deg}(\overline{\omega}_{E_H}) \leq \underline{\deg}(\overline{\omega}_E) + 2\cdot\log(l) = \mathrm{ht}^{\mathrm{Falt}}(E) + 2\cdot\log(l)$. Thus, Lemma 3.5 follows from Proposition 3.4. ◯

Before continuing, we observe the following result.

Lemma 3.6. (An Elementary Estimate) *Let* $\epsilon \in \mathbb{R}_{>0}$*. Then there exists a* **constant** $C_0 \in \mathbb{R}_{>0}$ *such that for all* $x, y \in \mathbb{R}$ *such that* $y \geq 1$ *and* $x \geq C_0 y^{1+\epsilon}$*, it holds that* $x \geq y\cdot\log(x)$*.*

Proof. This follows immediately from the well-known elementary fact that $x^{1/(1+\epsilon)} \cdot \log(x)/x = \log(x) \cdot x^{-\epsilon/(1+\epsilon)} \to 0$ as $x \to \infty$. ◯

Lemma 3.7. (Finite Exceptional Sets) *Let $\mathcal{K}_V \subseteq \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$ be a* **compactly bounded subset**, *$\epsilon \in \mathbb{R}_{>0}$. Then there exists a* **constant** *$C \in \mathbb{R}_{>0}$ and a* **Galois-finite** *[cf. Example 1.3, (i)] subset $\mathfrak{Exc} \subseteq \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$ that satisfy the following property:*

Let E_L be an **elliptic curve** *over a number field L with* **semi-stable reduction** *at all the finite primes of L; $d \stackrel{\mathrm{def}}{=} [L : \mathbb{Q}]$; $[E_L] \in \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$ the point determined by E_L; l a* **prime number**. *Consider the following two conditions on the above data:*

(a) $l \geq 100d \cdot (\mathrm{ht}^{\mathrm{Falt}}([E_L]) + C \cdot d^{\epsilon})$, and E_L has at least **one** *prime of [bad]* **multiplicative** *reduction;*

(b) $[E_L] \in \mathcal{K}_V$, and l is **prime** *to the* **local heights** *of E_L at all of its primes of multiplicative reduction.*

Then if (a) is satisfied, then l is $>$ the **local heights** *of E_L at all the primes of multiplicative reduction. If (b) is satisfied, and $[E_L] \notin \mathfrak{Exc}$, then E_L has at least* **one** *prime of multiplicative reduction. If either (a) or (b) is satisfied, and, moreover, E_L admits an* ***l*-cyclic** *subgroup scheme $H_L \subseteq E_L$, then $[E_L] \in \mathfrak{Exc}$.*

Proof. First, observe that if v is any *local height* of E_L, then $d \cdot \underline{\deg}_{\infty}([E_L]) \geq v \cdot \log(2)$. Next, let us observe that by Proposition 3.4, for an appropriate choice of C, we may assume that $\mathrm{ht}^{\mathrm{Falt}}([E_L]) + C \cdot d^{\epsilon} \geq \mathrm{ht}^{\mathrm{Falt}}([E_L]) + C \geq \frac{1}{14} \cdot \underline{\deg}_{\infty}([E_L])$ [i.e., where we take "$12(1+\epsilon)$" to be 14]. Thus, condition (a) implies that

$$l \;\geq\; \frac{100d}{14} \cdot \underline{\deg}_{\infty}([E_L]) \;\geq\; \Big(\frac{100 \cdot \log(2)}{14}\Big) \cdot v > v$$

— i.e., that l is $>$ the *local heights* of E_L at all the primes of multiplicative reduction. On the other hand, if condition (b) is satisfied, and, moreover E_L has *no primes of multiplicative reduction* [so $\underline{\deg}_{\infty}([E_L]) = 0$], then the fact that $[E_L] \in \mathcal{K}_V$ implies that $\mathrm{ht}_{\infty}([E_L])$ is *bounded* [independently of L, E_L, l], so, by Proposition 1.4, (iv), $[E_L]$ belongs to some [fixed] *finite exceptional set* $\mathfrak{Exc}_d$ [which we think of as $\mathfrak{Exc} \bigcap \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})^{\leq d}$], as desired.

For the remainder of the present proof, let us assume that either (a) or (b) is satisfied [so l is *prime* to the *local heights* of E_L], and that E_L admits an *l-cyclic* subgroup scheme $H_L \subseteq E_L$. Thus, by Lemma 3.5, we conclude that

$$\frac{l}{14} \cdot \underline{\deg}_{\infty}([E_L]) \;\leq\; \mathrm{ht}^{\mathrm{Falt}}([E_L]) + 2 \cdot \log(l) + C' \qquad (\dagger)$$

for some constant $C' \in \mathbb{R}$ [i.e., "C"] as in Lemma 3.5.

Now suppose that *condition (a)* is satisfied. Let C_0 be as in Lemma 3.6. Then let us observe that if we choose C *sufficiently large* [cf. Proposition 3.4] that the inequality of condition (a) implies that $l \geq C_0(\frac{56d}{\log(2)})^{1+\epsilon}$, then by Lemma 3.6 [where we take "x" to be l, and "y" to be $\frac{56d}{\log(2)}$], we conclude that $l \geq \frac{56d\cdot\log(l)}{\log(2)}$, hence that

$$\frac{l}{14}\cdot \underline{\deg}_\infty([E_L]) \;\leq\; \mathrm{ht}^{\mathrm{Falt}}([E_L]) + \frac{l\cdot\log(2)}{28d} + C' \qquad (\ddagger)$$

[i.e., by substituting into (†)]. Now since E_L *has at least one prime of bad reduction*, it follows that $\log(2) \leq d\cdot \underline{\deg}_\infty([E_L])$. Thus, substituting into (‡), we obtain that $\frac{l\cdot\log(2)}{28d} \leq \mathrm{ht}^{\mathrm{Falt}}([E_L]) + C'$. On the other hand, $\frac{\log(2)}{28} \geq \frac{2}{100}$, and, by assumption, $l \geq 100d\cdot \mathrm{ht}^{\mathrm{Falt}}([E_L])$, so, by substituting, we obtain that $2\,\mathrm{ht}^{\mathrm{Falt}}([E_L]) \leq \mathrm{ht}^{\mathrm{Falt}}([E_L]) + C'$, i.e., that $\mathrm{ht}^{\mathrm{Falt}}([E_L]) \leq C'$. But this implies, by Proposition 3.4, that $[E_L]$ belongs to some [fixed] *finite exceptional set* $\mathfrak{Exc}_d$ [which we think of as $\mathfrak{Exc}\bigcap \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})^{\leq d}$], as desired.

Now suppose that *condition (b)* is satisfied. Recall that by definition, $\mathrm{ht}_\infty([E_L])$ may be computed as the sum of $\underline{\deg}_\infty([E_L])$ and an *archimedean term* which, in the present situation, is *bounded*, since $[E_L] \in \mathcal{K}_V$. In particular, by modifying C' — in a fashion that depends on $\mathcal{K}_V$! — and applying Proposition 3.4, we may assume that $\underline{\deg}_\infty([E_L]) \geq \mathrm{ht}_\infty([E_L]) - C' \geq 7\cdot \mathrm{ht}^{\mathrm{Falt}}([E_L]) - 2C'$. Thus, by substituting into (†) [and perhaps modifying C' again], we obtain that

$$\frac{l}{2}\cdot \mathrm{ht}^{\mathrm{Falt}}([E_L]) \;\leq\; \frac{l}{14}\cdot \underline{\deg}_\infty([E_L]) + l\cdot C' \;\leq\; \mathrm{ht}^{\mathrm{Falt}}([E_L]) + 3l\cdot C'$$

— i.e., [since we may assume that C was chosen so that $l \geq 5$] that $l\cdot \mathrm{ht}^{\mathrm{Falt}}([E_L]) \leq 2(l-2)\mathrm{ht}^{\mathrm{Falt}}([E_L]) \leq 12l\cdot C'$, so $\mathrm{ht}^{\mathrm{Falt}}([E_L]) \leq 12\cdot C'$. Thus, again we conclude by Proposition 3.4 that $[E_L]$ belongs to some [fixed] *finite exceptional set* $\mathfrak{Exc}_d$ [which we think of as $\mathfrak{Exc}\bigcap \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})^{\leq d}$], as desired. ◯

Theorem 3.8. (Full Special Linear Galois Actions) *Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, $\mathcal{K}_V \subseteq \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$ a* **compactly bounded subset** *[cf. Example 1.3, (ii)], $\epsilon \in \mathbb{R}_{>0}$. Then there exist a* **constant** *$C \in \mathbb{R}_{>0}$ and a* **Galois-finite** *[cf. Example 1.3, (i)] subset $\mathfrak{Exc} \subseteq \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$ that satisfy the following property:*

Let E_L be an **elliptic curve** *over a number field $L \subseteq \overline{\mathbb{Q}}$ such that the isomorphism class $[E_L] \in \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$ of E_L does* **not** *belong to $\mathfrak{Exc}$; $d \stackrel{\mathrm{def}}{=} [L:\mathbb{Q}]$; l a* **prime number** *such that [at least]* **one** *of the following two conditions is satisfied:*

- *(a) $l \geq 23040\cdot 100d\cdot(\mathrm{ht}^{\mathrm{Falt}}([E_L]) + C\cdot d^\epsilon)$, and E_L has at least* **one** *prime of* **potentially multiplicative** *reduction;*
- *(b) $[E_L] \in \mathcal{K}_V$, and l is* **prime** *to the* **local heights** *of E_L at all of its primes of potentially multiplicative reduction [cf. Remark 3.3.1], as well as to the number $2\cdot 3\cdot 5 = 30$.*

Then the **image** *of the Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \to GL_2(\mathbb{Z}_l)$ associated to E_L* **contains** *$SL_2(\mathbb{Z}_l)$.*

Proof. First, let us observe that for an E_L as in the statement of Theorem 3.8, there exists a Galois extension L' of L of degree that divides $d_0 \stackrel{\text{def}}{=} (3^2-1)(3^2-3)(5^2-1)(5^2-5) = 23040$ [i.e., the order of $GL_2(\mathbb{F}_3)\times GL_2(\mathbb{F}_5)$], so as to render the 3- and 5-torsion points of E_L *rational* over L' [which has the effect of *eliminating automorphisms of elliptic curves in all characteristics*], we may assume that $E_{L'} \stackrel{\text{def}}{=} E_L \times_L L'$ has *semi-stable reduction* at all of the finite primes of L. [Here, we note that passing to such a Galois extension of L only affects the prime decomposition of the local heights via the primes that divide d_0, of which there are only *finitely* many, namely, 2, 3, and 5.] Next, let us observe that for a *suitable choice* of $C \in \mathbb{R}_{>0}$ and $\mathfrak{Exc} \subseteq \mathcal{M}_{\text{ell}}(\overline{\mathbb{Q}})$, if E_L and l satisfy condition (a) (respectively, (b)) of the statement of Theorem 3.8, then $E_{L'}$ and l satisfy condition (a) (respectively, (b)) of Lemma 3.7 [perhaps for a *different* "C"]. Thus, [cf. the portion of Lemma 3.7 that asserts that "l is $>$ the local heights"] for E_L, l as in the statement of Theorem 3.8, the *local height* of $E_{L'}$ at a finite prime of L' of multiplicative reduction is *not divisible by* l. Note, moreover, that *at least one* such finite prime exists [cf. the content of condition (a); Lemma 3.7 in the case of condition (b)]. Thus, it follows from the discussion of the *local theory* preceding Lemma 3.2 that the image of Galois in $GL_2(\mathbb{F}_l)$ contains the element "α" of Lemma 3.1, (iv), i.e., $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. On the other hand, by the portion of Lemma 3.7 concerning *l-cyclic subgroup schemes*, it follows that the image of Galois in $GL_2(\mathbb{F}_l)$ contains at least one matrix which is *not upper triangular*. Thus, we conclude from Lemma 3.1, (iv), that the image of Galois in $GL_2(\mathbb{Z}_l)$ contains $SL_2(\mathbb{Z}_l)$, as desired. ○

Section 4: Primes of Prescribed Size

In the present §4, we combine the *full Galois action* result given in Theorem 3.8 with some *classical analytic number theory* to give versions of Theorem 3.8 [cf. Corollaries 4.3, 4.4] that assert the *existence of bounded prime numbers l* satisfying various properties, such as the property of being *distinct* from various prime numbers that are, in some sense, *"characteristic" to the elliptic curve* under consideration.

We begin by reviewing the following result in *classical analytic number theory*.

Lemma 4.1. (The Existence of Primes of Prescribed Size) *Write $\mathbb{R}'_{>0} \subseteq \mathbb{R}_{>0}$ for the complement in $\mathbb{R}_{>0}$ of the set of prime numbers;*

$$\theta(x) \stackrel{\text{def}}{=} \sum_{p<x} \log(p)$$

— where the sum is over prime numbers $p < x$ — for $x \in \mathbb{R}'_{>0}$. Let M be a **positive integer***; $\epsilon, x_\epsilon, C_\epsilon \in \mathbb{R}_{>0}$ such that $0 < \epsilon < \frac{1}{4}$, $\epsilon \cdot x_\epsilon > C_\epsilon$, and, moreover, we have:*

(i) $\frac{5}{4}\cdot x + C_\epsilon > \theta(x)$, for all $x \in \mathbb{R}'_{>0}$; $\theta(x) > (1-\epsilon)x$, for all $x \in \mathbb{R}'_{>0}$ such that $x \geq x_\epsilon$;

(ii) $M \cdot \log(x) \leq \epsilon \cdot x$, *for all* $x \in \mathbb{R}_{>0}$ *such that* $x \geq x_\epsilon$.

Also, let us write

$$x_{\mathcal{A}} \stackrel{\text{def}}{=} \sum_{p \in \mathcal{A}} \log(p)$$

for any **finite set of prime numbers** $\mathcal{A}$. *Then for any nonnegative* $h \in \mathbb{R}$ *and any finite set of prime numbers* $\mathcal{A}$ *such that* $x_{\mathcal{A}} > x_\epsilon$, *there exist* M **distinct prime numbers** $p_1, \ldots, p_M$ *such that* $p_j \notin \mathcal{A}$, *and* $h \leq p_j \leq (1 + 6\epsilon) \cdot x_{\mathcal{A}} + 8h$, *for* $j = 1, \ldots, M$.

Proof. Indeed, write $\delta \stackrel{\text{def}}{=} 6\epsilon$, $y_{\mathcal{A}} \stackrel{\text{def}}{=} (1 + \delta) \cdot x_{\mathcal{A}} + 8h$, and suppose that the conclusion of Lemma 4.1 is *false*. Then it follows that there exists an *offending* finite set of primes $\mathcal{A}$ such that $x_{\mathcal{A}} > x_\epsilon$, and, moreover, *all prime numbers* p *such that* $h \leq p \leq y_{\mathcal{A}}$ *belong — with* $M - 1$ *possible exceptions — to* $\mathcal{A}$. But then it follows from the definitions that $x_{\mathcal{A}} \geq -(M-1) \cdot \log(y_{\mathcal{A}}) - \theta((1+\delta)h) + \theta(y_{\mathcal{A}}) \geq -M \cdot \log(y_{\mathcal{A}}) - \theta((1+\delta)h) + \theta(y_{\mathcal{A}})$. Thus, we compute:

$$\begin{aligned}
x_{\mathcal{A}} &\geq -M \cdot \log(y_{\mathcal{A}}) - \theta((1+\delta)h) + \theta(y_{\mathcal{A}}) \\
&\geq -\epsilon \cdot y_{\mathcal{A}} - 5(1+\delta)h/4 - C_\epsilon + (1-\epsilon) \cdot y_{\mathcal{A}} \\
&= (1 - 2\epsilon) \cdot y_{\mathcal{A}} - 5(1+\delta)h/4 - C_\epsilon \\
&= (1 + \delta - 2\epsilon - 2\delta \cdot \epsilon) \cdot x_{\mathcal{A}} + 8(1-2\epsilon)h - 5(1+\delta)h/4 - C_\epsilon \\
&\geq (1 + \delta/2 - 2\epsilon) \cdot x_{\mathcal{A}} + 4h - 5(1+\delta)h/4 - C_\epsilon \\
&\geq x_{\mathcal{A}} + (\epsilon \cdot x_{\mathcal{A}} - C_\epsilon) + (4h - 5(1+\delta)h/4)
\end{aligned}$$

— a *contradiction*, since $\epsilon \cdot x_{\mathcal{A}} > \epsilon \cdot x_\epsilon > C_\epsilon$, $5(1+\delta)/4 < 4$. Note that here we may assume without loss of generality that $y_{\mathcal{A}}, (1+\delta)h \in \mathbb{R}'_{>0}$, for instance by replacing δ, h by real numbers slightly greater than the given δ, h — which does not affect the above argument in any substantive way. ◯

Remark 4.1.1. The issue of finding ϵ, x_ϵ, C_ϵ which satisfy condition (ii) of Lemma 4.1 is entirely elementary. On the other hand, with regard to condition (i), the fact that $\theta(x)/x \to 1$ as $x \to \infty$ is a well-known consequence of the *prime number theorem* of classical analytic number theory — cf., e.g., [Edw], p. 76.

Lemma 4.2. (Some Elementary Estimates) *Let* n *be a positive integer;* $p_1, \ldots, p_n$ *prime numbers;* $h_1, \ldots, h_n$ *positive integers. Then we have*

$$\sum_{j=1}^n \log(p_j) \leq h$$

$$\sum_{j=1}^n \log(h_j) \leq \sum_{j=1}^n \log(h_j + 1) \leq 3h/2$$

— *where* $h \stackrel{\text{def}}{=} \sum_{j=1}^n h_j \cdot \log(p_j)$.

Proof. Indeed, the first and second inequalities are immediate; the third inequality follows from the easily verified fact that $\log(H+1) \leq (3H/2) \cdot \log(2)$ for any positive integer H. ◯

Corollary 4.3. (Full Galois Actions for Degenerating Elliptic Curves) *Let $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$; $\epsilon \in \mathbb{R}_{>0}$. Then there exists a* **constant** *$C \in \mathbb{R}_{>0}$ and a* **Galois-finite** *[cf. Example 1.3, (i)] subset $\mathfrak{Exc} \subseteq \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$ which satisfy the following property:*

Let E_L be an **elliptic curve** *over a number field $L \subseteq \overline{\mathbb{Q}}$, where L is a* **minimal field of definition** *of the point $[E_L] \in \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$, and $[E_L] \notin \mathfrak{Exc}$; $\mathcal{S}$ a* **finite set of prime numbers**. *Suppose that E_L has at least* **one** *prime of* **potentially multiplicative reduction**. *Write $d \stackrel{\text{def}}{=} [L : \mathbb{Q}]$; $x_{\mathcal{S}} \stackrel{\text{def}}{=} \sum_{p \in \mathcal{S}} \log(p)$. Then there* **exist** *prime numbers $l_\circ, l_\bullet \notin \mathcal{S}$ which satisfy the following conditions:*

(a) $l_\circ$, $l_\bullet$ are **prime** *to the primes of* **potentially multiplicative reduction**, *as well as to the* **local heights**, *of E_L. Moreover, $l_\bullet$ is* **prime** *to the primes of $\mathbb{Q}$ that* **ramify** *in L, as well as to the* **ramification indices** *of primes of $\mathbb{Q}$ in L.*

(b) The **image** *of the Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \to GL_2(\mathbb{Z}_{l_\circ})$ associated to E_L* **contains** *$SL_2(\mathbb{Z}_{l_\circ})$. The Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \to GL_2(\mathbb{Z}_{l_\bullet})$ associated to E_L is* **surjective**.

(c) The **inequalities**

$$l_\circ \leq 23040 \cdot 900d \cdot \mathrm{ht}^{\mathrm{Falt}}([E_L]) + 2x_{\mathcal{S}} + C \cdot d^{1+\epsilon}$$

$$l_\bullet \leq 23040 \cdot 900d \cdot \mathrm{ht}^{\mathrm{Falt}}([E_L]) + 6d \cdot \text{log-diff}_{\overline{\mathcal{M}}_{\mathrm{ell}}}([E_L])) + 2x_{\mathcal{S}} + C \cdot d^{1+\epsilon}$$

hold.

Proof. First, let us observe that if E_L is as in the statement of Corollary 4.3, and l is any prime number that is *unramified* in L, then the image of the Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \to GL_2(\mathbb{Z}_l)$ associated to E_L *contains* $SL_2(\mathbb{Z}_l)$ if and only if the Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \to GL_2(\mathbb{Z}_l)$ is *surjective*. [Indeed, this follows immediately from the well-known fact that the field extension $\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q}$ obtained by adjoining the l-th power roots of unity to $\mathbb{Q}$ is *totally ramified* over the prime l, hence *linearly disjoint* from the extension $L/\mathbb{Q}$.] Thus, by applying Theorem 3.8 — relative to condition (a) of Theorem 3.8 — we conclude that to complete the proof of Corollary 4.3, it suffices to show the existence of prime numbers $l_\circ$, $l_\bullet$ that satisfy the conditions (a), (c), and, moreover, are $\geq 23040 \cdot 100d \cdot (\mathrm{ht}^{\mathrm{Falt}}([E_L]) + C' \cdot d^\epsilon)$, where $C' \in \mathbb{R}_{>0}$ is a constant [i.e., the "C" of Theorem 3.8].

Now let us write $\mathcal{S}_\circ$ for the union of $\mathcal{S}$, the primes of $\mathbb{Q}$ that lie under primes of *potentially multiplicative reduction* of E_L, and the primes that appear in the prime decomposition of the *local heights* of E_L; write $\mathcal{S}_\bullet$ for the union of $\mathcal{S}_\circ$, the primes of $\mathbb{Q}$ that *ramify* in L, and the primes that divide the *ramification indices* of primes of $\mathbb{Q}$ in L. Thus, [in the notation of Lemma 4.1] we conclude from Lemma 4.2 and Proposition 3.4 that

$$\begin{aligned} x_{\mathcal{S}_\circ} &\leq x_{\mathcal{S}} + (1 + 3/2) \cdot 23040d \cdot \underline{\deg}_\infty([E_L]) \\ &\leq x_{\mathcal{S}} + 3 \cdot 12 \cdot 23040d \cdot \mathrm{ht}^{\mathrm{Falt}}([E_L]) + d \cdot C'' \end{aligned}$$

— where we take the "$1 + \epsilon$" of Proposition 3.4 to be $6/5$; C'' arises from the constant implicit in the inequalities of BD-classes in Proposition 3.4; the "h" of Lemma 4.2 corresponds to $23040d \cdot \underline{\deg}_\infty([E_L])$ [cf. the meaning of "$d_0 = 23040$" in the proof of Theorem 3.8]. In a similar vein, since [as is easily verified, by considering the *trace* of an extension of number fields] the primes appearing in the arithmetic divisor that gives rise to "log-diff$_{\overline{\mathcal{M}}_{\mathrm{ell}}}$" [cf. Definition 1.5, (iii)] appear with *multiplicity* $\geq$ one less than the *ramification indices* of $L/\mathbb{Q}$, we conclude that $x_{\mathcal{S}_\bullet} \leq x_{\mathcal{S}} + 3 \cdot 12 \cdot 23040d \cdot \mathrm{ht}^{\mathrm{Falt}}([E_L]) + 3d \cdot \text{log-diff}_{\overline{\mathcal{M}}_{\mathrm{ell}}}([E_L])) + d \cdot C''$. Now we apply Lemma 4.1 by taking "M" to be 1, "$1 + 6\epsilon$" to be 2, "h" to be $23040 \cdot 100d \cdot (\mathrm{ht}^{\mathrm{Falt}}([E_L]) + C' \cdot d^{\epsilon})$, and "$\mathcal{A}$" to be $\mathcal{S}_\circ$ or $\mathcal{S}_\bullet$ [and applying the estimate $2 \cdot 3 \cdot 12 + 8 \cdot 100 \leq 100 + 800 = 900$]; here, we observe that by enlarging $\mathcal{S}$ [and possibly increasing the "C" of condition (c)], we may always assume that $x_\epsilon \leq x_{\mathcal{S}}$ ($\leq x_{\mathcal{S}_\circ} \leq x_{\mathcal{S}_\circ}$). Thus, the existence of $l_\circ$, $l_\bullet$ as desired follows immediately from Lemma 4.1 [cf. also Remark 4.1.1]. ◯

Corollary 4.4. (Full Galois Actions for Compactly Bounded Subsets) *Let $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$; $\mathcal{K}_V \subseteq \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$ a* **compactly bounded subset** *[cf. Example 1.3, (ii)]. Then there exists a* **constant** *$C \in \mathbb{R}_{>0}$ and a* **Galois-finite** *[cf. Example 1.3, (i)] subset $\mathfrak{Exc} \subseteq \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$ which satisfy the following property:*

Let E_L be an **elliptic curve** *over a number field $L \subseteq \overline{\mathbb{Q}}$, where L is a* **minimal field of definition** *of the point $[E_L] \in \mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$, $[E_L] \in \mathcal{K}_V$, and $[E_L] \notin \mathfrak{Exc}$; $\mathcal{S}$ a* **finite set of prime numbers**. *Write $d \stackrel{\mathrm{def}}{=} [L : \mathbb{Q}]$; $x_{\mathcal{S}} \stackrel{\mathrm{def}}{=} \sum_{p \in \mathcal{S}} \log(p)$. Then there* **exist** *prime numbers $l_\circ, l_\bullet \notin \mathcal{S}$ which satisfy the following conditions:*

(a) $l_\circ$, $l_\bullet$ are **prime** *to the primes of* **potentially multiplicative reduction**, *as well as to the* **local heights**, *of E_L. Moreover, $l_\bullet$ is* **prime** *to the primes of $\mathbb{Q}$ that* **ramify** *in L, as well as to the* **ramification indices** *of primes of $\mathbb{Q}$ in L.*

(b) The **image** *of the Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \to GL_2(\mathbb{Z}_{l_\circ})$ associated to E_L* **contains** *$SL_2(\mathbb{Z}_{l_\circ})$. The Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \to GL_2(\mathbb{Z}_{l_\bullet})$ associated to E_L is* **surjective**.

(c) The **inequalities**

$$l_\circ \leq 23040 \cdot 100d \cdot \mathrm{ht}^{\mathrm{Falt}}([E_L]) + 2x_{\mathcal{S}} + C \cdot d$$

$$l_\bullet \leq 23040 \cdot 100d \cdot \mathrm{ht}^{\mathrm{Falt}}([E_L]) + 6d \cdot \text{log-diff}_{\overline{\mathcal{M}}_{\mathrm{ell}}}([E_L])) + 2x_{\mathcal{S}} + C \cdot d$$

hold.

Proof. The proof is entirely similar to [but slightly easier than] the proof of Corollary 4.3, except that instead of applying condition (a) of Theorem 3.8, we apply condition (b) of Theorem 3.8. Also, when applying Lemma 4.1, we take "h" to be 0. ◯

Remark 4.4.1. Typically, in computations of *arithmetic degrees*, such as *heights* [i.e., "$\mathrm{ht}^{\mathrm{Falt}}(-)$", etc.], the terms that appear in a sum that computes the arithmetic degree are not terms that are "polynomial in l", but rather terms that are *linear in* $\log(l)$. Thus, in the context of Corollaries 4.3, 4.4, if l is equal to $l_\circ$ or $l_\bullet$, then $\log(l)$ is *of the order of*

$$\log(\mathrm{ht}^{\mathrm{Falt}}(-)) + (1+\epsilon)\log(d)$$

or

$$\log(\mathrm{ht}^{\mathrm{Falt}}(-)) + \log(\text{log-diff}_{\overline{\mathcal{M}}_{\mathrm{ell}}}(-)) + (1+\epsilon)\log(d)$$

— hence *asymptotically bounded* by

$$\epsilon \cdot (\mathrm{ht}^{\mathrm{Falt}}(-) + d)$$

or

$$\epsilon \cdot (\mathrm{ht}^{\mathrm{Falt}}(-) + \text{log-diff}_{\overline{\mathcal{M}}_{\mathrm{ell}}}(-) + d)$$

— for $\epsilon > 0$.

Remark 4.4.2. Let $U_P \subseteq P$ be as in Theorem 2.1, (ii). Thus, by regarding U_P as the *"λ-line"* [i.e., regarding the standard coordinate on P as the "λ" in the *Legendre form* "$y^2 = x(x-1)(x-\lambda)$" of the Weierstrass equation defining an elliptic curve], one obtains a *natural* finite étale [classifying] *morphism* $U_P \to \mathcal{M}_{\mathrm{ell}} \times_{\mathbb{Z}} \mathbb{Q}$. Then one verifies immediately that [relative to the elliptic curves obtained from points $\in U_P(\overline{\mathbb{Q}})$ via this classifying morphism] one obtains a result *entirely similar to Corollary 4.4 by replacing "$\mathcal{M}_{\mathrm{ell}} \subseteq \overline{\mathcal{M}}_{\mathrm{ell}}$" by $U_P \subseteq P$*. In particular, in the context of Theorem 2.1, (ii), one may always assume the *existence of prime numbers* $l_\circ$, $l_\bullet$ as in [this $U_P \subseteq P$ version of] Corollary 4.4.

References

[Edw] H. M. Edwards, *Riemann's Zeta Function*, Academic Press (1974).

[Elkies] N. D. Elkies, ABC implies Mordell, *Internat. Math. Res. Notices* **7** (1991), pp. 99-109.

[vF] M. van Frankenhuysen, The ABC Conjecture Implies Vojta's Height Inequality for Curves, *Journal of Number Theory* **95** (2002), pp. 289-302.

[Falt] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), pp. 349-366.

[FC] G. Faltings and C.-L. Chai, *Degenerations of Abelian Varieties*, Springer (1990).

[Merel] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, *Invent. Math.* **124** (1996), pp. 437-449.

[Mzk1] S. Mochizuki, Noncritical Belyi Maps, *Math. J. Okayama Univ.* **46** (2004), pp. 105-113.

[Mzk2] S. Mochizuki, Galois Sections in Absolute Anabelian Geometry, *Nagoya Math. J.* **179** (2005), pp. 17-45.

[Mzk3] S. Mochizuki, Absolute anabelian cuspidalizations of proper hyperbolic curves, *J. Math. Kyoto Univ.* **47** (2007), pp. 451-539.

[Mzk4] S. Mochizuki, *Topics in Absolute Anabelian Geometry II: Decomposition Groups*, RIMS Preprint **1625** (March 2008).

[Serre] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, Benjamin (1968).

[Silv1] J.H. Silverman, The Theory of Height Functions in *Arithmetic Geometry*, ed. by G. Cornell and J.H. Silverman, Springer (1986).

[Silv2] J.H. Silverman, Heights and Elliptic Curves in *Arithmetic Geometry*, ed. by G. Cornell and J.H. Silverman, Springer (1986).

[Szp] L. Szpiro, *Degrés, intersections, hauteurs* in *Astérisque* **127** (1985), pp. 11-28.