ELLIPTIC CURVES OF BOUNDED DEGREE AND HEIGHT

JOSEPH H. SILVERMAN

(Communicated by William Adams)

ABSTRACT. We show that there are only finitely many elliptic curves of bounded degree and height, provided that one takes a naive height defined in terms of minimal Weierstrass equations. We show that the corresponding statement is false if instead one uses the Faltings-Parshin modular height.

Several theorems in algebraic number theory assert that there are only finitely many “objects” of bounded “degree” and “size”. Two important examples of such theorems are the following:

Theorem 1 (Hermite-Minkowski [2], p. 619). *There are only finitely many number fields of bounded degree and absolute discriminant.*

Theorem 2 (Northcott [5]). *There are only finitely many algebraic numbers of bounded degree and height.*

In [9] the author gave a “proof” of an analogous result for elliptic curves of bounded degree and height, where the degree was the degree of the field of definition and the height was the (Faltings-Parshin) modular height. Daniel Bertrand (personal communication) has noted that the proof in [9] is not correct. Further, even the statement of Corollary 2.5 in [9] is somewhat ambiguous. In this note we will formulate and prove a precise theorem for elliptic curves analogous to Theorems 1 and 2. We will use a naive definition for the height of an elliptic curve, and will indicate why our result is false if instead one uses the modular height.

It is important to fix precisely what is meant by the minimal field of definition of an elliptic curve. We begin by letting

$$\mathcal{E} = \left\{ (E, K) : \begin{array}{l} K \text{ is a number field} \\ E \text{ is a } K\text{-isomorphism class of elliptic curves} \end{array} \right\}.$$

Thus $\mathcal{E}$ consists of all elliptic curves with all possible fields of definition. There is a natural partial ordering on $\mathcal{E}$, defined by

$$(E', K') < (E, K) \quad \text{if} \quad K' \subseteq K \text{ and } E' \times_{K'} K \cong_K E.$$

Received by the editors May 27, 1988 and, in revised form, July 28, 1988.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 11G05; Secondary 14K07, 14K15.

Research supported by NSF grant #DMS-8612393 and a Sloan Foundation Fellowship.

Note that the isomorphism between E' and E is required to be defined over K . With this ordering, $\mathcal{E}$ has descending chain condition. (If (E', K') is strictly less than (E, K) , then K' is a proper subfield of K .) It thus makes sense to define

$$\mathcal{E}^* = \{\text{minimal elements } (E, K) \in \mathcal{E} \text{ relative to the partial order } \prec\}.$$

We will say that an element of $\mathcal{E}^*$ consists of an elliptic curve E with its minimal field of definition K .

Next we use the coefficients of a minimal Weierstrass equation to define the height of an elliptic curve. For any algebraic numbers a and b with $4a^3 + 27b^2 \neq 0$, let $E(a, b)$ denote the elliptic curve

$$E(a, b): Y^2 = X^3 + aX + b.$$

Then we define the (*naive*) height of an elliptic curve $(E, K) \in \mathcal{E}$ to be

$$h(E/K) = \frac{1}{12} \inf_{\substack{a, b \in K \\ E \cong_{/K} E(a, b)}} h([a^3, b^2, 1]).$$

(Here $h([x, y, z])$ is the usual absolute logarithmic height on P^2 . See [3] or [8].) In other words, the height of E/K is the smallest possible height for a Weierstrass equation defining E .

For real numbers $D \geq 1$ and $H \geq 1$, we let

$$\begin{aligned} \mathcal{E}(D, H) &= \{(E, K) \in \mathcal{E} : [K : \mathbb{Q}] \leq D \quad \text{and} \quad h(E/K) \leq H\}; \\ \mathcal{E}^*(D, H) &= \{(E, K) \in \mathcal{E}^* : [K : \mathbb{Q}] \leq D \quad \text{and} \quad h(E/K) \leq H\} \\ &= \mathcal{E}^* \cap \mathcal{E}(D, H). \end{aligned}$$

Our main result is the following:

Theorem 3. $\mathcal{E}^*(D, H)$ is finite.

Before giving the proof, we make several remarks.

Remark. It is necessary to restrict attention to minimal pairs (E, K) , since the set $\mathcal{E}(D, H)$ of all pairs (E, K) is never finite if $D \geq 2$. For example, let $E_0/\mathbb{Q}$ be the elliptic curve $Y^2 = X^3 + 1$, so $h(E_0/\mathbb{Q}) = 0$. Then for any quadratic field $K/\mathbb{Q}$ we can extend scalars to K and still have $h(E_0/K) = 0$. Thus $(E_0, K) \in \mathcal{E}(D, H)$. But K is arbitrary, so $\mathcal{E}(D, H)$ is infinite.

Remark. There is a more refined notion of height for elliptic curves (and Abelian varieties) called the *modular height*. We will denote the modular height of E/K by $h^{(\text{mod})}(E/K)$. (For the definition of $h^{(\text{mod})}$, see [1] or [9].) It is not hard to show that for any fixed number field K and any $\varepsilon > 0$, there is a constant $c = c(K, \varepsilon)$ so that for all elliptic curves E/K ,

$$(1 - \varepsilon)h(E/K) - c \leq h^{(\text{mod})}(E/K) \leq (1 + \varepsilon)h(E/K) + c.$$

(See, e.g., [9], Corollary 2.3 for the case $K = \mathbb{Q}$.) However, the fact that the constant c depends on K means that $h^{(\text{mod})}$ and h may behave quite

differently as K is varied. Let us denote by $\mathcal{E}^{(\text{mod})*}(D, H)$ the set defined in the same way as $\mathcal{E}^*(D, H)$ except that $h^{(\text{mod})}(E/K)$ is used in place of $h(E/K)$. Then we have the following rather distressing fact.

Proposition 4. *There is a constant $H_0 \geq 0$ such that the set $\mathcal{E}^{(\text{mod})*}(2, H_0)$ is infinite.*

Proof. For each squarefree integer $d > 1$, let u_d be the fundamental unit in the field $K_d = \mathbb{Q}(\sqrt{d})$, and let E_d/K_d be the elliptic curve

$$E_d: Y^2 = X^3 + u_d.$$

Since u_d is a unit, E_d has good reduction except possibly at primes lying above 2 and 3. Since further $j(E_d) = 0$ does not depend on d , it follows (e.g., from [9] Proposition 2.1) that $h^{(\text{mod})}(E_d/K_d)$ is bounded independently of d . Finally, we note that since u_d is a fundamental unit, (or, more generally, since it is not in $\mathbb{Q}^*K_d^{*6}$) the pair (E_d, K_d) is minimal with respect to the $<$ ordering. Hence for an appropriate choice of H_0 , the set $\mathcal{E}^{(\text{mod})*}(2, H_0)$ will contain all of the pairs (E_d, K_d) for all squarefree integers $d > 1$.

Remark. The reason that the modular height does not give a Hermite-Northcott type finiteness theorem is that it is insensitive to unramified twists. The modular height can be thought of as measuring two quantities: first the height of the point in moduli space corresponding to the given elliptic curve, second the norms of the prime ideals of bad (additive) reduction. Neither of these two quantities changes when the curve is twisted by a unit. Szpiro (personal communication) has pointed out that one can obtain a finiteness theorem by adding a level structure to the modular height. We briefly explain. Rather than classifying pairs (E, K) , we fix an integer $N \geq 3$ and classify triples (E, P, K) , where K is a number field, E/K is a K -isomorphism class of elliptic curves, and $P \in E(K)$ is a point of exact order N . Let $x = x_{(E, P)} \in X_1(N)(K)$ be the point on the modular curve $X_1(N)$ corresponding to (E, P) . Since $X_1(N)$ is a fine moduli space, there is an elliptic curve $E'/\mathbb{Q}(x)$ with a point $P' \in E'(\mathbb{Q}(x))$ and an isomorphism

$$\phi: E' \times_{\mathbb{Q}(x)} K \rightarrow E$$

defined over K and satisfying $\phi(P') = P$. Hence if the triple (E, P, K) is minimal (in the obvious sense), then necessarily $K = \mathbb{Q}(x_{(E, P)})$. Thus for a given field K , the minimal triples (E, P, K) are in one-to-one correspondence with the points of $X_1(K)$. (Note this is false for $N = 1$; the j -invariant does not determine E up to K isomorphism, only up to $\bar{\mathbb{Q}}$ -isomorphism.) On the other hand,

$$h^{(\text{mod})}(E/K) \gg h(j(E)) \gg\ll h(x_{(E, P)}),$$

where the $\gg\ll$ constants are absolute and the final height is for some fixed projective embedding of $X_1(N)$. It follows that minimal triples (E, P, K)

with $[K: \mathbb{Q}]$ and $h^{(\text{mod})}(E/K)$ bounded correspond to points of $X_1(\overline{\mathbb{Q}})$ with bounded degree and height. By Northcott's theorem, there are only finitely many.

Remark. It is natural to try to extend Theorem 3 to (principally polarized) Abelian varieties. There is no problem in defining a set of minimal pairs (A, K) corresponding to $\mathcal{E}^*$. However, as indicated by Proposition 4, it will not suffice to measure the height of an Abelian variety by using the modular height. It is not immediately clear what height should be used instead. One possibility might be to use the Mumford embeddings. (Cf. the work of Manin and Zarhin [4] on the canonical height.)

Proof (of Theorem 3). We begin by using Theorem 1 to show that there are only finitely many fields K which occur as part of a pair (E, K) in $\mathcal{E}^*(D, H)$. Let (E, K) be such a pair, let $d = [K: \mathbb{Q}]$, and let $\mathcal{D}_K$ be the absolute discriminant of $K/\mathbb{Q}$. Note that $d \leq D$.

Suppose now that $a, b \in K$ satisfy $E \cong_{/K} E(a, b)$. Then by definition we have

$$(E(a, b), \mathbb{Q}(a, b)) \prec (E, K).$$

But (E, K) is minimal, so $K = \mathbb{Q}(a, b)$. Hence for any such a, b , we can use [7] Theorem 2 to obtain the estimate

$$h([a, b, 1]) \geq \frac{1}{2d-2} \left\{ \frac{1}{d} \log(\mathcal{D}_K) - \log(d) \right\}.$$

On the other hand, from the definition of $h(E/K)$ we find that

$$H \geq h(E/K) = \frac{1}{12} \inf_{\substack{a, b \in K \\ E \cong_{/K} E(a, b)}} h([a^3, b^2, 1]).$$

Since $h([a, b, 1]) \gg h([a^3, b^2, 1])$ (with absolute constants), these last two inequalities imply that $\mathcal{D}_K$ is bounded in terms of D and H . Applying Theorem 1, we conclude that there are only finitely many possibilities for the field K .

We next show that there are only finitely many j -invariants associated to the elliptic curves in $\mathcal{E}^*(D, H)$. Let $(E, K) \in \mathcal{E}^*(D, H)$, and choose $a, b \in K$ so that $E \cong_{/K} E(a, b)$. Then

$$h(j(E)) = h(j(E(a, b))) = h([1728 \cdot 4a^3, 4a^3 + 27b^2]) \leq h([a^3, b^2, 1]) + O(1).$$

(Here and in what follows, the constants implicit in each $O(1)$ are absolute.) Taking the infimum over all appropriate a and b , we obtain

$$h(j(E)) \leq 12h(E/K) + O(1) \leq 12H + O(1).$$

Similarly, since E is defined over K , we have $j(E) \in K$, so

$$[Q(j(E)): \mathbb{Q}] \leq [K: \mathbb{Q}] \leq D.$$

Thus $j(E)$ has bounded degree and height, so from Northcott's theorem (Theorem 2) there are only finitely many possibilities for $j(E)$.

We are now reduced to the following problem. Fix a number field $K/\mathbb{Q}$ and an elliptic curve E_0/K . Then up to K -isomorphism, we must show that there are only finitely many elliptic curves E/K with $j(E) = j(E_0)$ and $h(E/K) \leq H$. Let us fix a Weierstrass equation for E_0/K , say $E_0 \cong_{/K} E(\alpha, \beta)$ for some fixed $\alpha, \beta \in K$. Then every E/K with $j(E) = j(E_0)$ has a Weierstrass equation of the form $E(\alpha\delta^2, \beta\delta^3)$ for some $\delta \in K^*$; and the K -isomorphism class of E is determined by the image of δ in K/K^{*2} . (See, e.g., [8], X.5.4. For simplicity we have assumed that $j(E_0) \neq 0, 1728$. The cases $j(E_0) = 0, 1728$ are done similarly, and may safely be left to the reader.)

We again use the definition of $h(E/K)$ to estimate

$$\begin{aligned} 12H &\geq 12h(E/K) \\ &= \inf_{u \in K^*} h([\alpha\delta^2 u^4]^3, [\beta\delta^3 u^6]^2, 1) \\ &= \inf_{u \in K^*} h([\alpha^3, \beta^2, (\delta u^2)^{-6}]) \\ &\geq \inf_{u \in K^*} 6h(\delta u^2) - h([\alpha^3, \beta^2, 1]). \end{aligned}$$

Let us define a "height" $h^{(2)}$ on K^*/K^{*2} by

$$h^{(2)}(x \bmod K^{*2}) = \inf_{u \in K^*} h(xu^2).$$

We are finally reduced to showing that K^*/K^{*2} contains only finitely many elements having bounded $h^{(2)}$. But this is an elementary exercise using the definition of height, finiteness of class number, and finite generation of the unit group. (For a similar calculation, see the proof of [6] Proposition 2.) This completes the proof of Theorem 3.

ACKNOWLEDGMENTS

I would like to thank Daniel Bertrand and Lucien Szpiro for their many helpful suggestions.

REFERENCES

1. G. Faltings, *Finiteness theorems for abelian varieties over number fields*, in: *Arithmetic Geometry* (G. Cornell and J. Silverman, eds.), Springer, New York, 1986.
2. H. Hasse, *Number theory*, Springer, Berlin, 1969.
3. S. Lang, *Fundamentals of diophantine geometry*, Springer, New York, 1983.
4. J. Manin and Y. Zarhin, *Heights on families of abelian varieties*, Math. USSR-Sb. **18** (1972), 169–179.
5. D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. **45** (1949), 502–518.
6. J. H. Silverman, *Integer points and the rank of Thue elliptic curves*, Invent. Math. **66** (1982), 395–404.

7. —, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
8. —, *The arithmetic of elliptic curves*, Springer, New York, 1986.
9. —, *Heights and elliptic curves*, in: *Arithmetic Geometry* (G. Cornell and J. Silverman, eds.), Springer, New York, 1986.

DEPARTMENT OF MATHEMATICS, BROWN UNIVERSITY, PROVIDENCE, RHODE ISLAND 02912