Pacific
Journal of
Mathematics

EFFECTIVE RESULTS ON LINEAR DEPENDENCE FOR ELLIPTIC CURVES

MIN SHA AND IGOR E. SHPARLINSKI

Volume 295 No. 1 July 2018

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.123

EFFECTIVE RESULTS ON LINEAR DEPENDENCE FOR ELLIPTIC CURVES

MIN SHA AND IGOR E. SHPARLINSKI

Given a subgroup Γ of rational points on an elliptic curve E defined over $\mathbb{Q}$ of rank $r \geq 1$ and any sufficiently large $x \geq 2$, assuming that the rank of Γ is less than r, we give upper and lower bounds on the canonical height of a rational point Q which is not in the group Γ but belongs to the reduction of Γ modulo every prime $p \leq x$ of good reduction for E.

1. Introduction

1A. ***Detecting linear dependence.*** Let A be an abelian variety defined over a number field F, and let Γ be a subgroup of the Mordell–Weil group $A(F)$. For any prime $\mathfrak{p}$ (of F) of good reduction for A and any point $Q \in A(F)$, we denote by $Q_{\mathfrak{p}}$ and $\Gamma_{\mathfrak{p}}$ the images of Q and Γ via the reduction map modulo $\mathfrak{p}$ respectively, and $F_{\mathfrak{p}}$ stands for the residue field of F modulo $\mathfrak{p}$. The following question was initiated in 2002 and was considered at the same time but independently by Wojciech Gajda in a letter to Kenneth Ribet in 2002 [Gajda and Górnisiewicz 2009, §1] and by Kowalski [2003], and it is now called *detecting linear dependence*.

Question 1.1. *Suppose that Q is a point of $A(F)$ such that for all but finitely many primes $\mathfrak{p}$ of F we have $Q_{\mathfrak{p}} \in \Gamma_{\mathfrak{p}}$. Does it then follow that $Q \in \Gamma$?*

An early result related to this question is due to Schinzel [1975], who has answered affirmatively the question for the multiplicative group in place of an abelian variety. Question 1.1 has been extensively studied in recent years and much progress has been made; see [Banaszak 2009; Banaszak et al. 2005; Banaszak and Krasoń 2011; Gajda and Górnisiewicz 2009; Jossen 2013; Jossen and Perucca 2010; Perucca 2010; Sadek 2016; Weston 2003] for more details and developments.

The answer is affirmative for all abelian varieties if the group Γ is cyclic, as proven by Kowalski [2003] (for elliptic curves) and by Perucca [2010] (in general). Banaszak, Gajda and Krasoń [Banaszak et al. 2005] established the result for all abelian varieties with the endomorphism ring $\mathrm{End}_F\, A = \mathbb{Z}$ if the group Γ is free

MSC2010: 11G05, 11G50.

Keywords: elliptic curve, linear dependence, pseudolinearly dependent point, pseudomultiple, canonical height.

and the point Q is nontorsion. More generally, Gajda and Górnisiewicz [2009] have solved the problem in the case when Γ is a free $\mathrm{End}_F\, A$-submodule and the point Q generates a free $\mathrm{End}_F\, A$-submodule, while Perucca [2010] has removed the assumption on the point Q. We remark that the answer of Question 1.1 is not always positive; see a counterexample due to Jossen and Perucca [2010].

We want to emphasize that Jossen [2013] has given an affirmative answer when A is a geometrically simple abelian variety, which automatically includes elliptic curves. Moreover, the result of [Jossen 2013] requires $Q_{\mathfrak{p}} \in \Gamma_{\mathfrak{p}}$ to hold only for a set of primes $\mathfrak{p}$ with natural density 1 (rather than for all but finitely many primes $\mathfrak{p}$ as in the settings of Question 1.1). Due to the crucial role of [Jossen 2013] in our paper, we reproduce this result as follows.

Theorem 1.2 [Jossen 2013]. *Assume that A is a geometrically simple abelian variety over F. Then, if the set of primes $\mathfrak{p}$ of F for which $Q_{\mathfrak{p}} \in \Gamma_{\mathfrak{p}}$ has natural density* 1, *we have $Q \in \Gamma$.*

In addition, to achieve the aforementioned results, one needs to apply the Chebotarev density theorem. So, it suffices to verify the condition for all primes up to a certain finite bound, which depends on the initial data (including the point Q). Banaszak and Krasoń [2011, Theorem 7.7] have established the finiteness result in a qualitative manner for certain abelian varieties which includes elliptic curves. Then, most recently Sadek [2016] has given a quantitative version for a large class of elliptic curves under the *generalized Riemann hypothesis* (GRH). However, the results in this paper (see Section 2) go in a different direction, because they imply that there is no such a bound independent of the point Q.

1B. ***Pseudolinear dependence.*** Following the setup of [Akbary et al. 2010], which is crucial for some of our approaches, we restrict ourselves to the case of elliptic curves over the rational numbers $\mathbb{Q}$; see Definitions 1.3 and 1.4 below. In particular, we consider Question 1.1 for an elliptic curve E over $\mathbb{Q}$.

Let r be the rank of $E(\mathbb{Q})$ and s the rank of Γ. We denote by Δ_E the minimal discriminant of E and by O_E the point at infinity of E.

For a prime p of good reduction for E (that is, $p \nmid \Delta_E$), we let $E(\mathbb{F}_p)$ be the group of $\mathbb{F}_p$-points in the reduction of E to the finite field $\mathbb{F}_p$ of p elements, and $E(\mathbb{Q})_p$ stands for the reduction of $E(\mathbb{Q})$ modulo p.

Definition 1.3 ($\mathbb{F}_p$-pseudolinear dependence). Given a prime p of good reduction for E, we call a point $Q \in E(\mathbb{Q})$ an *$\mathbb{F}_p$-pseudolinearly dependent point* with respect to Γ if $Q \notin \Gamma$ but $Q_p \in \Gamma_p$.

We remark that such a point Q is $\mathbb{F}_p$-pseudolinear dependent if and only if $Q \notin \Gamma$ but $Q \in \Gamma + \ker_p$, where $\ker_p$ denotes the kernel of the reduction map modulo p.

Definition 1.4 (x-pseudolinear dependence). We say that a point $Q \in E(\mathbb{Q})$ is an *x-pseudolinearly dependent point* with respect to Γ if $Q \notin \Gamma$ but it is an $\mathbb{F}_p$-pseudolinearly dependent point with respect to Γ for all primes $p \le x$ of good reduction for E.

We remark that the x-pseudolinear dependence trivially holds if there is no prime p of good reduction such that $p \le x$.

If $\Gamma = \langle P \rangle$, we call a point Q as in Definition 1.4 an *x-pseudomultiple* of P. This notion is an elliptic curve analogue of the notions of x-pseudosquares and x-pseudopowers over the integers, which dates back to the classical results of Schinzel [1960; 1970; 1997] and has recently been studied in [Bach et al. 1996; Bourgain et al. 2009; Konyagin et al. 2010; Pomerance and Shparlinski 2009].

1C. ***Overview.*** We give an explicit construction of an x-pseudolinearly dependent point Q with respect to Γ provided that $s < r$ and give upper bounds for its canonical height, and then we also deduce lower bounds for the canonical height of any x-pseudolinearly dependent point in some special cases. These upper and lower bounds are formulated in Sections 2A and 2B and proved in Sections 5 and 6, respectively.

Furthermore, we also consider the existence problem of x-pseudolinearly dependent points, with some explicit constructions; see Section 4 for precise details.

There is little doubt that one can extend [Akbary et al. 2010], and thus our results to elliptic curves over number fields, but this may require quite significant efforts.

1D. ***Convention and notation.*** Throughout the paper, we use the Landau symbols O and o and the Vinogradov symbol $\ll$ (sometimes written as $\gg$). We recall that the assertions $U = O(V)$ and $U \ll V$ are both equivalent to the inequality $|U| \le cV$ with some absolute constant c, while $U = o(V)$ means that $U/V \to 0$. Here, all implied constants in the symbols O and $\ll$ depend only possibly on E and Γ.

The letter p, with or without subscripts, always denotes a prime. As usual, $\pi(x)$ denotes the number of primes not exceeding x.

We use $\hat{h}$ to denote the canonical height of points on E; see Section 3A for a precise definition. For a finite set S, we use $\#S$ to denote its cardinality.

For any group G, if it is generated by some elements $g_1, \dots, g_m$, then we write $G = \langle g_1, \dots, g_m \rangle$.

From now on, we say that a prime is of good reduction, which means that the prime is of good reduction for E. When a point Q is said to be x-pseudolinearly dependent, it is automatically with respect to Γ.

2. Main results

2A. ***Upper bounds.*** We first state a primary result on the existence of pseudolinearly dependent points.

Theorem 2.1. *Suppose that $r \ge 1$ and $s < r$. Then for any sufficiently large x, there is a rational point $Q \in E(\mathbb{Q})$ of height*

$$\hat{h}(Q) \le \exp\bigl(2x + O(x/(\log x)^2)\bigr)$$

such that Q is an x-pseudolinearly dependent point.

With more efforts we can improve the result in Theorem 2.1 for various cases.

Theorem 2.2. *Suppose that $r \ge 1$ and $s = 0$. Then for any sufficiently large x, there is a rational point $Q \in E(\mathbb{Q})$ of height*

$$\hat{h}(Q) \le \exp\Bigl(2x - 2\log(\#\Gamma)\frac{x}{\log x} + O(x/(\log x)^2)\Bigr)$$

such that Q is an x-pseudolinearly dependent point.

Theorem 2.3. *Assume that $r \ge 2$ and $1 \le s < r$. Then for any sufficiently large x, there is a rational point $Q \in E(\mathbb{Q})$ of height*

$$\hat{h}(Q) \le \exp\Bigl(\frac{4}{s+2}x + O(x/\log x)\Bigr)$$

such that Q is an x-pseudolinearly dependent point.

Theorem 2.4. *Suppose that either $19 \le s < r$ if E is a non-CM curve, or $7 \le s < r$ if E is a CM curve. Then under the GRH and for any sufficiently large x, there is a rational point $Q \in E(\mathbb{Q})$ of height*

$$\hat{h}(Q) \le \exp\bigl(4x(\log\log x)/\log x + O(x/\log x)\bigr)$$

such that Q is an x-pseudolinearly dependent point.

The above results are proved in Section 5.

2B. *Lower bounds.* Notice that by Definition 1.4 the condition for x-pseudolinearly dependent points is quite strong when x tends to infinity. This convinces us that there may exist some lower bounds for the height of such points. Here, we establish some partial results. Define

$$\widetilde{\Gamma} = \{P \in E(\mathbb{Q}) : mP \in \Gamma \text{ for some nonzero } m \in \mathbb{Z}\}. \tag{2-1}$$

Theorem 2.5. *Suppose that $r \ge 1$ and $s = 0$. For any sufficiently large x and any x-pseudolinearly dependent point Q, we have*

$$\hat{h}(Q) \ge \frac{1}{\#\Gamma}x/\log x + O(x/(\log x)^2).$$

Theorem 2.6. *Assume that* $\mathrm{End}_{\overline{\mathbb{Q}}} E = \mathbb{Z}$, $r \geq 2$, $1 \leq s < r$, *and* Γ *is a free subgroup of* $E(\mathbb{Q})$. *Suppose further that* $\Gamma \equiv \widetilde{\Gamma}$ *modulo the torsion points of* $E(\mathbb{Q})$. *For any sufficiently large* x *and any* x*-pseudolinearly dependent point* Q, *we have*

$$\hat{h}(Q) \geq \exp((\log x)^{1/(2s+6)+o(1)}),$$

and furthermore assuming the GRH, *we have*

$$\hat{h}(Q) \geq \exp(x^{1/(4s+12)+o(1)}).$$

The above results are proved in Section 6.

We want to remark that for a non-CM elliptic curve E with no torsion points in $E(\mathbb{Q})$, assuming the GRH and some other wild conditions, Sadek [2016, Theorem 4.4] has shown that to detect whether a point $Q \in E(\mathbb{Q})$ is contained in Γ it suffices to determine whether $Q \in \Gamma_p$ for primes p of good reduction up to an explicit constant B satisfying (using only $K \geq 2$ in [Sadek 2016, Theorem 4.4])

$$B \gg \hat{h}(Q)^{3r/2+3}(\log \hat{h}(Q))^2. \tag{2-2}$$

If Q is an x-pseudolinearly dependent point, then to detect $Q \notin \Gamma$ as the above, testing primes p of good reduction up to x is not enough, and thus the constant B must satisfy $B > x$, which is consistent with the second lower bound of Theorem 2.6 and (2-2). On the other hand, the inequality $B > x$ restricts how much Theorem 2.6 and [Sadek 2016, Theorem 4.4] can be improved.

3. Preliminaries

3A. ***Heights on elliptic curves.*** We briefly recall the definitions of the Weil height and the canonical height for points in $E(\mathbb{Q})$; see [Silverman 2009, Chapter VIII, § 9] for more details.

For a point $P = (x, y) \in E(\mathbb{Q})$ with $x = a/b$, with coprime integers a and b, we define the *Weil height* and the *canonical height* of P as

$$\mathfrak{h}(P) = \log \max\{|a|, |b|\} \quad \text{and} \quad \hat{h}(P) = \lim_{n \to +\infty} \frac{\mathfrak{h}(2^n P)}{4^n},$$

respectively. These two heights are related because they satisfy

$$\hat{h}(P) = \mathfrak{h}(P) + O(1),$$

where the implied constant depends only on E. In addition, for any $P \in E(\mathbb{Q})$ and $m \in \mathbb{Z}$, we have:

- $\hat{h}(mP) = m^2 \hat{h}(P)$;
- $\hat{h}(P) = 0$ if and only if P is a torsion point.

Furthermore, for any $P, Q \in E(\mathbb{Q})$, we have

$$\hat{h}(P+Q)+\hat{h}(P-Q)=2\hat{h}(P)+2\hat{h}(Q). \tag{3-1}$$

Following the hints in [Silverman 2009, Chapter IX, Exercise 9.8] and using [Silverman 2009, Chapter VIII, Proposition 9.6], one can show that if $P_1, \dots, P_r$ is a basis for the free part of $E(\mathbb{Q})$ (assuming $r \ge 1$), then for any integers $m_1, \dots, m_r$, we have

$$\hat{h}(m_1 P_1 + \cdots + m_r P_r) \ge c \max_{1 \le i \le r} m_i^2, \tag{3-2}$$

where c is a constant depending on E and $P_1, \dots, P_r$.

3B. ***A useful fact about elliptic curves.*** Every rational point $P \ne O_E$ in $E(\mathbb{Q})$ has a representation of the form

$$P = \left(\frac{m}{k^2}, \frac{n}{k^3}\right), \tag{3-3}$$

where m, n, and k are integers with $k \ge 1$ and $\gcd(m,k) = \gcd(n,k) = 1$; see [Silverman and Tate 1992, p. 68]. So, for any prime p of good reduction for E, $P \equiv O_E$ modulo p if and only if $p \mid k$.

3C. ***Counting primes related to the size of*** $\boldsymbol{\Gamma}$ ***under reduction.*** Here, we reproduce some results on counting primes p such that the size of Γ_p is less than some given value. For any prime p, if it is of good reduction for E, we define

$$N_p = \#E(\mathbb{F}_p) \quad \text{and} \quad T_p = \#\Gamma_p,$$

otherwise we let $N_p = T_p = 1$. Note that there are only finitely many primes p such that $N_p = 1$.

We first quote the following result from [Akbary et al. 2010, Proposition 5.4] (see [Gupta and Murty 1986, Lemma 14] for a previous result). Recall that s is the rank of Γ.

Lemma 3.1. *Assume that $s \ge 1$. For any $x \ge 2$, we have*

$$\#\{p : T_p < x\} \ll x^{1+2/s}/\log x.$$

We then restate two general results from [Akbary et al. 2010, Theorems 1.2 and 1.4] in a form convenient for our applications.

Lemma 3.2. *Assume that E is a non-CM curve and $s \ge 19$. Under the GRH, for any $x \ge 2$ we have*

$$\#\{p \le x : T_p < p/(\log p)^2\} \ll x/(\log x)^2.$$

Proof. We can clearly only consider the primes of good reduction. Here, we directly use the notation and follow the arguments in [Akbary et al. 2010, Proof of Part (a) of Theorem 1.2] by choosing the functions f and g as

$$f(x) = (\log x)^2, \qquad g(x) = f(x/\log x)/3. \tag{3-4}$$

Let $i_p = [E(\mathbb{F}_p) : \Gamma_p]$ for any prime p of good reduction. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be the two sets defined in [Akbary et al. 2010, p. 381]:

$$\begin{aligned}\mathcal{B}_1 &= \{p \le x : p \nmid \Delta_E, i_p \in (x^{2/(s+2)} \log x, 3x]\},\\ \mathcal{B}_2 &= \{p \le x : p \nmid m\Delta_E, m \mid i_p \text{ for some } m \in (g(x), x^{2/(s+2)} \log x]\},\end{aligned}$$

such that

$$\#\{p \le x : p \nmid \Delta_E, T_p < p/(\log p)^2\} \le \#\mathcal{B}_1 + \#\mathcal{B}_2 + O(x/(\log x)^2),$$

where the term $O(x/(\log x)^2)$ comes from $\pi(x/\log x) = O(x/(\log x)^2)$. We note that the choice of the sets is motivated by

- for $\mathcal{B}_1$, the bound on the number of primes $p \le x$ with a small value of T_p given by [Akbary et al. 2010, Proposition 5.4] which we have presented in Lemma 3.1;
- for $\mathcal{B}_2$, the range of m compared to x in which the divisibility $m \mid i_p$ for $p \le x$ can be controlled via the Chebotarev density theorem as given by [Akbary et al. 2010, Proposition 5.3].

In particular, we have

$$\#\mathcal{B}_1 \ll \frac{x}{(\log x)^{(s+2)/s} \cdot (s(s+2)^{-1} \log x - \log\log x)}$$

and

$$\#\mathcal{B}_2 \ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O(x^{1/2+\alpha+(5+\alpha/2)\cdot(2/(s+2)+\alpha)}),$$

where the positive real number α is chosen such that

$$\tfrac{1}{2} + \alpha + \left(5 + \tfrac{1}{2}\alpha\right) \cdot \left(\frac{2}{s+2} + \alpha\right) < 1,$$

which at least requires that $\frac{1}{2} + 6\alpha < 1$, that is $\alpha < \frac{1}{12}$. Note that such α indeed exists because $s \ge 19$.

It is easy to see that

$$\#\mathcal{B}_1 \ll x/(\log x)^2 \quad \text{and} \quad \#\mathcal{B}_2 \ll x/(\log x)^2,$$

where the second upper bound comes from $2(1-\alpha) > 1$. Collecting these estimates, we get the desired upper bound. □

Lemma 3.3. *Assume that E is a CM curve and $s \geq 7$. Under the GRH, for any $x \geq 2$ we have*

$$\#\{p \leq x : T_p < p/(\log p)^2\} \ll x/(\log x)^2.$$

Proof. We follow the arguments in [Akbary et al. 2010, Proof of Theorem 1.4] with only minor modifications by choosing the functions f and g there as in (3-4). Let $i_p = [E(\mathbb{F}_p) : \Gamma_p]$ for any prime p of good reduction. The following can be derived as in [Akbary et al. 2010, Proof of Part (a) of Theorem 1.2]:

$$\#\bigl\{p \leq x : p \nmid \Delta_E, T_p < p/(\log p)^2\bigr\} \leq \#\widetilde{\mathcal{B}}_1 + \#\widetilde{\mathcal{B}}_2 + O(x/(\log x)^2),$$

where

$$\begin{aligned}\widetilde{\mathcal{B}}_1 &= \{p \leq x : p \nmid \Delta_E, i_p \in (x^\kappa, 3x]\},\\ \widetilde{\mathcal{B}}_2 &= \{p \leq x : p \nmid m\Delta_E, m \mid i_p, \text{ for some } m \in (g(x), x^\kappa]\},\end{aligned}$$

with some real $\kappa > 0$ to be chosen later on. The reason for the choice of $\widetilde{\mathcal{B}}_1$ and $\widetilde{\mathcal{B}}_2$ is the same as that for $\mathcal{B}_1$ and $\mathcal{B}_2$, which is explained in the proof of Lemma 3.2. However, in the CM-case we have stronger versions of the underlying results which allow us a better choice of parameters and in turn enable us to handle smaller values of the rank s of Γ.

Applying Lemma 3.1, we have

$$\begin{aligned}\#\widetilde{\mathcal{B}}_1 &= \#\{p \leq x \ : \ p \nmid \Delta_E,\ T_p < N_p/x^\kappa\}\\ &\leq \#\{p \leq x \ : \ p \nmid \Delta_E,\ T_p < 3x^{1-\kappa}\} \ll \frac{x^{(1-\kappa)(s+2)/s}}{(1-\kappa)\log x}.\end{aligned}$$

For any positive integer m, let $\omega(m)$ and $d(m)$ denote, respectively, the number of distinct prime divisors of m and the number of positive integer divisors of m.

Now, $\#\widetilde{\mathcal{B}}_2$ can be estimated as in [Akbary et al. 2010, p. 393] as follows:

$$\#\widetilde{\mathcal{B}}_2 \ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O\biggl(x^{1/2}\log x \cdot \sum_{1 \leq m \leq x^\kappa} m a^{\omega(m)/2} d(m)\biggr),$$

where α is an arbitrary real number in the interval (0, 1) such that $2(1-\alpha) > 1$, and a is the absolute constant of [Akbary et al. 2010, Proposition 6.7]. Now, using [Akbary et al. 2010, Equation (6.21)] we obtain

$$\begin{aligned}\#\widetilde{\mathcal{B}}_2 &\ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O(x^{1/2+2\kappa}(\log x)^{1+\beta})\\ &\ll \frac{x}{(\log x)^2} + O(x^{1/2+2\kappa}(\log x)^{1+\beta}),\end{aligned}$$

where $\beta > 2$ is some positive integer.

Moreover, we choose the real number κ such that

$$(1-\kappa)(s+2)/s < 1 \quad \text{and} \quad \tfrac{1}{2}+2\kappa < 1.$$

Thus, we get

$$\frac{2}{s+2} < \kappa < \tfrac{1}{4}. \tag{3-5}$$

Since $s \geq 7$, such real number κ indeed exists.

Therefore, gathering the above estimates, for any fixed real number κ satisfying (3-5) (for example, $\kappa = \frac{11}{45}$) we obtain

$$\#\{p \leq x \;:\; p \nmid \Delta_E, T_p < p/(\log p)^2\} \ll x/(\log x)^2, \qquad \square$$

which completes the proof of this lemma.

3D. ***Kummer theory on elliptic curves.*** Following [Akbary et al. 2010; Bachmakov 1970; Bertrand 1981; Gupta and Murty 1986], we recall some basic facts about the Kummer theory on elliptic curves. Here, we should assume that $E(\mathbb{Q})$ is of rank $r \geq 2$.

Let ℓ be a prime, and let $P_1, P_2, \ldots, P_n \in E(\mathbb{Q})$ be linearly independent points over $\mathrm{End}_{\mathbb{Q}} E$. Consider the number field

$$L = \mathbb{Q}(E[\ell], \ell^{-1}P_1, \ldots, \ell^{-1}P_n),$$

where $E[\ell]$ is the set of ℓ-torsion points on E, and each $\ell^{-1}P_i$ $(1 \leq i \leq n)$ is a fixed point whose ℓ-multiple is the point P_i. Moreover, we denote $K = \mathbb{Q}(E[\ell])$ and $K_i = \mathbb{Q}(E[\ell], \ell^{-1}P_i)$ for every $1 \leq i \leq n$.

Now, both extensions $K/\mathbb{Q}$ and $L/\mathbb{Q}$ are Galois extensions. For the Galois groups, $\mathrm{Gal}(K/\mathbb{Q})$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, and $\mathrm{Gal}(L/K)$ is a subgroup of $E[\ell]^n$. Clearly, we have

$$[K:\mathbb{Q}] < \ell^4 \quad \text{and} \quad [L:K] \leq \ell^{2n}. \tag{3-6}$$

As an analogue of the classical Kummer theory, the results of Bashmakov [1970] show that (see also the discussions in [Bertrand 1981, p. 85]):

Lemma 3.4. *Assume that the residue classes of points $P_1, \ldots, P_n$ in $E(\mathbb{Q})/\ell E(\mathbb{Q})$ are linearly independent over $\mathrm{End}_{\mathbb{Q}} E/\ell\, \mathrm{End}_{\mathbb{Q}} E$. Then, we have*

$$\mathrm{Gal}(L/K) \cong E[\ell]^n.$$

For each field K_i with $1 \leq i \leq n$, the primes which ramify in the extension $K_i/\mathbb{Q}$ are exactly those primes dividing $\ell\Delta_E$. Then, the primes which ramify in the extension $L/\mathbb{Q}$ are exactly those primes dividing $\ell\Delta_E$. Now, pick a prime $p \nmid \ell\Delta_E$ which splits completely in K, and let $\mathfrak{p}_i$ be a prime ideal of $\mathcal{O}_{K_i}$ above p

for $i = 1, \dots, n$, where $\mathcal{O}_{K_i}$ the ring of integers of K_i. By the construction of K_i and noticing the choice of p, we have:

Lemma 3.5. *For each $1 \le i \le n$, the equation*

$$\ell X = P_i \tag{3-7}$$

has a solution in $E(\mathbb{F}_p)$, where X is an unknown, if and only if $[\mathcal{O}_{K_i}/\mathfrak{p}_i : \mathbb{F}_p] = 1$, that is, p splits completely in K_i.

Note that given an arbitrary finite Galois extension M/F of number fields, for each unramified prime $\mathfrak{p}$ of F, $\mathfrak{p}$ splits completely in M if and only if the Frobenius element corresponding to $\mathfrak{p}$ is the identity map. Then, we can obtain the following lemma:

Lemma 3.6. *Under the assumption in Lemma 3.4, we further assume that $n \ge 2$. Then, for any integer m with $1 \le m < n$, there is a conjugation class C in the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ such that every prime number p with the Artin symbol $\left[\frac{L/\mathbb{Q}}{p}\right] = C$ is unramified in $L/\mathbb{Q}$, p is a prime of good reduction for E, and p splits completely in the fields K_i, $1 \le i \le m$, but it does not split completely in any of the fields K_j, $m+1 \le j \le n$.*

Proof. One only needs to note that by Lemma 3.4, for any nonempty subsets I, J of $\{1, 2, \dots, n\}$ if $I \cap J = \varnothing$, we have

$$\prod_{i \in I} K_i \cap \prod_{j \in J} K_j = K,$$

where "$\prod$" means the composition of fields. □

Combining Lemma 3.5 with Lemma 3.6, we know that for the primes p in Lemma 3.6, Equation (3-7) has a solution in $E(\mathbb{F}_p)$ for $1 \le i \le m$ but for the others there is no such solution.

3E. ***The Chebotarev density theorem.*** For the convenience of the reader, we restate two useful results. The first one is an upper bound on the discriminant of a number field due to Hensel, see [Serre 1981, Proposition 6], while the second is about the least prime ideal as in the Chebotarev density theorem due to Lagarias, Montgomery and Odlyzko; see [Lagarias and Odlyzko 1977, p. 462] and [Lagarias et al. 1979, Theorem 1.1 and Equation (1.2)].

Lemma 3.7. *Let $L/\mathbb{Q}$ be a Galois extension of degree d and ramified only at the primes $p_1, \dots, p_m$. Then, we have*

$$\log |D_L| \le d \log d + d \sum_{i=1}^{m} \log p_i,$$

where D_L is the discriminant of $L/\mathbb{Q}$.

Lemma 3.8. *There exists an effectively computable positive absolute constant c_1 such that for any number field K, any finite Galois extension L/K and any conjugacy class C in $\mathrm{Gal}(L/K)$, there exists a prime ideal $\mathfrak{p}$ of K which is unramified in L, for which the Artin symbol $[(L/K)/\mathfrak{p}] = C$ and the norm $\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{p})$ is a rational prime satisfying the bound*

$$\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{p}) \le 2|D_L|^{c_1};$$

furthermore, under the GRH, there is an effectively computable positive absolute constant c_2 such that we can choose $\mathfrak{p}$ as above with

$$\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{p}) \le c_2(\log|D_L|)^2.$$

3F. *Effective version of Theorem 1.2.* The following result can be viewed as an effective version of Theorem 1.2 in some sense for a specific case. Recall that r and s are the ranks of $E(\mathbb{Q})$ and Γ respectively.

Lemma 3.9. *Assume that $\mathrm{End}_{\mathbb{Q}} E = \mathbb{Z}$, Γ is a free subgroup of $E(\mathbb{Q})$, and $\Gamma \equiv \widetilde{\Gamma}$ modulo the torsion points of $E(\mathbb{Q})$. Let $Q \in E(\mathbb{Q}) \setminus \Gamma$ be a point of infinite order such that $\langle Q\rangle \cap \Gamma = \{O_E\}$. Then, there exists a prime p of good reduction satisfying*

$$\log p \ll (\log \hat{h}(Q))^{2s+6} \log\log \hat{h}(Q)$$

such that $Q \notin \Gamma_p$. Assuming the GRH, we further have

$$p \ll (\log \hat{h}(Q))^{4s+12} (\log\log \hat{h}(Q))^2.$$

Proof. Let $P_1, \dots, P_r$ be a basis of the free part of $E(\mathbb{Q})$. Since $\Gamma \equiv \widetilde{\Gamma}$ modulo the torsion points, we can assume that $P_1, \dots, P_s$ form a basis of Γ. Note that, since the point Q is of infinite order, it can be represented as

$$Q = Q_0 + m_1 P_1 + \cdots + m_r P_r,$$

where Q_0 is a torsion point of $E(\mathbb{Q})$, and there is at least one $m_i \ne 0$ $(1 \le i \le r)$. Moreover, by the choice of Q, there exists j with $s+1 \le j \le r$ such that $m_j \ne 0$.

By (3-2), we have

$$\hat{h}(Q - Q_0) \gg \max_{1\le i\le r} m_i^2.$$

Noticing that Q_0 is a torsion point, by (3-1) we obtain

$$\hat{h}(Q) \ge \tfrac{1}{2}\hat{h}(Q - Q_0) \gg \max_{1\le i\le r} m_i^2. \tag{3-8}$$

Now, let ℓ be the smallest prime such that $\ell \nmid m_j$. Since the number $\omega(m)$ of distinct prime factors of an integer $m \ge 2$ satisfies

$$\omega(m) \ll \frac{\log m}{\log\log m}$$

(because we obviously have $\omega(m)! \le m$), using the prime number theorem we get

$$\ell \ll \log |m_j|,$$

which together with (3-8) yields that

$$\ell \ll \log \hat{h}(Q). \tag{3-9}$$

By the choice of ℓ, we see that there is no point $R \in E(\mathbb{Q})$ such that $Q = \ell R$. This implies that the number field $\mathbb{Q}(E[\ell], \ell^{-1}Q)$ is not a trivial extension of $\mathbb{Q}(E[\ell])$. Furthermore, by noticing $\ell \nmid m_j$, it is straightforward to see that the residue classes of $Q, P_1, \dots, P_s$ in $E(\mathbb{Q})/\ell E(\mathbb{Q})$ are linearly independent over $\operatorname{End}_{\mathbb{Q}} E/\ell \operatorname{End}_{\mathbb{Q}} E = \mathbb{Z}/\ell\mathbb{Z}$.

Consider the number field

$$L = \mathbb{Q}(E[\ell], \ell^{-1}Q, \ell^{-1}P_1, \dots, \ell^{-1}P_s),$$

and set $K = \mathbb{Q}(E[\ell])$. Now, combining Lemma 3.5 with Lemma 3.6, we can choose a conjugation class C in the Galois group $\operatorname{Gal}(L/\mathbb{Q})$ such that every prime number p with Artin symbol $[(L/\mathbb{Q})/p] = C$ is unramified in $L/\mathbb{Q}$, p is a prime of good reduction for E, and especially the equation $\ell X = P_i$ has solution in $E(\mathbb{F}_p)$ for each $1 \le i \le s$ but the equation $\ell X = Q$ has no such solution. This implies that

$$Q \notin \Gamma_p.$$

By Lemma 3.8, we can choose such a prime p such that

$$\log p \ll \log |D_L|; \tag{3-10}$$

if under the GRH, we even have

$$p \ll (\log |D_L|)^2. \tag{3-11}$$

From Lemma 3.7 and noticing that only the primes dividing $\ell\Delta_E$ ramify in the extension $L/\mathbb{Q}$, we get

$$\log |D_L| \le d \log d + d \log(\ell\Delta_E) \ll d \log d + d \log \ell, \tag{3-12}$$

where $d = [L : \mathbb{Q}]$. Using (3-6), we obtain

$$d \le \ell^{2s+6}. \tag{3-13}$$

Combining (3-9), (3-10), (3-11), and (3-12) with (3-13), we unconditionally have

$$\log p \ll (\log \hat{h}(Q))^{2s+6} \log\log \hat{h}(Q),$$

and under the GRH we have

$$p \ll (\log \hat{h}(Q))^{4s+12} (\log\log \hat{h}(Q))^2. \qquad \square$$

4. The existence and construction of x-pseudolinearly dependent points

4A. ***Existence.*** Before proving our main results, we want to first consider the existence problem of pseudolinearly dependent points. Recall that r is the rank of $E(\mathbb{Q})$ and s is the rank of Γ.

If $s < r$, then x-pseudolinearly dependent points with respect to Γ do exist. Indeed, since $s < r$, we can take a point $R \in E(\mathbb{Q})$ of infinite order such that $\langle R\rangle \cap \Gamma = \{O_E\}$. Pick an arbitrary point $P \in \Gamma$; it is easy to see that the point

$$Q = P + \operatorname{lcm}\{\#E(\mathbb{Q})_p \#\Gamma_p : p \le x \text{ of good reduction}\}R \tag{4-1}$$

is an x-pseudolinearly dependent point for any $x > 0$, where the least common multiple of the empty set is defined to be 1.

In the construction (4-1), we can see that $\langle Q\rangle \cap \Gamma = \{O_E\}$. Actually, when x is sufficiently large, any x-pseudolinearly dependent point with respect to Γ must satisfy this property.

Proposition 4.1. *There exists a constant M depending on E and Γ such that for any $x > M$, every x-pseudolinearly dependent point Q is nontorsion and satisfies $\langle Q\rangle \cap \Gamma = \{O_E\}$.*

Proof. Consider the subgroup $\widetilde{\Gamma}$ defined in (2-1). Notice that $\widetilde{\Gamma}$ is a finitely generated group containing the torsion points of $E(\mathbb{Q})$, and by construction each element in the quotient group $\widetilde{\Gamma}/\Gamma$ is of finite order. So, $\widetilde{\Gamma}/\Gamma$ is a finite group. Then, we let $n = [\widetilde{\Gamma} : \Gamma]$ and assume that $\widetilde{\Gamma}/\Gamma = \{P_0 = O_E, P_1, \dots, P_{n-1}\}$. If $n = 1$, that is $\widetilde{\Gamma} = \Gamma$, then for any $P \in E(\mathbb{Q}) \setminus \Gamma$ we have $\langle P\rangle \cap \Gamma = \{O_E\}$, and thus everything is done. Now, we assume that $n > 1$.

For any P_i, $1 \le i \le n-1$, since $P_i \notin \Gamma$, by Theorem 1.2 there exists a prime p_i of good reduction such that $P_i \notin \Gamma_{p_i}$. Then, we choose a constant, say M, such that $M \ge p_i$ for any $1 \le i \le n-1$. Thus, when $x > M$, any P_i $(1 \le i \le n-1)$ is not an x-pseudolinearly dependent point with respect to Γ, and then any point $P \in \widetilde{\Gamma}$ is also not such a point. So, the x-pseudolinearly dependent point Q is not in $\widetilde{\Gamma}$. This actually completes the proof. □

The above result clearly implies the following:

Corollary 4.2. *If Γ is a full rank subgroup of $E(\mathbb{Q})$ (that is $s = r$), then there exists a constant M depending on E and Γ such that for any $x > M$, there is no x-pseudolinearly dependent point.*

In other words, the case (that is $s < r$) in (4-1) is the only one meaningful case for x-pseudolinearly dependent points when x is sufficiently large. We also remark that directly by Theorem 1.2, any fixed point in $E(\mathbb{Q})$ is not an x-pseudolinearly dependent point with respect to Γ for x sufficiently large.

4B. ***Construction.*** In this section, we assume that the rank r of $E(\mathbb{Q})$ and the rank s of Γ satisfy $r \geq 1$ and $s < r$.

In order to get upper bounds on the height of pseudolinearly dependent points, the following construction is slightly different from what we give in (4-1).

Recalling N_p and T_p defined in Section 3C, given any $x \geq 2$, we define

$$L_x = \operatorname{lcm}\{N_p/T_p : p \leq x\}.$$

Take a point $R \in E(\mathbb{Q})$ of infinite order such that $\langle R\rangle \cap \Gamma = \{O_E\}$, then pick an arbitrary point $P \in \Gamma$ and set

$$Q = P + L_x R.$$

It is easy to see that $Q \notin \Gamma$ but $Q_p \in \Gamma_p$ for every prime $p \leq x$ of good reduction, and so Q is an x-pseudolinearly dependent point.

Since the coordinates of points in $E(\mathbb{Q})$ are rational numbers, for any subset $S \subseteq E(\mathbb{Q})$ there exists a point with smallest Weil height among all the points in S. So, noticing $s < r$, we choose a point with smallest Weil height in the subset consisting of nontorsion points R in $E(\mathbb{Q}) \setminus \Gamma$ with $\langle R\rangle \cap \Gamma = \{O_E\}$; we denote this point by $R_{\min}$.

Now, we define a point $Q_{\min} \in E(\mathbb{Q})$ as follows:

$$Q_{\min} = L_x R_{\min}. \tag{4-2}$$

As before, $Q_{\min} \notin \Gamma$ but $Q_{\min} \in \Gamma_p$ for every prime $p \leq x$ of good reduction. We also have

$$\hat{h}(Q_{\min}) = L_x^2 \hat{h}(R_{\min}) = L_x^2(\mathfrak{h}(R_{\min}) + O(1)) \ll L_x^2, \tag{4-3}$$

which comes from the fact that $\mathfrak{h}(R_{\min})$ is fixed when E and Γ are given.

The point $Q_{\min}$ is exactly the point we claim in Theorems 2.1, 2.2, 2.3, and 2.4. So, it remains to prove the claimed upper bounds for $\hat{h}(Q_{\min})$.

5. Proofs of upper bounds

5A. ***Outline.*** As mentioned above, to achieve our purpose, it suffices to bound the canonical height of $Q_{\min}$ given by (4-2), that is, $\hat{h}(Q_{\min})$.

By definition, we directly have

$$L_x \leq \prod_{p \leq x} N_p/T_p.$$

In view of (4-3), our approach is to get upper and lower bounds respectively for

$$\prod_{p \leq x} N_p \quad \text{and} \quad \prod_{p \leq x} T_p.$$

5B. ***Proof of Theorem 2.1.*** Recalling the Hasse bound

$$|N_p - p - 1| \le 2p^{1/2}$$

for any prime p of good reduction (see [Silverman 2009, Chapter V, Theorem 1.1]), we derive the inequality

$$\begin{aligned}\prod_{p\le x} N_p \le \prod_{p\le x}(p+2p^{1/2}+1) &= \prod_{p\le x} p(1+p^{-1/2})^2 \\ &= \exp\Bigl(\sum_{p\le x}\log p + 2\sum_{p\le x}\log(1+p^{-1/2})\Bigr) \\ &\le \exp\Bigl(\sum_{p\le x}\log p + 2\sum_{p\le x} p^{-1/2}\Bigr) \\ &= \exp(O(\sqrt{x}/\log x))\prod_{p\le x} p.\end{aligned} \tag{5-1}$$

Now using the prime number theorem in a simple form:

$$\sum_{p\le x}\log p = x + O(x/(\log x)^2), \tag{5-2}$$

we obtain

$$\prod_{p\le x} N_p \le \exp(x + O(x/(\log x)^2)). \tag{5-3}$$

Combining (5-3) with (4-3), we derive the following upper bound for $\hat{h}(Q_{\min})$:

$$\hat{h}(Q_{\min}) \ll L_x^2 \le \prod_{p\le x} N_p^2 \le \exp(2x + O(x/(\log x)^2)). \tag{5-4}$$

This completes the proof.

We remark that a better error term for the prime number theorem such as that of [Iwaniec and Kowalski 2004, Corollary 8.30] would improve the result, however, the improvement is not substantial, as seen by regarding the main term.

5C. ***Proof of Theorem 2.2.*** Since Γ has rank zero, by the injectivity of the reduction map restricted to the torsion subgroup, we can see that $T_p = \#\Gamma$ for any prime p of good reduction and coprime to the size of the torsion subgroup.

We also recall the prime number theorem in the following simplified form

$$\pi(x) = \frac{x}{\log x} + O(x/(\log x)^2), \tag{5-5}$$

which follows from (5-2).

Now, using (5-3) and (5-5) we have

$$L_x \ll (\#\Gamma)^{-\pi(x)} \prod_{p\le x} N_p \le \exp\Bigl(x - \log(\#\Gamma)\frac{x}{\log x} + O(x/(\log x)^2)\Bigr).$$

From (4-3) we conclude that for any sufficiently large $x > 0$, we have

$$\hat{h}(Q_{\min}) \le \exp\Bigl(2x - 2\log(\#\Gamma)\frac{x}{\log x} + O(x/(\log x)^2)\Bigr),$$

which completes the proof.

5D. ***Proof of Theorem 2.3.*** For any sufficiently large x, we define

$$J = \Bigl\lfloor \frac{s}{s+2}\log x \Bigr\rfloor \ge 1 \quad \text{and} \quad Z_j = x^{s/(s+2)}e^{-j}, \quad j = 0, \dots, J,$$

where e is the base of the natural logarithm. Note that $1 \le Z_J < e$.

Since $s \ge 1$, the number of primes p such that $T_p = 1$ or 2 is finite; we denote this number by N, which depends on Γ. Let M_0 be the number of primes $p \le x$ with $T_p \ge Z_0$. Furthermore, for $j = 1, \dots, J$, we define M_j as the number of primes $p \le x$ with $Z_{j-1} > T_p \ge Z_j$. Clearly

$$N + \sum_{j=0}^{J} M_j \ge \pi(x).$$

So, noticing $Z_0 = x^{s/(s+2)}$ we now derive

$$\prod_{p\le x} T_p \ge \prod_{j=0}^{J} Z_j^{M_j} \ge Z_0^{\pi(x)-N} \prod_{j=0}^{J} e^{-jM_j} = Z_0^{\pi(x)-N}\exp(-\Lambda),$$

where

$$\Lambda = \sum_{j=1}^{J} jM_j.$$

Recalling the definition of Z_0, and using (5-5), we obtain

$$\prod_{p\le x} T_p \ge \exp\Bigl(\frac{s}{s+2}x - \Lambda + O(x/\log x)\Bigr). \tag{5-6}$$

To estimate Λ, we note that by Lemma 3.1, for any positive integer $I \le J$ we have

$$\sum_{j=I}^{J} M_j \le \#\{p : T_p < Z_0e^{-I+1}\} \ll \frac{(Z_0e^{-I+1})^{1+2/s}}{\log Z_0 - I + 1}.$$

Thus for $I \le \frac{1}{2}J$, noticing $J \le \log Z_0$ we obtain

$$\sum_{j=I}^{J} M_j \ll \frac{(Z_0 e^{-I})^{1+2/s}}{\log Z_0} \ll e^{-I(1+2/s)} \frac{x}{\log x}, \tag{5-7}$$

while for any $\frac{1}{2}J < I \le J$ we use the bound

$$\sum_{j=I}^{J} M_j \ll (Z_0 e^{-I+1})^{1+2/s} \ll (\sqrt{Z_0})^{1+2/s} = x^{1/2}. \tag{5-8}$$

Hence, via partial summation, combining (5-7) and (5-8), we derive

$$\begin{aligned}\Lambda = \sum_{I=1}^{J}\sum_{j=I}^{J} M_j &\ll \frac{x}{\log x} \sum_{1\le I\le J/2} e^{-I(1+2/s)} + x^{1/2} \sum_{J/2<I\le J} 1 \\ &\ll \frac{x}{\log x} + Jx^{1/2} \ll \frac{x}{\log x}.\end{aligned}$$

This bound on Λ, together with (5-6), implies

$$\prod_{p\le x} T_p \ge \exp\Big(\frac{s}{s+2}x + O(x/\log x)\Big).$$

Therefore using (5-3), we obtain

$$L_x \le \prod_{p\le x} N_p/T_p \le \exp\Big(\frac{2}{s+2}x + O(x/\log x)\Big).$$

Therefore, the desired result follows from the bound (4-3).

5E. ***Proof of Theorem 2.4.*** First, we have

$$\begin{aligned}\prod_{p\le x} T_p &\ge \prod_{\substack{p\le x\\ T_p\ge p/(\log p)^2}} \frac{p}{(\log p)^2} \cdot \prod_{\substack{p\le x\\ T_p< p/(\log p)^2}} T_p \\ &= \prod_{p\le x} \frac{p}{(\log p)^2} \cdot \prod_{\substack{p\le x\\ T_p< p/(\log p)^2}} \frac{T_p(\log p)^2}{p}.\end{aligned}$$

Using the trivial lower bound $T_p \ge 1$, we derive

$$\begin{aligned}\prod_{p\le x} T_p &\ge \prod_{p\le x} p \cdot \prod_{p\le x} (\log p)^{-2} \cdot \prod_{\substack{p\le x\\ T_p< p/(\log p)^2}} (\log p)^2/p \\ &\ge \Big(\frac{(\log x)^2}{x}\Big)^{O(x/(\log x)^2)} \prod_{p\le x} p \cdot \prod_{p\le x} (\log p)^{-2},\end{aligned}$$

where the last inequality follows from Lemma 3.2 and Lemma 3.3.

Thus, using (5-1), we obtain

$$\begin{aligned} L_x \le \prod_{p\le x} N_p/T_p &\le \exp(O(x/\log x)) \prod_{p\le x} (\log p)^2 \\ &\le \exp\Bigl(2\frac{x\log\log x}{\log x} + O(x/\log x)\Bigr), \end{aligned}$$

where the last inequality is derived from (5-5) and the trivial estimate

$$\sum_{p\le x} \log\log p \le \pi(x)\log\log x.$$

Therefore, the desired result follows from the bound $\hat{h}(Q_{\min}) \ll L_x^2$.

6. Proofs of lower bounds

6A. ***Proof of Theorem 2.5.*** By assumption, Γ is a torsion subgroup of $E(\mathbb{Q})$. Let $Q \in E(\mathbb{Q})$ be an arbitrary x-pseudolinearly dependent point for a sufficiently large x. Let m be the number of primes of bad reduction for E. Then, since $Q \in \Gamma_p$ for any prime $p \le x$ of good reduction, there exists a rational point $P \in \Gamma$ such that for at least $(\pi(x)-m)/\#\Gamma$ primes $p \le x$ of good reduction we have

$$Q \equiv P \pmod{p}.$$

In view of (3-3), this implies that

$$\mathfrak{h}(Q-P) \ge 2\log \prod_{p\le(\pi(x)-m)/\#\Gamma} p \ge \frac{2}{\#\Gamma} x/\log x + O(x/(\log x)^2),$$

where the last inequality follows from (5-2) and (5-5). Note that P is a torsion point; then using (3-1) we obtain

$$\begin{aligned} \text{(6-1)}\qquad \hat{h}(Q) = \hat{h}(Q) + \hat{h}(P) \ge \tfrac{1}{2}\hat{h}(Q-P) &\ge \tfrac{1}{2}\mathfrak{h}(Q-P) + O(1) \\ &\ge \frac{1}{\#\Gamma} x/\log x + O(x/(\log x)^2), \end{aligned}$$

which gives the claimed lower bound for the height of the point Q.

6B. ***Proof of Theorem 2.6.*** For any sufficiently large x, by Proposition 4.1, any x-pseudolinearly dependent point Q of Γ is nontorsion and satisfies $\langle Q\rangle \cap \Gamma = \{O_E\}$. Then, from Lemma 3.9, there is an unconditional prime p of good reduction for E satisfying

$$\log p \ll (\log \hat{h}(Q))^{2s+6} \log\log \hat{h}(Q)$$

such that $Q \notin \Gamma_p$. Since $x < p$, by definition we obtain

$$\log x \ll (\log \hat{h}(Q))^{2s+6} \log\log \hat{h}(Q),$$

which implies that $\hat{h}(Q) \geq \exp((\log x)^{1/(2s+6)+o(1)})$.

Similarly, assuming the GRH, we obtain

$$\hat{h}(Q) \geq \exp(x^{1/(4s+12)+o(1)}),$$

which completes the proof.

7. Comments

In Section 6, we get some partial results on the lower bound for the height of x-pseudolinearly dependent points. In fact, the height of such points certainly tends to infinity as $x \to +\infty$.

Indeed, let E be an elliptic curve over $\mathbb{Q}$ of rank $r \geq 1$, and let Γ be a subgroup of $E(\mathbb{Q})$ with rank $s < r$. We have known that for any sufficiently large x, there exist infinitely many x-pseudolinearly dependent points with respect to Γ. For any $x > 0$, if such points exist, as before we can choose a point, denoted by Q_x, with smallest Weil height among all these points; otherwise if there are no such points, we let $Q_x = O_E$. Thus, we get a subset

$$S = \{Q_x : x > 0\}$$

of $E(\mathbb{Q})$, and for any $x < y$ we have $\mathfrak{h}(Q_x) \leq \mathfrak{h}(Q_y)$. By Theorem 1.2, we know that for any fixed point $Q \in E(\mathbb{Q})$, it can not be an x-pseudolinearly dependent point for any sufficiently large x. So, S is an infinite set. Since it is well-known that there are only finitely many rational points of $E(\mathbb{Q})$ with bounded height, we obtain

$$\lim_{x \to +\infty} \mathfrak{h}(Q_x) = +\infty,$$

which implies that $\lim_{x \to +\infty} \hat{h}(Q_x) = +\infty$. This immediately implies that for the point $Q_{\min}$ constructed in Section 4B, its height $\hat{h}(Q_{\min})$ also tends to infinity as $x \to +\infty$.

Moreover, let p_n denote the n-th prime, that is $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$ For any $n \geq 1$, denote by T_n the set of p_n-pseudolinearly dependent points of Γ. Obviously, $T_{n+1} \subseteq T_n$ and $\mathfrak{h}(Q_{p_{n+1}}) \geq \mathfrak{h}(Q_{p_n})$ for any $n \geq 1$. For any sufficiently large n, we conjecture that $T_{n+1} \subsetneq T_n$. If furthermore one could prove that $\mathfrak{h}(Q_{p_{n+1}}) > \mathfrak{h}(Q_{p_n})$ for any sufficiently large n, this would lead to a lower bound of the form

$$\mathfrak{h}(Q_x) \geq \log x + O(\log\log x),$$

as the values of $\mathfrak{h}(Q_x)$ are logarithms of rational integers and there are about $x/\log x$ primes not greater than x.

In Lemma 3.9, if we choose Γ as a torsion subgroup, we can also get a similar unconditional upper bound. Indeed, for a prime p of good reduction for E, suppose that $Q \in \Gamma_p$. Then, $Q - P \equiv O_E$ modulo p for some $P \in \Gamma$. According to (3-3), we have $p \le \exp(\mathfrak{h}(Q - P)/2)$. Since P is a torsion point, as in (6-1) we get $p \le \exp(\hat{h}(Q) + O(1))$. Thus, we can choose a prime p of good reduction satisfying

$$p \le \exp(\hat{h}(Q) + O(1))$$

such that $Q \notin \Gamma_p$.

Acknowledgements

The authors are very grateful to the referees for their careful reading and valuable comments and suggestions. The authors also thank Wojciech Gajda for his very stimulating discussions which led to the idea of this work and also for his valuable comments on an early version of the paper. These discussions took place at the Max Planck Institute for Mathematics, Bonn, whose support and hospitality are gratefully acknowledged.

This work was also supported in part by the Australian Research Council Grants DP140100118 and DP170100786.

References

[Akbary et al. 2010] A. Akbary, D. Ghioca, and V. K. Murty, "Reductions of points on elliptic curves", *Math. Ann.* **347**:2 (2010), 365–394. MR

[Bach et al. 1996] E. Bach, R. Lukes, J. Shallit, and H. C. Williams, "Results and estimates on pseudopowers", *Math. Comp.* **65**:216 (1996), 1737–1747. MR Zbl

[Bachmakov 1970] M. Bachmakov, "Un théorème de finitude sur la cohomologie des courbes elliptiques", *C. R. Acad. Sci. Paris Sér. A-B* **270** (1970), A999–A1001. MR Zbl

[Banaszak 2009] G. Banaszak, "On a Hasse principle for Mordell–Weil groups", *C. R. Math. Acad. Sci. Paris* **347**:13-14 (2009), 709–714. MR Zbl

[Banaszak and Krasoń 2011] G. Banaszak and P. Krasoń, "On arithmetic in Mordell–Weil groups", *Acta Arith.* **150**:4 (2011), 315–317. MR Zbl

[Banaszak et al. 2005] G. Banaszak, W. Gajda, and P. Krasoń, "Detecting linear dependence by reduction maps", *J. Number Theory* **115**:2 (2005), 322–342. MR Zbl

[Bertrand 1981] D. Bertrand, "Kummer theory on the product of an elliptic curve by the multiplicative group", *Glasgow Math. J.* **22**:1 (1981), 83–88. MR

[Bourgain et al. 2009] J. Bourgain, S. V. Konyagin, C. Pomerance, and I. E. Shparlinski, "On the smallest pseudopower", *Acta Arith.* **140**:1 (2009), 43–55. MR Zbl

[Gajda and Górnisiewicz 2009] W. Gajda and K. Górnisiewicz, "Linear dependence in Mordell–Weil groups", *J. Reine Angew. Math.* **630** (2009), 219–233. MR Zbl

[Gupta and Murty 1986] R. Gupta and M. R. Murty, “Primitive points on elliptic curves”, *Compositio Math.* **58**:1 (1986), 13–44. MR Zbl

[Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications **53**, American Mathematical Society, Providence, RI, 2004. MR Zbl

[Jossen 2013] P. Jossen, “Detecting linear dependence on an abelian variety via reduction maps”, *Comment. Math. Helv.* **88**:2 (2013), 323–352. MR Zbl

[Jossen and Perucca 2010] P. Jossen and A. Perucca, “A counterexample to the local-global principle of linear dependence for abelian varieties”, *C. R. Math. Acad. Sci. Paris* **348**:1-2 (2010), 9–10. MR Zbl

[Konyagin et al. 2010] S. V. Konyagin, C. Pomerance, and I. E. Shparlinski, “On the distribution of pseudopowers”, *Canad. J. Math.* **62**:3 (2010), 582–594. MR Zbl

[Kowalski 2003] E. Kowalski, “Some local-global applications of Kummer theory”, *Manuscripta Math.* **111**:1 (2003), 105–139. MR Zbl

[Lagarias and Odlyzko 1977] J. C. Lagarias and A. M. Odlyzko, “Effective versions of the Chebotarev density theorem”, pp. 409–464 in *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham)* (Durham, NC, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR Zbl

[Lagarias et al. 1979] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, “A bound for the least prime ideal in the Chebotarev density theorem”, *Invent. Math.* **54**:3 (1979), 271–296. MR Zbl

[Perucca 2010] A. Perucca, “On the problem of detecting linear dependence for products of abelian varieties and tori”, *Acta Arith.* **142**:2 (2010), 119–128. MR Zbl

[Pomerance and Shparlinski 2009] C. Pomerance and I. E. Shparlinski, “On pseudosquares and pseudopowers”, pp. 171–184 in *Combinatorial number theory*, edited by B. Landman et al., Walter de Gruyter, Berlin, 2009. MR Zbl

[Sadek 2016] M. Sadek, “On dependence of rational points on elliptic curves”, *C. R. Math. Acad. Sci. Soc. R. Can.* **38**:2 (2016), 75–84. MR Zbl

[Schinzel 1960] A. Schinzel, “On the congruence $a^x \equiv b \pmod{p}$”, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **8** (1960), 307–309. MR Zbl

[Schinzel 1970] A. Schinzel, “A refinement of a theorem of Gerst on power residues”, *Acta Arith.* **17** (1970), 161–168. MR Zbl

[Schinzel 1975] A. Schinzel, “On power residues and exponential congruences”, *Acta Arith.* **27** (1975), 397–420. MR Zbl

[Schinzel 1997] A. Schinzel, “On pseudosquares”, pp. 213–220 in *New trends in probability and statistics* (Palange, 1996), vol. 4, edited by A. Laurinčikas et al., VSP, Utrecht, The Netherlands, 1997. MR Zbl

[Serre 1981] J.-P. Serre, “Quelques applications du théorème de densité de Chebotarev”, *Inst. Hautes Études Sci. Publ. Math.* 54 (1981), 323–401. MR Zbl

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, 2009. MR Zbl

[Silverman and Tate 1992] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer, 1992. MR Zbl

[Weston 2003] T. Weston, “Kummer theory of abelian varieties and reductions of Mordell–Weil groups”, *Acta Arith.* **110**:1 (2003), 77–88. MR Zbl

Received June 10, 2016. Revised October 18, 2017.

MIN SHA
SCHOOL OF MATHEMATICS AND STATISTICS
UNIVERSITY OF NEW SOUTH WALES
SYDNEY, NSW
AUSTRALIA

shamin2010@gmail.com

IGOR E. SHPARLINSKI
SCHOOL OF MATHEMATICS AND STATISTICS
UNIVERSITY OF NEW SOUTH WALES
SYDNEY, NSW
AUSTRALIA

igor.shparlinski@unsw.edu.au

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2018 is US $475/year for the electronic version, and $640/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS

Volume 295 No. 1 July 2018

0030-8730(201807)295:1;1-Q