ACTA ARITHMETICA
166.2 (2014)

On the average value of the canonical height in higher dimensional families of elliptic curves

by

Wei Pin Wong (Providence, RI)

1. Introduction. Let K be the function field $\mathbb{Q}(T_1,\dots,T_n)$ and $\mathbf{T} = (T_1,\dots,T_n)$. Let E/K be an elliptic curve with Weierstrass equation

$$Y^2 = X^3 + A(\mathbf{T})X + B(\mathbf{T})$$

where by a change of variable, we can assume $A(\mathbf{T}), B(\mathbf{T}) \in \mathbb{Z}[\mathbf{T}]$ and there is no nonconstant $g(\mathbf{T}) \in \mathbb{Q}[\mathbf{T}]$ such that

$$A(\mathbf{T})/g(\mathbf{T})^4, B(\mathbf{T})/g(\mathbf{T})^6 \in \mathbb{Z}[\mathbf{T}].$$

We further assume that E/K is not split over K, i.e. E is not K-birational isomorphic to $E_0 \times_{\mathbb{Q}} K$ for any elliptic curve $E_0/\mathbb{Q}$. This implies that $A(\mathbf{T})$ and $B(\mathbf{T})$ cannot both be constant. The discriminant

$$\Delta_E(\mathbf{T}) = -16(4A^3(\mathbf{T}) + 27B^2(\mathbf{T}))$$

is a nonzero element in $\mathbb{Z}[\mathbf{T}]$. Let $\mathbb{Q}^n(\Delta_E)$ be the set of all $\omega = (\omega_1,\dots,\omega_n) \in \mathbb{Q}^n$ such that $\Delta_E(\omega) \neq 0$. Thus for every $P \in E(K)$, for ω such that $P_\omega := P(\omega)$ is defined, the point P_ω is a rational point on the elliptic curve $E_\omega/\mathbb{Q}$ defined by the Weierstrass equation

$$Y^2 = X^3 + A(\omega)X + B(\omega).$$

We denote the canonical height on E_ω by $\hat{h}_{E_\omega}$ and the logarithmic height on $\mathbb{P}^n_{\mathbb{Q}}$ by h, i.e.

$$h(\omega) = \log H(\omega) := \log H([1,\omega_1,\dots,\omega_n]),$$

where

$$H([\nu_0,\dots,\nu_n]) = \max_i\{|\nu_i|\} \quad \text{if } \nu_i \in \mathbb{Z} \text{ and } \gcd(\nu_0,\dots,\nu_n) = 1.$$

To ease the notation, we will write $\|\nu\| := \max_i\{|\nu_i|\}$ for any $\nu \in \mathbb{Z}^n$.

We will prove the following theorems about the average value of $\hat{h}_{E_\omega}(P_\omega)/h(\omega)$.

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11G50, 14G40.
Key words and phrases: height function, elliptic curve, function field, average, lower bound.

DOI: 10.4064/aa166-2-1

THEOREM 1. *With notation as above, let*

$$\begin{aligned}\mathbb{Q}_B^n(\Delta_E) &:= \{\omega \in \mathbb{Q}^n \mid 1 < H(\omega) \le B \text{ and } \Delta_E(\omega) \ne 0\},\\ E(K)_{\mathrm{nt}} &:= \{P \in E(K) \mid P \text{ nontorsion}\},\\ \mathbb{Q}_B^n(\Delta_E, P) &:= \{\omega \in \mathbb{Q}_B^n(\Delta_E) \mid P_\omega \text{ is defined}\} \quad \text{for } P \in E(K).\end{aligned}$$

Then there exists an $L_1 > 0$ depending only on Δ_E such that for all P in $E(K)_{\mathrm{nt}}$,

$$\underline{Ah}_E^{\mathbb{Q}}(P) := \liminf_{B\to\infty} \frac{1}{\#\mathbb{Q}_B^n(\Delta_E, P)} \sum_{\omega\in\mathbb{Q}_B^n(\Delta_E,P)} \frac{\hat{h}_{E_\omega}(P_\omega)}{h(\omega)} \ge L_1.$$

When $n = 1$, Silverman [11] proved that

$$\lim_{\substack{\omega\in\bar{\mathbb{Q}}^n\\ h(\omega)\to\infty}} \frac{\hat{h}_{E_\omega}(P_\omega)}{h(\omega)} = \hat{h}_E(P),$$

where $\hat{h}_E(P)$ is the canonical height of P in E/K. One would like to obtain a similar result for general n but by a simple observation this limit cannot exist for $n \ge 2$. This is because we can restrict the ω to lie on a particular algebraic curve γ for $h(\omega)$ tending to infinity, reducing this to the case of $n = 1$, but now the limit obtained will depend on P_γ and the elliptic curve E_γ in which it lies. For illustration, consider the elliptic curve

$$E/\mathbb{Q}(S,T) : Y^2 = X^3 - S^2X + T^2$$

and $P = (S,T) \in E(\mathbb{Q}(S,T))$. If we restrict ω to $\gamma : S = 0$, a simple calculation shows that $P_\gamma = (0,T)$ is a torsion point on $E_\gamma(\mathbb{Q}(T)) : Y^2 = X^3 + T^2$. Thus the limit of $\hat{h}_{E_\omega}(P_\omega)/h(\omega)$ is zero when $h(\omega)$ tends to infinity by restricting $\omega \in \gamma$. On the other hand, if we restrict ω to the curve $\gamma' : S = T$, then $P_{\gamma'} = (T,T)$ is in a basis of $E_{\gamma'}(\mathbb{Q}(T)) : Y^2 = X^3 - T^2X + T^2$ (this is an example given in [12]). Thus Silverman's theorem implies a nonzero limit of the quotient when $h(\omega)$ tends to infinity by restricting $\omega \in \gamma'$. In fact, this limit is $1/6$. One can also look at the restriction $T = 1$ (resp. $S = 1$) and get the limit of the quotient equal to $1/2$ (resp. $1/3$).

Since the limit of $\hat{h}_{E_\omega}(P_\omega)/h(\omega)$ fails to exist in general for $n \ge 2$, we turn our attention to the average of this quotient:

$$Ah_E^{\mathbb{Q}}(P)_B := \frac{1}{\#\mathbb{Q}_B^n(\Delta_E, P)} \sum_{\omega\in\mathbb{Q}_B^n(\Delta_E,P)} \frac{\hat{h}_{E_\omega}(P_\omega)}{h(\omega)}.$$

Following the idea of Silverman, we make the following conjecture:

CONJECTURE 2. *In the setting of Theorem 1, for any $P \in E(K)$,*

$$\lim_{B\to\infty} Ah_E^{\mathbb{Q}}(P)_B = \hat{h}_E(P).$$

The case $n = 1$ of this conjecture follows trivially from Silverman's theorem and the Cesàro mean theorem. However, proving this conjecture for $n \geq 2$ appears to be difficult, so we first check whether the conjecture makes sense, i.e.: if the limit of the average exists as a function of $P \in E(K)$, does it have the properties of the canonical height function ([13, Chapter VIII, Theorem 9.3] or [6, Chapter 5])?

One such property is that $\hat{h}_E$ is a quadratic form. By linearity of average, it is straightforward that the limit of $Ah_E^{\mathbb{Q}}(-)_B$, if it exists, is a quadratic form too. Another important property of the canonical height on E/K is that $\hat{h}_E(P) = 0$ if and only if P is in the subgroup generated by the torsion points and the image of the $K/\mathbb{Q}$-trace of E [6, Chapter 6, Theorem 5.4]. Since we assume E is not split over K, the $K/\mathbb{Q}$-trace is of dimension zero, which means it is the trivial group and hence its image in E is the identity. In other words, if E is not split over K, then

$$\hat{h}_E(P) = 0 \quad \text{if and only if} \quad P \text{ is a torsion point.} \tag{1}$$

So we investigate property (1) for $\liminf Ah_E^{\mathbb{Q}}(P)_B$. We shall prove that $\liminf Ah_E^{\mathbb{Q}}(P)_B$ is zero if and only if P is a torsion point of $E(K)$. The "if" part is trivial since if P is a torsion point of $E(K)$, then P_ω is a torsion point of $E_\omega(\mathbb{Q})$ and so the average is always zero. It turns out that the other direction is also true. We first look at the average over $\mathbb{Z}^n$:

PROPOSITION 3. *With notation as above, let further*

$$\mathbb{Z}_B^n(\Delta_E) := \{\nu \in \mathbb{Z}^n \mid 1 < \|\nu\| \leq B \text{ and } \Delta_E(\nu) \neq 0\}.$$
$$\mathbb{Z}_B^n(\Delta_E, P) := \{\nu \in \mathbb{Z}_B^n(\Delta_E) \mid P_\nu \text{ is defined}\} \quad \text{for } P \in E(K).$$

Then there exists an $L_2 > 0$, depending only on Δ_E, such that for all P in $E(K)_{\mathrm{nt}}$,

$$\underline{Ah}_E^{\mathbb{Z}}(P) := \liminf_{B\to\infty} \frac{1}{(2B)^n} \sum_{\nu \in \mathbb{Z}_B^n(\Delta_E, P)} \frac{\hat{h}_{E_\nu}(P_\nu)}{h(\nu)} \geq L_2.$$

Proposition 3 is the key tool to prove Theorem 1 via a standard inclusion-exclusion argument. Notice that Proposition 3 and Theorem 1 state something stronger: there exists a uniform nonzero lower bound of $\underline{Ah}_E^{\mathbb{Z}}(-)$ and $\underline{Ah}_E^{\mathbb{Q}}(-)$ for all nontorsion P in $E(K)$. One might think that the uniform lower bound is expected once we prove that $\underline{Ah}_E^{\mathbb{Z}}(P) > 0$ and $\underline{Ah}_E^{\mathbb{Q}}(P) > 0$ for P in $E(K)_{\mathrm{nt}}$, due to the fact that $E(K)_{\mathrm{nt}}$ is finitely generated and $\hat{h}_{E_\omega}$ can be extended to a positive definite quadratic form on $E_\omega(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$. At the level of $E_\omega(\mathbb{Q})$, one can get a uniform lower bound of $\hat{h}_{E_\omega}$ on the lattice $E_\omega(\mathbb{Q})_{\mathrm{nt}} \subset E_\omega(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$ in terms of the canonical height of a nice basis of $E_\omega(\mathbb{Q})_{\mathrm{nt}}$ [6, Chapter 5, Theorem 7.7 and Corollary 7.9]. However, at the average level, it is not obvious at all whether one can find a basis $\{P_i\}_{i\in I}$

of $E(K)_{\mathrm{nt}}$ such that the specialization $\{P_i(\omega)\}_{i\in I}$ is always a nice basis in the image of the specialization $(E(K)_{\mathrm{nt}})_\omega \subseteq E_\omega(\mathbb{Q})_{\mathrm{nt}}$ for all ω. Our proofs produce the uniform lower bounds without exploiting these facts.

We will postpone the proofs of Proposition 3 and Theorem 1 to Sections 5 and 6 respectively. On the other hand, we also prove that $\limsup Ah_E^{\mathbb{Q}}(P)_B$ is finite.

THEOREM 4. *With the same hypothesis as in Theorem* 1 *and for any* $P \in E(K)$*, there exists a constant* U_P*, depending only on* P*, such that*

$$\hat{h}_{E_\omega}(P_\omega) \le U_P(1 + h(\omega))$$

for all $\omega \in \mathbb{Q}_B^n(\Delta_E, P)$*. Consequently,*

$$\overline{Ah}_E^{\mathbb{Q}}(P) := \limsup_{B\to\infty} \frac{1}{\#\mathbb{Q}_B^n(\Delta_E, P)} \sum_{\omega\in\mathbb{Q}_B^n(\Delta_E,P)} \frac{\hat{h}_{E_\omega}(P_\omega)}{h(\omega)} < \infty.$$

In fact Theorem 4 is true in a more general setting as stated in the following theorem:

THEOREM 5. *Let* k *be a number field, let* S *and* A *be nonsingular, irreducible, projective varieties defined over* k*, and let* $\pi : A \to S$ *be a flat morphism defined over* k *so that the generic fiber* A_η *of* π *is an abelian variety over* $k(S)$*. Let*

$$S^0 := \{\omega \in S(k) \mid A_\omega \text{ is a nonsingular abelian variety defined over } k\}.$$

Fix a divisor $D \in \mathrm{Div}_{\overline{k}}(A)$*. For each* $\omega \in S^0$*, let* $D_\omega \in \mathrm{Div}(A_\omega)$ *be any divisor in the restriction of the divisor class of* D *to* A_ω *and let the corresponding canonical height be* $\hat{h}_{A_\omega,D_\omega}$*. Fix a projective embedding* $i : S \subset \mathbb{P}^n$*. Then for any* $P \in A_\eta(k(S))$*, there exists a constant* c_0 *depending on* $h_{A,D}$*,* D*,* i *and* P *such that*

$$\hat{h}_{A_\omega,D_\omega}(P_\omega) < c_0(1 + h(i(\omega)))$$

for all $\omega \in S^0$ *for which* P_ω *is defined. As a consequence, if we let*

$$S_B^0(P) := \{\omega \in S^0 \mid 1 < H(i(\omega)) < B,\ P_\omega \text{ is defined}\},$$

then

$$\overline{Ah}_{A_\eta}^{\mathbb{Q}}(P) := \limsup_{B\to\infty} \frac{1}{\#S_B^0(P)} \sum_{\omega\in S_B^0(P)} \frac{\hat{h}_{A_\omega,D_\omega}(P_\omega)}{h(i(\omega))} < \infty.$$

Theorem 5 is easier to prove than Theorem 1, so we will prove the former theorem first in Section 2. The we prove Theorem 4 in Section 3 in a similar fashion.

The behavior of $\hat{h}_{E_\omega}(P_\omega)$ for $n = 1$ is well studied in the literature in a more general setting of an abelian variety A defined over a function field

$k(C)$ of a nonsingular projective curve C over a number field k. In fact, this is the original setting of [11] where Silverman proved

$$\lim_{\substack{t\in C(\bar{k})\\ h(t)\to\infty}} \frac{\hat{h}_{A_t}(P_t)}{h(t)} = \hat{h}_A(P).$$

For the special case where $A = E$ is an elliptic surface, Tate [17] obtained a stronger result by showing that

$$\hat{h}_{E_t}(P_t) = \hat{h}_E(P)h(t) + O_P(\sqrt{h(t)} + 1)$$

and if $C = \mathbb{P}^1$, the error is only $O_P(1)$. This stronger result was extended to the general case of abelian varieties by Lang [6, Chapter 12, Section 5] under the assumption that the Néron model of the generic fiber has a good completion. Call [2] reproved Lang's result using a theorem on canonical heights and further discussed cases where the good completion assumption may be weakened or eliminated. Readers can consult Chapter III of [15] for a nice introduction and other results on elliptic surfaces.

Although the behavior of $\hat{h}_{E_\omega}(P_\omega)$ for $n \geq 2$ is not yet well studied in the literature, we know something about the density of ω such that $\hat{h}_{E_\omega}(P_\omega) = 0$, i.e. P_ω is torsion. Again, this is known in the setting of an abelian variety A defined over the function field $k(V)$ of a variety V over a number field k. Masser [8] proved that for a finitely generated subgroup Γ of A the specialization homomorphism

$$\sigma_\omega : \Gamma \to A_\omega(k(\omega))$$

is injective "almost always" for $\omega \in V(\bar{k})$.

2. Proof of Theorem 5. Notice that it suffices to prove that $\hat{h}_{A_\omega,D_\omega}(P_\omega)/h(i(\omega))$ is bounded above uniformly for all $\omega \in S_B^0(P)$. This is an immediate consequence of Theorem A of [11], due to Silverman and Tate. In fact, under the hypothesis of Theorem 5 let further $h_{A,D}$ be the Weil height (defined up to equivalence) corresponding to D. Then Theorem A says that there exists a constant c depending on D and A such that for all $P \in A_\eta(K)$,

$$|\hat{h}_{A_\omega,D_\omega}(P_\omega) - h_{A,D}(P_\omega)| < ch(i(\omega)) + O(1),$$

where $O(1)$ depends on the choice of particular Weil heights $h_{A,D}$ and the embedding i. So we reduce the problem to estimating $h_{A,D}(P_\omega)$.

We recall the definition of $h_{A,D}$. If $D \in \mathrm{Div}_{\bar{k}}(A)$ is very ample, then choose an embedding $\phi_D : A \to \mathbb{P}^m_{\bar{k}}$ corresponding to the linear system $|D|$. Then $h_{A,D}$ is defined by

$$h_{A,D} : A(\bar{k}) \to \mathbb{R}, \qquad p \mapsto h(\phi_D(p)).$$

For a general divisor $D \in \mathrm{Div}_{\overline{k}}(A)$, write $D = X - Y$, where $X, Y \in \mathrm{Div}_{\overline{k}}(A)$ are very ample divisors, and define

$$h_{A,D}(p) := h_{A,X}(p) - h_{A,Y}(p).$$

Any $P \in A_\eta(K)$ defines a rational map

$$\psi_P : S \dashrightarrow A, \quad \omega \mapsto P_\omega.$$

So we have

$$\begin{aligned} h_{A,D}(P_\omega) &= h_{A,X}(P_\omega) - h_{A,Y}(P_\omega) = h(\phi_X(\psi_P(\omega))) - h(\phi_Y(\psi_P(\omega))) \\ &\le h(\phi_X(\psi_P(\omega))), \end{aligned}$$

where $f_X := \phi_X \circ \psi_P$ is a rational map from S to $\mathbb{P}^m$. By using the triangle inequality for absolute values of k, one can show the following standard property of height on projective space [6, Chapter 4, Lemma 1.6]:

$$h(f_X(\omega)) \le dh(i(\omega)) + c_1$$

for some constants c_1 and d that depend on f_X only. Finally, by applying Theorem A, we get

$$\begin{aligned} \hat{h}_{A_\omega, D_\omega}(P_\omega) &\le h_{A,D}(P_\omega) + ch(i(\omega)) + O(1) \\ &\le dh(i(\omega)) + c_1 + ch(i(\omega)) + O(1), \end{aligned}$$

which is the first part of the theorem. Since the set of points of bounded height in $\mathbb{P}^n(k)$ is finite, there is a nonzero lower bound (which depends on k) for $h(i(\omega)) > 0$. We obtain our desired uniform upper bound for $\hat{h}_{A_\omega, D_\omega}(P_\omega)/h(i(\omega))$ by dividing the inequality above by $h(i(\omega)) > 0$, and hence prove the second part of the theorem.

3. Proof of Theorem 4. We remark that Theorem 4 does not follow trivially from Theorem 5 even if we can find a nonsingular irreducible projective variety $\mathcal{E}/\mathbb{Q}$ and a flat morphism $\pi : \mathcal{E} \to \mathbb{P}^n$ with generic fiber $\mathcal{E}_\eta$ isomorphic to E/K. This is because in general we cannot find a divisor $D \in \mathrm{Div}_{\overline{\mathbb{Q}}}(\mathcal{E})$ such that

$$h_{\mathcal{E},D}(p) = h_{\mathbb{P}^1}([x(p), 1]) + O(1),$$

due to the fact that the X-coordinate map

$$\phi : \mathcal{E} \dashrightarrow \mathbb{P}^1, \quad p \mapsto [x(p), 1],$$

is just a rational map in general. By mimicking the idea of the proof of Theorem A in [11], one can overcome this by blowing up $\mathcal{E}$ and extending ϕ to a morphism. However, we found a more direct and elementary proof for Theorem 4, which is the one that we are going to present.

Using just the definition of height on elliptic curves and the triangle inequality for absolute values of $\mathbb{Q}$, we first prove that there exist positive

constants c_1, c_2 such that for all $\omega \in \mathbb{Q}^n(\Delta_E)$ and all $p \in E_\omega(\mathbb{Q})$, we have

$$h_{E_\omega}([2]p) - 4h_{E_\omega}(p) \le c_1 h(\omega) + c_2. \tag{2}$$

Recall that E_ω is defined by the Weierstrass equation

$$Y^2 = X^3 + A(\omega)X + B(\omega).$$

For any $p = (x, y) \in E_\omega(\mathbb{Q})$, we may assume $[2]p \neq O_{E_\omega}$, as otherwise (2) is trivially true for any positive c_1, c_2. The duplication formula gives

$$x([2]p) = \frac{x^4 - 2A(\omega)x^2 - 8B(\omega) + A(\omega)^2}{4x^3 + 4A(\omega)x + 4B(\omega)}.$$

Thus, we have

$$\begin{aligned} H_{E_\omega}([2]p) &:= H([x([2]p), 1]) \\ &= H([x^4 - 2A(\omega)x^2 - 8B(\omega)x + A(\omega)^2, 4x^3 + 4A(\omega)x + 4B(\omega)]) \\ &\le 4H([1, -2A(\omega), -8B(\omega), A(\omega)^2, 4, 4A(\omega), 4B(\omega)])H([x, 1])^4 \\ &\le 4N_{A,B}H(\omega)^{d_{A,B}}H_{E_\omega}(p)^4 \end{aligned} \tag{3}$$

where the inequalities follow from the triangle inequality for absolute values of $\mathbb{Q}$. The constant $N_{A,B}$ depends on the coefficients and the number of monomials in A and B, whereas $d_{A,B}$ is the maximum of $\deg A^2$ and $\deg B$. Inequality (2) is obtained by taking the natural logarithm of (3).

Now, we use Tate's telescoping sum trick to prove an analogue of Theorem A in [11]:

$$\begin{aligned} \hat{h}_{E_\omega}(p) - h_{E_\omega}(p) &= \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \big(h_{E_\omega}([2^{n+1}]p) - 4h_{E_\omega}([2^n]p)\big) \\ &= \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \big(h_{E_\omega}([2] \circ [2^n]p) - 4h_{E_\omega}([2^n]p)\big) \\ &\le \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} (c_1 h(\omega) + c_2) \quad \text{(using (2))} \\ &= \frac{c_1}{3} h(\omega) + \frac{c_2}{3}. \end{aligned} \tag{4}$$

Finally, given any $P = (x(\mathbf{T}), y(\mathbf{T})) \in E(K)$, the X-coordinate of P defines a rational map

$$\psi_P : \mathbb{P}^n \dashrightarrow \mathbb{P}^1, \quad \omega \mapsto [x(\omega), 1].$$

Just as in the proof of Theorem 5, the standard property of height on projective space gives

$$h_{E_\omega}(P_\omega) := h([x(\omega), 1]) = h(\psi_P(\omega)) \le dh(\omega) + c_3 \tag{5}$$

for some constants d, c_3 that depend on ψ_P only. We get the conclusion of Theorem 4 by combining (4) and (5).

4. Lemmas. Besides some results on elliptic curves over $\mathbb{Q}$, the proof of Proposition 3 requires several nontrivial facts about polynomials with integer coefficients. In this section, we will state these results and give complete proofs with appropriate references. We keep all the notation defined previously. In addition, for the specialized elliptic curve E_ω, let $\Delta_{E_\omega} = \Delta_E(\omega)$ and $\Delta_{E_\omega}^{\min}$ be the discriminant and minimum discriminant of $E_\omega/\mathbb{Q}$ respectively. Also, for any UFD R, whenever we say $P_1, \dots, P_n$ are relatively prime in $R[\mathbf{T}]$, we always mean that they have no common irreducible factor in $R[\mathbf{T}]$.

LEMMA 6. *There exists an absolute constant $C_1 > 0$ such that the following holds. Let $k \geq 4$ be an integer, $N_k := \operatorname{lcm}(1, \dots, k)$ and suppose $\nu \in \mathbb{Z}^n$ is such that $\Delta_E(\nu)$ is nonzero and kth-power-free (briefly, k-free). Then for any nontorsion point $q \in E_\nu(\mathbb{Q})$, we have*

$$\hat{h}_{E_\nu}(q) > \frac{C_1}{N_k^2} \log |\Delta_{E_\nu}^{\min}|.$$

Proof. We make use of a weakened form of a conjecture of Serge Lang proved by Silverman in [10, Section 4]. We apply it to a nontorsion point $q \in E_\nu(\mathbb{Q})$ such that q is in

$$(E_\nu)_0(\mathbb{Q}_p) := \{q \in E_\nu(\mathbb{Q}_p) \mid q \pmod p \text{ is nonsingular}\}$$

for every prime p in $\mathbb{Q}$. This is possible by the Kodaira–Néron Theorem [15, Chapter VII, Theorem 6.1] which implies that the order of $E_\nu(\mathbb{Q}_p)/(E_\nu)_0(\mathbb{Q}_p)$ is either $\operatorname{ord}_p(\Delta_{E_\nu}^{\min})$ or at most 4. So if $\Delta_E(\nu)$ is k-free, we have $\operatorname{ord}_p(\Delta_{E_\nu}^{\min}) \leq k$ and thus $[N_k]q$ is in $(E_\nu)_0(\mathbb{Q}_p)$ for all p with $N_k := \operatorname{lcm}(1, \dots, k)$. Then the special case of the conjecture gives

$$\hat{h}_{E_\nu}([N_k]q) > C_1 \log |\Delta_{E_\nu}^{\min}|$$

for an absolute constant $C_1 > 0$. Using the fact that $\hat{h}_{E_\nu}$ is a quadratic form completes the proof. ∎

LEMMA 7.

$$\sum_{\substack{\nu \in \mathbb{Z}^n \\ 1 < \|\nu\| \leq B}} \frac{1}{\log \|\nu\|} = o(B^n),$$

where the implicit constant depends only on n.

Proof. In this proof, the implicit constants depend only on n. By symmetry of each quadrant in $\mathbb{Z}^n$, we have

$$\sum_{\substack{\nu\in\mathbb{Z}^n\\ 1<\|\nu\|\le B}} \frac{1}{\log\|\nu\|} = O\Bigg(\sum_{1<x_1\le\cdots\le x_n\le B} \frac{1}{\log x_n}\Bigg)$$

$$= O\Bigg(\int_2^B \int_0^{x_n} \cdots \int_0^{x_2} \frac{1}{\log x_n}\, dx_1 \cdots dx_n\Bigg) = O\Bigg(\int_2^B \frac{1}{(n-1)!}\,\frac{x_n^{n-1}}{\log x_n}\, dx_n\Bigg)$$

$$= O\Bigg(\int_2^{\sqrt{B}} \frac{t^{n-1}}{\log t}\, dt + \int_{\sqrt{B}}^B \frac{t^{n-1}}{\log t}\, dt\Bigg) = O\Bigg(\frac{B^n}{\log B}\Bigg). \ \blacksquare$$

LEMMA 8. *Let $k, m, r \in \mathbb{N}$ satisfy*

$$\frac{1}{k} + \frac{1}{m} + \frac{1}{r} \le 1.$$

If $P, Q, R \in \mathbb{C}[\mathbf{T}]$ satisfy $P^k + Q^m = R^r$, then either P, Q, R are all constant, or else they are not relatively prime.

Proof. We first prove the case $n = 1$, which is an immediate consequence of the Mason–Stothers theorem ([5, Chapter IV, Theorem 7.1] or [16, Theorem 1.1]). Suppose to the contrary that P, Q, R are not all constant and relatively prime. Then by the Mason–Stothers theorem, we have

$$\begin{aligned}\max\{k\deg P, m\deg Q, r\deg R\} + 1 &\le \#\{\text{distinct roots of } P^kQ^mR^r\}\\ &\le \deg P + \deg Q + \deg R.\end{aligned}$$

Without loss of generality, suppose $k\deg P \ge m\deg Q$, which implies $k\deg P \ge r\deg R$, so the inequality above becomes

$$k\deg P + 1 \le \deg P + \frac{k}{m}\deg P + \frac{k}{r}\deg P,$$

hence

$$1 \le \left(\frac{1}{k} + \frac{1}{m} + \frac{1}{r} - 1\right) k\deg P \le 0,$$

which is absurd.

Now, let $P, Q, R \in \mathbb{C}[\mathbf{T}]$ satisfy the hypothesis of the lemma. Suppose P, Q, R are not all constant and relatively prime. Without loss of generality, we can assume the degrees of T_n in P, Q are at least 1. We will make use of some standard results about the resultant of two polynomials in $R[x]$, where R is a UFD. These results eventually boil down to linear algebra [4, Chapter VIII, Theorem 8.1]. Consider P, Q as elements in $\mathbb{C}[T_1, \ldots, T_{n-1}][T_n]$ and let $f \in \mathbb{C}[T_1, \ldots, T_{n-1}]$ be their resultant with respect to T_n. Then there exist nonzero $u, v \in \mathbb{C}[\mathbf{T}]$ with $\deg_{T_n} u < \deg_{T_n} Q$ and $\deg_{T_n} v < \deg_{T_n} P$ such that

$$uP + vQ = f.$$

Since P, Q have no common factor in $\mathbb{C}[\mathbf{T}]$, f cannot be identically zero. We can choose $y := (y_1, \ldots, y_{n-1}) \in \mathbb{C}^{n-1}$ such that $f(y) \neq 0$ and $P(y, T_n)$ is nonconstant. Then $P_y(T_n) := P(y, T_n)$ and $Q_y(T_n) := Q(y, T_n)$ are relatively prime in $\mathbb{C}[T_n]$ and $P_y(T_n)$ is nonconstant. So we get relatively prime $P_y, Q_y, R_y \in \mathbb{C}[T_n]$ that are not all constant and satisfy the hypothesis of the lemma for $n = 1$, which is impossible as we have shown previously. ∎

LEMMA 9. *Let $k, m, r \in \mathbb{N}$ satisfy*

$$\frac{1}{k} + \frac{1}{m} + \frac{1}{r} \leq 1.$$

Let $\ell = \operatorname{lcm}(k, m)$ and $g = \gcd(k, m)$, and assume that $\ell \mid r$. Let $P, Q, R \in \mathbb{C}[T]$ be polynomials with $R \neq 0$ that satisfy

$$P^k + Q^m = R^r.$$

Then there exist $\alpha_1, \alpha_2 \in \mathbb{C}$ such that

$$P = \alpha_1 R^{\frac{m}{g}\frac{r}{\ell}} \quad \text{and} \quad Q = \alpha_2 R^{\frac{k}{g}\frac{r}{\ell}}.$$

Proof. The case where P, Q, R are all constant is trivial. So suppose P, Q, R are not all constant. We let $S := R^{r/\ell}$; then

$$P^k + Q^m = S^\ell. \tag{6}$$

Let $G_1, \ldots, G_s$ be the distinct irreducible factors of PQS and write

$$P = \alpha \prod_i G_i^{a_i}, \quad Q = \beta \prod_i G_i^{b_i}, \quad S = \gamma \prod_i G_i^{c_i}$$

with $\alpha, \beta, \gamma \in \mathbb{C}$. Then we can rewrite (6) as

$$\alpha^k \prod_i G_i^{a_i k} + \beta^m \prod_i G_i^{b_i m} = \gamma^\ell \prod_i G_i^{c_i \ell}. \tag{7}$$

We claim that $a_i k = b_i m = c_i \ell$ for all i. Notice that we cannot have one exponent of G_i in (7) that is strictly less than the other two, since otherwise by dividing by the least power G_i factor, we get a contradiction. So two of the exponents of G_i in (7) are equal and at most equal to the third one. We divide (7) by G_i with the common lower exponent and we do this for all i. Since $\ell = \operatorname{lcm}(k, m)$, the resulting equation can be written in the form

$$P_1^k + Q_1^m = S_1^\ell,$$

where P_1, Q_1, S_1 are either all constant or relatively prime. Notice that the former case corresponds to our claim $a_i k = b_i m = c_i \ell$ for all i, and we are going to prove that this must be the case. Since $1/k + 1/m + 1/r \leq 1$, without loss of generality, $k \geq 2$ and $m \geq 3$ and one easily verifies that $\ell := \operatorname{lcm}(k, m) \geq 6$ except for $(k, m, \ell) = (3, 3, 3), (2, 4, 4), (4, 4, 4), (5, 5, 5)$.

So we always have $1/k + 1/m + 1/\ell \leq 1$, and hence we can apply Lemma 8 to P_1, Q_1, S_1 to conclude that they are all constant. So we have

$$P = \alpha_1 S^{\ell/k} = \alpha_1 S^{m/g} \quad \text{and} \quad Q = \alpha_2 S^{\ell/m} = \alpha_2 S^{k/g}.$$

Substituting back $S = R^{r/\ell}$ completes the proof. ∎

To avoid heavy notation in the proofs below, we denote

$$\mathbb{Z}_B := \mathbb{Z} \cap [-B, B]$$

and for any $F \in \mathbb{Z}[\mathbf{T}]$,

$$\rho_F(m) := \{\nu \in (\mathbb{Z}/m\mathbb{Z})^n \mid F(\nu) \equiv 0 \pmod m\},$$
$$\|F\| := \max\{|c| \mid c \text{ is a coefficient of } F\}.$$

Note:

(1) By abuse of notation, the symbol $\equiv$ in the proofs of Lemmas 10 and 11 has three different meanings depending on the context. When f is an element of $\mathbb{Z}[\mathbf{x}]$, $f \equiv 0$ means f is the zero polynomial. The notation $f \equiv 0$ in $\mathbb{Z}/p\mathbb{Z}[\mathbf{x}]$ means the reduction modulo p of f is the zero polynomial in $\mathbb{Z}/p\mathbb{Z}[\mathbf{x}]$. If we evaluate f at x and $f(x)$ is an integer, the notation $f(x) \equiv 0 \pmod p$ means p divides $f(x)$.

(2) By definition, a polynomial $F \in \mathbb{Z}[\mathbf{T}]$ contains the information about its domain, which is $\mathbb{Z}^n$ in our case. Thus, if an implicit constant in the big O or small o notation is said to be dependent on F, that means that it depends on $\deg F$ and n as well.

LEMMA 10. *Let $F \in \mathbb{Z}[\mathbf{T}]$ with total degree $d \geq 1$. Then for all prime $p > \|F\|$, we have*

$$N_p(F, B) := \#\{\nu \in \mathbb{Z}_B^n \mid F(\nu) \equiv 0 \pmod p\} = O(B^n/p + B^{n-1}),$$

where the implicit constant depends only on n and d.

Proof. In this proof, the implicit constants depend only on n and d. We argue by induction on n. For $n = 1$, by the condition on p, $F \not\equiv 0 \in \mathbb{Z}/p\mathbb{Z}[T_1]$. So

$$N_p(F, B) \leq \rho_F(p)(2B/p + 1) \leq d(2B/p + 1).$$

Now let $F \in \mathbb{Z}[\mathbf{T}]$ and for $y \in \mathbb{Z}^{n-1}$, $F_y(T_n) := F(y, T_n) \in \mathbb{Z}[T_n]$. The condition $F_y \equiv 0$ in $\mathbb{Z}/p\mathbb{Z}[T_n]$ becomes a bunch of (at most d) polynomials of degree at most d in $\mathbb{Z}[T_1, \ldots, T_{n-1}]$, all equal to zero modulo p. Thus, by induction hypothesis,

$$\#\{y \in \mathbb{Z}_B^{n-1} \mid F_y \equiv 0 \text{ in } \mathbb{Z}/p\mathbb{Z}[T_n]\} = O(B^{n-1}/p + B^{n-2}).$$

So we get

$$\begin{aligned} N_p(F,B) &= \sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ F_y\equiv 0 \text{ in } \mathbb{Z}/p\mathbb{Z}[T_n]}} N_p(F_y,B) + \sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ F_y\not\equiv 0 \text{ in } \mathbb{Z}/p\mathbb{Z}[T_n]}} N_p(F_y,B) \\ &\le O((2B)^{n-1}/p + (2B)^{n-2})(2B+1) + (2B+1)^{n-1}d(2B/p+1) \\ &= O(B^n/p + B^{n-1}). \ \blacksquare \end{aligned}$$

LEMMA 11. *Suppose $F(\mathbf{T}) \in \mathbb{Z}[\mathbf{T}]$ has total degree $d \ge 1$ and has no multliple irreducible factor in $\mathbb{Z}[\mathbf{T}]$. Then except for finitely many prime p,*

$$N_{p^2}(F,B) := \#\{\nu \in \mathbb{Z}_B^n \mid F(\nu) \equiv 0 \pmod{p^2}\} = O(B^n/p^2 + B^{n-1}),$$

whenever $p \le B$. The implicit constant depends only on F.

Proof. In this proof, the implicit constants depend only on F, which includes d and n. Since we allow finitely many exceptions for p, we can assume that F is primitive, i.e. the content of F is 1. For $n = 1$, if $p \nmid \mathrm{Disc}(F) \ne 0$, then $N_{p^2}(F,B) \le d(2B/p^2+1)$. Now let $F \in \mathbb{Z}[\mathbf{T}]$ and for $y \in \mathbb{Z}^{n-1}$, $F_y(T_n) := F(y,T_n) \in \mathbb{Z}[T_n]$. Let $\mathbf{Y} := (T_1,\dots,T_{n-1})$. By Gauss' lemma for UFDs, the fact that F has no multliple irreducible factor in $\mathbb{Z}[\mathbf{T}] = \mathbb{Z}[\mathbf{Y}][T_n]$ implies the same in $\mathbb{Q}(\mathbf{Y})[T_n]$. So $D(\mathbf{Y}) := \mathrm{Disc}(F_{\mathbf{Y}}) \not\equiv 0 \in \mathbb{Z}[\mathbf{Y}]$. Also, for $p > \|D\|$, $D(\mathbf{Y}) \not\equiv 0 \in \mathbb{Z}/p\mathbb{Z}[\mathbf{Y}]$. We write $F_{\mathbf{Y}}(T_n) = a_d(\mathbf{Y})T_n^d + \cdots + a_0(\mathbf{Y})$ and we consider two cases:

CASE 1: $\gcd(a_d(\mathbf{Y}),\dots,a_0(\mathbf{Y})) = 1$. We decompose $N_{p^2}(F,B)$ into

$$\sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ D(y)\not\equiv 0 \,(\mathrm{mod}\, p)}} N_{p^2}(F_y,B) + \sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ F_y\not\equiv 0 \text{ in } \mathbb{Z}/p\mathbb{Z}[T_n]\\ D(y)\equiv 0 \,(\mathrm{mod}\, p)}} N_{p^2}(F_y,B) + \sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ F_y\equiv 0 \text{ in } \mathbb{Z}/p\mathbb{Z}[T_n]}} N_{p^2}(F_y,B).$$

The first sum is trivially bounded by $(2B+1)^{n-1}d(2B/p^2+1)$. For the second sum, we apply Lemma 10 on $D(\mathbf{Y})$ to get an upper bound

$$O(B^{n-1}/p + B^{n-2})dp(2B/p^2+1) = O(B^n/p^2 + B^{n-1}).$$

Lastly, since $\gcd(a_d(\mathbf{Y}),\dots,a_0(\mathbf{Y})) = 1$, if we look at the $y \in (\mathbb{Z}/p\mathbb{Z})^{n-1}$ such that $F_y \equiv 0$ in $\mathbb{Z}/p\mathbb{Z}[T_n]$, then either y is a common root in $(\mathbb{Z}/p\mathbb{Z})^{n-1}$ of at least two polynomials that are relatively prime in $\mathbb{Z}[T_1,\dots,T_{n-1}]$ or there is no such y because there is only one nonzero $a_i(\mathbf{Y})$ and it must be 1 by the assumption of Case 1. From the proof of Theorem 3.1 of Poonen [9], the set of such $y \in (\mathbb{Z}/p\mathbb{Z})^{n-1}$ has size $O(p^{(n-1)-2})$ for large p. Hence for $p \le B$,

$$\sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ F_y\equiv 0 \text{ in } \mathbb{Z}/p\mathbb{Z}[T_n]}} N_{p^2}(F_y,B) \le O(p^{n-3})(2B/p+1)^{n-1}(2B+1)$$
$$= O(p^{n-3})O(B^{n-1}/p^{n-1}+B^{n-2}/p^{n-2})(2B+1) = O(B^n/p^2+B^{n-1}),$$

and we are done.

Case 2: $\gcd(a_d(\mathbf{Y}),\dots,a_0(\mathbf{Y})) = g(\mathbf{Y}) \neq 1$. Then $F(\mathbf{T}) = A(\mathbf{T})g(\mathbf{Y})$ for some nonconstant $A(\mathbf{T}) \in \mathbb{Z}[\mathbf{T}]$. Then

$$N_{p^2}(F,B) = \sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ g(y)\equiv 0 \,(\mathrm{mod}\, p^2)}} O(2B) + \sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ p\| g(y)}} N_p(A_y,B) + \sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ p\nmid g(y)}} N_{p^2}(A_y,B),$$

where $p \,\|\, g(y)$ means $p|g(y)$ but $p^2 \nmid g(y)$. Since $g(\mathbf{Y})$ does not have multiple irreducible factors in $\mathbb{Z}[T_1,\dots,T_{n-1}]$ either, we use induction on n to bound the first sum by $O_{d,n}(B^{n-1}/p^2+B^{n-2})O(2B)$. As for the third sum, it is trivially bounded by $N_{p^2}(A,B)$, and this reduces to Case 1. Finally, we split the middle sum as follows:

$$\sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ p\| g(y)}} N_p(A_y,B) = \sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ p\| g(y)\\ A_y\not\equiv 0 \text{ in } \mathbb{Z}/p\mathbb{Z}[T_n]}} N_p(A_y,B) + \sum_{\substack{y\in\mathbb{Z}_B^{n-1}\\ p\| g(y)\\ A_y\equiv 0 \text{ in } \mathbb{Z}/p\mathbb{Z}[T_n]}} O(2B).$$

Using Lemma 10, we can bound the first sum by

$$O(B^{n-1}/p+B^{n-2})d(2B/p+1) = O(B^n/p^2+B^{n-1}).$$

As for the second sum, since A is of Case 1, the number of $y \in (\mathbb{Z}/p\mathbb{Z})^{n-1}$ such that $A_y \equiv 0$ in $\mathbb{Z}/p\mathbb{Z}[T_n]$ is $O(p^{(n-1)-2})$ and so the sum is bounded by

$$O(p^{n-3})(2B/p+1)^{n-1}O(2B) = O(p^{n-3}(3B/p)^{n-1}B) = O(B^n/p^2)$$

for large $p \le B$. ∎

Lemma 12. *Suppose $F(\mathbf{T}) \in \mathbb{Z}[\mathbf{T}]$ has total degree d and has no multiple irreducible factor in $\mathbb{Z}[\mathbf{T}]$. Then for all integers $k \gg d$ we have*

$$\#\{\nu \in \mathbb{Z}_B^n \mid F(\nu) \text{ is } k\text{-free}\} \sim \gamma_{k,F}(2B)^n,$$

where $\gamma_{k,F} := \prod_{\text{prime } p\in\mathbb{Z}}(1-\rho_F(p^k)/p^{nk})$ is a nonzero convergent Euler product. Here, we adopt the convention that 0 is k-free for all integers $k \ge 2$.

Proof. In this proof, we will introduce some arbitrary constants $\xi, \epsilon > 0$, and all implicit constants depend only on F, k, ξ and ϵ. We adapt the idea of Browning in [1, Section 4]. Let $\xi > 0$ be a constant and define

$$N_{\mathrm{fr}}^{(k)} := \{\nu \in \mathbb{Z}_B^n \mid F(\nu) \text{ is } k\text{-free}\},$$

$$N_{\mathrm{nfr},1}^{(k)} := \left\{\nu \in \mathbb{Z}_B^n \;\middle|\; \begin{array}{l} F(\nu) \text{ is not } k\text{-free, and for all prime } p \text{ such} \\ \text{that } p^k \mid F(\nu), \text{ we have } \xi < p \le B \end{array}\right\},$$

$$N_{\mathrm{nfr},2}^{(k)} := \left\{\nu \in \mathbb{Z}_B^n \;\middle|\; \begin{array}{l} F(\nu) \text{ is not } k\text{-free, and for all prime } p \text{ such} \\ \text{that } p^k \mid F(\nu), \text{ we have } p > \xi, \text{ and} \\ p^k \mid F(\nu) \text{ for some prime } p > B \end{array}\right\},$$

$$N_{\xi}^{(k)} := \{\nu \in \mathbb{Z}_B^n \mid \text{if } p^k \mid F(\nu) \text{ then } p > \xi\} = N_{\mathrm{fr}}^{(k)} \sqcup N_{\mathrm{nfr},1}^{(k)} \sqcup N_{\mathrm{nfr},2}^{(k)},$$

$$M_{\mathrm{fr}}^{(2)} := \left\{\nu \in \mathbb{Z}_B^n \;\middle|\; \begin{array}{l} F(\nu) \text{ is } k\text{-free, and} \\ p^2 \mid F(\nu) \text{ for some prime } \xi < p \le B \end{array}\right\},$$

$$M_{\mathrm{nfr}}^{(2)} := \left\{\nu \in \mathbb{Z}_B^n \;\middle|\; \begin{array}{l} F(\nu) \text{ is not } k\text{-free, and} \\ p^2 \mid F(\nu) \text{ for some prime } \xi < p \le B \end{array}\right\},$$

$$M^{(2)} := \{\nu \in \mathbb{Z}_B^n \mid p^2 \mid F(\nu) \text{ for some prime } \xi < p \le B\} = M_{\mathrm{fr}}^{(2)} \sqcup M_{\mathrm{nfr}}^{(2)}.$$

Then obviously $M_{\mathrm{fr}}^{(2)} \subset N_{\mathrm{fr}}^{(k)}$ and $N_{\mathrm{nfr},1}^{(k)} \subset M_{\mathrm{nfr}}^{(2)}$ and thus

$$\#N_{\xi}^{(k)} \ge \#N_{\mathrm{fr}}^{(k)} \ge \#N_{\xi}^{(k)} - \#M^{(2)} - \#N_{\mathrm{nfr},2}^{(k)}.$$

We first estimate $\#N_{\xi}^{(k)}$ using the Möbius function μ. Let

$$\rho_F(m) := \#\{\nu \in (\mathbb{Z}/m\mathbb{Z})^n \mid F(\nu) \equiv 0 \pmod m\}.$$

Then we can write

$$\begin{aligned} \#N_{\xi}^{(k)} &= \sum_{\substack{h \in \mathbb{N} \\ p \mid h \Rightarrow p \le \xi}} \mu(h) \#\{\nu \in \mathbb{Z}_B^n \mid h^k \mid F(\nu)\} \\ &= \sum_{\substack{h \in \mathbb{N} \\ p \mid h \Rightarrow p \le \xi}} \mu(h) \rho_F(h^k) \left(\frac{2B}{h^k} + O(1)\right)^n \\ &= \sum_{\substack{h \in \mathbb{N} \\ p \mid h \Rightarrow p \le \xi}} \mu(h) \rho_F(h^k) \left(\frac{(2B)^n}{h^{kn}} + O\left(\left(\frac{2B}{h^k}\right)^{n-1} + 1\right)\right). \end{aligned}$$

Since the summation is over square-free h only, the condition $p \mid h \Rightarrow p \le \xi$ implies

$$h \le \prod_{p \le \xi} p = \exp\Big(\sum_{p \le \xi} \log p\Big) \le e^{2\xi},$$

where the last inequality is a consequence of the prime number theorem. Moreover, it follows from the proof of Theorem 3.2 of Poonen [9] that $\rho_F(p^2) = O(p^{2n-2})$ (or we can deduce this from Lemma 11 with $B = p^2$). Subsequent lifting will lead to $\rho_F(p^j) = O(p^{jn-2})$ for $j \ge 2$. Together

with the fact that ρ_F is multiplicative, for square-free h we have $\rho_F(h^k) = O(h^{nk-2+\epsilon})$ for any $\epsilon > 0$. The ϵ is needed here in order to bound the product of r_h copies of the implicit constant of $O(p^{2n-2})$, where r_h is the number of distinct prime factors of h. Using the fact that h is square-free, we have $h \geq r_h!$ and the Stirling formula will give us the desired bound. Hence

$$\#N_\xi^{(k)} = (2B)^n \prod_{p \leq \xi} \left(1 - \frac{\rho_F(p^k)}{p^{nk}}\right) + O((2B)^{n-1} e^{2\xi(k-1+\epsilon)} + e^{2\xi(nk-1+\epsilon)}).$$

Again because $\rho_F(p^k) = O(p^{kn-2})$, the infinite product

$$\gamma_{k,F} := \prod_{\text{prime } p \in \mathbb{Z}} \left(1 - \frac{\rho_F(p^k)}{p^{nk}}\right)$$

converges and we have

$$\#N_\xi^{(k)} \geq (2B)^n \gamma_{k,F} + O(B^{n-1}).$$

Next, by Lemma 11, we have

$$\begin{aligned} \#M^{(2)} &\leq \sum_{\xi < p \leq B} \#\{\nu \in \mathbb{Z}_B^n \mid p^2 | F(\nu)\} = \sum_{\xi < p \leq B} O\left(\frac{B^n}{p^2} + B^{n-1}\right) \\ &\leq c\left(\frac{B^n}{\xi} + \frac{B^n}{\log B}\right) \end{aligned}$$

for some constant $c > 0$ depending only on n and d. The first term of the upper bound is obtained by an integral estimate and the second is by the prime number theorem.

Lastly, $\#N_{\text{nfr},2}^{(k)} = 0$ for B large enough. Indeed, there exists a constant $C_F > 0$ such that $|F(\nu)| \leq C_F \|\nu\|^d$. Thus, for all $B > C_F$, prime $p > B$, $\nu \in \mathbb{Z}_B^n$ and $k > d$, we have

$$p^k > B^k \geq B^{d+1} > C_F B^d \geq |F(\nu)|,$$

so no such p^k divides $F(\nu)$.

Combining all the estimates, we get

$$\#N_{\text{fr}}^{(k)} \geq \gamma_{k,F}(2B)^n + O(B^{n-1}) - \frac{c}{\xi}(2B)^n + o_{d,n}(B^n)$$

for $B > \max\{\xi, C_F\}$. The fact that $\rho_F(p^k) = O(p^{kn-2})$ implies $\gamma_{k,F}$ converges, and $\gamma_{k,F}$ is zero if and only if one of its factors is zero. So in order to make $\gamma_{k,F} > 0$, it is sufficient to choose k so large that $\rho_F(p^k) < p^{nk}$ for all prime p. More explicitly, choose a ν_0 such that $F(\nu_0) \neq 0$ and look at its prime factorization $\prod_i p_i^{\beta_i}$ in $\mathbb{Z}$. Then any $k > \max_i\{\beta_i, d\}$ will do. We fix this k and for any $\lambda \in (0,1)$, by choosing ξ so large that $c/\xi \ll \gamma_{k,F}$, we get

$$\#N_{\text{fr}}^{(k)} \geq \lambda \gamma_{k,F}(2B)^n$$

for B large enough. Since for all $\xi \gg 0$, $\#N_\xi^{(k)} \geq \#N_{\mathrm{fr}}^{(k)}$ and

$$\#N_\xi^{(k)} \sim (2B)^n \prod_{p \leq \xi} \left(1 - \frac{\rho_F(p^k)}{p^{nk}}\right),$$

we get

$$\prod_{p \leq \xi} \left(1 - \frac{\rho_F(p^k)}{p^{nk}}\right) \geq \limsup_{B \to \infty} \frac{\#N_{\mathrm{fr}}^{(k)}}{(2B)^n} \geq \liminf_{B \to \infty} \frac{\#N_{\mathrm{fr}}^{(k)}}{(2B)^n} \geq \lambda \gamma_{k,F}$$

for all $\xi \gg 0$ and $\lambda \in (0,1)$. Taking $\lambda \to 1$ (which forces $\xi \to \infty$) completes the proof. ∎

Corollary 13. *For any $F(\mathbf{T}) \in \mathbb{Z}[\mathbf{T}]$, there exists an integer k_0 such that for all integers $k \geq k_0$ and for all $\lambda \in (0,1)$, there exist $B_0 > 0$ depending on F, k, λ and $c_{k,F} > 0$ depending on F, k such that*

$$\#\{\nu \in \mathbb{Z}_B^n \mid F(\nu) \text{ is } k\text{-free}\} \geq \lambda c_{k,F} (2B)^n$$

whenever $B \geq B_0$.

Proof. Write $F = \prod_{i=1}^r f_i^{\alpha_i}$ where f_i are distinct irreducible factors of F in $\mathbb{Z}[\mathbf{T}]$. Let $f := \prod_{i=1}^r f_i$ with total degree d and $\alpha := \max_i\{\alpha_i\}$. Now it is immediate by the previous lemma that for all $k \geq k'\alpha$ with $k' > d$ large enough as in the previous lemma, we obtain our corollary with $c_{k,F} = \gamma_{k',f} > 0$. ∎

Lemma 14. *For any integer $N \geq 2$, denote by $\mathrm{fr}_N(m)$ the Nth free part of the integer m, i.e. the smallest positive integer ℓ such that $|m|/\ell$ is an Nth power of an integer. Suppose a primitive $F(\mathbf{T}) \in \mathbb{Z}[\mathbf{T}]$ is not a pth power in $\mathbb{C}[\mathbf{T}]$ for all prime $p \mid N$. Then for all $M > 2$, we have*

$$\#\{\nu \in \mathbb{Z}_B^n \mid (\mathrm{fr}_N(F(\nu)))^M > \|\nu\|\} \sim (2B)^n.$$

Proof. Let the total degree of F be d, so there exists a constant $C_F \geq 1$ such that $|F(\nu)| \leq C_F \|\nu\|^d$. Define

$$S_M(F,B) := \left\{ (\nu, y, z) \in \mathbb{Z}^{n+2} \;\middle|\; \begin{array}{l} \|\nu\| \leq B, \\ |y| \leq (C_F B^d)^{1/N},\ F(\nu) = y^N z, \\ 0 < |z| \leq B^{1/M}, \end{array} \right\}.$$

We will prove by induction that

$$\#S_M(F,B) \ll_{F,\epsilon,M,N} C_F^\epsilon B^{(n-1)+1/N+1/M+2d\epsilon} \log B \quad \forall \epsilon > 0.$$

The implicit constants in this proof will depend only on F, ϵ, M and N. We are going to apply Theorem 15 of Heath-Brown [3], so we try to use

notation coherent with it. For $n = 1$, for all $z_0 \in \mathbb{Z}$, let

$$N(f_{z_0}, B, (C_F B^d)^{1/N}) := \left\{ (\nu, y) \in \mathbb{Z}^2 \;\middle|\; \begin{array}{l} \|\nu\| \le B,\ |y| \le (C_F B^d)^{1/N}, \\ f_{z_0}(\nu, y) := F(\nu) - z_0 y^N = 0 \end{array} \right\}.$$

Then

$$\#S_M(F, B) = \sum_{0<|z_0|\le B^{1/M}} \#N(f_{z_0}, B, (C_F B^d)^{1/N}).$$

Since for all prime $p \,|\, N$, F is not a pth power in $\mathbb{C}[T_1]$, the same holds in $\mathbb{C}(T_1)$. By Capelli's lemma [5, Chapter VI, Theorem 9.1], $f_{z_0}(T_1, Y) = F(T_1) - z_0 Y^N$ is absolutely irreducible in $\mathbb{C}(T_1)[Y]$ for all $z_0 \neq 0$. We need this fact for the next step.

Now we apply Theorem 15 of Heath-Brown [3] on $N(f_{z_0}, B, (C_F B^d)^{1/N})$. Let $T := \max\{B^d, C_F B^d\} = C_F B^d$. Then for all $\epsilon > 0$, there exists a constant $D = D_{d,\epsilon}$ and $k \in \mathbb{N}$, with

$$\begin{aligned} k &\ll_{d,\epsilon} T^\epsilon \exp\left\{ \frac{\log B \log(C_F B^d)^{1/N}}{\log(C_F B^d)} \right\} \log \|f_{z_0}\| \\ &\ll_{d,\epsilon} (C_F B^d)^\epsilon B^{1/N} \log \|f_{z_0}\|, \end{aligned}$$

such that there exist $\tilde{f}_1, \dots, \tilde{f}_k \in \mathbb{Z}[T_1, Y]$, coprime to f_{z_0} and with degrees at most D, such that every (ν, y) counted by $N(f_{z_0}, B, (C_F B^d)^{1/N})$ is a zero of some polynomial $\tilde{f}_i$. By Bézout's theorem, the number of points of intersection of the curves $\tilde{f}_i = 0$ and $f_{z_0} = 0$ is bounded by $\deg \tilde{f}_i \cdot \deg f_{z_0} \le D(d + N)$. This gives immediately

$$\#N(f_{z_0}, B, (C_F B^d)^{1/N}) \ll_{d,\epsilon} D(d+N)(C_F B^d)^\epsilon B^{1/N} \log \|f_{z_0}\|.$$

So

$$\begin{aligned} (8) \qquad \#S_M(F, B) &\ll_{d,\epsilon,N} \sum_{0<|z_0|\le B^{1/M}} (C_F B^d)^\epsilon B^{1/N} \log \|f_{z_0}\| \\ &\ll_{d,\epsilon,N} \sum_{0<|z_0|\le B^{1/M}} (C_F B^d)^\epsilon B^{1/N} \log B \ll_{d,\epsilon,N} C_F^\epsilon B^{1/N+1/M+d\epsilon} \log B, \end{aligned}$$

where we may choose $B \ge \|F\|$ and hence $\|f_{z_0}\| \le B$ for $|z_0| \le B^{1/M}$.

Now we proceed to general $n \ge 2$. For all $x \in \mathbb{Z}^{n-1}$, let $F_x(T_n) := F(x, T_n) \in \mathbb{Z}[T_n]$. For all $p \,|\, N$, since $F(\mathbf{T})$ is not a pth power, we look at the pth power-free part of $F(\mathbf{T})$ in $\mathbb{Z}[\mathbf{T}]$, call it $G_p(\mathbf{T})$. In other words, $G_p(\mathbf{T})$ is the smallest degree polynomial such that $F(\mathbf{T})/G_p(\mathbf{T})$ is a pth power in $\mathbb{Z}[\mathbf{T}]$. So $G_p(\mathbf{T}) = \prod_j G_{p,j}(\mathbf{T})^{\beta_j}$ where $G_{p,j}$ are distinct irreducible factors and $0 < \beta_j < p$. Let $g_p(\mathbf{T}) := \prod_j G_{p,j}(\mathbf{T})$, which has no multliple irreducible factor in $\mathbb{Z}[\mathbf{T}]$. By Gauss' lemma on UFDs and by reindexing if necessary, the discriminant of $g_p(\mathbf{X}, T_n) \in \mathbb{Z}[\mathbf{X}][T_n]$ is not a zero polynomial in $\mathbb{Z}[\mathbf{X}]$. So there are at most $O(B^{n-2})$ of $x \in \mathbb{Z}_B^{n-1}$ such that $g_{p,x}(T_n) := g_p(x, T_n)$

has a multiple irreducible factor in $\mathbb{Z}[T_n]$. This will imply that there are at most $O(B^{n-2})$ of $x \in \mathbb{Z}_B^{n-1}$ such that $F_x(T_n)$ is a pth power in $\mathbb{Z}[T_n]$. So we have

$$\#S_M(F,B) = \sum_{\substack{x\in\mathbb{Z}_B^{n-1}\\ F_x \text{ non-}p\text{th power}\\ \text{for all } p|N}} \#S_M(F_x,B) + \sum_{\substack{x\in\mathbb{Z}_B^{n-1}\\ F_x\ p\text{th power}\\ \text{for some } p|N}} \#S_M(F_x,B). \tag{9}$$

Notice that $|F_x(\nu_n)| \le (C_F B^d)|\nu_n|^d$ for $x \in \mathbb{Z}_B^{n-1}$ and $\deg F_x \le d$. So using the result from the case $n = 1$, we get

$$\begin{aligned}\#S_M(F,B) &\ll_{d,\epsilon,N} (2B)^{n-1}(C_F B^d)^\epsilon B^{1/N+1/M+d\epsilon}\log B + O(B^{n-2}\cdot B\cdot B^{1/M})\\ &\ll_{F,\epsilon,M,N} C_F^\epsilon B^{(n-1)+1/N+1/M+2d\epsilon}\log B,\end{aligned}$$

where to estimate the second sum, we use the fact that y is determined (up to sign for N even) once (ν_n, z_0) is fixed in F_x. When ϵ is sufficiently small relative to d and $M > 2$, we get $\#S_M(F,B) = o(B^n)$. Lastly, define

$$\mathrm{Bad}_M(F,B) := \{\nu \in \mathbb{Z}_B^n \mid (\mathrm{fr}_N(F(\nu)))^M \le \|\nu\|\},$$

which is the complement of $\{\nu \in \mathbb{Z}_B^n \mid (\mathrm{fr}_N(F(\nu)))^M > \|\nu\|\}$ in $\mathbb{Z}_B^n$. It is a simple exercise to show that $\mathrm{Bad}_M(F,B)$ injects into $S_M(F,B)$ via the map $\nu \mapsto (\nu, \sqrt[N]{|F(\nu)|/\mathrm{fr}_N(F(\nu))}, \mathrm{sign}(F(\nu))\,\mathrm{fr}_N(F(\nu)))$, proving the lemma. ∎

Corollary 15. *With the same hypothesis as in the previous lemma, let $g \in \mathbb{N}$ be such that $0 < g \le B^{1/(N+2)}$. Then for M large enough, we have*

$$\#\{\nu \in \mathbb{Z}_{B/g}^n \mid (\mathrm{fr}_N(F(\nu)))^M > g^{M(N-1)+1}\|\nu\|\} \sim (2B/g)^n.$$

In particular, when $N = 2$ or 3, then any $M > 8$ is admissible.

Proof. The proof is just a slight modification of the previous proof, so we will keep all the same notation. Again, the implicit constants in this proof depend only on F, ϵ, M and N. We are going to show that the complement of

$$\{\nu \in \mathbb{Z}_{B/g}^n \mid (\mathrm{fr}_N(F(\nu)))^M > g^{M(N-1)+1}\|\nu\|\},$$

which is

$$\mathrm{Bad}_M(F,B,g) := \{\nu \in \mathbb{Z}_{B/g}^n \mid (\mathrm{fr}_N(F(\nu)))^M \le g^{M(N-1)+1}\|\nu\|\},$$

has size $o(2B/g)^n$. Just as in the previous proof, $\mathrm{Bad}_M(F,B,g)$ injects into

$$S_M(F,B,g) := \left\{ (\nu,y,z) \in \mathbb{Z}^{n+2} \;\middle|\; \begin{array}{l} \|\nu\| \le B/g,\\ |y| \le (C_F(B/g)^d)^{1/N},\ F(\nu) = y^N z,\\ 0 < |z| \le g^{N-1+1/M}(B/g)^{1/M}\end{array} \right\}.$$

Thus, it suffices to show that $\#S_M(F,B,g) = o(2B/g)^n$. Comparing $S_M(F,B,g)$ to $S_M(F,B)$ from the previous proof, this boils down to just

changing B to B/g and slightly increasing the upper bound for z with a factor of $g^{N-1+1/M}$. So for $n=1$, from (8), we have

$$\begin{aligned}\#S_M(F,B,g) &\ll_{d,\epsilon,N} \sum_{0<|z_0|\le g^{N-1+1/M}(B/g)^{1/M}} (C_F(B/g)^d)^\epsilon (B/g)^{1/N}\log\|f_{z_0}\|\\ &\ll_{d,\epsilon,N} C_F^\epsilon (B/g)^{1/N+1/M+d\epsilon} g^{N-1+1/M}\log B,\end{aligned}$$

where we choose $B \ge \|F\|$ and hence $\|f_{z_0}\| \le \max\{B, g^{N-1}B^{1/M}\} \le B^2$. Since $g \le B^{1/(N+2)}$, we have $B/g \ge g^{N+1}$ and $B \le (B/g)^{(N+2)/(N+1)} < (B/g)^2$, so

$$\#S_M(F,B,g) \ll_{d,\epsilon,N} C_F^\epsilon \left(\frac{B}{g}\right)^{1/N+1/M+d\epsilon} \left(\frac{B}{g}\right)^{\frac{N-1}{N+1}+\frac{1}{(N+1)M}} \log\left(\frac{B}{g}\right),$$

which is $o(2B/g)$ for M sufficiently large and ϵ sufficiently small. Using the same induction argument as in (9), we have for $n \ge 2$,

$$\begin{aligned}(10)\qquad &\#S_M(F,B,g)\\ &\ll_{d,\epsilon,M,N} \left(2\frac{B}{g}\right)^{n-1}\left(C_F\left(\frac{B}{g}\right)^d\right)^\epsilon \left(\frac{B}{g}\right)^{1/N+1/M+d\epsilon+\frac{N-1}{N+1}+\frac{1}{(N+1)M}}\log\left(\frac{B}{g}\right)\\ &\quad + O\left(\left(\frac{B}{g}\right)^{n-2}\cdot\frac{B}{g}\cdot g^{N-1+1/M}\left(\frac{B}{g}\right)^{1/M}\right)\\ &\ll_{F,\epsilon,M,N} C_F^\epsilon \left(\frac{B}{g}\right)^{n-1+1/N+1/M+2d\epsilon+\frac{N-1}{N+1}+\frac{1}{(N+1)M}}\log\left(\frac{B}{g}\right),\end{aligned}$$

which is also $o(2B/g)^n$ for M sufficiently large and ϵ sufficiently small. We remark that for $N=2,3$, the exponents of B/g in (10) are $n-1+2d\epsilon+5/6+4/(3M)$ and $n-1+2d\epsilon+5/6+5/(4M)$ respectively. For any $M>8$, there exists $\epsilon>0$ such that these exponents are strictly less than n, hence giving us Corollary 15 for $N=2,3$, and these are the instances where we will apply this corollary. ∎

5. Proof of Proposition 3. We keep all the previous notation. The implicit constants in this proof will depend only on Δ_E, n and P. The main idea in this proof is to first apply Lemma 6. This allows us to get a lower bound of $\hat{h}_{E_\nu}(P_\nu)$ in terms of $\Delta_{E_\nu}^{\min}$, for all "nice" $\nu \in \mathbb{Z}^n$. Then we try to bound $\Delta_{E_\nu}^{\min}$ below in terms of Δ_{E_ν} and then in term of $h(\nu)$, again for all "nice" ν. The nontrivial part of the proof is to show that after we impose again and again certain niceness conditions on ν, this set of "nice" ν has a positive density in $\mathbb{Z}_B^n(\Delta_E, P)$.

Fix a large integer $k \ge 4$, which we will specify at the end of the proof, and let $N_k := \operatorname{lcm}(1,\dots,k)$. Then by Lemma 6, there is an absolute constant $C_1 > 0$ such that for any $P \in E(K)_{\mathrm{nt}}$ and for any $\nu \in \mathbb{Z}_B^n(\Delta_E, k, P_\nu^{\mathrm{nt}})$,

where

$$\mathbb{Z}_B^n(\Delta_E, k, P_\nu^{\mathrm{nt}}) := \{\nu \in \mathbb{Z}_B^n(\Delta_E, P) \mid \Delta_E(\nu) \text{ is } k\text{-free}, P_\nu \in E_\nu(\mathbb{Q})_{\mathrm{nt}}\},$$

we have

$$\sum_{\nu \in \mathbb{Z}_B^n(\Delta_E, P)} \frac{\hat{h}_{E_\nu}(P_\nu)}{h(\nu)} \geq \frac{C_1}{N_k^2} \sum_{\nu \in \mathbb{Z}_B^n(\Delta_E, k, P_\nu^{\mathrm{nt}})} \frac{\log|\Delta_{E_\nu}^{\min}|}{h(\nu)} = \frac{C_1}{N_k^2} \sum_{\nu \in \mathbb{Z}_B^n(\Delta_E, k, P_\nu^{\mathrm{nt}})} \frac{\log|\Delta_{E_\nu}^{\min}|}{\log\|\nu\|}. \tag{11}$$

We obtain the second line because of the convention that we made earlier: $h(\nu) = \log H([1, \nu_1, \ldots, \nu_n])$.

Next, we claim that $\Delta_E(\mathbf{T}) = -16(4A^3(\mathbf{T}) + 27B^2(\mathbf{T}))$ is never a constant times a twelfth power in $\mathbb{Z}[\mathbf{T}]$, as otherwise Lemma 9 says that there exists $g(\mathbf{T}) \in \mathbb{Q}[\mathbf{T}]$ such that $A(\mathbf{T})/g(\mathbf{T})^4, B(\mathbf{T})/g(\mathbf{T})^6 \in \mathbb{Z}$. So using Gauss' lemma, we can write $\Delta_E(\mathbf{T}) = \alpha(F(\mathbf{T}))^{a+12b}$, where $\alpha \in \mathbb{Z}$, $F(\mathbf{T})$ is primitive in $\mathbb{Z}[\mathbf{T}]$, nonpower in $\mathbb{C}[\mathbf{T}]$, $a \in \{1, \ldots, 11\}$ and $b \in \mathbb{N}$. Recall that for all primes p in $\mathbb{Q}$,

$$0 \leq \mathrm{ord}_p(\Delta_{E_\nu}^{\min}) \equiv \mathrm{ord}_p(\Delta_{E_\nu}) \pmod{12},$$

so $\mathrm{ord}_p(\Delta_{E_\nu}^{\min})$ is at least the unique integer in $\{0, 1, \ldots, 11\}$ congruent to $\mathrm{ord}_p(\Delta_{E_\nu})$ (mod 12). We split into two cases in order to get a lower bound of $\Delta_{E_\nu}^{\min}$.

Case 1: $a \neq 4, 8$. If we let $\mathrm{sqfr}(m) := \mathrm{fr}_2(m)$ and $\mathrm{sq}(m) := |m|/\mathrm{sqfr}(m)$ be the square-free part and square part of an integer m, then

$$|\Delta_E(\nu)| = |\alpha|\,|\mathrm{sq}(F(\nu))|^{a+12b}|\,\mathrm{sqfr}(F(\nu))|^{a+12b}.$$

Notice that for every prime factor p of $\mathrm{sqfr}(F(\nu))$ that is relatively prime to α, its power β_p in $F(\nu)$ is odd and thus $a\beta_p \not\equiv 0 \pmod{12}$ for $a \neq 4, 8$. So p is a factor of $\Delta_{E_\nu}^{\min}$ and we have, for $\nu \in \mathbb{Z}_B^n(\Delta_E, k, P_\nu^{\mathrm{nt}})$,

$$|\Delta_{E_\nu}^{\min}| \geq |\mathrm{sqfr}(F(\nu))|/|\alpha|.$$

Case 2: $a = 4$ or 8. The argument is similar to Case 1 except that we look at $\mathrm{cufr}(F(\nu)) := \mathrm{fr}_3(F(\nu))$, the cube-free part of $F(\nu)$. Then for every prime factor p of $\mathrm{cufr}(F(\nu))$ that is relatively prime to α, its power β_p in $F(\nu)$ is not a multiple of 3 and thus $a\beta_p \not\equiv 0 \pmod{12}$ for $a = 4$ or 8. In fact, $a\beta_p \equiv 4$ or 8 (mod 12). So again, for $\nu \in \mathbb{Z}_B^n(\Delta_E, k, P_\nu^{\mathrm{nt}})$, we have

$$|\Delta_{E_\nu}^{\min}| \geq |\mathrm{cufr}(F(\nu))|/|\alpha|^2.$$

Fix $M > 2$ and let

$$\mathrm{Good}_M(F, B) := \begin{cases} \{\nu \in \mathbb{Z}_B^n(\Delta_E) \mid |\mathrm{sqfr}(F(\nu))|^M > \|\nu\|\} & \text{if } a \neq 4, 8, \\ \{\nu \in \mathbb{Z}_B^n(\Delta_E) \mid |\mathrm{cufr}(F(\nu))|^M > \|\nu\|\} & \text{if } a = 4, 8. \end{cases}$$

Then from (11), we have

$$\sum_{\nu\in\mathbb{Z}_B^n(\Delta_E,P)}\frac{\hat{h}_{E_\nu}(P_\nu)}{h(\nu)}\ge\frac{C_1}{N_k^2}\sum_{\nu\in\mathbb{Z}_B^n(\Delta_E,k,P_\nu^{\mathrm{nt}})\cap\mathrm{Good}_M(F,B)}\frac{\log\|\nu\|^{1/M}-\log|\alpha|^2}{\log\|\nu\|}$$
$$=\frac{C_1}{N_k^2M}\sum_{\nu\in\mathbb{Z}_B^n(\Delta_E,k,P_\nu^{\mathrm{nt}})\cap\mathrm{Good}_M(F,B)}1+o(B^n),$$

where we use Lemma 7 to bound the sum of the second term. Now we are at the final step of analyzing the asymptotic cardinality of $\mathbb{Z}_B^n(\Delta_E,k,P_\nu^{\mathrm{nt}})\cap\mathrm{Good}_M(F,B)$. It is straightforward that

$$\#\mathbb{Z}_B^n(\Delta_E,P)\sim(2B)^n,$$

as the set of points for which $\Delta_E(\mathbf{T})$ vanishes or P_ν is not defined is of size at most $O(B^{n-1})$. Next, by Mazur's theorem [13, Chapter VIII, Theorem 7.5], the order of $E_\nu(\mathbb{Q})_{\mathrm{tor}}$ is at most 12. Hence if P_ν is torsion, ν must satisfy one of the twelve algebraic equations of torsion points that depends on P. Since P is nontorsion in $E(K)$, none of the twelve equations is identically zero and so

$$\#\{\nu\in\mathbb{Z}^n\mid H(\nu)\le B\text{ and }P_\nu\text{ is torsion}\}=O(B^{n-1}).$$

This gives

$$\#\mathbb{Z}_B^n(\Delta_E,P_\nu^{\mathrm{nt}}):=\#\{\nu\in\mathbb{Z}_B^n(\Delta_E,P)\mid P_\nu\in E_\nu(\mathbb{Q})_{\mathrm{nt}}\}\sim(2B)^n.$$

We now apply Corollary 13 to $\Delta_E(\mathbf{T})$, and we specify that k is large enough to have $c_{k,\Delta_E}>0$ in the corollary. Then for any $\lambda\in(0,1)$ and for B large enough, we get

$$\#\mathbb{Z}_B^n(\Delta_E,k,P_\nu^{\mathrm{nt}})\ge\lambda c_{k,\Delta_E}(2B)^n.$$

Lastly, since F is primitive and is neither a square nor a cube in $\mathbb{Z}[\mathbf{T}]$, we use Lemma 14 to conclude that

$$\#\big(\mathbb{Z}_B^n(\Delta_E,k,P_\nu^{\mathrm{nt}})\cap\mathrm{Good}_M(F,B)\big)\ge\lambda c_{k,\Delta_E}(2B)^n,$$

and this gives us

$$\sum_{\nu\in\mathbb{Z}_B^n(\Delta_E,P)}\frac{\hat{h}_{E_\nu}(P_\nu)}{h(\nu)}\ge\frac{C_1}{N_k^2M}\lambda c_{k,\Delta_E}(2B)^n+o(B^n).$$

This proves Proposition 3 with a lower bound $\frac{C_1}{N_k^2M}\lambda c_{k,\Delta_E}$ for any $\lambda\in(0,1)$ and $M>2$, hence we can take $L_2=\frac{C_1}{2N_k^2}c_{k,\Delta_E}$.

6. Proof of Theorem 1. The idea of this proof is to reduce to the case of Proposition 3, since a point in $\mathbb{P}^n_{\mathbb{Q}}$ can be represented with integer coordinates. Again, the implicit constants that appear in this proof will depend only on Δ_E, n and P, unless stated otherwise. Let $\omega=(u_1/v_1,\dots,u_n/v_n)$

$\in \mathbb{Q}^n$ in the lowest form and let $\ell_\omega := \operatorname{lcm}(v_1, \ldots, v_n)$. Recall that the Weierstrass equation of E_ω is

$$Y^2 = X^3 + A(\omega)X + B(\omega),$$

which might not have integer coefficients. In order to estimate $\Delta_{E_\omega}^{\min}$, we need to look at a Weierstrass equation that is $\mathbb{Q}$-isomorphic to E_ω with integer coefficients. Let d be the maximum of $\deg A$ and $\deg B$. By the change of variable $Y' = \ell_\omega^{3d} Y$ and $X' = \ell_\omega^{2d} X$, we obtain an integral coefficients Weierstrass equation:

$$Y'^2 = X'^3 + \ell_\omega^{4d} A(\omega) X' + \ell_\omega^{6d} B(\omega)$$

with discriminant

$$\Delta'_{E_\omega} := -16\ell_\omega^{12d}(4A(\omega)^3 + 27B(\omega)^2) = \ell_\omega^{12d}\Delta_E(\omega).$$

Let us set up the following correspondence to ease our argument. If we write

$$\Delta_E(\mathbf{T}) = \sum_{|\alpha| \le d} \delta_\alpha T_1^{\alpha_1} \ldots T_n^{\alpha_n},$$

then let

$$\widetilde{\Delta}_E(T_0, \mathbf{T}) := \sum_{|\alpha| \le d} \delta_\alpha T_0^{12d-|\alpha|} T_1^{\alpha_1} \ldots T_n^{\alpha_n}.$$

Notice that $\widetilde{\Delta}_E$ is a homogeneous polynomial of degree $12d$. We have a one-to-one correspondence between

$$\mathbb{Q}_B^n(\Delta_E) = \{\omega \in \mathbb{Q}^n \mid 1 < H(\omega) \le B \text{ and } \Delta_E(\omega) \ne 0\}$$

and

$$\{\nu = (\nu_0, \nu_1, \ldots, \nu_n) \in \mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E) \mid \gcd(\nu_0, \nu_1, \ldots, \nu_n) = 1 \text{ and } \nu_0 > 0\}$$

via the map

$$\omega \mapsto \nu := (\ell_\omega, u_1\ell_\omega/v_1, \ldots, u_n\ell_\omega/v_n).$$

This correspondence gives

$$\sum_{\omega \in \mathbb{Q}_B^n(\Delta_E, P)} \frac{\hat{h}_{E_\omega}(P_\omega)}{h(\omega)} = \frac{1}{2} \sum_{\substack{\nu \in \mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E, P) \\ \gcd \nu = 1}}{}' \frac{\hat{h}_{E_{(\nu_1/\nu_0, \ldots, \nu_n/\nu_0)}}(P_{(\nu_1/\nu_0, \ldots, \nu_n/\nu_0)})}{h([\nu_0, \ldots, \nu_n])},$$

where $\gcd \nu := \gcd(\nu_0, \ldots, \nu_n)$ and the primed summation means $\nu_0 \ne 0$ with the factor $1/2$ taking care of the negative ν_0. In order to use the inclusion-exclusion argument effectively in the later part, we need to modify the estimate on the set of ν for which $\widetilde{\Delta}_E(\nu)$ is k-free. Let

$$\operatorname{sqfr} \widetilde{\Delta}_E(T_0, \mathbf{T}) := f_E(T_0, \mathbf{T}),$$

which is a homogeneous polynomial too, and let

$$\mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E, k, P^{\mathrm{nt}}) := \left\{ \nu = (\nu_0, \dots, \nu_n) \in \mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E, P) \;\middle|\; \begin{array}{l} \nu_0 \neq 0,\ f_E(\nu) \text{ is } k\text{-free}, \\ P_\omega \in E_\omega(\mathbb{Q})_{\mathrm{nt}} \\ \text{where } \omega = (\nu_1/\nu_0, \dots, \nu_n/\nu_0) \end{array} \right\},$$

for some $k \geq 4$ large enough as in Lemma 12. If α is the maximum of the exponents of distinct irreducible factors of $\widetilde{\Delta}_E(T_0, \mathbf{T})$, then for all $\nu \in \mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E, k, P^{\mathrm{nt}})$ with $\gcd \nu = 1$, and $\omega = (\nu_1/\nu_0, \dots, \nu_n/\nu_0)$, we have

$$\widetilde{\Delta}_E(\nu) = \Delta'_{E_\omega} \quad \text{is } k\alpha\text{-free.}$$

Thus, letting $N_k := \operatorname{lcm}(1, \dots, k\alpha)$ and using the same argument as in Lemma 6, we get

$$\sum_{\omega \in \mathbb{Q}_B^n(\Delta_E, P)} \frac{\hat{h}_{E_\omega}(P_\omega)}{h(\omega)} \geq \frac{1}{2} \sum_{\substack{\nu \in \mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E, k, P^{\mathrm{nt}}) \\ \gcd \nu = 1}}{}' \frac{C_1}{N_k^2} \frac{\log \Delta_{E_\omega}^{\min}}{\log \|\nu\|}.$$

Notice that $\widetilde{\Delta}_E(T_0, \mathbf{T})$ is not a constant times a twelfth power in $\mathbb{Z}[T_0, \mathbf{T}]$, since otherwise so will be $\widetilde{\Delta}_E(1, \mathbf{T}) = \Delta_E(\mathbf{T})$. Just as in the proof of Proposition 3, we write $\widetilde{\Delta}_E(T_0, \mathbf{T}) = \beta(F(T_0, \mathbf{T}))^{a+12b}$, where $\beta \in \mathbb{Z}$, $F(T_0, \mathbf{T})$ is primitive homogeneous in $\mathbb{Z}[T_0, \mathbf{T}]$ and nonpower in $\mathbb{C}[T_0, \mathbf{T}]$, $b \in \mathbb{N}$ and $a \in \{1, \dots, 11\}$. Since the property

$$0 \leq \operatorname{ord}_p(\Delta_{E_\omega}^{\min}) \equiv \operatorname{ord}_p(\widetilde{\Delta}_E(\nu)) \pmod{12}$$

still holds for all primes p in $\mathbb{Q}$, we can repeat the entire corresponding argument of Section 5 to get

$$\sum_{\omega \in \mathbb{Q}_B^n(\Delta_E, P)} \frac{\hat{h}_{E_\omega}(P_\omega)}{h(\omega)} \geq \frac{1}{2} \sum_{\substack{\nu \in \mathrm{Good}_M(F,B) \\ \nu \in \mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E, k, P^{\mathrm{nt}}) \\ \gcd \nu = 1}}{}' \frac{C_1}{N_k^2} \frac{1}{M} + O\Bigg(\sum_{\nu \in \mathbb{Z}_B^{n+1}} \frac{1}{\log \|\nu\|} \Bigg)$$

where

$$\mathrm{Good}_M(F, B) := \begin{cases} \{\nu \in \mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E) \mid |\mathrm{sqfr}(F(\nu))|^M > \|\nu\|\} & \text{if } a \neq 4, 8, \\ \{\nu \in \mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E) \mid |\mathrm{cufr}(F(\nu))|^M > \|\nu\|\} & \text{if } a = 4, 8, \end{cases}$$

for any fixed $M > 2$. We know from Lemma 7 that the second term is $o(B^{n+1})$. As for the first term, we estimate it by an inclusion-exclusion argument using the Möbius function:

$$\sum_{\substack{\nu\in\mathrm{Good}_M(F,B)\\ \nu\in\mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E,k,P^{\mathrm{nt}})\\ \gcd\nu=1}}{}' 1 = \sum_{\substack{\nu\in\mathrm{Good}_M(F,B)\\ \nu\in\mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E,k,P^{\mathrm{nt}})}}{}' \sum_{g\mid\gcd\nu}\mu(g) = \sum_{g=1}^{B}\mu(g)\sum_{\substack{\nu\in\mathrm{Good}_M(F,B)\\ \nu\in\mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E,k,P^{\mathrm{nt}})\\ g\mid\gcd(\nu)}}{}' 1. \tag{12}$$

To deal with the inner sum, we have to analyse the sets we are summing over. Recall that F is a homogeneous polynomial, so $F(g\nu)=g^tF(\nu)$ where $t=\deg F$, and we have the trivial inequalities

$$\mathrm{sqfr}(F(g\nu))\ge\frac{\mathrm{sqfr}(F(\nu))}{g},\qquad \mathrm{cufr}(F(g\nu))\ge\frac{\mathrm{cufr}(F(\nu))}{g^2}.$$

These imply the following inclusions:

$$\begin{aligned}\mathrm{Good}_M(F,B,g)&:=\{\nu\in\mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E)\mid g\mid\gcd(\nu)\}\cap\mathrm{Good}_M(F,B)\\ &=\begin{cases} g\cdot\{\nu\in\mathbb{Z}_{B/g}^{n+1}(\widetilde{\Delta}_E)\mid|\mathrm{sqfr}(F(g\nu))|^M>\|g\nu\|\} & \text{if } a\neq4,8\\ g\cdot\{\nu\in\mathbb{Z}_{B/g}^{n+1}(\widetilde{\Delta}_E)\mid|\mathrm{cufr}(F(g\nu))|^M>\|g\nu\|\} & \text{if } a=4,8\end{cases}\\ &\supseteq\begin{cases} g\cdot\{\nu\in\mathbb{Z}_{B/g}^{n+1}(\widetilde{\Delta}_E)\mid|\mathrm{sqfr}(F(\nu))/g|^M>g\|\nu\|\} & \text{if } a\neq4,8\\ g\cdot\{\nu\in\mathbb{Z}_{B/g}^{n+1}(\widetilde{\Delta}_E)\mid|\mathrm{cufr}(F(\nu))/g^2|^M>g\|\nu\|\} & \text{if } a=4,8,\end{cases}\end{aligned}$$

where the notation $g\cdot S$ means $\{g\nu\mid\nu\in S\}$ for any set S of vectors. By Corollary 15, for $g\le B^{1/5}$ and $M>8$, we have

$$\mathrm{Good}_M(F,B,g)\sim(2B/g)^{n+1}. \tag{13}$$

On the other hand, f_E is also homogeneous, say of degree r. We have

$$\begin{aligned}\mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E,k,P^{\mathrm{nt}},g)&:=\{\nu\in\mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E)\mid g\mid\gcd(\nu)\}\cap\mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E,k,P^{\mathrm{nt}})\\ &=g\cdot\left\{\nu=(\nu_0,\dots,\nu_n)\in\mathbb{Z}_{B/g}^{n+1}(\widetilde{\Delta}_E,P)\;\middle|\;\begin{array}{l}\nu_0\neq0,\ g^rf_E(\nu)\text{ is }k\text{-free},\\ P_\omega\in E_\omega(\mathbb{Q})_{\mathrm{nt}}\\ \text{where }\omega=(\nu_1/\nu_0,\dots,\nu_n/\nu_0)\end{array}\right\}.\end{aligned}$$

For $\mu(g)\neq0$, i.e. g squarefree, we have the inclusions

$$g\cdot\mathbb{Z}_{B/g}^{n+1}(\widetilde{\Delta}_E,k-r,P^{\mathrm{nt}})\subseteq\mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E,k,P^{\mathrm{nt}},g)\subseteq g\cdot\mathbb{Z}_{B/g}^{n+1}(\widetilde{\Delta}_E,k,P^{\mathrm{nt}}).$$

From (13), Lemma 12 and Mazur's theorem again, for any $\epsilon>0$, there exists B_ϵ such that if $B/g\ge B_\epsilon$, $g\le B^{1/5}$ and $\mu(g)\neq0$ then

$$\gamma_{k-r,f_E}-\epsilon\le\frac{\#\big(\mathbb{Z}_B^{n+1}(\widetilde{\Delta}_E,k,P^{\mathrm{nt}},g)\cap\mathrm{Good}_M(F,B,g)\big)}{(2B/g)^{n+1}}\le\gamma_{k,f_E}+\epsilon.$$

It is important to note that the implicit constants in the rest of the proof depend only on n. From (12), for $B > B_\epsilon^{5/4}$,

$$\sum_{\substack{\nu\in\mathrm{Good}_M(F,B)\\ \nu\in\mathbb{Z}_B^{n+1}(\tilde{\Delta}_E,k,P^{\mathrm{nt}})\\ \gcd\nu=1}}{}' 1 \ge \sum_{g=1}^{\lfloor B^{1/5}\rfloor}\mu(g)\sum_{\substack{\nu\in\mathrm{Good}_M(F,B,g)\\ \nu\in\mathbb{Z}_B^{n+1}(\tilde{\Delta}_E,k,P^{\mathrm{nt}},g)}}{}' 1 + \sum_{g=\lfloor B^{1/5}\rfloor+1}^{B}\mu(g)\sum_{\substack{\nu\in\mathrm{Good}_M(F,B,g)\\ \nu\in\mathbb{Z}_B^{n+1}(\tilde{\Delta}_E,k,P^{\mathrm{nt}},g)}}{}' 1$$

$$\ge \sum_{\substack{g=1\\ \mu(g)=1}}^{\lfloor B^{1/5}\rfloor}\mu(g)(\gamma_{k-r,f_E}-\epsilon)(2B/g)^{n+1} + \sum_{\substack{g=1\\ \mu(g)=-1}}^{\lfloor B^{1/5}\rfloor}\mu(g)(\gamma_{k,f_E}+\epsilon)(2B/g)^{n+1}$$

$$+ O\Big(\sum_{g=\lfloor B^{1/5}\rfloor+1}^{B}(2B/g)^{n+1}\Big)$$

$$= (\gamma_{k-r,f_E}-\epsilon)(2B)^{n+1}\sum_{g=1}^{\lfloor B^{1/5}\rfloor}\frac{\mu(g)}{g^{n+1}}$$

$$+(2\epsilon+\gamma_{k,f_E}-\gamma_{k-r,f_E})(2B)^{n+1}\sum_{\substack{g=1\\ \mu(g)=-1}}^{\lfloor B^{1/5}\rfloor}\frac{\mu(g)}{g^{n+1}} + (2B)^{n+1}O\Big(\sum_{g=\lfloor B^{1/5}\rfloor+1}^{B}\frac{1}{g^{n+1}}\Big).$$

So we get

$$\liminf_{B\to\infty}\frac{1}{(2B)^{n+1}}\sum_{\omega\in\mathbb{Q}_B^n(\Delta_E,P)}\frac{\hat{h}_{E_\omega}(P_\omega)}{h(\omega)}$$

$$\ge \frac{1}{2}\frac{C_1}{N_k^2}\frac{1}{M}\left((\gamma_{k-r,f_E}-\epsilon)\frac{1}{\zeta(n+1)} + (2\epsilon+\gamma_{k,f_E}-\gamma_{k-r,f_E})O(1)\right)$$

where ζ is the Riemann zeta function, and one possible bound for the $O(1)$ here is $\zeta(n+1)$. So

$$\liminf_{B\to\infty}\frac{2\zeta(n+1)}{(2B)^{n+1}}\sum_{\omega\in\mathbb{Q}_B^n(\Delta_E,P)}\frac{\hat{h}_{E_\omega}(P_\omega)}{h(\omega)}$$

$$\ge \frac{C_1}{MN_k^2}\big((\gamma_{k-r,f_E}-\epsilon)+(2\epsilon+\gamma_{k,f_E}-\gamma_{k-r,f_E})O(1)\big).$$

Since this holds for all $\epsilon > 0$ and $M > 8$, and the same inclusion-exclusion argument will give

$$\#\{\omega\in\mathbb{Q}^n \mid H(\omega)\le B\} \sim \frac{(2B)^{n+1}}{2\zeta(n+1)},$$

we have proven Theorem 1 with $L_1 = \frac{C_1}{8N_k^2}(\gamma_{k-r,f_E} + (\gamma_{k,f_E} - \gamma_{k-r,f_E})O(1))$. Notice that L_1 is positive for k large enough because the sequence $(\gamma_{k,f_E})_{k=1}^{\infty}$ is increasing and bounded above by 1.

7. Discussion. Our proofs of Proposition 3 and Theorem 1 use the weakened form of Lang's height conjecture proven by Silverman, mentioned in the proof of Lemma 6, which is a key tool in our proof that the set of $\omega \in \mathbb{Q}^n$ such that $\hat{h}_{E_\omega}(P_\omega) > \frac{C_1}{8N_k^2}h(\omega)$ has a positive density at least $\gamma_{k-r,f_E} + (\gamma_{k,f_E} - \gamma_{k-r,f_E})O(1)$. In view of this, the corollary below follows immediately from Corollary 4.2 of [14].

COROLLARY 16. *Keeping all the above notation, let further Γ be a subgroup of $E(K)$ of rank r and Γ_ω be its image under the specialization map. Then there exists a constant c, depending only on E, such that the set*

$$\left\{\omega \in \mathbb{Q}^n(\Delta_E) \;\middle|\; \#(E_\omega(\mathbb{Z}) \cap \Gamma_\omega) \le 12c^{1+r}\left(\sqrt{\frac{8N_k^2}{C_1}}\right)^r\right\}$$

has density at least $\gamma_{k-r,f_E} + (\gamma_{k,f_E} - \gamma_{k-r,f_E})O(1)$.

We remark that if Lang's conjecture is true, then we can improve both Proposition 3 and Theorem 1 to $L_2 = C_1/2$ and $L_1 = C_1/8$, independent of E. Also, Corollary 16 will then be improved to stating density 1.

One might be interested whether we can generalize our initial setting of $\mathbb{Q}$ to any number field F. In order to do that, we first have to replace $\mathbb{Z}$ by the F integers $\mathcal{O}_F$ in Proposition 3, and scrutinize all the lemmas used in the proof to see whether they are still valid in F. Lemma 6 can be easily generalized to F, as both the Silverman Theorem [10] and Kodaira–Néron Theorem [15] were originally proven for number fields. Further, Lemmas 7, 9 generalize immediately, and Mazur's theorem also has its generalized counterpart, Merel's Theorem. Alternatively, we can use the following Masser bound (we thank the referee for pointing this out). Using methods from transcendence theory, Masser obtained the upper bound [7, Corollary 2]

$$\#E(K)_{\mathrm{tor}} \le C_k\sqrt{h([1,g_1,g_2])}[K:k](h([1,g_1,g_2]) + \log[K:k])$$

for the elliptic curve $E/k : y^2 = 4x^3 - g_1x - g_3$, where C_k is an effective constant that depends only on the number field k, and K/k is any finite field extension. Applying this to our setting over the number field F, we can easily deduce that for all $\nu \in (\mathcal{O}_F)_B^n$,

$$\#E_\nu(F)_{\mathrm{tor}} \le C_F\big(h([1,4A(\nu),4B(\nu)])\big)^{3/2} \le C_F'(\log B)^{3/2}$$

where C_F' is an effective constant that depends on F and the polynomials

$A(\mathbf{T}), B(\mathbf{T})$. This is sufficient for our application as it gives the bound

$$\#\{\nu \in \mathcal{O}_F^n \mid H(\nu) \le B \text{ and } P_\nu \text{ is torsion}\} = O(B^{n-1}(\log B)^{3/2}) = o(B^n).$$

Besides having the advantage of a computable effective constant, Masser's bound is also true for general abelian varieties [8, Main Theorem and Scholium 2].

What is left to be worked on is Lemmas 12 and 14. Another, and possibly more interesting problem is to prove convergence of the average, or even better, to prove that the average converges to $\hat{h}_E(P)$.

Acknowledgements. I would like to thank my advisor, Joseph Silverman, for many enlightening discussions. Also, many thanks to the referee for the valuable and insightful comments and suggestions.

References

[1] T. D. Browning, *Power-free values of polynomials*, Arch. Math. (Basel) 96 (2011), 139–150.

[2] G. H. Call, *Variation of local heights on an algebraic family of abelian varieties*, in: Théorie des nombres (Québec, PQ, 1987), de Gruyter, Berlin, 1989, 72–96.

[3] D. R. Heath-Brown, *Counting rational points on algebraic varieties*, in: Analytic Number Theory, Lecture Notes in Math. 1891, Springer, Berlin, 2006, 51–95.

[4] A. W. Knapp, *Advanced Algebra*, Cornerstones, Springer, Boston, 2007.

[5] S. Lang, *Algebra*, Grad. Texts in Math. 211, Springer, New York, 2002.

[6] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, New York, 1983.

[7] D. W. Masser, *Counting points of small height on elliptic curves*, Bull. Soc. Math. France 117 (1989), 247–265.

[8] D. W. Masser, *Specializations of finitely generated subgroups of abelian varieties*, Trans. Amer. Math. Soc. 311 (1989), 413–424.

[9] B. Poonen, *Squarefree values of multivariable polynomials*, Duke Math. J. 118 (2003), 353–373.

[10] J. H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. 48 (1981), 633–648.

[11] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. 342 (1983), 197–211.

[12] J. H. Silverman, *Divisibility of the specialization map for families of elliptic curves*, Amer. J. Math. 107 (1985), 555–565.

[13] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

[14] J. H. Silverman, *A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves*, J. Reine Angew. Math. 378 (1987), 60–100.

[15] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 2007.

[16] W. W. Stothers, *Polynomial identities and Hauptmoduln*, Quart. J. Math. Oxford Ser. (2) 32 (1981), 349–370.

[17] J. Tate, *Variation of the canonical height of a point depending on a parameter*, Amer. J. Math. 105 (1983), 287–294.

Wei Pin Wong
Mathematics Department
Box 1917
Brown University
Providence, RI 02912, U.S.A.
E-mail: wongpin101@math.brown.edu

Received on 17.6.2013
and in revised form on 26.3.2014 (7484)