Functiones et Approximatio
52.1 (2015), 127–132
doi: 10.7169/facm/2015.52.1.10

A HEIGHT INEQUALITY FOR RATIONAL POINTS ON ELLIPTIC CURVES IMPLIED BY THE ABC-CONJECTURE

Ulf Kühn, Jan Steffen Müller

Abstract: In this short note we show that the uniform *abc*-conjecture puts strong restrictions on the coordinates of rational points on elliptic curves. For the proof we use a variant of Vojta's height inequality formulated by Mochizuki. As an application, we generalize a result of Silverman on elliptic non-Wieferich primes.

Keywords: elliptic curves, abc-conjecture, rational points, heights, Wieferich primes.

1. Introduction

If $E/\mathbb{Q}$ is an elliptic curve in Weierstrass form with point at infinity O and $P \in E(\mathbb{Q}) \setminus \{O\}$, then it is well known that we can write

$$P = \left(\frac{a_P}{d_P^2}, \frac{b_P}{d_P^3}\right),$$

where a_P, b_P, $d_P \in \mathbb{Z}$ satisfy $\gcd(d_P, a_P b_P) = 1$ and $d_P > 0$.

The structure of the *denominators* d_P has been studied, for instance, by Everest-Reynolds-Stevens [3] and Stange [10], and has recently received increasing attention in the context of elliptic divisibility sequences first studied by Ward [13]. See for instance [2] or [7] and the references therein. In this paper we derive strong conditions on the denominators d_P from the uniform *abc*-conjecture over number fields (see Conjecture 2.2 or [4]).

If n is a positive integer, then the *radical* $\mathrm{rad}(n)$ of n is defined as the product of the distinct prime divisors of n. We call n *powerful* if $\mathrm{ord}_p(n) \neq 1$ for all prime numbers p. The *powerful part* of n is defined to be the largest powerful integer dividing n.

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve in Weierstrass form and suppose that the uniform abc-conjecture holds. Then, for all $\varepsilon > 0$, there exist constants c*

2010 Mathematics Subject Classification: primary: 11G05; secondary: 11G50

and c', only depending on E and ε, such that for all $P \in E(\mathbb{Q}) \setminus \{O\}$ the following hold:

(i) *We have*

$$\max\left\{\frac{1}{2}\log|a_P|, \log d_P\right\} \leqslant (1+\varepsilon)\log \operatorname{rad}(d_P) + c.$$

(ii) *Let v_P be the powerful part of d_P and write $d_P = u_P v_P$; then*

$$\log v_P \leqslant \varepsilon \log|u_P| + c'.$$

Remark 1.2. A strong form of Siegel's Theorem implies a weaker upper bound (and an analogous lower bound) on $\log|a_P|$: There is a constant $c = c(E,\varepsilon)$ such that

$$(1-\varepsilon)\log d_P - c \leqslant \frac{1}{2}\log|a_P| \leqslant (1+\varepsilon)\log d_P + c,$$

see [8, Example IX.3.3].

Remark 1.3. Mochizuki [6] has recently announced a proof of the uniform *abc*-conjecture over number fields.

If, in the notation of Theorem 1.1, d_P is powerful, then $|u_P| = 1$. Hence the following result is an immediate consequence of Theorem 1.1 (ii):

Corollary 1.4. *Let $E/\mathbb{Q}$ be an elliptic curve in Weierstrass form and suppose that the uniform abc-conjecture holds. Then the set of all $P \in E(\mathbb{Q}) \setminus \{O\}$ such that d_P is powerful is finite.*

Remark 1.5. In particular, Corollary 1.4 implies that only finitely many $P \in E(\mathbb{Q}) \setminus \{O\}$ have prime power denominator if the uniform *abc*-conjecture holds. The question of prime power denominators was studied, for instance, in [3]; there it is shown ([3, Theorem 1.1]) that for a fixed exponent $n > 1$, there are only finitely many $P \in E(\mathbb{Q}) \setminus \{O\}$ such that d_P is an nth power. Moreover, it is claimed ([3, Remark 1.2]) that the uniform *abc*-conjecture over number fields implies that for $n \gg 0$, there are no $P \in E(\mathbb{Q}) \setminus \{O\}$ such that d_P is an nth power. Together, these results would also imply that the finiteness of the set of $P \in E(\mathbb{Q}) \setminus \{O\}$ such that d_P is a perfect power is a consequence of the uniform *abc*-conjecture. However, no proof of [3, Remark 1.2] has been published so far.

Another application of Theorem 1.1 concerns *elliptic non-Wieferich primes*. For a prime p of good reduction for an elliptic curve $E/\mathbb{Q}$, we define $N_p := \#E(\mathbb{F}_p)$. If $P \in E(\mathbb{Q})$ is non-torsion, let

$$W_{E,P} := \left\{p \text{ good prime for } E : N_p P \not\equiv O \bmod p^2\right\}$$

be the set of elliptic non-Wieferich primes to base P.

Corollary 1.6. *Let $E/\mathbb{Q}$ be an elliptic curve in Weierstrass form and suppose that the uniform abc-conjecture holds. If $P \in E(\mathbb{Q})$ is non-torsion, then*

$$|\{p \in W_{E,P} : p \leqslant X\}| \geqslant \sqrt{\log(X)} + \mathcal{O}_{E,P}(1) \qquad \text{as } X \to \infty. \tag{1}$$

Remark 1.7. Assuming the *abc*-conjecture over $\mathbb{Q}$, Silverman has already proved that (1) holds for all non-torsion $P \in E(\mathbb{Q})$ if $j(E) \in \{0, 1728\}$, cf. [9, Theorem 2].

Proof. The only place in Silverman's proof of (1) where the *abc*-conjecture and the assumption $j(E) \in \{0, 1728\}$ are invoked is in the proof of [9, Lemma 13]. In order to deduce the statement of [9, Lemma 13] for arbitrary E, it suffices to show that for all $\varepsilon > 0$ there exists a constant $c = c(E, \varepsilon)$ such that

$$\log v_{nP} \leqslant \varepsilon \log(d_{nP}) + c$$

for all $n \geqslant 1$, where v_{nP} is the powerful part of d_{nP}. But this follows at once from part (ii) of Theorem 1.1. ■

Corollary 1.6 is the analogue of [9, Theorem 1], giving an asymptotic lower bound (dependent on the *abc*-conjecture over $\mathbb{Q}$) for the number of classical non-Wieferich primes up to a given bound. See [12] for further results concerning elliptic non-Wieferich primes.

In Section 2 we recall work of Mochizuki from [5], which we use in Section 3 for the proof of Theorem 1.1.

Acknowledgements. We thank Joe Silverman for helpful comments and his suggestion that Corollary 1.6 should hold. We also thank Jonathan Reynolds for helpful discussions and an anonymous referee for useful advice on an earlier draft of this paper. The second author was supported by DFG-grant KU 2359/2-1.

2. The uniform *abc*-conjecture and Vojta's height inequality

In this section, we discuss the uniform *abc*-conjecture and a variant of Vojta's height conjecture.

Let K be a number field with ring of integers $\mathcal{O}_K$, let X be a smooth, proper, geometrically connected curve over K and let D be an effective divisor on X. Extend X to a proper regular model $\mathcal{X}$ over $\operatorname{Spec}(\mathcal{O}_K)$ and D to an effective horizontal divisor $\mathcal{D} \in \operatorname{Div}(\mathcal{X})$.

Suppose that $P \in X(F)$, where F is some finite extension of K. We can define the *conductor* $\operatorname{cond}_{\mathcal{X},\mathcal{D}}(P)$ of P as follows: Let $\pi : \mathcal{X}' \to \mathcal{X} \times \operatorname{Spec}(\mathcal{O}_F)$ be the minimal desingularization and let $\mathcal{P} \in \operatorname{Div}(\mathcal{X}')$ be the Zariski closure of P in $\mathcal{X}'$. Then we define

$$\operatorname{cond}_{\mathcal{X},\mathcal{D}}(P) := \prod_{\mathfrak{p} \in S} \operatorname{Nm}(\mathfrak{p})^{\frac{1}{[F:\mathbb{Q}]}} \in \mathbb{R},$$

where S is the set of finite primes $\mathfrak{p}$ of F such that the intersection multiplicity $(\mathcal{P} \,.\, \pi^*\mathcal{D})_{\mathfrak{p}} \neq 0$.

Remark 2.1. For different constructions of the (logarithmic) conductor, see [5, §1] or [1, §14.4]. It is easy to see that, up to a bounded function, these constructions are all equivalent. By [5, Remark 1.5.1], changing the model $\mathcal{X}$ only changes $\log \mathrm{cond}_{\mathcal{X},\mathcal{D}}$ by a bounded function. Hence, up to a bounded function, $\mathrm{cond}_{\mathcal{X},\mathcal{D}}$ only depends on D.

If $P \in X(\overline{K})$, then we write $k(P)$ for the minimal field of definition of P. Mochizuki [5, §2] has rewritten the uniform *abc*-conjecture over number fields (see [4]) as follows:

Conjecture 2.2 (Uniform *abc*-conjecture). *Let* $D = (0)+(1)+(\infty) \in \mathrm{Div}(\mathbb{P}^1)$ *and let* h *denote a Weil height on* $\mathbb{P}^1$ *with respect to the divisor* (∞)*. Extend* D *to an effective horizontal divisor* $\mathcal{D}$ *on* $\mathcal{X} = \mathbb{P}^1_{\mathbb{Z}}$*.*

If $\varepsilon > 0$ *and* $d \in \mathbb{N}$*, then there exists a constant* $c = c(\varepsilon, d)$ *such that*

$$h(P) \leqslant (1+\varepsilon)\left(\log|\operatorname{disc}(k(P))| + \log \mathrm{cond}_{\mathcal{X},\mathcal{D}}(P)\right) + c$$

for all $P \in X(\overline{\mathbb{Q}})$ *satisfying* $[k(P) : \mathbb{Q}] \leqslant d$*.*

Remark 2.3. The *abc*-conjecture over $\mathbb{Q}$ (see for instance [1, Conjecture 12.2.2]) is a special case of Conjecture 2.2. Indeed, let a and b be coprime positive integers, let $c = a + b$ and consider the point $P = [a : c] \in \mathbb{P}^1$. Then, up to a bounded function, we have $h(P) = \log \max\{|a|, |c|\} = \log c$. Moreover, $\operatorname{disc}(k(P)) = 1$ and

$$\mathrm{cond}_{\mathcal{X},\mathcal{D}}(P) = \prod_{p \in S} p = \mathrm{rad}(abc),$$

where S is the set of prime numbers p such that $\mathrm{ord}_p(a) > 0$, $\mathrm{ord}_p(b) > 0$ or $\mathrm{ord}_p(c) > 0$.

The following version of Vojta's conjectured height inequality was stated by Mochizuki [5, §2].

Conjecture 2.4 (Vojta's height inequality). *Let* X *be a smooth, proper, geometrically connected curve over a number field* K*. Let* $D \subset X$ *be an effective reduced divisor, and* ω_X *the canonical sheaf on* X*. Fix a proper regular model* $\mathcal{X}$ *of* X *over* $\mathrm{Spec}(\mathcal{O}_K)$ *and extend* D *to an effective horizontal divisor* $\mathcal{D}$ *on* $\mathcal{X}$*. Suppose that* $\omega_X(D)$ *is ample and let* $h_{\omega_X(D)}$ *be a Weil height function on* X *with respect to* $\omega_X(D)$*.*

If $\varepsilon > 0$ *and* $d \in \mathbb{N}$*, then there exists a constant* $c = c(\varepsilon, d, \mathcal{X}, \mathcal{D})$ *such that*

$$h_{\omega_X(D)}(P) \leqslant (1+\varepsilon)\left(\log|\operatorname{disc}(k(P))| + \log \mathrm{cond}_{\mathcal{X},\mathcal{D}}(P)\right) + c$$

for all $P \in X(\overline{K}) \setminus \mathrm{supp}(D)$ *satisfying* $[k(P) : \mathbb{Q}] \leqslant d$*.*

Obviously Conjecture 2.4 contains Conjecture 2.2 as a special case. In fact, the converse also holds:

Theorem 2.5. *Conjecture 2.2 and Conjecture 2.4 are equivalent.*

Proof. See [5, Theorem 2.1]), [1, Theorem 14.4.16] or [11, Theorem 5.1]. ∎

3. Proof of Theorem 1.1

Proof. We specialize Conjecture 2.4 to the case $K = \mathbb{Q}$, $X = E$, $d = 1$ and $D = (O)$. Let $P \in E(\mathbb{Q}) \setminus \{O\}$; then we have $\omega_E(D) \cong \mathcal{O}_E(D)$ and hence

$$h_{\omega_E(D)}(P) = \max\left\{\frac{1}{2}\log|a_P|, \log d_P\right\} + \mathcal{O}(1),$$

since the function $P \mapsto \max\left\{\frac{1}{2}\log|a_P|, \log d_P\right\}$ is a Weil height on E with respect to $\mathcal{O}_E(D)$.

In order to compute the logarithmic conductor of P we consider the minimal desingularization $\mathcal{X}$ of the normal model over $\operatorname{Spec}(\mathbb{Z})$ determined by the given Weierstrass equation of E and extend D to $\mathcal{D} \in \operatorname{Div}(\mathcal{X})$ by taking the Zariski closure. Then a prime number p of good reduction satisfies $(\mathcal{P}\,.\,\mathcal{D})_p \neq 0$ if and only if $p \mid d_P$; therefore we have

$$|\log \operatorname{cond}_{\mathcal{X},\mathcal{D}}(P) - \log \operatorname{rad}(d_P)| \leqslant \sum_{p \text{ bad}} \log p.$$

Hence the functions $P \mapsto \log \operatorname{cond}_{\mathcal{X},\mathcal{D}}(P)$ and $P \mapsto \log \operatorname{rad}(d_P)$ coincide up to a bounded function and Conjecture 2.4 implies

$$\max\left\{\frac{1}{2}\log|a_P|, \log d_P\right\} \leqslant (1+\varepsilon)\log \operatorname{rad}(d_P) + c.$$

By Theorem 2.5, this finishes the proof of (i).

To prove part (ii), let $\varepsilon > 0$, let $c = c(E,\varepsilon)$ be the corresponding constant from part (i) of the theorem and fix some $\varepsilon' > 0$ such that $\frac{2\varepsilon'}{1-\varepsilon'} < \varepsilon$.

Let $P \in E(\mathbb{Q}) \setminus \{O\}$. Then (i) implies

$$\begin{aligned} \log|u_P| + \log v_P &\leqslant (1+\varepsilon')\left(\log \operatorname{rad}(u_P) + \log \operatorname{rad}(v_P)\right) + c \\ &\leqslant (1+\varepsilon')\left(\log|u_P| + \frac{1}{2}\log v_P\right) + c \end{aligned}$$

and hence we conclude

$$\log v_P \leqslant \frac{2\varepsilon'}{1-\varepsilon'}\log|u_P| + \frac{2c}{1-\varepsilon'},$$

which proves (ii). ■

References

[1] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.
[2] M. Einsiedler, G. Everest, and T. Ward, *Primes in elliptic divisibility sequences*, LMS J. Comput. Math. **4** (2001), 1–13.

[3] G. Everest, J. Reynolds, and S. Stevens, *On the denominators of rational points on elliptic curves*, Bull. Lond. Math. Soc. **39** (2007), no. 5, 762–770.
[4] A. Granville and H.M. Stark, *ABC implies no "Siegel zeros" for L-functions of characters with negative discriminant*, Inventiones Math. **139** (2000), 509–523.
[5] S. Mochizuki, *Arithmetic elliptic curves in general position*, Math. J. Okayama Univ. **52** (2010), 1–28.
[6] S. Mochizuki, *Inter-universal Teichmüller theory IV: Log-volume computations and set-theoretic foundations*, Preprint (2012).
[7] J. Reynolds, *Perfect powers in elliptic divisibility sequences*, J. Number Theory **132** (2012), no. 5, 998–1015.
[8] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
[9] J.H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237.
[10] K. Stange, *Elliptic nets and elliptic curves*, Algebra and Number Theory **5** (2011), no. 2, 197–229.
[11] M. Van Frankenhuysen, *The ABC conjecture implies Vojta's height inequality for curves*, J. Number Theory **95** (2002), no. 2, 289–302.
[12] J.F. Voloch, *Elliptic Wieferich primes*, J. Number Theory **81** (2000), no. 2, 205–209.
[13] M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31–74.

Addresses: Ulf Kühn: Fachbereich Mathematik, Universität Hamburg, Bundesstrasse 55, 20146 Hamburg, Germany;
Jan Steffen Müller: Institut für Mathematik, Carl von Ossietzky Universität Oldenburg, 26111 Oldenburg, Germany.

E-mail: kuehn@math.uni-hamburg.de, jan.steffen.mueller@uni-oldenburg.de

Received: 3 December 2013; **revised:** 30 January 2014