New York Journal of Mathematics

New York J. Math. **16** (2010) 1–12.

Lang's height conjecture and Szpiro's conjecture

Joseph H. Silverman

ABSTRACT. It is known that Szpiro's conjecture, or equivalently the ABC-conjecture, implies Lang's conjecture giving a uniform lower bound for the canonical height of nontorsion points on elliptic curves. In this note we show that a significantly weaker version of Szpiro's conjecture, which we call "prime-depleted," suffices to prove Lang's conjecture.

CONTENTS

Introduction

Let E/K be an elliptic curve defined over a number field, let $P \in E(K)$ be a nontorsion point on E, and write $\mathfrak{D}(E/K)$ and $\mathfrak{F}(E/K)$ for the discriminant and the conductor of E/K. In this paper we discuss the relationship between the following conjectures of Serge Lang [12, page 92] and Lucien Szpiro (1983).

Conjecture 1 (Lang Height Conjecture)**.** *There are constants $C_1 > 0$ and C_2, depending only on K, such that the canonical height of P is bounded below by*

$$\hat{h}(P) \geq C_1 \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{D}(E/K) - C_2.$$

Received August 26, 2009.

2000 *Mathematics Subject Classification.* Primary: 11G05; Secondary: 11G50, 11J97, 14H52.

Key words and phrases. elliptic curve, canonical height, Szpiro conjecture, Lang conjecture.

The author's research partially supported by NSF grants DMS-0650017 and DMS-0854755.

ISSN 1076-9803/00

Conjecture 2 (Szpiro Conjecture). *There are constants C_3 and C_4, depending only on K, such that*

$$\log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{D}(E/K) \le C_3 \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{F}(E/K) + C_4.$$

(We remark that stronger versions of Conjectures 1 and 2 say, respectively, that C_1 may be chosen to depend only on $[K : \mathbb{Q}]$ and that $C_3 > 6$ is sufficient.)

In [9] Marc Hindry and the author proved that Szpiro's conjecture implies Lang's height conjecture, and the dependence of C_1 and C_2 on K and on the constants in Szpiro's conjecture were subsequently improved by David [4] and Petsche [15]. It is thus tempting to try to prove the opposite implication, i.e., prove that Lang's height conjecture implies Szpiro's conjecture. Since Szpiro's conjecture is easily seen to imply the ABC-conjecture of Masser and Oesterlé [14] (with some exponent), such a proof would be of interest.

It is the purpose of this note to explain how the pigeonhole argument in [16] may be combined with the Fourier averaging methods in [9] to prove Lang's height conjecture using a weaker form of Szpiro's conjecture. Roughly speaking, the "prime-depleted" version of Szpiro's conjecture that we use allows us to discard a bounded number of primes from $\mathfrak{D}(E/K)$ and $\mathfrak{F}(E/K)$ before comparing them. It thus seems unlikely that there is a direct proof that Lang's height conjecture implies the standard Szpiro's conjecture. We also note that the prime-depleted conjecture is insufficient for many Diophantine applications; see Remark 12.

We briefly summarize the contents of this paper. In Section 1 we describe the prime-depleted Szpiro conjecture and prove that it implies Lang's height conjecture. Section 2 contains various elementary properties of the prime-depleted Szpiro ratio. Finally, in Section 3 we state a prime-depleted ABC-conjecture and show that it is a consquence of the prime-depleted Szpiro conjecture.

Acknowledgements. The author would like to thank the referee for suggestions on improving the exposition.

1. The prime-depleted Szpiro conjecture

We begin with some definitions.

Definition. Let $\mathfrak{D}$ be an integral ideal of K, let $\nu(\mathfrak{D})$ denote the number of distinct prime ideals dividing $\mathfrak{D}$, and factor

$$\mathfrak{D} = \prod_{i=1}^{\nu(\mathfrak{D})} \mathfrak{p}_i^{e_i}$$

as a product of prime powers. The *Szpiro ratio of* $\mathfrak{D}$ is the quantity

$$\sigma(\mathfrak{D}) = \frac{\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{D}}{\log \mathsf{N}_{K/\mathbb{Q}} \prod_{i=1}^{\nu(\mathfrak{D})} \mathfrak{p}_i} = \frac{\sum_{i=1}^{\nu(\mathfrak{D})} e_i \log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}_i}{\sum_{i=1}^{\nu(\mathfrak{D})} \log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}_i}.$$

(If $\mathfrak{D} = (1)$, we set $\sigma(\mathfrak{D}) = 1$.) More generally, for any integer $J \ge 0$, the *J-depleted Szpiro ratio of* $\mathfrak{D}$ is defined as follows:

$$\sigma_J(\mathfrak{D}) = \min_{\substack{I \subset \{1,2,\ldots,\nu(\mathfrak{D})\} \\ \#I \ge \nu(\mathfrak{D}) - J}} \sigma\biggl(\prod_{i \in I} \mathfrak{p}_i^{e_i}\biggr).$$

Thus $\sigma_J(\mathfrak{D})$ is the smallest value that can be obtained by removing from $\mathfrak{D}$ up to J of the prime powers dividing $\mathfrak{D}$ before computing the Szpiro ratio. We note that if $\nu(\mathfrak{D}) \le J$, then $\sigma_J(\mathfrak{D}) = 1$ by definition.

Example 3.

$$\sigma_0(1728) = \frac{\log 1728}{\log 6} \approx 4.16, \quad \sigma_1(1728) = \frac{\log 27}{\log 3} = 3, \quad \sigma_2(1728) = 1.$$

Conjecture 4 (Prime-Depleted Szpiro Conjecture)**.** *Let $K/\mathbb{Q}$ be a number field. There exist an integer $J \ge 0$ and a constant C_5, both depending only on K, such that for all elliptic curves E/K,*

$$\sigma_J\bigl(\mathfrak{D}(E/K)\bigr) \le C_5.$$

It is clear from the definition that $\sigma_0(\mathfrak{D}) = \sigma(\mathfrak{D})$. An elementary argument (Proposition 9) shows that the value of σ_J decreases as J increases,

$$\sigma_0(\mathfrak{D}) \ge \sigma_1(\mathfrak{D}) \ge \sigma_2(\mathfrak{D}) \ge \cdots.$$

Hence the prime-depleted Szpiro conjecture is weaker than the classical version, which says that $\sigma_0\bigl(\mathfrak{D}(E/K)\bigr)$ is bounded independent of E. Before stating our main result, we need one further definition.

Definition. Let E/K be an elliptic curve defined over a number field. The *height of E/K* is the quantity

$$h(E/K) = \max\bigl\{h\bigl(j(E)\bigr), \log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{D}(E/K)\bigr\}.$$

For a given field K, there are only finitely many elliptic curves E/K of bounded height, although there may be infinitely many elliptic curves of bounded height defined over fields of bounded degree [18].

We now state our main result.

Theorem 5. *Let $K/\mathbb{Q}$ be a number field, let $J \ge 1$ be an integer, let E/K be an elliptic curve, and let $P \in E(K)$ be a nontorsion point. There are* *constants $C_6 > 0$ and C_7, depending only on $[K:\mathbb{Q}]$, J, and the J-depleted Szpiro ratio $\sigma_J\bigl(\mathfrak{D}(E/K)\bigr)$, such that*

$$\hat{h}(P) \ge C_6 h(E/K) - C_7.$$

In particular, the prime-depleted Szpiro conjecture implies Lang's height conjecture.

Remark 6. As in [15], it is not hard to give explicit expressions for C_6 and C_7 in terms of $[K:\mathbb{Q}]$, J, and $\sigma_J\bigl(\mathfrak{D}(E/K)\bigr)$. In terms of the dependence on the Szpiro ratio, probably the best that comes out of a careful working of the proof is something like

$$C_6 = C_6' \sigma_J\bigl(\mathfrak{D}(E/K)\bigr)^{cJ}$$

for an absolute constant c and a constant C_6' depending on $[K:\mathbb{Q}]$ and J. But until the (prime-depleted) Szpiro conjecture is proven or a specific application arises, such explict expressions seem of limited utility.

Proof. We refer the reader to [19, Chapter 6] for basic material on canonical local heights on elliptic curves. Replacing P with $12P$, we may assume without loss of generality that the local height satisfies

$$\hat{\lambda}(P;v) \ge \frac{1}{12}\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{D}(E/K)$$

for all nonarchimedean places v at which E does not have split multiplicative reduction. We factor the discriminant $\mathcal{D}(E/K)$ into a product

$$\mathfrak{D}(E/K) = \mathfrak{D}_1\mathfrak{D}_2 \quad \text{with} \quad \nu(\mathfrak{D}_2) \le J \quad \text{and} \quad \sigma_J\bigl(\mathfrak{D}(E/K)\bigr) = \sigma(\mathfrak{D}_1).$$

We also choose an integer $M \ge 1$ whose value will be specified later, and for convenience we let $d = [K:\mathbb{Q}]$.

Using a pigeon-hole principle argument as described in [16], we can find an integer k with

$$1 \le k \le (6M)^{J+d}$$

such that for all $1 \le m \le M$ we have

$$\hat{\lambda}(mkP;v) \ge c_1 \log\max\bigl\{|j(E)|_v, 1\bigr\} - c_2 \quad \text{for all } v \in \mathcal{M}_K^\infty,$$
$$\hat{\lambda}(mkP;v) \ge c_3 \log\bigl|\mathsf{N}_{K/\mathbb{Q}}\mathfrak{D}(E/K)\bigr|_v^{-1} \quad \text{for all } v \in \mathcal{M}_K^0 \text{ with } \mathfrak{p}_v \mid \mathfrak{D}_2.$$

(Here and in what follows, $c_1, c_2, \ldots$ are absolute positive constants. We also use the standard notation $\mathcal{M}_K^\infty$ and $\mathcal{M}_K^0$ for complete normalized sets of archimedean, respectively non-archimedean, absolute values on K.) Roughly speaking, we need to force $J+d$ local heights to be positive for all mP with $1 \le m \le M$, which is why we may need to take k as large as $O(M)^{J+d}$.

We next use the Fourier averaging technique described in [9]; see also [10, 15]. Let $\mathfrak{p}_v \mid \mathfrak{D}_1$ be a prime at which E has split multiplicative reduction. The group of components of the special fiber of the Néron model of E at v is a cyclic group of order

$$n_v = \operatorname{ord}_v\bigl(\mathfrak{D}(E/K)\bigr),$$

and we let $0 \le a_v(P) < n_v$ be the component that is hit by P. (In practice, there is no prefered orientation to the cyclic group of components, so $a_v(P)$ is only defined up to ± 1. This will not affect our computations.) The formula for the local height at a split multiplicative place (due to Tate, see [19, VI.4.2]) says that

$$\hat{\lambda}(P;v) \ge \frac{1}{2}\mathbb{B}\left(\frac{a_v(P)}{n_v}\right)\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}_v^{n_v}.$$

In this formula, $\mathbb{B}(t)$ is the periodic second Bernoulli polynomial, equal to $t^2 - t + \frac{1}{6}$ for $0 \le t \le 1$ and extended periodically modulo 1. As in [9], we are going to take a weighted sum of this formula over mP for $1 \le m \le M$.

The periodic Bernoulli polynomial has a Fourier expansion

$$\mathbb{B}(t) = \frac{1}{2\pi^2}\sum_{\substack{n\in\mathbb{Z}\\ n\ne 0}}\frac{e^{2\pi int}}{n^2} = \frac{1}{\pi^2}\sum_{n=1}^{\infty}\frac{\cos(2\pi nt)}{n^2}.$$

We also use the formula (Fejér kernel)

$$\sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)\cos(mt) = \frac{1}{2(M+1)}\left|\sum_{m=0}^{M} e^{imt}\right|^2 - \frac{1}{2}.$$

Hence

$$\begin{aligned}
&\sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)\hat{\lambda}(mP;v)\\
&\quad\ge \sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)\frac{1}{2}\mathbb{B}\left(\frac{ma_v(P)}{n_v}\right)\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}_v^{n_v}\\
&\quad= \sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)\frac{1}{2\pi^2}\sum_{n=1}^{\infty}\frac{\cos(2\pi n m a_v(P)/n_v)}{n^2}\\
&\quad= \frac{1}{2\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2}\sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)\cos\left(\frac{2\pi n m a_v(P)}{n_v}\right)\\
&\quad= \frac{1}{2\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2}\left(\frac{1}{2(M+1)}\left|\sum_{m=0}^{M} e^{2\pi i n m a_v(P)/n_v}\right|^2 - \frac{1}{2}\right).
\end{aligned}$$

We split the sum over n into two pieces. If n is a multiple of n_v, then the quantity between the absolute value signs is equal to $M+1$, and if n is not a multiple of n_v, we simply use the fact that the absolute value is non-negative. This yields the local estimate

$$\sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)\hat{\lambda}(mP;v)$$

$$\geq \left(\frac{1}{4\pi^2(M+1)} \sum_{n=1}^{\infty} \frac{(M+1)^2}{(nn_v)^2} - \frac{1}{4\pi^2} \sum_{n=1}^{\infty} \frac{1}{n^2} \right) \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{p}_v^{n_v}$$
$$= \left(\frac{M+1}{24n_v^2} - \frac{1}{24} \right) \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{p}_v^{n_v}.$$

We next sum the local heights over all primes dividing $\mathfrak{D}_1$,

$$\sum_{\mathfrak{p}_v|\mathfrak{D}_1} \sum_{m=1}^{M} \left(1 - \frac{m}{M+1}\right) \hat{\lambda}(mP;v) \geq \frac{1}{24} \sum_{\mathfrak{p}_v|\mathfrak{D}_1} \left(\frac{M+1}{n_v} - n_v \right) \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{p}_v.$$

We set

$$M+1 = \left\lfloor 2 \sum_{\mathfrak{p}_v|\mathfrak{D}_1} n_v \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{p}_v \Big/ \sum_{\mathfrak{p}_v|\mathfrak{D}_1} n_v^{-1} \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{p}_v \right\rfloor + 1,$$

which gives the height estimate

$$\sum_{\mathfrak{p}_v|\mathfrak{D}_1} \sum_{m=1}^{M} \left(1 - \frac{m}{M+1}\right) \hat{\lambda}(mP;v) \geq \frac{1}{24} \sum_{\mathfrak{p}_v|\mathfrak{D}_1} n_v \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{p}_v$$
$$= \frac{1}{24} \sum_{\mathfrak{p}_v|\mathfrak{D}_1} \log \left| \mathsf{N}_{K/\mathbb{Q}} \mathfrak{D}(E/K) \right|_v^{-1}.$$

We also need to estimate the size of M. This is done using the elementary inequality

$$\left(\sum_{i=1}^{n} a_i x_i\right)\left(\sum_{i=1}^{n} a_i x_i^{-1}\right) \geq \left(\sum_{i=1}^{n} a_i\right)^2, \tag{1}$$

valid for all $a_i, x_i > 0$. (This is a special case of Jensen's inequality, applied to the function $1/x$.) Applying (1) with $x_i = n_v$ and $a_i = \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{p}_v$ allows us to estimate

$$M+1 \leq 2 \left(\frac{\sum_{\mathfrak{p}_v|\mathfrak{D}_1} n_v \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{p}_v}{\sum_{\mathfrak{p}_v|\mathfrak{D}_1} n_v^{-1} \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{p}_v} \right) + 1$$
$$\leq 2 \left(\frac{\sum_{\mathfrak{p}_v|\mathfrak{D}_1} n_v \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{p}_v}{\sum_{\mathfrak{p}_v|\mathfrak{D}_1} \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{p}_v} \right)^2 + 1 \quad \text{using (1)},$$
$$= \sigma(\mathfrak{D}_1)^2 + 1 = \sigma_J\big(\mathfrak{D}(E/K)\big)^2 + 1.$$

In particular, the value of M is bounded solely in terms of $\sigma_J\bigl(\mathfrak{D}(E/K)\bigr)$.

We now combine the estimates for the local heights to obtain

$$\begin{aligned}
&\sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)\hat{h}(mkP)\\
&\quad\geq \sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)\Biggl(\sum_{v\in\mathcal{M}_K^\infty}+\sum_{\mathfrak{p}_v\mid\mathfrak{D}(E/K)}\Biggr)\hat{\lambda}(mkP;v)\\
&\quad= \Biggl(\sum_{v\in\mathcal{M}_K^\infty}+\sum_{\mathfrak{p}_v\mid\mathfrak{D}_1}+\sum_{\mathfrak{p}_v\mid\mathfrak{D}_2}\Biggr)\sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)\hat{\lambda}(mkP;v)\\
&\quad\geq \sum_{v\in\mathcal{M}_K^\infty}\sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)\bigl(c_1\log\max\bigl\{|j(E)|_v,1\bigr\}-c_2\bigr)\\
&\qquad\quad+\frac{1}{24}\sum_{\mathfrak{p}_v\mid\mathfrak{D}_1}\log\bigl|\mathsf{N}_{K/\mathbb{Q}}\mathfrak{D}(E/K)\bigr|_v^{-1}\\
&\qquad\quad+\sum_{\mathfrak{p}_v\mid\mathfrak{D}_2}\sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)c_3\log\bigl|\mathsf{N}_{K/\mathbb{Q}}\mathfrak{D}(E/K)\bigr|_v^{-1}\\
&\quad\geq c_4h\bigl(j(E)\bigr)+c_5\log\mathsf{N}_{K/\mathbb{Q}}\mathfrak{D}(E/K)-c_6.
\end{aligned}$$

In the last line we have used the fact that $\mathfrak{D}(E/K)j(E)$ is integral, so

$$\sum_{v\in\mathcal{M}_K^\infty}\log\max\bigl\{|j(E)|_v,1\bigr\}+\sum_{\mathfrak{p}_v\mid\mathfrak{D}_1\mathfrak{D}_2}\log\bigl|\mathsf{N}_{K/\mathbb{Q}}\mathfrak{D}(E/K)\bigr|_v^{-1}\geq h\bigl(j(E)\bigr).$$

On the other hand,

$$\begin{aligned}
\sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)\hat{h}(mkP)&=\sum_{m=1}^{M}\left(1-\frac{m}{M+1}\right)m^2k^2\hat{h}(P)\\
&=\frac{k^2M(M+1)(M+2)}{12}\hat{h}(P).
\end{aligned}$$

Adjusting the constants yet again yields

$$\hat{h}(P)\geq\frac{c_7h\bigl(j(E)\bigr)+c_8\log\mathsf{N}_{K/\mathbb{Q}}\mathfrak{D}(E/K)-c_9}{k^2M^3}\geq\frac{c_{10}h(E/K)-c_9}{k^2M^3}.$$

Since M depends only on $\sigma_J\bigl(\mathfrak{D}(E/K)\bigr)$ and since $k\leq(6M)^{J+d}$, this gives the desired lower bound for $\hat{h}(P)$. □

Remark 7. As in [15], a similar argument can be used to prove that $\#E(K)_{\text{tors}}$ is bounded by a constant that depends only on $[K:\mathbb{Q}]$, J, and $\sigma_J\bigl(\mathfrak{D}(E/K)\bigr)$.

2. Some elementary properties of the prime-depleted Szpiro ratio

We start with an elementary inequality.

Lemma 8. *Let $n \ge 2$, and let $\alpha_1, \ldots, \alpha_n$ and $x_1, \ldots, x_n$ be positive real numbers, labeled so that $\alpha_n = \max \alpha_i$. Then*

$$\frac{\alpha_1 x_1 + \cdots + \alpha_n x_n}{x_1 + \cdots + x_n} \ge \frac{\alpha_1 x_1 + \cdots + \alpha_{n-1} x_{n-1}}{x_1 + \cdots + x_{n-1}},$$

with strict inequality unless $\alpha_1 = \cdots = \alpha_n$.

Proof. Let $A = \sum_{i=1}^n \alpha_i x_i$ and $X = \sum_{i=1}^n x_i$. Then

$$\begin{aligned} A(X - x_n) - (A - \alpha_n x_n)X &= (\alpha_n X - A)x_n \\ &= \left(\sum_{i=1}^n (\alpha_n - \alpha_i)x_i\right)x_n \ge 0. \end{aligned} \tag{2}$$

Hence

$$\frac{A}{X} \ge \frac{A - \alpha_n x_n}{X - x_n}, \tag{3}$$

and since the x_i are assumed to be positive, inequalities (2) and (3) are strict unless the α_i are all equal. □

We apply the lemma to prove some basic properties of the J-depleted Szpiro ratio.

Proposition 9. *Let $J \ge 1$.*

(a) *For all integral ideals $\mathfrak{D}$,*

$$\sigma_{J-1}(\mathfrak{D}) \ge \sigma_J(\mathfrak{D}).$$

Further, the inequality is strict unless $\mathfrak{D}$ has the form $\mathfrak{D} = \mathfrak{I}^e$ for a squarefree ideal $\mathfrak{I}$.

(b) *Assume that $\nu(\mathfrak{D}) \ge J$. Then there exists an ideal $\mathfrak{d} \mid \mathfrak{D}$ satisfying*

$$\nu(\mathfrak{d}) = J \qquad \textit{and} \qquad \sigma_J(\mathfrak{D}) = \sigma(\mathfrak{D}/\mathfrak{d}).$$

(c) *Let $\mathfrak{p}$ be a prime ideal and $\mathfrak{D}$ an ideal with $\mathfrak{p} \nmid \mathfrak{D}$. Then*

$$\sigma_J(\mathfrak{D}) \ge \sigma_J(\mathfrak{p}^e\mathfrak{D}) \ge \frac{\sigma_J(\mathfrak{D})}{\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}}.$$

(d) *Let $\mathfrak{p}$ be a prime ideal and let $\mathfrak{D}$ an arbitrary ideal (so $\mathfrak{p}$ is allowed to divide $\mathfrak{D}$). Then*

$$(\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p})\sigma_J(\mathfrak{D}) \ge \sigma_J(\mathfrak{p}^e\mathfrak{D}) \ge \frac{\sigma_J(\mathfrak{D})}{\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}}.$$

Proof. (a) Write $\mathfrak{D} = \prod \mathfrak{p}_i^{e_i}$. To ease notation, we let

$$q_i = \log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}_i.$$

If $\nu(\mathfrak{D}) \le J-1$, then $\sigma_{J-1}(\mathfrak{D}) = \sigma_J(\mathfrak{D}) = 1$, so there is nothing to prove. Assume now that $\nu(\mathfrak{D}) \ge J$. Let $I \subset \{1, 2, \ldots, \nu(\mathfrak{D})\}$ be a set of indices with $\#I \ge \nu(\mathfrak{D}) - (J-1)$ satisfying

$$\sigma_{J-1}(\mathfrak{D}) = \sum_{i\in I} e_i q_i \Big/ \sum_{i\in I} q_i.$$

Let $k \in I$ be an index satisfying $e_k = \max\{e_i : i \in I\}$. Then Lemma 8 with $\alpha_i = e_i$ and $x_i = q_i$ yields

$$\sigma_{J-1}(\mathfrak{D}) = \frac{\displaystyle\sum_{i\in I} e_i q_i}{\displaystyle\sum_{i\in I} q_i} \ge \frac{\displaystyle\sum_{i\in I,\, i\ne k} e_i q_i}{\displaystyle\sum_{i\in I,\, i\ne k} q_i} \ge \sigma_J(\mathfrak{D}).$$

Further, Lemma 8 says that the inequality is strict unless all of the e_i are equal, in which case $\mathfrak{D}$ is a power of a squarefree ideal.

(b) If $\mathfrak{D} = \mathfrak{I}^e$ is a power of a squarefree ideal, then $\sigma_J(\mathfrak{D}) = \sigma(\mathfrak{D}/\mathfrak{c}^e)$ for every ideal $\mathfrak{c} \mid \mathfrak{I}$ satisfying $\nu(\mathfrak{c}) = J$, so the assertion to be proved is clear. We may thus assume that $\mathfrak{D}$ is not a power of a squarefree ideal.

Suppose in this case that $\sigma_J(\mathfrak{D}) = \sigma(\mathfrak{D}/\mathfrak{d})$ for some $\mathfrak{d} \mid \mathfrak{D}$ with $\nu(\mathfrak{d}) \le J-1$. Then

$$\sigma_{J-1}(\mathfrak{D}) \le \sigma(\mathfrak{D}/\mathfrak{d}) = \sigma_J(\mathfrak{D}),$$

contradicting the strict inequality $\sigma_{J-1}(\mathfrak{D}) > \sigma_J(\mathfrak{D})$ proven in (a).

(c) We always have

$$\sigma_J(\mathfrak{p}^e\mathfrak{D}) \le \sigma_{J-1}(\mathfrak{D}),$$

since in computing $\sigma_J(\mathfrak{p}^e\mathfrak{D})$, we can always remove $\mathfrak{p}$ and $J-1$ other primes from $\mathfrak{D}$. If this inequality is an equality, we're done. Otherwise the value of $\sigma_J(\mathfrak{p}^e\mathfrak{D})$ is obtained by removing J primes from $\mathfrak{D}$. Continuing with the notation from (a) and letting $q = \log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}$, this means that there is an index set I with $\#I \ge \nu(\mathfrak{D}) - J$ such that

$$\sigma_J(\mathfrak{D}) = \frac{eq + \displaystyle\sum_{i\in I} e_i q_i}{q + \displaystyle\sum_{i\in I} q_i} \ge \frac{q + \displaystyle\sum_{i\in I} e_i q_i}{q + \displaystyle\sum_{i\in I} q_i} = \frac{q+X}{q+Y},$$

where to ease notation, we write X and Y for the indicated sums.

If $Y = 0$, then also $X = 0$ and $\nu(\mathfrak{D}) \le J$, so $\sigma_J(\mathfrak{p}^e\mathfrak{D})$ equals either e or 1. In either case, it is greater than $\sigma_J(\mathfrak{D}) = 1$. So we may assume that $Y > 0$, which implies that $Y \ge \log 2$.

We observe that

$$\frac{X}{Y} = \frac{\displaystyle\sum_{i\in I} e_i q_i}{\displaystyle\sum_{i\in I} q_i} \ge \sigma_J(\mathfrak{D}).$$

Hence

$$\sigma_J(\mathfrak{D}) = \frac{X}{Y} \cdot \frac{1+q/X}{1+q/Y} \ge \frac{\sigma_J(\mathfrak{D})}{1+q/Y} \ge \frac{\sigma_J(\mathfrak{D})}{3q}.$$

(The final inequality is true since $q \ge \log 2$ and $Y \ge \log 2$.) This proves that $\sigma_J(\mathfrak{D})$ is greater than the smaller of $\sigma_{J-1}(\mathfrak{D})$ and $\sigma_J(\mathfrak{D})/3q$. But from (a) we have $\sigma_{J-1}(\mathfrak{D}) \ge \sigma_J(\mathfrak{D})$, so the latter is the minimum.

(d) Let $\mathfrak{D} = \mathfrak{p}^i\mathfrak{D}'$ with $\mathfrak{p} \nmid \mathfrak{D}'$. Then writing $q = \log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}$ as usual and applying (c) several times, we have

$$\sigma_J(\mathfrak{p}^e\mathfrak{D}) = \sigma_J(\mathfrak{p}^{e+i}\mathfrak{D}') \le \sigma_J(\mathfrak{D}') \le q\sigma_J(\mathfrak{p}^i\mathfrak{D}') = q\sigma_J(\mathfrak{D}).$$

Similarly

$$\sigma_J(\mathfrak{p}^e\mathfrak{D}) = \sigma_J(\mathfrak{p}^{e+i}\mathfrak{D}') \ge \frac{\sigma_J(\mathfrak{D}')}{q} \ge \frac{\sigma_J(\mathfrak{p}^i\mathfrak{D}')}{q} = \frac{\sigma_J(\mathfrak{D})}{q}. \qquad \square$$

3. The prime-depleted Szpiro and *ABC* conjectures

In this section we describe a prime-depleted variant of the ABC-conjecture and show that it is a consequence of the prime-depleted Szpiro conjecture. For ease of notation, we restrict attention to $K = \mathbb{Q}$ and leave the generalization to arbitrary fields to the reader. For other variants of the ABC-conjecture, see for example [1, 2, 7, 11].

Conjecture 10 (Prime-Depleted ABC-conjecture)**.** *There exist an integer $J \ge 0$ and an absolute constant C_8 such that if $A, B, C \in \mathbb{Z}$ are integers satisfying*

$$A + B + C = 0 \qquad \textit{and} \qquad \gcd(A,B,C) = 1,$$

then

$$\sigma_J(ABC) \le C_8.$$

The classical ABC-conjecture (with non-optimal exponent) says that $\sigma(ABC)$ is bounded, which is stronger than the prime-depleted version, since $\sigma_J(ABC)$ is less than or equal to $\sigma(ABC)$.

Proposition 11. *If the prime-depleted Szpiro conjecture is true, then the prime-depleted ABC-conjecture is true.*

Proof. We suppose that the prime-depleted Szpiro conjecture is true, say with J primes deleted. Let $A, B, C \in \mathbb{Z}$ be as in the statement of the depleted ABC-conjecture. We consider the Frey curve

$$E : y^2 = x(x+A)(x-B).$$

An easy calculation [20, VIII.11.3] shows that the minimal discriminant of E is either $2^4(ABC)^2$ or $2^{-8}(ABC)^2$, so in any case we can write

$$\mathfrak{D}(E/\mathbb{Q}) = 2^e(ABC)^2$$

for some exponent $e \in \mathbb{Z}$. Then using Proposition 9 we find that

$$\sigma_J\bigl(\mathfrak{D}(E/\mathbb{Q})\bigr) = \sigma_J\bigl(2^e(ABC)^2\bigr) \ge \frac{\sigma_J\bigl((ABC)^2\bigr)}{\log 2} = \frac{2\sigma_J(ABC)}{\log 2}.$$

So the boundedness of $\sigma_J\bigl(\mathfrak{D}(E/\mathbb{Q})\bigr)$ implies the boundedness of $\sigma_J(ABC)$. □

Remark 12. The Szpiro and ABC-conjectures have many important consequences, including asymptotic Fermat (trivial), a strengthened version of Roth's theorem [3, 6], the infinitude of non-Wieferich primes [17], nonexistence of Siegel zeros [8], Faltings' theorem (Mordell conjecture) [5, 6],.... (For a longer list, see [13].) It is thus of interest to ask which, if any, of these results follows from the prime-depleted Szpiro conjecture. As far as the author has been able to determine, the answer is none of them, which would seem to indicate that the prime-depleted Szpiro conjecture is qualitatively weaker than the original Szpiro conjecture.

References

[1] Baker, A. Logarithmic forms and the *abc*-conjecture. *Number theory* (Eger, 1996), 37–44. *de Gruyter, Berlin*, 1998. MR1628831 (99e:11101), Zbl 0973.11047.

[2] Baker, Alan. Experiments on the *abc*-conjecture. *Publ. Math. Debrecen* **65** (2004) 253–260. MR2107944 (2005g:11051), Zbl 1064.11050.

[3] Bombieri, E. Roth's theorem and the *abc*-conjecture. Preprint, ETH, Zürich, 1994.

[4] David, Sinnou. Points de petite hauteur sur les courbes elliptiques. *J. Number Theory* **64** (1997) 104–129. MR1450488 (98k:11067), Zbl 0873.11035.

[5] Elkies, Noam D. *ABC* implies Mordell. *Internat. Math. Res. Notices* **1991**, no. 7, 99–109. MR1141316 (93d:11064), Zbl 0763.11016.

[6] Van Frankenhuysen, Machiel. The *ABC* conjecture implies Vojta's height inequality for curves. *J. Number Theory* **95** (2002) 289–302. MR1924103 (2003g:11070), Zbl 1083.11042.

[7] Van Frankenhuysen, Machiel. About the *ABC* conjecture and an alternative. Preprint, February 2010.

[8] Granville, Andrew; Stark, H. M. *abc* implies no "Siegel zeros" for L-functions of characters with negative discriminant. *Invent. Math.* **139** (2000) 509–523. MR1738058 (2002b:11114), Zbl 0967.11033.

[9] Hindry, Marc; Silverman, Joseph H. The canonical height and integral points on elliptic curves. *Invent. Math.* **93** (1988) 419–450. MR0948108 (89k:11044), Zbl 0657.14018.

[10] Hindry, Marc; Silverman, Joseph H. On Lehmer's conjecture for elliptic curves. *Séminaire de Théorie des Nombres, Paris 1988–1989*, 103–116. Progr. Math., 91. *Birkhäuser Boston, Boston, MA*, 1990. MR1104702 (92e:11062), Zbl 0741.14013.

[11] Lagarias, Jeffrey C.; Soundararajan, K. Smooth solutions to the equation $A + B = C$. November, 2009. arXiv:0911.4147.

[12] Lang, Serge. Elliptic curves: Diophantine analysis. Grundlehren der Mathematischen Wissenschaften, 231. *Springer-Verlag, Berlin*, 1978. xi+261 pp. ISBN: 3-540-08489-4. MR0518817 (81b:10009), Zbl 0388.10001.

[13] Nitaj, Abderrahmane. The *abc* conjecture home page. `http://www.math.unicaen.fr/~nitaj/abc.html`.

[14] Oesterlé, Joseph. Nouvelles approches du “théorème” de Fermat. *Astérisque*, (161-162):Exp. No. 694, 4, 165–186 (1989), 1988. Séminaire Bourbaki, Vol. 1987/88. MR0992208 (90g:11038), Zbl 0668.10024.

[15] Petsche, Clayton. Small rational points on elliptic curves over number fields. *New York J. Math.* **12** (2006) 257–268. MR2259240 (2007g:11061), Zbl 1163.11327.

[16] Silverman, Joseph H. Lower bound for the canonical height on elliptic curves. *Duke Math. J.* **48** (1981) 633–648. MR0630588 (82k:14043), Zbl 0475.14033.

[17] Silverman, Joseph H. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory* **30** (1988) 226–237. MR0961918 (89m:11027), Zbl 0654.10019.

[18] Silverman, Joseph H. Elliptic curves of bounded degree and height. *Proc. Amer. Math. Soc.* **105** (1989) 540–545. MR0953747 (89i:11063), Zbl 0698.14027.

[19] Silverman, Joseph H. Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. *Springer-Verlag, New York*, 1994. xiv+525 pp. ISBN: 0-387-94328-5. MR1312368 (96b:11074), Zbl 0911.14015.

[20] Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. *Springer-Verlag, Dordrecht*, 2009. xx+513 pp. ISBN: 978-0-387-09493-9. MR2514094.

Mathematics Department, Box 1917 Brown University, Providence, RI 02912 USA

`jhs@math.brown.edu`

This paper is available via `http://nyjm.albany.edu/j/2010/16-1.html`.