ACTA ARITHMETICA
173.3 (2016)

Lang's conjecture and sharp height estimates for the elliptic curves $y^2 = x^3 + b$

by

Paul Voutier (London) and Minoru Yabuta (Osaka)

1. Introduction. The canonical height, $\widehat{h}$ (defined in Section 2), on an elliptic curve E defined over a number field $\mathbb{K}$ is a measure of the arithmetic complexity of points on the curve. It has many desirable properties. For example, it is a positive definite quadratic form on the lattice $E(\mathbb{K})/(\text{torsion})$, behaving well under the group law on $E(\mathbb{K})$. See [17, Chapter VIII] and [1, Chapter 9] for more information on this height.

There is another important, and closely related, height function defined for points on elliptic curves, the absolute logarithmic height (also defined in Section 2). It has a very simple definition which makes it very easy to compute.

In this paper, we provide sharp lower bounds for the canonical height as well as bounding the difference between the heights for a well-known and important family of elliptic curves, the Mordell curves defined by $E_b : y^2 = x^3 + b$ where b is a sixth-power-free integer (i.e., quasi-minimal Weierstrass equations for all $E_b/\mathbb{Q}$).

1.1. Lower bounds. Lang's conjecture proposes a lower bound for the heights of nontorsion points on a curve which varies with the curve.

Conjecture 1.1 (Lang's conjecture). *Let $E/\mathbb{K}$ be an elliptic curve with minimal discriminant $\mathcal{D}_{E/\mathbb{K}}$. There exist constants $C_1 > 0$ and C_2, depending only on $[\mathbb{K} : \mathbb{Q}]$, such that for all nontorsion points $P \in E(\mathbb{K})$ we have*

$$\widehat{h}(P) > C_1 \log(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\mathcal{D}_{E/\mathbb{K}})) + C_2.$$

See [13, p. 92] along with the strengthened version in [17, Conjecture VIII.9.9].

2010 *Mathematics Subject Classification*: 11G05, 11G50.
Key words and phrases: elliptic curve, canonical height, Lang's conjecture.
Received 24 March 2014; revised 17 January 2016.
Published online 11 May 2016.

DOI: 10.4064/aa7761-2-2016

Such lower bounds have applications to counting the number of integral points on elliptic curves [10], questions involving elliptic divisibility sequences [4, 5, 23] and several other problems.

Silverman [16, Section 4, Theorem] showed that Lang's conjecture holds for any elliptic curve with j-invariant nonintegral for at most R places of $\mathbb{K}$ (note that this includes our curves, E_b, since their j-invariant is 0), but with C_1 dependent on $\mathbb{K}$ and R. Gross and Silverman [9, Proposition 3(3)] proved an explicit version of this result from which it follows that for nontorsion points, P, on E_b, we have

$$\widehat{h}(P) > 3 \cdot 10^{-14} \log |\Delta(E_b)|.$$

Furthermore, Hindry and Silverman [10] proved an explicit version of Lang's conjecture whenever Szpiro's ratio, $\sigma_{E/\mathbb{K}}$, of $E/\mathbb{K}$ is known. Hence Lang's conjecture follows from Szpiro's conjecture (or the ABC conjecture). Subsequently, David [3] and Petsche [14] improved Hindry and Silverman's result. It can be shown that $\sigma_{E_b/\mathbb{Q}} < 5$, hence from Petsche's Theorem 2, for example, a weaker result than the above follows with $3 \cdot 10^{-14}$ replaced by $2 \cdot 10^{-22}$.

However, these results for $E_b/\mathbb{Q}$ all follow from more general results. By focusing specifically on $E_b/\mathbb{Q}$, much better results can be obtained.

When b is a nonzero integer that is sixth-power-free, Krir [12, Proposition 3.1] showed that for any nontorsion point, P,

$$\widehat{h}(P) > 10^{-3} \log |b| + 10^{-3}.$$

In the special case of $b = -432m^2$ for a cube-free integer m, Jędrzejak [11] proved a sharper result, which was improved by Everest, Ingram and Stevens [4, Lemma 4.3] and further improved very recently by Fujita and Nara [8, Proposition 2.5]:

$$\widehat{h}(P) > \tfrac{1}{18} \log |b| - 1.1009.$$

The coefficient of $\log |b|$ is correct in their result, but as we show below in Theorem 1.2(c), the constant should be $-\frac{2}{9} \log 2 - \frac{1}{4} \log 3 = -0.4286\ldots$.

Also, if b is a positive square-free integer, Fujita and Nara [7, Proposition 4.3] showed that

$$\widehat{h}(P) > \tfrac{1}{24} \log |b| - 0.073576,$$

upon noting that their canonical height is twice ours (compare with our results for this case in Theorem 1.2(a) or (5.3) below).

We express the hypotheses of our theorem in terms of the *Tamagawa index at p* for p a prime. Letting $E_0(\mathbb{Q}_p)$ be the connected component of the identity in $E(\mathbb{Q}_p)$, the Tamagawa index, c_p, at p is the order of the component group, $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, of E at p. See [2] and [20, Section IV.9] for more details.

THEOREM 1.2. *Let b be an integer which is sixth-power-free and let P in $E_b(\mathbb{Q})$ be a nontorsion point.*

(a) *If $c_p = 1$ for all primes $p > 3$, then*

$$\widehat{h}(P) > \begin{cases} \frac{1}{6}\log|b| - \log 2 - \frac{1}{2}\log 3 & \text{if } b < 0, \\ \frac{1}{6}\log|b| - \frac{2}{3}\log 2 - \frac{3}{4}\log 3 - 0.006 & \text{if } b > 0. \end{cases}$$

(b) *If $c_p \mid 4$ for all primes $p > 3$ and $2 \mid c_p$ for at least one such prime, then*

$$\widehat{h}(P) > \begin{cases} \frac{1}{24}\log|b| - \frac{1}{4}\log 2 - \frac{5}{48}\log 3 & \text{if } b < 0, \\ \frac{1}{24}\log|b| - \frac{1}{6}\log 2 - \frac{1}{6}\log 3 - 0.002 & \text{if } b > 0. \end{cases}$$

(c) *If $c_p \mid 3$ for all primes $p > 3$ and $c_p = 3$ for at least one such prime, then*

$$\widehat{h}(P) > \begin{cases} \frac{1}{18}\log|b| - \frac{2}{9}\log 2 - \frac{1}{4}\log 3 - 0.004 & \text{if } b < 0, \\ \frac{1}{18}\log|b| - \frac{1}{3}\log 2 - \frac{1}{6}\log 3 - 0.004 & \text{if } b > 0. \end{cases}$$

(d) *If $c_p \mid 12$ for all primes $p > 3$, $2 \mid c_p$ for at least one such prime p, and $3 \mid c_q$ for at least one other such prime q, then*

$$\widehat{h}(P) > \begin{cases} \frac{1}{36}\log|b| - 0.2247 & \text{if } b < 0, \\ \frac{1}{36}\log|b| - 0.2262 & \text{if } b > 0. \end{cases}$$

REMARK. In the course of the proof of Theorem 1.2, we establish the minimum value of $\widehat{h}(P)$ for all possibilities of b modulo powers of 2 and 3. As such bounds can be important for obtaining sharp results for other problems (e.g., primitive divisor problems for elliptic divisibility sequences), we refer the reader to these bounds in (5.2) and (5.3) for part (a), (5.5) and (5.6) for part (b), (5.18) and (5.19) (as well as (5.17) and (5.20)) for part (c), and (5.13) and (5.14) for part (d).

All that is required to apply these bounds is knowing the congruence classes of b modulo powers of 2 and 3, the reduction of P (or $[2]P$ for part (b)) at 2 and 3, and then referring to Tables 4 and 5.

In [24], we were able to show that our results are best possible. See Section 7 below for examples showing that Theorem 1.2(a) and (b) for $b < 0$ are the best possible results, and the other lower bounds are within 0.006 of the best possible result. By "best possible", we mean that the value for C_1 in Conjecture 1.1 is best possible and then, fixing C_1, the value for C_2 is best possible.

The constants in part (d) are not as "nice" as the ones in (a)–(c), but they do arise in a natural way in this setting. For example, the best possible constant for $b < 0$ is $0.19155\ldots - \frac{1}{3}\log 2 - \frac{1}{6}\log 3$, and the minimal value of $\frac{1}{2}\log c - \frac{1}{12}\log(c^5 - c^2)$ plus the sum in (3.4) is $-0.19155\ldots$, where c is

defined by $x(P) = c|b|^{1/3}$. The log terms here again arise naturally in the proof of the theorem.

As in [24], our proof is based on the decomposition of the canonical height as the sum of local height functions. However, there are differences in the behaviour of the local height functions for the curves in each family. One of particular interest to us is that the local archimedean height function here has an error term near its critical point that is $O(\epsilon^2)$, whereas in [24], the analogous error term is $O(\epsilon)$. In general, it appears that the archimedean height function for all elliptic curves behaves in one of these two ways near critical points. Our work to understand this function better is ongoing.

Lastly, note that while the formulation of our results is not in terms of $\Delta(E_b)$, it is equivalent to such a formulation since $\Delta(E_b) = -432b^2$.

1.2. Difference of heights. Our proof of our lower bound for the canonical height also allows us to prove sharp bounds on the difference between the canonical height and the logarithmic height of points on $E_b(\mathbb{Q})$.

In [19, Example 2.1], Silverman showed that

$$-\tfrac{1}{6}\log|b| - 1.576 \le \tfrac{1}{2}h(P) - \widehat{h}(P) \le \tfrac{1}{6}\log|b| + 1.48$$

and that the coefficients of $\log|b|$ are best possible.

Using a combination of [15, Proposition 5.18(a) and Theorem 5.35(c)], one can obtain

$$-\tfrac{1}{6}\log|b| - 0.578 \le \tfrac{1}{2}h(P) - \widehat{h}(P) \le \tfrac{1}{6}\log|b| + 1.156.$$

THEOREM 1.3. *Let b be a nonzero integer and let $P \in E_b(\mathbb{Q})$. Then for $b < 0$,*

$$-\tfrac{1}{4}\log 3 - 0.005 < \tfrac{1}{2}h(P) - \widehat{h}(P) < \tfrac{1}{6}\log|b| + \tfrac{1}{3}\log 2 + \tfrac{1}{4}\log 3,$$

and for $b > 0$,

$$-\tfrac{1}{6}\log|b| - \tfrac{1}{3}\log 2 - 0.007 - 0.076b^{-1/3} < \tfrac{1}{2}h(P) - \widehat{h}(P) < \tfrac{1}{6}\log|b| + \tfrac{1}{3}\log 2 + \tfrac{1}{4}\log 3 + 0.004.$$

In all cases,

$$-\tfrac{1}{6}\log|b| - 0.299 < \tfrac{1}{2}h(P) - \widehat{h}(P) < \tfrac{1}{6}\log|b| + 0.51.$$

REMARK. Only the upper bound when $b < 0$ is best possible here. It appears that the terms -0.005 in the lower bound for $b < 0$, -0.007 in the lower bound for $b > 0$, and 0.004 in the upper bound for $b > 0$ are not required. Examples demonstrating these claims are provided in Section 7.

REMARK. As with Theorem 1.2, improved results can often be obtained for specific congruence classes of b modulo powers of 2 and 3, here by using (6.2) and (6.3).

2. Notation. For what follows in the remainder of this paper, we will require some standard notation (see [17, Chapter 3], for example).

Let $\mathbb{K}$ be a number field and let $E/\mathbb{K}$ be an elliptic curve given by the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_1, \ldots, a_6 \in \mathbb{K}$.

Set

$$b_2 = a_1^2 + 4a_2, \qquad b_6 = a_3^2 + 4a_6,$$
$$b_4 = 2a_4 + a_1a_3, \quad b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

Then $E/\mathbb{K}$ is also given by $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$.

Furthermore, for any $m \in \mathbb{Z}$, $[m] : E/\mathbb{K} \to E/\mathbb{K}$ is the multiplication-by-m isogeny.

For a point $P \in E(\mathbb{K})$, we define the canonical height of P by

$$\widehat{h}(P) = \tfrac{1}{2} \lim_{n\to\infty} \frac{h([2^n](P))}{4^n},$$

with $h(P) = h(x(P))$, where $h(P)$ and $h(x(P))$ are the absolute logarithmic heights of P and $x(P)$, respectively (see [17, Sections VIII.6, 7 and 9]). Also recall that for $\mathbb{Q}$, $h(s/t) = \log\max\{|s|, |t|\}$ with s/t in lowest terms is the absolute logarithmic height of s/t.

Let $M_{\mathbb{K}}$ be the set of valuations of $\mathbb{K}$, and for each $v \in M_{\mathbb{K}}$, let n_v be the local degree and let $\widehat{\lambda}_v(P) : E(\mathbb{K}_v) \setminus \{O\} \to \mathbb{R}$ be the local height function, where $\mathbb{K}_v$ is the completion of $\mathbb{K}$ at v. From [20, Theorem VI.2.1], we have the following decomposition of the canonical height into local height functions:

$$\widehat{h}(P) = \sum_{v\in M_{\mathbb{K}}} n_v\widehat{\lambda}_v(P).$$

For $\mathbb{K} = \mathbb{Q}$, the nonarchimedean valuations on $\mathbb{K}$ can be identified with the set of rational primes. For a nonarchimedean valuation, v, we let q_v be the associated prime,

$$v(x) = -\log|x|_v = \operatorname{ord}_{q_v}(x)\log q_v$$

for $x \neq 0$ and $v(0) = +\infty$.

Remark. We refer the reader to [2, Section 4] and [17, Remark VIII.9.2] for notes about the various normalisations of both the canonical and local height functions. In what follows, our local height functions, $\widehat{\lambda}_v(P)$, are those that [2] denotes as $\lambda_v^{\mathrm{SilB}}(P)$, that is, as defined in Silverman's book [20, Chapter VI]. So as stated in [2, (11)], their $\lambda_v(P)$ equals $2\widehat{\lambda}_v(P) + \frac{1}{6}\log|\Delta(E)|_v$ here.

Our canonical height also follows Silverman and is half that found in [2] as well as half that returned from the height function, `ellheight`, in PARI.

3. Archimedean estimates

3.1. Case $b < 0$

LEMMA 3.1. *Suppose $b \in \mathbb{R}$ is negative and let $P = (x(P), y(P)) \in E_b(\mathbb{R})$ be a point of infinite order.*

(a) *We have*

$$\widehat{\lambda}_\infty(P) > -\tfrac{1}{3}\log 2 = \tfrac{1}{6}\log|b| + \tfrac{1}{4}\log 3 - \tfrac{1}{12}\log|\Delta(E_b)|. \tag{3.1}$$

(b) *Suppose that $x(P) = c|b|^{1/3}$ where $c > 1$. Then*

$$\begin{aligned}\widehat{\lambda}_\infty(P) &> \tfrac{1}{3}\log c - \tfrac{1}{36}\log 6912 - 0.004\\ &= \tfrac{1}{6}\log|b| + \tfrac{1}{3}\log c + \tfrac{1}{18}\log 108 - 0.004 - \tfrac{1}{12}\log|\Delta(E_b)|\end{aligned} \tag{3.2}$$

and

$$\begin{aligned}\widehat{\lambda}_\infty(P) &> \tfrac{1}{12}\log\frac{c^5 - c^2}{432} + 0.1895\\ &= \tfrac{1}{6}\log|b| + \tfrac{1}{12}\log(c^5 - c^2) + 0.1895 - \tfrac{1}{12}\log|\Delta(E_b)|.\end{aligned} \tag{3.3}$$

(c) *We have*

$$-\tfrac{1}{4}\log 3 - 0.005 < \left(\tfrac{1}{2}\log\max\{1, |x(P)|\} - \tfrac{1}{12}\log|\Delta(E_b)|\right) - \widehat{\lambda}_\infty(P) < 0.$$

REMARK. We have expressed the bounds in parts (a) and (b) both with and without the $\frac{1}{12}\log|\Delta(E_b)|$ term. The former expression will be used in the proof of our theorems, while the latter is of interest as it demonstrates that these results are actually independent of b.

All of the bounds are either best possible or within at most 0.005 of the best possible results.

The actual dependence of $\widehat{\lambda}_\infty(P)$ on c as $c \to \infty$ is $\frac{1}{2}\log c$, but the lower bounds in (3.2) and (3.3) allow us to obtain nearly best possible lower bounds for the canonical height.

Proof of Lemma 3.1. We will estimate the archimedean contribution to the canonical height by using Tate's series (see [22] as well as the presentation in [18]). Let

$$t(P) = 1/x(P) \quad \text{and} \quad z(P) = 1 - b_4 t(P)^2 - 2b_6 t(P)^3 - b_8 t(P)^4,$$

for a point $P = (x(P), y(P)) \in E(\mathbb{R})$. Then the archimedean local height of $P \in E(\mathbb{R})$ is given by the series

$$\widehat{\lambda}_\infty(P) = \tfrac{1}{2}\log|x(P)| + \tfrac{1}{8}\sum_{k=0}^{\infty} 4^{-k}\log|z([2^k](P))| - \tfrac{1}{12}\log|\Delta(E)|, \tag{3.4}$$

provided $x([2^k](P)) \neq 0$ for all $k \neq 0$.

Here we have $b_2 = b_4 = b_8 = 0$ and $b_6 = 4b$, so $t(P) = 1/x(P)$ and $z(P) = 1 - 8bt(P)^3$.

Since $b < 0$, for any $Q \in E_b(\mathbb{R})$, $x(Q) \geq |b|^{1/3}$. Hence $1 \leq z(Q) \leq 9$. In particular, $1 \leq z([2^k](P)) \leq 9$.

(a) Applying the above inequality for $k \geq 1$ and the definition of $z(P)$ to (3.4), we obtain

$$0 \leq \widehat{\lambda}_\infty(P) - \left(\tfrac{1}{8}\log(x(P)^4 - 8bx(P)) - \tfrac{1}{12}\log|\Delta(E_b)|\right) \leq \tfrac{1}{12}\log 3.$$

Since $x(P) \geq |b|^{1/3}$, we have $x(P)^4 - 8bx(P) \geq 9|b|^{4/3}$. Hence

$$\begin{aligned}\widehat{\lambda}_\infty(P) &\geq \tfrac{1}{8}\log(x(P)^4 - 8bx(P)) - \tfrac{1}{12}\log|\Delta(E_b)| \\ &\geq \tfrac{1}{6}\log|b| + \tfrac{1}{4}\log 3 - \tfrac{1}{12}\log|\Delta(E_b)|.\end{aligned}$$

(b) We first consider (3.2). From (3.4), our expression for $x(P)$ and our lower bound for $z([2^k](P))$, we have

$$\widehat{\lambda}_\infty(P) \geq \tfrac{1}{6}\log|b| + \tfrac{1}{2}\log c + \tfrac{1}{8}\sum_{k=0}^{2} 4^{-k}\log|z([2^k](P))| - \tfrac{1}{12}\log|\Delta(E)|,$$

so we now proceed to bound from below

$$\tfrac{1}{6}\log c + \tfrac{1}{128}\log\bigl(z^{16}(P)z^4([2](P))z([4](P))\bigr). \tag{3.5}$$

The derivative of this quantity is a rational function of c whose numerator is of degree 63 with leading coefficient 1 and whose denominator is of degree 64 with leading coefficient 6. The numerator has only one root ≥ 1, which is $1.71216\ldots$, while the denominator has no roots ≥ 1. Therefore, the minimum value of (3.5) is $\frac{1}{18}\log 108 - 0.00372\ldots$, which occurs at $c = 1.71216\ldots$.

We now consider (3.3). Proceeding as in the proof for (3.2), we bound from below

$$\tfrac{1}{2}\log c - \tfrac{1}{12}\log(c^5 - c^2) + \tfrac{1}{128}\log\bigl(z^{16}(P)z^4([2](P))z([4](P))\bigr).$$

The derivative of this quantity is a rational function of c whose numerator is of degree 66 with leading coefficient 1 and whose denominator is of degree 67 with leading coefficient 12. The numerator has only one root ≥ 1, which is $4.21378\ldots$, while the denominator has no roots > 1. Therefore, the minimum value occurs at $4.21378\ldots$ and is $0.1895\ldots$.

(c) We estimate

$$\sum_{k=0}^{\infty} 4^{-k}\log|z([2^k](P))|.$$

We will proceed in a similar way to the proof of (b). We group adjacent triples of summands together and consider $z^{16}(P)z^4([2](P))z([4](P))$, which is a rational function of c whose numerator and denominator are both of degree 63.

Neither the numerator nor the denominator of the derivative of this rational function has a root ≥ 1. So this function is decreasing for $c \geq 1$. Hence

it takes its maximum value, 3^{32}, at $c = 1$ and its minimum value is 1, which is approached from above as $c \to \infty$.

Therefore

$$0 < \tfrac{1}{8} \sum_{k=0}^{\infty} 4^{-k} \log\bigl(z([2^k](P))\bigr)$$
$$\leq \tfrac{1}{8} \sum_{k=0}^{\infty} \frac{\log(3^{32})}{16 \cdot 64^k} = \tfrac{16}{63} \log 3 = \tfrac{1}{4} \log 3 + 0.0043\ldots,$$

so part (c) follows from (3.4) and since $\max\{1, |x(P)|\} = |x(P)|$ here. ∎

3.2. Case $b > 0$. We use Tate's series here too. However, for $b > 0$, $E_b(\mathbb{R})$ includes the point $(0, b^{1/2})$, which causes a problem since we require $x([2^k](P))$ to be bounded away from 0 to ensure that Tate's series converges. To get around this, we use an idea of Silverman's (see [18, p. 340]) and translate the curve to the right using $x' = x + 2b^{1/3}$, noting that $\widehat{\lambda}_\infty$ is fixed under such translations. In this way, we obtain the elliptic curve

$$E_b' : y^2 = x^3 - 6b^{1/3}x^2 + 12b^{2/3}x - 7b,$$

and every point $P'(x, y)$ in $E_b'(\mathbb{R})$ satisfies $x(P') \geq b^{1/3}$. Here we have $b_2 = -24b^{1/3}$, $b_4 = 24b^{2/3}$, $b_6 = -28b$ and $b_8 = 24b^{4/3}$. Hence

$$t(P') = 1/x(P') \quad \text{and} \quad z(P') = 1 - 24b^{2/3}t(P')^2 + 56bt(P')^3 - 24b^{4/3}t(P')^4.$$

We could take the same approach here as in the proof of [24, Lemma 3.4]. However, there is a significant complication. Whereas in [24], for $x(P') = (1+\epsilon)\sqrt{a}$, we have

$$\widehat{\lambda}_\infty(P') - \bigl\{\tfrac{1}{4}\log a - \tfrac{1}{12}\log|\Delta(E_a)|\bigr\} = O(\epsilon),$$

here we find that for $x(P') = 2(1+\epsilon)b^{1/3}$,

$$\widehat{\lambda}_\infty(P') - \bigl\{\tfrac{1}{6}\log b + \tfrac{1}{3}\log 2 - \tfrac{1}{12}\log|\Delta(E_b)|\bigr\} = O(\epsilon^2),$$

so we would need to proceed much more carefully. We have done so in an earlier version of this paper. Here we take a more direct, although more computational, approach and instead work with the actual expressions in the first terms of Tate's series. The cost is a small additional constant term.

Despite this change in approach from earlier versions, the following result may still be of interest to readers.

LEMMA 3.2. *Suppose $b \in \mathbb{R}$ is positive and $P' \in E_b'(\mathbb{R})$ where $x(P') = 2(1+\epsilon)b^{1/3}$.*

(a) *For $-0.1745 \leq \epsilon \leq 0.6$,*

$$\log|x(P')^4 z(P')| \geq \log(8b^{4/3}) - 2\epsilon - 2\epsilon^2 + \tfrac{16}{3}\epsilon^3 + 9.7\epsilon^4.$$

(b) *Suppose k is a positive integer and $-0.379 \le (-2)^{k-1}\epsilon \le 1.044$. Then*

$$\left|\frac{x([2^k](P'))}{2b^{1/3}} - \{1 + (-2)^k\epsilon + ((-2)^{4k} - (-2)^k)\epsilon^4\}\right| \le 2 \cdot 2^{7k}|\epsilon|^7.$$

(c) *If k is a positive integer and $-1.0 \le (-2)^k\epsilon \le 0.36$, then*

$$\begin{aligned}\log\big(z([2^k](P'))\big) \ge\ & -\log 2 - 6(-2)^k\epsilon + 4(-2)^{3k}\epsilon^3 \\ & + \big(9(-2)^{4k} + 6(-2)^k\big)\epsilon^4 + (144/5)(-2)^{5k}\epsilon^5.\end{aligned}$$

Proof. These are parts (a), (b) and (d) of Lemma 3.2 in the first arXiv version of this paper (arXiv:1305.6560v1). ∎

LEMMA 3.3. *Suppose $b \in \mathbb{R}$ is positive and $P' \in E'_b(\mathbb{R})$ is a point of infinite order. If K is a nonnegative integer, then*

$$-1.8 \cdot 4^{-K} < \sum_{k=K}^{\infty} 4^{-k} \log\big(z([2^k](P'))\big) < 2.24 \cdot 4^{-K}. \tag{3.6}$$

REMARK. These bounds are close to best possible. The best possible constants appear to be $-1.7835\ldots$ when $x(P')$ is near $2.9399\ldots \cdot b^{1/3}$, and $\log 9 = 2.197\ldots$ as $x(P')$ approaches $b^{1/3}$.

Proof of Lemma 3.3. We write $x(P') = 2(1+\epsilon)b^{1/3}$, noting that $\epsilon \ge -0.5$. We will group adjacent triples of summands together and consider

$$f_{16}(\epsilon) = z^{16}(P')z^4([2](P'))z([4](P')),$$

which is a rational function of ϵ whose numerator and denominator are both of degree 64.

For $\epsilon \ge -0.5$, the numerator of the derivative of $f_{16}(\epsilon)$ has just one root, $\epsilon = 0.41859\ldots$. The denominator of the derivative is $262144(1+\epsilon)^{65}$ and is positive for $\epsilon \ge -0.5$. So $f_{16}(\epsilon)$ is decreasing in the interval $-0.5 \le \epsilon \le 0.41859\ldots$ and increases towards 1 for larger ϵ. Hence $f_{16}(\epsilon)$ takes its maximum value 3^{32} at $\epsilon = -0.5$ and its minimum value $5.182\ldots \cdot 10^{-13}$ at $\epsilon = 0.41859\ldots$.

Therefore

$$\begin{aligned}-1.8 \cdot 4^{-K} &< 4^{-K} \sum_{k=0}^{\infty} \frac{\log(5.182\ldots \cdot 10^{-13})}{16 \cdot 64^k} \\ &< \sum_{k=K}^{\infty} 4^{-k} \log\big(z([2^k](P'))\big) < 4^{-K} \sum_{k=0}^{\infty} \frac{\log(3^{32})}{16 \cdot 64^k} < 2.24 \cdot 4^{-K}.\end{aligned}$$ ∎

LEMMA 3.4. *Let $b \in \mathbb{R}$ be positive and let $P \in E_b(\mathbb{R})$ be a point of infinite order.*

(a) *We have*

$$\widehat{\lambda}_\infty(P) > -\tfrac{1}{4}\log 3 - 0.006 = \tfrac{1}{6}\log|b| + \tfrac{1}{3}\log 2 - 0.006 - \tfrac{1}{12}\log|\Delta(E_b)|. \tag{3.7}$$

(b) *Suppose that* $x(P) = c|b|^{1/3}$ *with* $c > -1$ *and* $c \neq 0$. *Then*

$$\widehat{\lambda}_\infty(P) > \tfrac{1}{3}\log|c| - \tfrac{1}{3}\log 2 - 0.004 = \tfrac{1}{6}\log|b| + \tfrac{1}{3}\log|c| + \tfrac{1}{4}\log 3 - 0.004 - \tfrac{1}{12}\log|\Delta(E_b)|, \tag{3.8}$$

$$\widehat{\lambda}_\infty(P) > \tfrac{1}{12}\log(c^5+c^2) - \tfrac{1}{12}\log 432 + 0.188 = \tfrac{1}{6}\log|b| + \tfrac{1}{12}\log(c^5+c^2) + 0.188 - \tfrac{1}{12}\log|\Delta(E_b)|. \tag{3.9}$$

(c) *For* $b \geq 2$,

$$-\tfrac{1}{6}\log b - \tfrac{1}{3}\log 2 - 0.007 - 0.076b^{-1/3} < \left(\tfrac{1}{2}\log\max\{1,|x(P)|\} - \tfrac{1}{12}\log|\Delta(E_b)|\right) - \widehat{\lambda}_\infty(P) < 0.004.$$

Remark. As in Lemma 3.1, we have expressed the bounds in parts (a) and (b) both with and without the $\frac{1}{12}\log|\Delta(E_b)|$ term.

All of the bounds are either best possible or within at most 0.007 of the best possible results.

For (3.7), our proof shows that the -0.006 term is not required if $x(P') = 2(1+\epsilon)b^{1/3}$ with $\epsilon \leq -0.033$ or $\epsilon \geq 0.128$. It is only for ϵ approaching 0 that a more careful analysis is required to eliminate this term. Likewise, the small constant terms in the other inequalities are only required for small intervals around the location of the minimal value.

As in Lemma 3.1, the actual dependence of $\widehat{\lambda}_\infty(P)$ on c as $c \to \infty$ is $\frac{1}{2}\log c$, but the lower bounds in (3.8) and (3.9) allow us to obtain nearly best possible lower bounds for the canonical height.

Lastly, in part (c), it appears that the correct lower order term is $O(b^{-2/3})$, not $O(b^{-1/3})$.

Proof of Lemma 3.4. (a) Write $x(P') = 2(1+\epsilon)b^{1/3}$ where $\epsilon \geq -0.5$ (i.e., we use the point where $\widehat{\lambda}_\infty(P')$ takes its minimum value as the centre).

We proceed in a similar way to the proof of Lemma 3.3 and consider $f_{64}(\epsilon) = x(P')^{64}z(P')^{16}z([2](P'))^4 z([4](P'))/b^{64/3}$. This is a polynomial in ϵ of degree 64.

The derivative of $f_{64}(\epsilon)$ has two roots ≥ -0.5, one at $\epsilon = -0.48899\ldots$ and the second at $\epsilon = 0.07196\ldots$. The former is a local maximum, while the latter is a local minimum. We find that

$$\widehat{\lambda}_\infty(P') - \tfrac{1}{6}\log|b| + \tfrac{1}{12}\log|\Delta(E)| > \frac{\log(f_{64}(\epsilon))}{8\cdot 4^2} - \frac{1.8}{8\cdot 4^3} - \tfrac{1}{3}\log 2 = -0.0056\ldots$$

(the second term coming from Lemma 3.3 with $K = 3$), and the desired inequality follows.

(b) We apply (3.4) with P' rather than P, where $x(P') = (c+2)|b|^{1/3}$ with $c \geq -1$, and the lower bound in Lemma 3.3 with $K = 3$. We have

$$\widehat{\lambda}_\infty(P') \geq \tfrac{1}{6}\log|b| + \tfrac{1}{2}\log(c+2) - \frac{1.8}{512} - \tfrac{1}{12}\log|\Delta(E)| + \tfrac{1}{128}\log\bigl(z^{16}(P')z^4([2](P'))z([4](P'))\bigr). \tag{3.10}$$

For (3.8), we proceed similarly, using (3.10), and bound from below

$$\tfrac{1}{2}\log(c+2) - \tfrac{1}{3}\log c + \tfrac{1}{128}\log\bigl(z^{16}(P')z^4([2](P'))z([4](P'))\bigr).$$

The derivative of this quantity is a rational function of c whose numerator is of degree 64 with leading coefficient 1 and whose denominator is of degree 65 with leading coefficient 6. The numerator has only one positive root, which is $1.71508\ldots$, while the denominator has no such roots. Therefore, the minimum value occurs at $c = 1.71508\ldots$ and is $\frac{1}{4}\log 3 - 0.00029\ldots$, establishing (3.8) for $c > 0$.

For $-1 \leq c < 0$, we proceed in the same way, but bound from below

$$\tfrac{1}{2}\log(c+2) - \tfrac{1}{3}\log(-c) + \tfrac{1}{128}\log\bigl(z^{16}(P')z^4([2](P'))z([4](P'))\bigr).$$

For (3.9), we again proceed similarly using (3.10), and here bound from below

$$\tfrac{1}{2}\log(c+2) - \tfrac{1}{12}\log(c^5+c^2) + \tfrac{1}{128}\log\bigl(z^{16}(P')z^4([2](P'))z([4](P'))\bigr).$$

Using the derivative of this quantity, we find that its minimum value occurs at $c = 3.6038\ldots$ and is $0.1880\ldots$.

(c) We handle separately the cases of $|x(P)| > 1$ and $|x(P)| \leq 1$. In both, we write $x(P) = cb^{1/3}$ and consider

$$\log \frac{x(P')^{64}z(P')^{16}z([2](P'))^4z([4](P'))}{\max\{1,|x(P)|\}^{64}}.$$

So for $|x(P)| \leq 1$, we consider

$$g_{64}(c) = x(P')^{64}z(P')^{16}z([2](P'))^4z([4](P')).$$

This is $b^{64/3}$ times a polynomial in c of degree 64 with integer coefficients. For $c \geq -1$, $g_{64}(c)$ has roots at $c = -0.9779\ldots$ and $c = 0.1439\ldots$. The former is a local maximum, while the latter is a local minimum. The value of $g_{64}(c)$ at this local minimum is $5.28\ldots \cdot 10^{12}b^{64/3}$. Note that the local maximum corresponds to $|x(P)| \leq 1$ only if $b < 1.069\ldots$, while the same holds for the local minimum for $b < 335.59\ldots$. So for $1.069\ldots < b < 335.59\ldots$, $g_{64}(c)$ decreases from $x(P) = -1$ to $x(P) = 0.1439\ldots \cdot b^{1/3}$ (where its value is greater than 1) and then increases to $x(P) = 1$. For $b > 335.59\ldots$, $g_{64}(c)$ is decreasing for $x(P) \in [-1, 1]$.

Now we must examine the values of $g_{64}(c)$ corresponding to $x(P) = \pm 1$. At $x(P) = -1$, we have $g_{64}(c) = 2^{43}b^{64/3} + 4 \cdot 2^{43}b^{63/3} - 48 \cdot 2^{43}b^{61/3} + \cdots$, and we find that for $b \geq 18.5$, $g_{64}(c) - 2^{43}b^{64/3} < 2^{45}b^{63/3}$, so

$$\log(g_{64}(c)) < \log(2^{43}b^{64/3}) + 4b^{-1/3},$$

since $\log(1+x) < x$ for $x > 0$.

By considering the extrema found via calculus, we find that

$$\log(g_{64}(c)) < \log(2^{43}b^{64/3}) + 9.7b^{-1/3}$$

for $2 \leq b \leq 18.5$ too.

At $x(P) = 1$, we have $g_{64}(c) = 2^{43}b^{64/3} - 4 \cdot 2^{43}b^{63/3} + 48 \cdot 2^{43}b^{61/3} + \cdots$ and we proceed in the same way to show $\log(g_{64}(c)) < \log(2^{43}b^{64/3}) + 9.7b^{-1/3}$ for $b \geq 2$ here too. Furthermore, $g_{64}(c) > 1$ for such b as well.

Therefore,

$$0 < \log(g_{64}(c)) < \tfrac{64}{3}\log b + 43\log 2 + 9.7b^{-1/3}.$$

Now we consider the case $|x(P)| \geq 1$ and

$$\frac{x(P')^{64}z(P')^{16}z([2](P'))^4 z([4](P'))}{|x(P)|^{64}},$$

which is a rational function of c. The numerator of the derivative of this rational function is of degree 63, has -128 as its leading coefficient and no roots ≥ -1, while the denominator is of degree 65, has 1 as its leading coefficient and only has a root at $c = 0$. Therefore, the rational function is increasing for $-1 \leq c < 0$ and decreasing for $c > 0$. Combining this with the above results for $x(P) = \pm 1$ establishes

$$\begin{aligned} 0 &< \log \frac{x(P')^{64}z(P')^{16}z([2](P'))^4 z([4](P'))}{\max\{1, |x(P)|\}^{64}} \\ &< \tfrac{64}{3}\log b + 43\log 2 + 9.7b^{-1/3} \end{aligned}$$

for $b \geq 2$.

Applying this to our expression for $\widehat{\lambda}_\infty(P')$ in (3.4), we obtain

$$\begin{aligned} &\tfrac{1}{6}\log b - \tfrac{43}{128}\log 2 + 0.076b^{-1/3} \\ &\quad < \Big(\tfrac{1}{2}\log\max\{1, |x(P)|\} + \tfrac{1}{8}\sum_{k=3}^{\infty} 4^{-k}\log|z([2^k](P'))| - \tfrac{1}{12}\log|\Delta(E_b)|\Big) \\ &\qquad\qquad - \widehat{\lambda}_\infty(P') < 0. \end{aligned}$$

Using Lemma 3.3 with $K = 3$, we find that

$$\begin{aligned} &-\tfrac{1}{6}\log b - \tfrac{1}{3}\log 2 - 0.007 - 0.076b^{-1/3} \\ &\qquad < \big(\tfrac{1}{2}\log\max\{1, |x(P)|\} - \tfrac{1}{12}\log|\Delta(E_b)|\big) - \widehat{\lambda}_\infty(P') < 0.004. \end{aligned}$$

Part (c) now follows upon recalling that $\widehat{\lambda}_\infty$ is fixed under translation, so the same inequalities also hold for $\widehat{\lambda}_\infty(P)$. ∎

4. Nonarchimedean estimates

4.1. Nonarchimedean estimates for $q_v > 3$

LEMMA 4.1. *Let v be a nonarchimedean valuation on $\mathbb{Q}$ associated with a prime number $q_v > 3$, and let b be an integer such that $q_v^6 \nmid b$. The Kodaira types and Tamagawa indices of E_b at v are as in Table* 1.

Table 1. E_b reduction information for $q_v > 3$

b	Kodaira type	c_v
$\mathrm{ord}_{q_v}(b) = 0$	I_0	1
$\mathrm{ord}_{q_v}(b) = 1$	II	1
$\mathrm{ord}_{q_v}(b) = 2$ b/q_v^2 a quadratic residue modulo q_v	IV	3
$\mathrm{ord}_{q_v}(b) = 2$ b/q_v^2 a quadratic nonresidue modulo q_v	IV	1
$\mathrm{ord}_{q_v}(b) = 3$, $q_v \equiv 1 \bmod 6$ b/q_v^3 a cubic nonresidue modulo q_v	I_0^*	1
$\mathrm{ord}_{q_v}(b) = 3$, $q_v \equiv 5 \bmod 6$	I_0^*	2
$\mathrm{ord}_{q_v}(b) = 3$, $q_v \equiv 1 \bmod 6$ b/q_v^3 a cubic residue modulo q_v	I_0^*	4
$\mathrm{ord}_{q_v}(b) = 4$ b/q_v^4 a quadratic residue modulo q_v	IV^*	3
$\mathrm{ord}_{q_v}(b) = 4$ b/q_v^4 a quadratic nonresidue modulo q_v	IV^*	1
$\mathrm{ord}_{q_v}(b) = 5$	II^*	1

Proof. We use Tate's algorithm with $K = \mathbb{Q}_v$ (using the steps and notation in Silverman's presentation of Tate's algorithm in [20, Section IV.9]).

STEP 1. This step applies when $\mathrm{ord}_{q_v}(\Delta(E_b)) = 0$. Since $\Delta(E_b) = -432b^2$ and $432 = 2^4 3^3$, the reduction type is I_0 at v when $\mathrm{ord}_{q_v}(b) = 0$.

STEP 2. We have $\mathrm{ord}_{q_v}(\Delta(E_b)) > 0$. The singular point, $P = (x(P), y(P))$, is already at $(0,0)$ since $\mathrm{ord}_{q_v}(2y(P)), \mathrm{ord}_{q_v}(3x(P)) > 0$ implies that we have $\mathrm{ord}_{q_v}(x(P)) > 0$ too, so no change of variables is needed. Therefore, $b_2 = 0$ and hence $\mathrm{ord}_{q_v}(b_2) > 0$. Thus Step 2 does not apply.

STEP 3. Since $a_6 = b$, if $\mathrm{ord}_{q_v}(b) = 1$, then the reduction type is II.

STEP 4. We may now assume that $\mathrm{ord}_{q_v}(b) \geq 2$. Note that $b_6 = 4b$ and $b_8 = 0$. Hence $\mathrm{ord}_{q_v}(b_8) \geq 3$ and so Step 4 cannot apply.

STEP 5. If $\mathrm{ord}_{q_v}(b) = 2$, then the reduction type is IV. If b/q_v^2 is a quadratic residue modulo q_v, then $c_v = 3$. Otherwise, $c_v = 1$.

STEP 6. We write $P(T) = T^3 + b/q_v^3$, since $a_2 = a_4 = 0$. Its discriminant is $-27b^2/q_v^6$. If $\mathrm{ord}_{q_v}(b) = 3$, then the discriminant is not zero modulo q_v and the reduction type is I_0^*.

If $-b/q_v^3$ is a cubic residue modulo q_v, then $P(T)$ has at least one root in k. Since -1 is always a cubic residue, this condition is equivalent to b/q_v^3 being a cubic residue modulo q_v, so we will always consider b/q_v^3 instead in what follows. Note that if -3 is a quadratic residue modulo q_v (that is, $q_v \equiv 1 \bmod 6$), then $P(T)$ has three roots in k and $c_v = 4$, otherwise (that is, $q_v \equiv 5 \bmod 6$) it only has one root in k and $c_v = 2$.

If b/q_v^3 is not a cubic residue modulo q_v, then $c_v = 1$. It is an easy consequence of Fermat's little theorem that this is only possible for $q_v \equiv 1 \bmod 6$.

STEP 7. Here we assume that $P(T)$ has one simple root and one double root. But the third roots of unity are distinct, since $q_v > 3$, so this is not possible.

STEP 8. Again, since the third roots of unity are distinct, this can only occur if the triple root of $P(T)$ is zero. That is, $\mathrm{ord}_{q_v}(b) > 3$. So we consider the polynomial $Y^2 - b/q_v^4$. It has distinct roots if and only if $\mathrm{ord}_{q_v}(b) = 4$.

If $\mathrm{ord}_{q_v}(b) = 4$ and b/q_v^4 is a quadratic residue modulo q_v, then the reduction type is IV^* and $c_v = 3$. If $\mathrm{ord}_{q_v}(b) = 4$ and b/q_v^4 is a nonquadratic residue modulo q_v, then the reduction type is IV^* and $c_v = 1$.

STEP 9. Since $a_4 = 0$, this step does not apply.

STEP 10. This is the last remaining case if b is sixth-power-free. Here the reduction type is II^*.

This completes the proof of Lemma 4.1. ∎

LEMMA 4.2. *Let v be a nonarchimedean valuation on $\mathbb{Q}$ associated with a prime number $q_v > 3$, and let b be an integer such that $q_v^6 \nmid b$.*

(a) *$P \in E_b(\mathbb{Q}_v)$ has singular reduction if and only if*

$$\mathrm{ord}_{q_v}(x(P)), \mathrm{ord}_{q_v}(y(P)) > 0.$$

(b) *For any* $P \in E_b(\mathbb{Q}_v) \setminus \{O\}$,

$$\widehat{\lambda}_v(P) = \tfrac{1}{2}\log\max\{1, |x(P)|_v\} - \tfrac{1}{12}\log|\Delta(E_b)|_v \tag{4.1}$$
$$- \begin{cases} \frac{1}{3}\log q_v & \text{if } \operatorname{ord}_{q_v}(x(P)) > 0,\ \operatorname{ord}_{q_v}(b) = 2 \text{ and} \\ & b/q_v^2 \text{ is a quadratic residue modulo } q_v, \\ \frac{1}{2}\log q_v & \text{if } \operatorname{ord}_{q_v}(x(P)) > 0,\ \operatorname{ord}_{q_v}(b) = 3 \text{ and} \\ & b/q_v^3 \text{ is a cubic residue modulo } q_v, \\ \frac{2}{3}\log q_v & \text{if } \operatorname{ord}_{q_v}(x(P)) > 0,\ \operatorname{ord}_{q_v}(b) = 4 \text{ and} \\ & b/q_v^4 \text{ is a quadratic residue modulo } q_v, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. (a) We require $\operatorname{ord}_{q_v}(3x(P)^2) = 2\operatorname{ord}_{q_v}(x(P)) > 0$ and $\operatorname{ord}_{q_v}(2y(P)) = \operatorname{ord}_{q_v}(y(P)) > 0$.

(b) This follows from our results in Lemma 4.1 along with [2, Proposition 6, Table 2, and equation (11)]. ∎

4.2. Nonarchimedean estimates for $q_v = 3$

LEMMA 4.3. *Let b be an integer and suppose that $3^6 \nmid b$. The Kodaira types and Tamagawa indices of E_b at 3 are as in Table 2.*

Table 2. E_b reduction information for $q_v = 3$

b	Kodaira type	c_3
$2, 3, 4, 5, 6, 7 \bmod 9$	II	1
$1, 8 \bmod 9$	III	2
$9 \bmod 27$	IV	3
$18 \bmod 27$	IV	1
$54, 81, 108 \bmod 243$	IV*	3
$135, 162, 189 \bmod 243$	IV*	1
$27, 216 \bmod 243$	III*	2
$0 \bmod 243$	II*	1

Proof. As in the proof of the previous lemma, Tate's algorithm is used here. But we do not provide all the details. The conservative reader is referred to an earlier version of this paper, arXiv:1305.6560v2, which contains the full exposition. Also, since $\mathbb{Q}_3^*/\mathbb{Q}_3^{*6}$ is a finite group of small size, the reader can verify this lemma using an implementation of Tate's algorithm like `elllocalred` in PARI. ∎

LEMMA 4.4. *Let b be an integer and suppose that $3^6 \nmid b$.*

(a) *$P \in E_b(\mathbb{Q}_3)$ has singular reduction if and only if* $\operatorname{ord}_3(x(P) + b) > 0$.

(b) *For any* $P \in E_b(\mathbb{Q}_3) \setminus \{O\}$,

$$\widehat{\lambda}_3(P) = \tfrac{1}{2}\log\max\{1, |x(P)|_3\} - \tfrac{1}{12}\log|\Delta(E_b)|_3 - \begin{cases} \frac{1}{4}\log 3 & \text{if } b \equiv 1, 8 \bmod 9 \text{ and } \operatorname{ord}_3(x(P)+b) > 0, \\ \frac{1}{3}\log 3 & \text{if } b \equiv 9 \bmod 27 \text{ and } \operatorname{ord}_3(x(P)) > 0, \\ \frac{2}{3}\log 3 & \text{if } b \equiv 54, 81, 108 \bmod 243 \text{ and } \operatorname{ord}_3(x(P)) > 0, \\ \frac{3}{4}\log 3 & \text{if } b \equiv 27, 216 \bmod 243 \text{ and } \operatorname{ord}_3(x(P)) > 0, \\ 0 & \text{otherwise.} \end{cases} \tag{4.2}$$

Proof. (a) We require $\operatorname{ord}_3(3x(P)^2) > 0$ and $\operatorname{ord}_3(2y(P)) = \operatorname{ord}_3(y(P)) > 0$, so $\operatorname{ord}_3(x(P)^3 + b) > 0$.

Writing $x(P) = x_n/x_d$, we have $x(P)^3 + b = (x_n^3 + bx_d^3)/x_d^3$. Since $x^3 \equiv x \bmod 3$ for all x, we see that $x_n^3 + bx_d^3 \equiv x_n + bx_d \bmod 3$, and therefore $\operatorname{ord}_3(x(P)^3 + b) > 0$ if and only if $\operatorname{ord}_3(x(P) + b) > 0$.

(b) This follows from Lemma 4.3, along with [2, Proposition 6 and equation (11)]. ∎

4.3. Nonarchimedean estimates for $q_v = 2$

LEMMA 4.5. *Let b be an integer with $2^6 \nmid b$. The Kodaira types and Tamagawa indices of E_b at 2 are as in Table 3.*

Table 3. E_b reduction information for $q_v = 2$

b	Kodaira type	c_2
16 mod 64	–	1
2, 3 mod 4	II	1
5 mod 8	IV	1
1 mod 8	IV	3
8, 12 mod 16	I_0^*	2
4 mod 32	IV^*	3
20 mod 32	IV^*	1
32, 48 mod 64	II^*	1

REMARK. For $b \equiv 16 \bmod 64$, the minimal model is given by $y^2 + y = x^3 + (b-16)/64$ and its Kodaira type is I_0.

Proof of Lemma 4.5. As above, we apply Tate's algorithm and refer the reader to either the earlier version of this paper arXiv:1305.6560v2, or the use of an implementation of Tate's algorithm like `elllocalred` in PARI.

We only add that in Step 9 for $b \equiv 16 \bmod 64$ we need to apply the translation $y = y' + 4$, obtaining the curve $y^2 + 8y = x^3 + b - 16$. Neither Step 9 nor Step 10 apply, and in Step 11 we find that our Weierstrass equation

is not minimal and we obtain a new Weierstrass equation

$$y'^2 + y' = x'^3 + (b-16)/64.$$

The discriminant of the latter is $-27b^2/2^8$. Since this is odd, the reduction type is I_0. ∎

LEMMA 4.6. *Let b be an integer and suppose that $2^6 \nmid b$.*

(a) *$P \in E_b(\mathbb{Q}_2)$ has singular reduction if and only if $\mathrm{ord}_2(x(P)) > 0$.*

(b) *For any $P \in E_b(\mathbb{Q}_2) \setminus \{O\}$,*

$$\widehat{\lambda}_2(P) = \tfrac{1}{2}\log\max\{1, |x(P)|_2\} - \tfrac{1}{12}\log|\Delta(E_b)|_2 - \begin{cases} \frac{1}{3}\log 2 & \text{if } b \equiv 1 \bmod 8 \text{ and } \mathrm{ord}_2(x(P)) > 0, \\ \frac{1}{2}\log 2 & \text{if } b \equiv 8, 12 \bmod 16 \text{ and } \mathrm{ord}_2(x(P)) > 0, \\ \frac{2}{3}\log 2 & \text{if } b \equiv 4 \bmod 32 \text{ and } \mathrm{ord}_2(x(P)) > 0, \\ \log 2 & \text{if } b \equiv 16 \bmod 64 \text{ and } \mathrm{ord}_2(x(P)) > 0, \\ 0 & \text{otherwise.} \end{cases} \tag{4.3}$$

REMARK. Note that for $b \equiv 16 \bmod 64$, E_b is not a minimal model. However, since it arises in several cases, including the Mordell curve $y^2 = x^3 - 432m^2$ associated with the cubic twists of the Fermat cubic, we include the result here.

Furthermore, this inclusion allows us to handle all E_b by simply removing any sixth powers.

Proof of Lemma 4.6. (a) We require $\mathrm{ord}_2(3x(P)^2) = 2\,\mathrm{ord}_2(x(P)) > 0$ and $\mathrm{ord}_2(2y(P)) > 0$. Since $b \in \mathbb{Z}$ and $\mathrm{ord}_2(x(P)) > 0$, $\mathrm{ord}_2(2y(P)) > 0$ always holds. Hence $\mathrm{ord}_2(x(P)) > 0$ is a necessary and sufficient condition.

(b) The proof is identical to that for parts (b) of Lemmas 4.2 and 4.4, unless $b \equiv 16 \bmod 64$ when $\mathrm{ord}_2(x(P)) > 0$ (in which case P has singular reduction).

When $b \equiv 16 \bmod 64$ and $\mathrm{ord}_2(x(P)) > 0$, we will use a minimal model. From Step 11 in the proof of Lemma 4.5, if $P = (x(P), y(P)) \in E_b(\mathbb{Q}_2)$, then $Q = (x(P)/4, y(P)/8 - 1/2) \in E_{b,\min}(\mathbb{Q}_2)$ is defined by $y^2 + y = x^3 + (b-16)/64$. We observe that Q has nonsingular reduction and so

$$\begin{aligned} \widehat{\lambda}_2(P) = \widehat{\lambda}_2(Q) &= \tfrac{1}{2}\log\max\{1, |x(P)/4|_2\} - \tfrac{1}{12}\log|\Delta(E_{b,\min})|_2 \\ &= \tfrac{1}{2}\log\max\{1, |x(P)|_2\} - \tfrac{1}{12}\log|\Delta(E_b)|_2 - \log 2, \end{aligned}$$

since $\mathrm{ord}_2(x(P)) > 0$ implies $\mathrm{ord}_2(x(P)) \geq 2$ (because $\mathrm{ord}_2(b) = 4$) and $\Delta(E_{b,\min}) = \Delta(E_b)/2^{12}$. ∎

4.4. Contributions from $p = 2$ and 3. It will be useful for the proofs of our theorems to collect the information required for the contributions from $p = 2$ and $p = 3$. We do so in Tables 4 and 5.

Below, $C_{3,2}$ and $C_{3,3}$ are the reciprocals of the exponentials of the quantities from Lemmas 4.4(b) and 4.6(b) above.

For a point $P \in E_b(\mathbb{Q})$, we have $C_{4,p} = p^{\max(0,\mathrm{ord}_p(x(P)))}$. Similarly, $C_{5,p} = p^{\max(0,2\,\mathrm{ord}_p(y(P)))}$ and $C_{6,p} = p^{\max(0,-\mathrm{ord}_p(x(2P)))}$. Our computations showed that $C_{6,3} = 1$ is possible for each entry in our table below, so we leave it out and write C_6 for $C_{6,2}$.

Letting $\mathrm{ord}_2(b) = k$ and $\mathrm{ord}_3(b) = \ell$, we set $C_{7,2} = C_{3,2}/2^{k/6}$ and $C_{7,3} = C_{3,3}/3^{\ell/6}$.

We define $C_3 = C_{3,2}C_{3,3}$, $C_4 = C_{4,2}C_{4,3}$, $C_5 = C_{5,2}C_{5,3}$ and $C_7 = C_{7,2}C_{7,3}$.

In the tables below, the values of $C_{3,p}$, $C_{4,p}$ and $C_{5,p}$ are expressed as $(v_1 : v_2)$, where v_1 is the minimum possible value when $x(P)$ has good reduction modulo p and under the conditions on b, while v_2 is the minimum possible value when $x(P)$ has singular reduction modulo p and under the conditions on b. A "$-$" indicates that the given case is not possible.

Table 4. Quantities for $p = 2$

b	$C_{3,2}$	$C_{4,2}$	$C_{5,2}$	$C_{6,2}$	$C_{7,2}$
1 mod 8	$(1 : 2^{1/3})$	$(1 : 2)$	$(1 : 1)$	$(16 : 1)$	$(1 : 2^{1/3})$
8 mod 16	$(1 : 2^{1/2})$	$(1 : 2)$	$(1 : 16)$	$(4 : 4)$	$(2^{-1/2} : 1)$
12 mod 16	$(1 : 2^{1/2})$	$(1 : 2)$	$(1 : 4)$	$(4 : 1)$	$(2^{-1/3} : 2^{1/6})$
4 mod 32	$(1 : 2^{2/3})$	$(1 : 4)$	$(1 : 4)$	$(4 : 1)$	$(2^{-1/3} : 2^{1/3})$
16 mod 64	$(1 : 2)$	$(1 : 4)$	$(1 : 16)$	$(4 : 1)$	$(2^{-2/3} : 2^{1/3})$
32 mod 64	$(1 : -)$	$(1 : -)$	$(1 : -)$	$(4 : -)$	$(2^{-5/6} : -)$
48 mod 64	$(1 : -)$	$(1 : -)$	$(1 : -)$	$(4 : -)$	$(2^{-2/3} : -)$
20 mod 32	$(1 : -)$	$(1 : -)$	$(1 : -)$	$(4 : -)$	$(2^{-1/3} : -)$
2 mod 4	$(1 : -)$	$(1 : -)$	$(1 : -)$	$(4 : -)$	$(2^{-1/6} : -)$
3, 5, 7 mod 8	$(1 : -)$	$(1 : -)$	$(4 : -)$	$(16 : -)$	$(1 : -)$

The values of $C_{4,p}$, $C_{5,p}$ and $C_{6,2}$ are obtained by computation. Using PARI, we calculate these values for each possibility modulo p^6 of $x(P) = \alpha/\delta^2$, where α and δ are relatively prime integers, and b modulo p^6.

4.5. Global minimal Weierstrass equation for $E_b/\mathbb{Q}$. Putting together the information we obtained from Tate's algorithm in the above three subsections, we obtain the following result.

LEMMA 4.7. *Let b_1 be the sixth-power-free part of b. If $b_1 \equiv 16 \bmod 64$, then a global minimal Weierstrass equation for $E_b/\mathbb{Q}$ is*

$$y^2 + y = x^3 + (b_1 - 16)/64.$$

Otherwise, a global minimal Weierstrass equation for $E_b/\mathbb{Q}$ is

$$y^2 = x^3 + b_1.$$

Table 5. Quantities for $p = 3$

b	$C_{3,3}$	$C_{4,3}$	$C_{5,3}$	$C_{7,3}$
$1, 8 \bmod 9$	$(1 : 3^{1/4})$	$(1 : 1)$	$(1, 9)$	$(1 : 3^{1/4})$
$9 \bmod 27$	$(1 : 3^{1/3})$	$(1 : 3)$	$(1, 9)$	$(3^{-1/3} : 1)$
$54, 108 \bmod 243$	$(1 : 3^{2/3})$	$(1 : 3)$	$(1, 81)$	$(3^{-1/2} : 3^{1/6})$
$81 \bmod 243$	$(1 : 3^{2/3})$	$(1 : 9)$	$(1, 81)$	$(3^{-2/3} : 1)$
$27, 216 \bmod 243$	$(1 : 3^{3/4})$	$(1 : 3)$	$(1, 729)$	$(3^{-1/2} : 3^{1/4})$
$243, 486 \bmod 729$	$(1 : -)$	$(1 : -)$	$(1 : -)$	$(3^{-5/6} : -)$
$162 \bmod 243$	$(1, -)$	$(1 : -)$	$(1 : -)$	$(3^{-2/3} : -)$
$135, 189 \bmod 243$	$(1, -)$	$(1 : -)$	$(1 : -)$	$(3^{-1/2} : -)$
$18 \bmod 27$	$(1, -)$	$(1 : -)$	$(1 : -)$	$(3^{-1/3} : -)$
$3, 6 \bmod 9$	$(1, -)$	$(1 : -)$	$(1 : -)$	$(3^{-1/6} : -)$
$2, 4, 5, 7 \bmod 9$	$(1, -)$	$(1 : -)$	$(1 : -)$	$(1 : -)$

5. Proof of Theorem 1.2

5.1. Proof of part (a) ($c_p = 1$). We compute the canonical height by summing local heights.

From Lemma 4.1 and our hypotheses, P has nonsingular reduction for all $P \in E_b(\mathbb{Q}_v)$ and all primes $q_v > 3$. Hence we can apply Lemma 4.2(b) for these primes. Combining this with Lemmas 4.4(b) and 4.6(b) gives

$$\sum_{v \neq \infty} \widehat{\lambda}_v(P) \geq -\log C_3 + \tfrac{1}{12} \log |\Delta(E_b)|. \tag{5.1}$$

Case $b < 0$. Adding (5.1) to the lower bound obtained from (3.1) for $\widehat{\lambda}_\infty(P)$, we get

$$\widehat{h}(P) > \tfrac{1}{6} \log |b| - \log C_3 + \tfrac{1}{4} \log 3. \tag{5.2}$$

From Tables 4 and 5, we see that the minimum value of C_3 is $2 \cdot 3^{3/4}$, which occurs when $b \equiv 16 \bmod 64$ and $b \equiv 27, 216 \bmod 243$.

Case $b > 0$. Adding (5.1) to the lower bound from (3.7) for $\widehat{\lambda}_\infty(P)$, we obtain

$$\widehat{h}(P) > \tfrac{1}{6} \log |b| - \log C_3 + \tfrac{1}{3} \log 2 - 0.006. \tag{5.3}$$

5.2. Proof of part (b) ($c_p \mid 4$). Again, we compute the canonical height by summing local heights.

From Lemma 4.1 and our hypotheses, $[2]P$ has nonsingular reduction for all $P \in E_b(\mathbb{Q}_v)$ and all primes $q_v > 3$. Hence we can apply Lemma 4.2(b) for these primes. Combining this with Lemmas 4.4(b) and 4.6(b), and writing $x([2]P) = \alpha/\delta^2$ as a fraction in lowest terms with $\delta > 0$, gives the inequality

$$\sum_{v\neq\infty}\widehat{\lambda}_v([2](P)) \geq \log\delta - \log C_3' + \tfrac{1}{12}\log|\Delta(E_b)| \geq \tfrac{1}{2}\log C_6 - \log C_3' + \tfrac{1}{12}\log|\Delta(E_b)|, \tag{5.4}$$

where C_3' is the value of C_3 for $[2]P$ (not P). These values can be different since $c_3 = 2$ for $b \equiv 1, 8 \bmod 9$ and $b \equiv 27, 216 \bmod 243$, so all points have nonsingular reduction, and $c_2 = 2$ for $b \equiv 8, 12 \bmod 16$, so again all points have nonsingular reduction.

Note that the worst cases occur for $b \equiv 54, 81, 108 \bmod 243$ and $b \equiv 16 \bmod 64$, when $C_3'/C_6^{1/2} = 2\cdot 3^{2/3}$.

Case $b < 0$. Adding (5.4) to the lower bound obtained from (3.1) for $\widehat{\lambda}_\infty([2](P))$ and using $\widehat{h}([2](P)) = 4\widehat{h}(P)$, we get

$$\widehat{h}(P) > \tfrac{1}{24}\log|b| + \tfrac{1}{8}\log C_6 - \tfrac{1}{4}\log C_3' + \tfrac{1}{16}\log 3. \tag{5.5}$$

In the worst cases, $C_3'^{1/4}/(C_6^{1/8}\cdot 3^{1/16}) = 2^{1/4}\cdot 3^{5/48}$, Theorem 1.2(b) immediately follows.

Case $b > 0$. Adding (5.4) to the lower bound from (3.7) for $\widehat{\lambda}_\infty([2](P))$ and using $\widehat{h}([2](P)) = 4\widehat{h}(P)$, we obtain

$$\widehat{h}(P) > \tfrac{1}{24}\log|b| + \tfrac{1}{8}\log C_6 - \tfrac{1}{4}\log C_3' + \tfrac{1}{12}\log 2 - 0.002. \tag{5.6}$$

Here in the worst cases, $C_3'^{1/4}/(C_6^{1/8}\cdot 3^{1/16}) = 2^{1/6}\cdot 3^{1/6}$, completing the proof of Theorem 1.2(b).

5.3. Proof of part (d) ($c_p \mid 12$). We prove part (d) first as we can then use simplified versions of some of the statements here in the proof of part (c).

Write $b = 2^k 3^\ell q_2^2 q_3^3 q_4^4 q$ where q_2 is the product of all distinct primes $p \geq 5$ with $\mathrm{ord}_p(b) = 2$, $\mathrm{ord}_p(x(P)) > 0$ and b/p^2 a quadratic residue modulo p; q_3 is the product of all distinct primes $p \geq 5$ with $\mathrm{ord}_p(b) = 3$, $\mathrm{ord}_p(x(P)) > 0$ and b/p^3 a cubic residue modulo p; q_4 is the product of all distinct primes $p \geq 5$ with $\mathrm{ord}_p(b) = 4$, $\mathrm{ord}_p(x(P)) > 0$ and b/p^4 a quadratic residue modulo p; and q denotes the remaining divisors of b with $\gcd(6q_2q_3q_4, q) = 1$. We set $Q_2 = q_2q_4^2$.

Notice that if a prime p is a divisor of q_4 and $\mathrm{ord}_p(x(P)) > 0$, then, in fact, $\mathrm{ord}_p(x(P)) \geq 2$. Otherwise, if p is a prime dividing q_4 with $\mathrm{ord}_p(x(P)) = 1$, then $\mathrm{ord}_p(x(P)^3 + b) = 3$, but it must be even (since it equals $\mathrm{ord}_p(y(P)^2)$). Similarly, if $k \geq 4$ or $\ell \geq 4$, then $\mathrm{ord}_2(x(P)) \geq 2$ or $\mathrm{ord}_3(x(P)) \geq 2$, respectively.

Writing $x(P) = \alpha/\delta^2$ with α and $\delta > 0$ relatively prime integers (see, for example, [21, §III.2]), we have

$$(C_4 q_2' q_3' q_4'^2) \mid \alpha, \tag{5.7}$$

where C_4 is as above, $q_2' \mid q_2$, $q_3' \mid q_3$ and $q_4' \mid q_4$. We set $Q_2' = q_2'q_4'^2$, noting that $Q_2' \mid Q_2$. So we can write $\alpha = C_4 Q_2' q_3' q'$ for an integer q'.

We write $x(P) = c|b|^{1/3}$ for $c \geq -1$; combining this with (5.7), we find that $C_4 Q_2' q_3' \leq c|b|^{1/3}\delta^2$. That is,

$$Q_2'^2 q_3'^2 \leq c^2 |b|^{2/3}\delta^4 / C_4^2. \tag{5.8}$$

Since $x(P)^3 + b = (C_4 q' Q_2' q_3'/\delta^2)^3 + 2^k 3^\ell q Q_2^2 q_3^3$ is a perfect square, so is

$$q_3'\left(C_4^3 q'^3 Q_2' + 2^k 3^\ell q \left(\frac{Q_2 q_3}{Q_2' q_3'}\right)^2 (q_3/q_3')\delta^6\right) = q_3' Q'.$$

Since $\gcd(6, q_3') = 1$, it must be the case that q_3' divides Q'/C_5. Thus

$$q_3' \leq \left(C_4^3 q'^3 Q_2' + 2^k 3^\ell q \left(\frac{Q_2 q_3}{Q_2' q_3'}\right)^2 (q_3/q_3')\delta^6\right)/C_5.$$

Substituting $q' = c|b|^{1/3}\delta^2/(C_4 Q_2' q_3')$ and our expression for b into this upper bound for q_3', we have

$$q_3' \leq 2^k 3^\ell |q| \delta^6 (c^3 + \operatorname{sgn}(b))/C_5. \tag{5.9}$$

Combining (5.9) with our expression for b to eliminate q, we obtain

$$Q_2'^2 q_3'^4 \leq \frac{\delta^6(c^3 + \operatorname{sgn}(b))}{C_5}|b|. \tag{5.10}$$

So, from (5.8) and (5.10), we have

$$(Q_2'^2 q_3'^3)^2 \leq \frac{c^2\delta^{10}(c^3 + \operatorname{sgn}(b))}{C_4^2 C_5}|b|^{5/3}. \tag{5.11}$$

From Lemmas 4.2(b), 4.4(b) and 4.6(b), along with (5.7) and (5.11), we obtain

$$\begin{aligned}\sum_{v\neq\infty} \widehat{\lambda}_v(P) &\geq \log\delta - \tfrac{1}{6}\log(Q_2'^2 q_3'^3) - \log C_4 + \tfrac{1}{12}\log|\Delta(E_b)| \\ &\geq \log\delta - \tfrac{1}{12}\log\big(c^2\delta^{10}(c^3 + \operatorname{sgn}(b))|b|^{5/3}/(C_4^2 C_5)\big) \\ &\quad - \log C_3 + \tfrac{1}{12}\log|\Delta(E_b)|.\end{aligned} \tag{5.12}$$

Case $b < 0$. Here we have $x(P) = c|b|^{1/3}$ for $c \geq 1$.

For $c > 1$, we combine (5.12) with (3.3) of Lemma 3.1 to obtain

$$\begin{aligned}\widehat{h}(P) &> \tfrac{1}{6}\log|b| + \tfrac{1}{12}\log(c^5 - c^2) + 0.1895 + \log\delta \\ &\quad - \tfrac{1}{12}\log(c^2\delta^{10}(c^3 - 1)|b|^{5/3}/(C_4^2 C_5)) - \log C_3 + \tfrac{1}{12}\log|\Delta(E_b)| \\ &\geq \tfrac{1}{36}\log|b| + \tfrac{1}{12}\log(C_4^2 C_5/C_3^{12}) + 0.1895,\end{aligned} \tag{5.13}$$

since $\delta \geq 1$.

From Tables 4 and 5, the minimum value of $C_4^2 C_5/C_3^{12}$ is $2^{-4}\cdot 3^{-2}$, which can occur for $b \equiv 54, 108 \bmod 243$ and $b \equiv 16 \bmod 64$.

Note that in Lemma 3.1(b), we exclude $c = 1$. However, this is a torsion point, which is excluded from our results (see the argument in the next section using [6]).

Case $b > 0$. Here we have $x(P) = cb^{1/3}$ for $c \geq -1$.

The argument is identical to that for $b < 0$, except that we use (3.9) of Lemma 3.4 rather than (3.3) of Lemma 3.1. Thus

$$\widehat{h}(P) > \tfrac{1}{36}\log|b| + \tfrac{1}{12}\log(C_4^2 C_5/C_3^{12}) + 0.188. \tag{5.14}$$

In Lemma 3.4(b), we exclude $c = -1$ and $c = 0$. But, as above, these are torsion points and are not under consideration here.

Hence the theorem holds for $b > 0$ too.

5.4. Proof of part (c) ($c_p \,|\, 3$). We proceed as in the proof of part (d), using the same notation, except here we have $q_3 = q_3' = 1$. Thus

$$\sum_{v \neq \infty} \widehat{\lambda}_v(P) \geq \log\delta - \tfrac{1}{3}\log Q_2' - \log C_3 + \tfrac{1}{12}\log|\Delta(E_b)| \tag{5.15}$$

and

$$Q_2'^2 \leq c^2|b|^{2/3}\delta^4/C_4^2. \tag{5.16}$$

Case $b < 0$. Note that here $c \geq 1$.

We combine (5.15) with (3.2) of Lemma 3.1(b) to obtain

$$\begin{aligned}\widehat{h}(P) > {} & \tfrac{1}{6}\log|b| + \tfrac{1}{3}\log c + \tfrac{1}{18}\log 108 \\ & - 0.004 + \log\delta - \tfrac{1}{3}\log Q_2' - \log C_3.\end{aligned} \tag{5.17}$$

Now we apply $\delta \geq 1$ and (5.16) to (5.17), obtaining

$$\begin{aligned}\widehat{h}(P) &> \tfrac{1}{6}\log|b| + \tfrac{1}{3}\log c + \tfrac{1}{18}\log 108 - 0.004 + \log\delta - \log C_3 \\ &\quad - \tfrac{1}{3}\log c - \tfrac{1}{9}\log|b| - \tfrac{2}{3}\log\delta + \tfrac{1}{3}\log C_4 \\ &\geq \tfrac{1}{18}\log|b| + \tfrac{1}{18}\log 108 + \tfrac{1}{3}\log(C_4/C_3^3) - 0.004.\end{aligned} \tag{5.18}$$

Again, from Tables 4 and 5, the minimum value of C_4/C_3^3 is $2^{-4}\cdot 3^{-9/2}$, which can occur for $b \equiv 27, 216 \bmod 243$ and $b \equiv 16 \bmod 64$.

Case $b > 0$. We proceed in the same way as for $b < 0$, except for using (3.8) of Lemma 3.4(b), to obtain

$$\widehat{h}(P) > \tfrac{1}{18}\log|b| + \tfrac{1}{12}\log 27 + \tfrac{1}{3}\log(C_4/C_3^3) - 0.004. \tag{5.19}$$

The minimum value of $27C_4^4/C_3^{12}$ is $2^{-4}\cdot 3^{-2}$, which can occur for $b \equiv 27, 216 \bmod 243$ and $b \equiv 16 \bmod 64$.

We also record here the analogue of (5.17) which can be useful in many specific cases:

$$\begin{aligned}\widehat{h}(P) > {} & \tfrac{1}{6}\log|b| + \tfrac{1}{3}\log c + \tfrac{1}{27}\log 27 - 0.004 \\ & + \log\delta - \tfrac{1}{3}\log Q_2' - \log C_3.\end{aligned} \tag{5.20}$$

As in the proof of part (d), where appropriate, the points with $c = -1$, 0 or 1, correspond to torsion points and are not considered here. Hence part (c) of Theorem 1.2 holds too.

6. Proof of Theorem 1.3. As in the previous section, write $b = 2^k 3^\ell q_2^2 q_3^3 q_4^4 q$ and $x(P) = C_4 q_2' q_3' q_4^2 q'$. From Lemmas 4.2(b), 4.4(b) and 4.6(b), along with the definitions of C_3 and C_7 in Subsection 4.4, we get

$$\begin{aligned}(6.1)\qquad 0 &\le \sum_{v\neq\infty} \big(\tfrac{1}{2}\log\max\{1,|x(P)|_v\} - \tfrac{1}{12}\log|\Delta(E_b)|_v - \widehat{\lambda}_v(P)\big)\\ &= \tfrac{1}{3}\log|q_2'| + \tfrac{1}{2}\log|q_3'| + \tfrac{2}{3}\log|q_4'| - \tfrac{k}{6}\log 2 - \tfrac{\ell}{6}\log 3 + \log C_3\\ &\le \tfrac{1}{6}\log|b| + \log C_7,\end{aligned}$$

with the upper bound achieved when for every prime $p > 3$ that divides b, we are in one of the first three cases of (4.1). That is, $|q'| = |q| = 1$, $q_2' = q_2$, $q_3' = q_3$ and $q_4' = q_4$.

If $b < 0$, then from Lemma 3.1(c) and (6.1),

$$(6.2)\qquad -\tfrac{1}{4}\log 3 - 0.005 < \tfrac{1}{2}h(P) - \widehat{h}(P) < \tfrac{1}{6}\log|b| + \log C_7.$$

Note from Tables 4 and 5 that the maximum value of C_7 is $2^{1/3}\cdot 3^{1/4}$, which can occur for $b \equiv 1 \bmod 8$, 4 mod 32 or 16 mod 64, and $b \equiv 1, 8 \bmod 9$ or $27, 216 \bmod 243$.

Now suppose that $b \ge 2$; then from Lemma 3.4(c) and (6.1),

$$\begin{aligned}(6.3)\qquad -\tfrac{1}{6}\log|b| - \tfrac{1}{3}\log 2 - 0.007 - 0.076b^{-1/3}&\\ < \tfrac{1}{2}h(P) - \widehat{h}(P) &< \tfrac{1}{6}\log|b| + \log C_7 + 0.004.\end{aligned}$$

For $b = 1$, $E_b(\mathbb{Q})$ consists only of torsion points, which we consider next for all b.

From [6] (see also [15, Proposition 6.31]), the torsion group of $E_b(\mathbb{Q})$ is isomorphic to:

- $\mathbb{Z}/6\mathbb{Z}$ if $b = 1$ (the torsion points are $(2, \pm 3)$, $(0, \pm 1)$, $(-1, 0)$, O);
- $\mathbb{Z}/3\mathbb{Z}$ if $b = b_1^2 \neq 1$ or $b = -432$ (the torsion points are $(0, \pm b_1)$ and O in the former case, and $(12, \pm 36)$ and O in the latter);
- $\mathbb{Z}/2\mathbb{Z}$ if $b = b_1^3 \neq 1$ (the torsion points are $(-b_1, 0)$ and O);
- $\{O\}$ otherwise.

In the first case, $0 \le \frac{1}{2}h(P) - \widehat{h}(P) \le \frac{1}{2}\log 2$.

In the second case, when $b = b_1^2$, $h(P) = \widehat{h}(P) = 0$.

In the second case, when $b = -432$, $0 \le \frac{1}{2}h(P) - \widehat{h}(P) \le \frac{1}{2}\log 12$.

Lastly, in the third case, $0 \le \frac{1}{2}h(P) - \widehat{h}(P) \le \frac{1}{2}\log b_1 = \frac{1}{6}\log b$.

So in all these cases, Theorem 1.3 holds as well.

For the last inequality in the theorem, we observe that for $b = \pm 1$, $E_b(\mathbb{Q})$ contains only the torsion points, so we may assume that $|b| \geq 2$.

For $b \leq -2$, $-\frac{1}{6}\log|b| - 0.299 < -0.41 < -\frac{1}{4}\log 3 - 0.005$.

For $b \geq 2$, $-\frac{1}{3}\log 2 - 0.007 - 0.076/b^{1/3} = -0.298\ldots$, so this inequality holds.

7. Sharpness of results. For each part of our theorems, we produce infinite families of pairs of curves and points on those curves demonstrating that the results, without the small constant "error terms", are best possible (excluding Theorem 1.2(d) where our examples are within a very small constant of what we believe are the best possible results).

7.1. Theorem 1.2(a)

Case $b < 0$. Set

$$b = -46656b_1^3 - 93312b_1^2 - 62208b_1 - 2160 \quad \text{and} \quad P = (36b_1 + 24, 108)$$

where b_1 is a positive integer and we let it approach ∞. We find that $x(P) \to |b|^{1/3}$ and hence the archimedean height approaches the lower bound in Lemma 3.1(a). Since $b \equiv 16 \bmod 64$ and $b \equiv 27 \bmod 243$, such values of b have the smallest nonarchimedean height functions at both 2 and 3. Furthermore, by our conditions on b in Theorem 1.2(a), our points P have nonsingular reduction for the other primes.

Case $b > 0$. Take

$$b = 46656b_1^2 + 46656b_1 + 13392 \quad \text{and} \quad P = (-12, 54(4b_1 + 2))$$

where b_1 is a positive integer and we let it approach ∞.

For such pairs of curves and points, we find that $x(P)/|b|^{1/3} \to 0$ as $b_1 \to \infty$, and hence the archimedean height approaches the lower bound in Lemma 3.4(a). As in the case of $b < 0$, the required conditions at each of the primes are satisfied too.

7.2. Theorem 1.2(b)

Case $b < 0$. Let b_1 be an odd positive integer, and define $b_2 = [12b_1^3/(3 + 2\sqrt{3})]$ where $[z]$ is the nearest integer to z. Set

$$b = -432(12b_1^3 - b_2)^3(3b_2 - 4b_1^3), \qquad P = \big(24b_1(12b_1^3 - b_2), 36(12b_1^3 - b_2)^2\big).$$

Suppose that b_1 and b_2 are relatively prime and that $2^6 \nmid b$ and $3^6 \nmid b$.

For such pairs,

$$x([2](P)) = 48b_1b_2 \quad \text{and} \quad x([2](P))^3 \approx 191102976b_1^{12}/(3 + 2\sqrt{3})^3.$$

We also find that $b = -191102976b_1^{12}/(3+2\sqrt{3})^3 + O(b_1^9)$. Therefore, $x([2](P)) \to |b|^{1/3}$ as $b_1 \to \infty$ and the lower bound for the archimedean height is sharp.

CASE $b > 0$. Let b_1 be a positive integer, and set

$$b = 432(162b_1 + 31)(6b_1 + 1)^3 \quad \text{and} \quad P = (-72b_1 - 12, 108(6b_1 + 1)^2).$$

For such pairs, $x([2](P)) = 144b_1 + 28$, so $x([2](P))/|b|^{1/3} \to 0$ as $b \to \infty$ and the lower bound for the archimedean height in Lemma 3.4(a) is sharp as $b_1 \to \infty$. As above, the desired conditions on all the primes are satisfied too (note $b \equiv 16 \bmod 64$ and $b \equiv 27 \bmod 243$).

7.3. Theorem 1.2(c)

CASE $b < 0$. Let b_1 be a positive integer; set $b_2 = 36b_1^2 + 36b_1 + 11$, $b = -432(b_2 + 6)b_2^2$ and $P = (12b_2, 324(2b_1 + 1)b_2)$.

Here $x([2^n](P)) \to 4^{1/3}|b|^{1/3}$ and $z([2^n](P)) \to 3$ as $b_1 \to \infty$ for $n \geq 0$. Therefore $\widehat{\lambda}_\infty(P) \to \frac{1}{6}\log|b| + \frac{1}{6}\log 12 - \frac{1}{12}\log|\Delta_b|$.

Note that $b \to -432b_2^3$, so the sum of the nonarchimedean heights is $-\frac{1}{9}\log|b| - \frac{5}{9}\log 2 - \frac{5}{12}\log 3 + \frac{1}{12}\log|\Delta_b|$. Combining this with the above, we find that

$$\widehat{h}(P) \to \tfrac{1}{18}\log|b| - \tfrac{2}{9}\log 2 - \tfrac{1}{4}\log 3 \quad \text{as } b_1 \to \infty.$$

CASE $b > 0$. Let b_1 be a positive integer; set $b_2 = 24b_1^2 + 24b_1 + 5$, $b = 216(b_2 + 9)b_2^2$ and $P = (12b_2, 324(2b_1 + 1)b_2)$.

Here $x(P) \to 2b^{1/3}$ as $b_1 \to \infty$. We translate the point and see that $x(P') \to 4b^{1/3}$. So $x(P')^4 z(P') \to 72b^{4/3}$. Furthermore $x([2^n](P')) \to 2b^{1/3}$ and $z([2^n](P')) \to 1/2$ for $n \geq 1$. Therefore $\widehat{\lambda}_\infty(P') \to \frac{1}{6}\log b + \frac{1}{8}\log 72 - \frac{1}{24}\log 2 - \frac{1}{12}\log|\Delta_b|$.

Note that $b \to 216b_2^3$, so the sum of the nonarchimedean heights is $-\frac{1}{9}\log|b| - \frac{2}{3}\log 2 - \frac{5}{12}\log 3 + \frac{1}{12}\log|\Delta_b|$. So in this case,

$$\widehat{h}(P) \to \tfrac{1}{18}\log|b| - \tfrac{1}{3}\log 2 - \tfrac{1}{6}\log 3 \quad \text{as } b_1 \to \infty.$$

7.4. Theorem 1.2(d). Here we produce families where the constants are slightly larger than in the theorem.

CASE $b < 0$. Let k be a positive integer and set $b_1 = 54k-1$, $b_2 = 720k-1$ and $b_3 = 942k - 1$. Note that they are relatively prime and none of them are divisible by 2 or 3. Further, assume that b_1 and b_3 are square-free and that b_2 is cube-free. Let $b = -432b_1b_2^2b_3^3$ and $P = (12b_2b_3, 36b_2b_3^2)$.

As k increases, $x(P)/|b|^{1/3}$ approaches $(160/3)^{1/3} = 3.764\ldots$. Hence $\widehat{\lambda}_\infty(P) \to \frac{1}{6}\log|b| + 0.74341680776086\ldots - \frac{1}{12}\log|\Delta_b|$.

The sum of the nonarchimedean heights is $-\frac{1}{3}\log b_2 - \frac{1}{2}\log b_3 - \log 2 - \frac{2}{3}\log 3 + \frac{1}{12}\log|\Delta_b|$. Now

$$b_2^6 \to \frac{2^8 \cdot 5^4}{3 \cdot 157^3}|b| \quad \text{and} \quad b_3^6 \to \frac{157^3}{2^{10} \cdot 3^7 \cdot 5^2}|b|,$$

so we find that

$$\widehat{h}(P) \to \tfrac{1}{36}\log|b| - 0.221457178\ldots \qquad \text{as } k \to \infty.$$

Here the constant is approximately $2 \cdot 10^{-7}$ larger than the conjectured constant. The actual value of b_1 required to obtain the constant in the conjecture is smaller than we used here. Here we have $b_1 \approx (3/40)b_2$, whereas for the conjecture we require $b_1 \approx 0.074429578933\ldots \cdot b_2$.

Case $b > 0$. We proceed just as for $b < 0$.

Let k be a positive integer, and set $b_1 = 54k - 1$, $b_2 = 720k + 1$ and $b_3 = 978k + 1$. Note that these numbers are relatively prime and none of them are divisible by 2 or 3. Further, assume that b_1 and b_3 are square-free and b_2 is cube-free. Let $b = 432b_1b_2^2b_3^3$ and $P = (12b_2b_3, 36b_2b_3^2)$.

With this family of examples, we obtain

$$\widehat{h}(P) \to \tfrac{1}{36}\log|b| - 0.22252005826\ldots \qquad \text{as } k \to \infty.$$

As for $b < 0$, the constant here is slightly larger than the conjectured constant, and for the same reason. Here we require $b_1 \approx 0.085629143\ldots \cdot b_2$.

7.5. Theorem 1.3. Silverman (see [19, Example 2.1]) shows that the coefficients of the $\log|b|$ terms are best possible.

For the upper bound for $b < 0$, we consider $b = -2^2 \cdot 3^3 \cdot 5^3 b_1^2$ where $b_1 = 2160b_2^2 + 1350b_2 + 211$ and $P = (60b_1, 1350b_1(16b_2 + 5))$, with the condition that b_1 be cube-free.

For the upper bound for $b > 0$, we consider

$$b = b_1^2 \quad \text{and} \quad P = (2b_1, 3b_1(8b_2 + 15))$$

where $b_1 = (6b_2 + 11)(12b_2 + 23)$ and is cube-free.

For the lower bound for $b > 0$, we consider $b = (3b_1 + 1)^2 + 1$ and $P = (-1, 3b_1 + 1)$.

For the lower bound for $b < 0$, we consider $b = 1 - (2b_1 + 1)^3$ and $P = (2b_1 + 1, 1)$.

In the last inequality of the theorem, -0.299 cannot be replaced by anything greater than $-0.29228\ldots$. Indeed, consider the point $[956](-1, 1)$ on $y^2 = x^3 + 2$ (note that $x([956](-1, 1)) = 0.99818\ldots$). Taking the archimedean height function evaluated at $x = 1$ for $b = 2$, we see that $-0.29250\ldots$ is the smallest possible constant.

Acknowledgements. The authors would like to express their gratitude to the anonymous referee for a careful reading of the manuscript, as well as for many useful suggestions that led to significant improvements in this paper.

References

[1] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge Univ. Press, 2006.

[2] J. E. Cremona, M. Prickett and S. Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory 116 (2006), 42–68.

[3] S. David, *Points de petite hauteur sur les courbes elliptiques*, J. Number Theory 64 (1997), 104–129.

[4] G. Everest, P. Ingram and S. Stevens, *Primitive divisors on twists of Fermat's cubic*, LMS J. Comput. Math. 12 (2009), 54–81.

[5] G. Everest, G. Mclaren and T. Ward, *Primitive divisors of elliptic divisibility sequences*, J. Number Theory 118 (2006), 71–89.

[6] R. Fueter, *Über kubische diophantische Gleichungen*, Comment. Math. Helv. 2 (1930), 69–89.

[7] Y. Fujita and T. Nara, *On the Mordell–Weil group of the elliptic curve* $y^2 = x^3 + n$, J. Number Theory 132 (2012), 448–466.

[8] Y. Fujita and T. Nara, *Generators and integral points on twists of the Fermat cubic*, Acta Arith. 168 (2015), 1–16.

[9] R. Gross and J. H. Silverman, *S-integer points on elliptic curves*, Pacific J. Math. 167 (1995), 263–288.

[10] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. 93 (1988), 419–450.

[11] T. Jędrzejak, *Height estimates on cubic twists of the Fermat elliptic curve*, Bull. Austral. Math. Soc. 72 (2005), 177–186.

[12] M. Krir, *À propos de la conjecture de Lang sur la minoration de la hauteur de Néron–Tate pour les courbes elliptiques sur* $\mathbb{Q}$, Acta Arith. 100 (2001), 1–16.

[13] S. Lang, *Elliptic Curves: Diophantine Analysis*, Grundlehren Math. Wiss. 231, Springer, Berlin, 1978.

[14] C. Petsche, *Small rational points on elliptic curves over number fields*, New York J. Math. 12 (2006), 257–268.

[15] S. Schmitt and H. G. Zimmer, *Elliptic Curves: A Computational Approach*, de Gruyter Stud. Math. 31, Gruyter, 2004.

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

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

[18] J. H. Silverman, *Computing heights on elliptic curves*, Math. Comp. 51 (1988), 339–358.

[19] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. 55 (1990), 723–743.

[20] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.

[21] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergrad. Texts Math., Springer, New York, 1992.

[22] J. Tate, Letter to J.-P. Serre, 1 Oct. 1979; arXiv:1207.5765 (2012).

[23] P. Voutier and M. Yabuta, *Primitive divisors of certain elliptic divisibility sequences*, Acta Arith. 151 (2012), 165–190.

[24] P. Voutier and M. Yabuta, *Lang's conjecture and sharp height estimates for the elliptic curves* $y^2 = x^3 + ax$, Int. J. Number Theory 9 (2013), 1141–1170.

Paul Voutier
London, UK
E-mail: paul.voutier@gmail.com

Minoru Yabuta
Senri High School
17-1, 2 chome, Takanodai, Suita
Osaka, 565-0861, Japan
E-mail: rinri216@msf.biglobe.ne.jp