MATHEMATICS OF COMPUTATION
VOLUME 55, NUMBER 192
OCTOBER 1990, PAGES 723–743

THE DIFFERENCE BETWEEN THE WEIL HEIGHT AND THE CANONICAL HEIGHT ON ELLIPTIC CURVES

JOSEPH H. SILVERMAN

ABSTRACT. Estimates for the difference of the Weil height and the canonical height of points on elliptic curves are used for many purposes, both theoretical and computational. In this note we give an explicit estimate for this difference in terms of the j-invariant and discriminant of the elliptic curve. The method of proof, suggested by Serge Lang, is to use the decomposition of the canonical height into a sum of local heights. We illustrate one use for our estimate by computing generators for the Mordell-Weil group in three examples.

Let E be an elliptic curve defined over a number field K, say given by a Weierstrass equation

$$y^2 = x^3 + Ax + B \tag{1}$$

with A and B in the ring of integers of K. The *canonical height* on E is a quadratic form

$$\hat{h} : E(K) \to \mathbf{R}.$$

(For the definition and basic properties of $\hat{h}$, see [10, Chapter VIII, §9 or 6, Chapter VI].) The canonical height is determined by this property together with the fact that the difference

$$\hat{h}(P) - \tfrac{1}{2}h(x(P)) \tag{2}$$

is bounded as P ranges over $E(K)$, where h is the Weil height on K. In this paper we will give explicit upper and lower bounds for the difference (2) in terms of the coefficients of the Weierstrass equation (1). For example, an immediate consequence of Theorem 1.1 will be the estimate

$$\begin{aligned} -\tfrac{1}{8}h(j) - \tfrac{1}{12}h(\Delta) - 0.973 &\le \hat{h}(P) - \tfrac{1}{2}h(x(P)) \\ &\le \tfrac{1}{12}h(j) + \tfrac{1}{12}h(\Delta) + 1.07. \end{aligned} \tag{3}$$

Here $\Delta = -16(4A^3 + 27B^2)$ and $j = -1728(4A)^3/\Delta$ are the discriminant of (1) and the j-invariant of E, respectively.

Received August 7, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G05, 11Y50.
This work was partially supported by NSF grant #DMS-8913113 and a Sloan Foundation Fellowship.

Estimates of this sort have been given by other authors. Dem'janenko [4] and Zimmer [13] give general, explicit bounds for the Weierstrass equation (1). However, our estimates are somewhat more precise, and since these are *logarithmic* heights, a small improvement in the bounds may translate into large savings for numerical applications. For the family of curves $y^2 = x^3 + px$, Bremner and Cassels [1] give an estimate for (2), and for the particular curve $y^2 = 4x^3 - 28x + 25$, Buhler, Gross, and Zagier [3] give essentially best possible bounds. We will compare our results with these earlier estimates and give examples in §2.

Except for [3], all of the earlier results depend on first giving an explicit estimate for the difference $h(2P) - 4h(P)$. Lang [8] has pointed out that one can also obtain an estimate for (2) by adding up estimates for the difference of the local heights

$$\lambda_v(P) - \tfrac{1}{2}\log\max\{|x(P)|_v, 1\}. \tag{4}$$

He gives such estimates in [6, Chapter I, Theorem 8.4, and Chapter III, Theorem 4.5], making explicit the dependence on j and Δ, but leaving undetermined various absolute constants. This makes his results useful for theoretical purposes, but unsuited to actual computations.

In this paper we will follow (with some modifications) the program described by Lang in [6] to give completely explicit estimates for (2) and (4). We begin in §1 by stating our main results. After some examples (§2) and preliminaries on local heights (§3), we give our principal local estimates in §4 (non-Archimedean) and §5 (Archimedean). It is worth noting that the absolute constants in (3) arise only from the Archimedean places; we have taken some care to keep these constants small, which will help explain the length of §5. In §6 we add up the local results to prove our main theorems.

One practical application of an estimate such as (3) is related to the problem of finding generators for the Mordell-Weil group $E(K)$. A standard descent will often (if one is lucky) produce generators for the quotient group $E(K)/mE(K)$ for some small integer $m \geq 2$. (See, e.g., [2 or 10, Chapter X].) The usual proof of the Mordell-Weil theorem then shows how, in principle, one can find generators for $E(K)$. However, in order to carry this out in practice, one needs an explicit estimate for the difference (2). In the last section, we will illustrate this procedure with three examples.

1. Statement of the main theorems

We set the following notation, which will remain fixed throughout this paper:

K, a field;
E/K, an elliptic curve defined over K;
h, the absolute logarithmic height on $\overline{\mathbf{Q}}$;
$\hat{h}$, the canonical height on $E(\overline{K})$, when K is a number field.

If K is a number field, we also let h_∞ be the Archimedean contribution to the height. Thus, with the usual notation (cf. [10, Chapter VIII, §5]),

$$h_\infty(t) = \frac{1}{[K:\mathbf{Q}]} \sum_{v \in M_K^\infty} n_v \log^+ |t|_v \quad \text{for } t \in K.$$

The following result gives our main global estimate for the difference of the Weil height and the canonical height.

Theorem 1.1. *Let K be a number field, and let E/K be given by a Weierstrass equation*

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5}$$

whose coefficients are in the ring of integers of K. Let Δ be the discriminant of (5) and let j be the j-invariant of E. Further let

$$b_2 = a_1^2 + 4a_2 \quad \text{and} \quad 2^* = \begin{cases} 2 & \text{if } b_2 \neq 0, \\ 1 & \text{if } b_2 = 0. \end{cases}$$

Define a "height of E" (really of the Weierstrass equation (5)) by

$$\mu(E) = \tfrac{1}{12}h(\Delta) + \tfrac{1}{12}h_\infty(j) + \tfrac{1}{2}h_\infty(b_2/12) + \tfrac{1}{2}\log 2^*.$$

Then for all $P \in E(\overline{K})$,

$$-\tfrac{1}{24}h(j) - \mu(E) - 0.973 \leq \hat{h}(P) - \tfrac{1}{2}h(x(P)) \leq \mu(E) + 1.07.$$

Remark 1.2. If E is given by a Weierstrass equation

$$y^2 = x^3 + Ax + B,$$

then $\Delta = -16(4A^3 + 27B^2)$ and $j = -(48A)^3/\Delta$. If we replace $h_\infty(j)$ by the larger quantity $h(j)$, then in this case Theorem 1.1 gives the estimate

$$\begin{aligned} -\tfrac{1}{8}h(j) - \tfrac{1}{12}h(\Delta) - 0.973 &\leq \hat{h}(P) - \tfrac{1}{2}h(x(P)) \\ &\leq \tfrac{1}{12}h(j) + \tfrac{1}{12}h(\Delta) + 1.07. \end{aligned} \tag{6}$$

This is the version we stated in the introduction. Of course, it is often possible to do better. For example, if $K = \mathbf{Q}$ and $A > 0$, then $|j|_\infty \leq 1728$, so $h_\infty(j) \leq \log(1728)$. This gives a substantial improvement over (6) if A and B are large.

In special cases it is possible to improve the estimates of Theorem 1.1, especially the more important lower bound. Rather than try to give the most general such improvements, we will illustrate the techniques for a particular class of curves, and leave it to the reader to adapt these ideas to other examples.

Theorem 1.3. *Let $E/\mathbf{Q}$ be given by a Weierstrass equation*

$$y^2 = x^3 + Ax + B, \tag{7}$$

and suppose that $A, B \in \mathbf{Z}$ satisfy the conditions $4A^3 + 27B^2$ is square-free and $\gcd(A, 3B) = \gcd(2, B) = 1$. Then $\frac{1}{2}h(x(P)) \leq \hat{h}(P) + \frac{1}{8}\log^+|j| + 1.205$. If in addition $A > 0$, then

$$\tfrac{1}{2}h(x(P)) \leq \hat{h}(P) + 2.137.$$

2. Examples and comparison with earlier estimates

Example 2.1. An often-studied family of elliptic curves is given by the equation

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

This family of curves has $j = 0$, $\Delta = -2^4 3^3 B^2 = -432B^2$, $b_2 = 0$, and $2^* = 1$, so Theorem 1.1 gives the estimate

$$-\tfrac{1}{6}h(B) - 1.48 \le \hat{h}(P) - \tfrac{1}{2}h(x(P)) \le \tfrac{1}{6}h(B) + 1.576. \tag{8}$$

By way of comparison, Zimmer's estimate [13] gives in this case

$$|\hat{h}(P) - \tfrac{1}{3}h([x(P), y(P), 1])| \le \tfrac{1}{3}h(B) + 1.3863. \tag{9}$$

We see that the constants in (8) are not as good as those in (9), but the dependence on B is much better. Of course, for computational purposes it is also preferable to have a bound for $h(x)$, rather than for $h([x, y, 1])$, since the latter will generally be $\frac{3}{2}$ as large as the former, requiring a much larger search region.

Let us show that the dependence on B in (8) is best possible. For each integer $t \in \mathbf{Z}$, consider the curve and point

$$E_t : y^2 = x^3 + t^3, \qquad P_t = (-t, 0).$$

Since P_t is a two-torsion point, we have $\hat{h}(P_t) = 0$. On the other hand,

$$h(x(P_t)) = \log|t| \quad \text{and} \quad h(B_t) = \log|t^3|,$$

so

$$\hat{h}(P_t) - \tfrac{1}{2}h(x(P_t)) = -\tfrac{1}{6}h(B_t).$$

Since also $h(B_t) \to \infty$ as $t \to \infty$, this shows that the lower bound (8) has best possible dependence on B.

In order to show the same for the upper bound, we cannot look at torsion points, since we want $\hat{h}(P)$ to be large. Again for $t \in \mathbf{Z}$, we consider the elliptic curves and points

$$E_t : y^2 = x^3 + (t^2 + 1), \qquad P_t = (-1, t).$$

Using [11], one finds that the canonical height of P_t over the function field $\mathbf{C}(t)$ is equal to $\frac{1}{3}$. It then follows from [9] that

$$\lim_{t\to\infty} \frac{\hat{h}(P_t)}{h(t)} = \frac{1}{3}.$$

On the other hand, for the given equation we have

$$h(B_t) = h(t^2 + 1) \sim 2h(t) \quad \text{as } t \to \infty.$$

Since $h(x(P_t)) = h(-1) = 0$, we find

$$\lim_{t\to\infty} \frac{\hat{h}(P_t) - \frac{1}{2}h(x(P_t))}{h(B_t)} = \frac{1}{6},$$

which shows that the dependence on B in the upper bound of (8) is also best possible.

Example 2.2. Similarly, the elliptic curves

$$E: y^2 = x^3 + Ax \tag{10}$$

with complex multiplication by $\mathbf{Z}[i]$ are frequently studied. These curves have $j = 1728$, $\Delta = -2^6 A^3$, $b_2 = 0$, and $2^* = 1$, so Theorem 1.1 reads

$$-\tfrac{1}{4}h(A) - 2.252 \le \hat{h}(P) - \tfrac{1}{2}h(x(P)) \le \tfrac{1}{4}h(A) + 2.038. \tag{11}$$

Just as in Example 2.1, it is possible to show that the dependence on A is best possible. (For example, for the lower bound, look at the torsion point $(t, 0)$ on the curve $y^2 = x^3 - t^2 x$; and for the upper bound, look at $(1, t)$ on the curve $y^2 = x^3 + (t^2 - 1)x$.)

We compare (11) with an estimate of Bremner and Cassels [1]. They work over $\mathbf{Q}$ and consider equation (10) with $A = p \ge 3$ prime. They deal only with points $P = (x, y)$ satisfying $x = r/s$, $\gcd(r, p) = 1$. In this situation they obtain the estimate

$$-\tfrac{1}{6}h(p) - 0.232 \le \hat{h}(P) - \tfrac{1}{2}h(x(P)) \le \tfrac{2}{3}h(p). \tag{12}$$

Notice that the lower bound in (12) has a better dependence on $A = p$ than (11), although we observed above that (11) is best possible. The reason that Bremner and Cassels do better is their restriction to points with $\gcd(r, p) = 1$. Geometrically, this ensures that P is on the identity component of the Néron model for the prime p. By using this additional fact, we can improve on (12) as follows: For the equation (10) with $A = p \ge 3$ prime, we have

$$-2.252 \le \hat{h}(P) - \tfrac{1}{2}h(x(P)) \quad \text{if } x(P) = r/s,\ \gcd(r, p) = 1. \tag{13}$$

This is better than (12) as soon as $p \ge 183506$. So for practical purposes, (12) will often be preferable. We briefly indicate the proof of (13).

For the Archimedean place of $\mathbf{Q}$ we use Theorem 5.5, obtaining

$$-\tfrac{1}{12}\log(64p^3) - \tfrac{1}{8}\log(1728) - 0.973 \le \lambda_\infty(P) - \tfrac{1}{2}\log^+ |x(P)|_\infty.$$

For all primes $q \ne p$, we use Theorem 4.1(a), which gives

$$0 \le \lambda_q(P) - \tfrac{1}{2}\log^+ |x(P)|_q.$$

Finally, for the local height at p we use the condition that $\gcd(r, p) = 1$ to observe that P reduces to a nonsingular point modulo p. This means that the local height at p is given by the exact formula

$$\tfrac{1}{12}\log(p^3) = \lambda_p(P) - \tfrac{1}{2}\log^+ |x(P)|_p.$$

Summing all of the local heights, the dependence on p vanishes, yielding the estimate given in (13).

Example 2.3. Consider the curve

$$E: y^2 + y = x^3 - 7x + 6$$

of conductor 5077 and rank 3 over $\mathbf{Q}$. For this curve, Buhler, Gross, and Zagier [3] give the estimate

$$0 \le \hat{h}(P) - \tfrac{1}{2}h(x(P)) \le 0.60254\ldots \quad \text{for all } P \in E(\mathbf{Q}). \tag{14}$$

(Note that their $\hat{h}$ is twice ours.) This curve has $\Delta = 5077$, $j = 2^{12}3^3 7^3/5077$, $b_2 = 0$, and $2^* = 1$, so applying Theorem 1.1 directly gives

$$-2.7 \le \hat{h}(P) - \tfrac{1}{2}h(x(P)) \le 2.46.$$

Of course, this can be substantially improved by using the fact that there is only one component on the fiber of the Néron model at $p = 5077$, so

$$\lambda_{5077}(P) - \tfrac{1}{2}h(x(P)) = \tfrac{1}{12}\log(5077).$$

However, this will still yield something much worse than (14). The reason is that $|j|$ is quite large. To get an estimate close to (14), one would need to redo the Archimedean bound in Theorem 5.5, using the fact that $q = e^{2\pi i\tau}$ is extremely small. In fact, Buhler, Gross, and Zagier use a series for λ_∞ due to Tate to obtain a very accurate estimate for the local height at the Archimedean place.

Example 2.4. Consider the curve with equation

$$E\colon y^2 = x^3 - x + 1$$

with $j = 6912/23$. Since $4(-1)^3 + 27(1)^2 = 23$ is square-free, we see that this equation satisfies the conditions of Theorem 1.3. Hence we obtain the estimate

$$\tfrac{1}{2}h(x(P)) \le \hat{h}(P) + \tfrac{1}{8}\log\tfrac{6912}{23} + 1.205 \le \hat{h}(P) + 1.92. \tag{15}$$

Example 2.5. Similarly, the curve given by

$$E\colon y^2 = x^3 - x + 15$$

has $4(-1)^3 + 27(15)^2 = 6071 = 13 \cdot 467$, so again we can apply Theorem 1.3. This gives

$$\tfrac{1}{2}h(x(P)) \le \hat{h}(P) + \tfrac{1}{8}\log\tfrac{6912}{6071} + 1.205 \le \hat{h}(P) + 1.222. \tag{16}$$

Example 2.6. The curve with equation

$$E\colon y^2 = x^3 - 28x - 48 = (x+4)(x+2)(x-6)$$

was considered in [10, Chapter X, Example 1.5]. (Actually, the equation in [10] is $Y^2 = X^3 - 12X^2 + 20X$. We have made the substitution $X = x + 4$ to eliminate the x^2 term.) This curve has

$$\Delta = 409600 = 2^{14}5^2 \quad \text{and} \quad j = \frac{148176}{25} = \frac{2^4 3^3 7^3}{5^2}.$$

Applying Theorem 1.1, we find that every point $P \in E(\mathbf{Q})$ satisfies

$$-3.27 \le \hat{h}(P) - \tfrac{1}{2}h(x(P)) \le 2.871. \tag{17}$$

By comparison, Zimmer's estimate [13] gives

$$-3.053 \le \hat{h}(P) - \tfrac{1}{3}h([x(P), y(P), 1]) \le 3.053.$$

In §7 we will use these estimates to compute generators for the Mordell-Weil group over $\mathbf{Q}$ of the curves in Examples 2.4, 2.5, and 2.6.

3. Preliminaries on local heights

In this section we set notation and briefly review the basic facts about local heights that we will need in the sequel. For further explanation and proofs, see [6, Chapters I, III; 10, Appendix C, §18].

Let K be a field complete with respect to an absolute value v, and let E/K be an elliptic curve given by a Weierstrass equation

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

with discriminant Δ and j-invariant j. The local height function

$$\lambda = \lambda_v : E(K)\backslash\{O\} \to \mathbf{R}$$

is a continuous function, with a logarithmic pole at O, which satisfies the duplication formula

$$\lambda(2P) = 4\lambda(P) + v((2y + a_1x + a_3)(P)) - \tfrac{1}{4}v(\Delta)$$

for all $P \in E(K)$ with $2P \neq O$. As usual, we will let

$$v(t) = -\log|t|_v \quad \text{and} \quad \log^+|t|_v = \log\max\{|t|_v, 1\}.$$

The local height is independent of the choice of a Weierstrass equation, and does not change for finite extensions of K.

In case v is non-Archimedean, if all of the a_i coefficients are v-integral and if $P \in E(K)$ reduces modulo v to a smooth point, the local height is given by the formula

$$\lambda(P) = \tfrac{1}{2}\log^+|x(P)|_v - \tfrac{1}{12}\log|\Delta|_v.$$

Again, if v is non-Archimedean and if $|j|_v > 1$, then (possibly after a quadratic extension of K) the curve E has a Tate parametrization $E(K) \cong K^*/q^{\mathbf{Z}}$ for some $q \in K^*$ with $|q|_v = |j|_v^{-1} < 1$. If $u \in K^*/q^{\mathbf{Z}}$ is normalized by $|q|_v < |u|_v \le 1$, then the local height is given by

$$\lambda(u) = \log^+\left|\frac{1}{1-u}\right|_v + \frac{1}{2}B_2(\alpha)v(q),$$

where $\alpha = \alpha(u) = v(u)/v(q)$ and B_2 is the second Bernoulli polynomial $B_2(T) = T^2 - T + \frac{1}{6}$.

In case v is Archimedean, we can assume that $K = \mathbf{C}$; then $E(\mathbf{C}) \cong \mathbf{C}^*/q^{\mathbf{Z}}$ for some $q \in \mathbf{C}^*$, $|q| < 1$. In this case the local height of $u \in \mathbf{C}^*/q^{\mathbf{Z}}$ is given by

$$\lambda(u) = \tfrac{1}{2}B_2(\alpha)v(q) + v(1-u) + \sum_{n\ge 1} v((1-q^nu)(1-q^nu^{-1})),$$

where α and B_2 are as above.

Finally, if K is a number field, then the canonical height $\hat{h}$ on $E(K)$ can be computed locally as

$$\hat{h}(P) = \frac{1}{[K:\mathbf{Q}]} \sum_{v \in M_K} n_v \lambda_v(P) \quad \text{for all } P \in E(K),\ P \neq O.$$

We conclude this section with an elementary inequality which will prove useful.

Lemma 3.1. *For all real numbers* $a, b > 0$,

$$-\log^+(b^{-1}) \leq \log^+(a/b) - \log^+(a) + \log(b) \leq \log^+(b).$$

Proof. Note that

$$\log^+(a/b) - \log^+(a) + \log(b) = \log(\max\{a, b\}/\max\{a, 1\}).$$

Now one need merely check the six possible size orderings of $\{1, a, b\}$. □

4. Non-Archimedean local heights

Theorem 4.1 (Tate). *Let* K *be complete with respect to a non-Archimedean absolute value* v, *and let* E/K *be an elliptic curve with Weierstrass equation*

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{18}$$

such that all of the a_i*'s are* v*-integral. Let* Δ *be the discriminant of* (18), *and let* j *be the* j*-invariant of* E.

(a) *For all* $P \in E(K)$,

$$-\tfrac{1}{24}\log^+|j|_v \leq \lambda(P) - \tfrac{1}{2}\log^+|x(P)|_v \leq \tfrac{1}{12}v(\Delta).$$

(b) *If in addition we have*

$$\operatorname{ord}_v(j) = -1 \quad \textit{and} \quad \operatorname{ord}_v(c_4) = 0,$$

then the lower bound in (a) *can be replaced by*

$$\tfrac{1}{12}\log^+|j|_v \leq \lambda(P) - \tfrac{1}{2}\log^+|x(P)|_v.$$

Proof. The inequality in (a) is proven in [6, Chapter III, Theorem 4.5]. During the course of the proof it is shown that if E is a Tate curve (i.e., if it has split multiplicative reduction), then the lower bound is

$$\frac{1}{2}B_2\left(\frac{\operatorname{ord}_v(u)}{\operatorname{ord}_v(q)}\right)v(j^{-1}).$$

Here we have chosen a v-analytic parametrization

$$E(K) \cong K^*/q^{\mathbf{Z}}$$

for a certain $q \in K^*$ with $\operatorname{ord}_v(q) = -\operatorname{ord}_v(j)$, and $u \in K^*$ is chosen normalized to satisfy $0 \leq \operatorname{ord}_v(u) < \operatorname{ord}_v(q)$.

Now under the hypothesis in (b), namely $\operatorname{ord}_v(j) = -1$, we must have $\operatorname{ord}_v(u) = 0$, which gives the required lower bound of $\frac{1}{12}\log^+|j|_v$.

Suppose now the E is not a Tate curve. Since $|j|_v > 1$, it becomes isomorphic to a Tate curve after a quadratic extension L/K. Further, the condition $\operatorname{ord}_v(c_4) = 0$ means that L/K is unramified. In this case, E has nonsplit multiplicative reduction and is isomorphic to a Tate curve in the unramified quadratic extension over which it attains split multiplicative reduction. Now the above argument works for points in $E(L)$, so a fortiori it is valid for points in $E(K)$. [N.B. It is vital that L/K be unramified; otherwise the valuation w in L would give $\operatorname{ord}_w(j) = 2$, vitiating the entire argument.] □

5. Archimedean local heights

In this section we estimate the difference between local heights for Archimedean absolute values. This will involve using q-expansions to estimate various functions. Throughout this section, we use the following notation:

$$\tau, z \in \mathbf{C}, \qquad \operatorname{Im}\tau > 0,$$
$$q = e^{2\pi i\tau}, \quad u = e^{2\pi iz},$$
$$\alpha = \frac{\operatorname{Im} z}{\operatorname{Im}\tau} = \frac{\log|u|}{\log|q|}.$$

We will sometimes also impose one or both of the following conditions:

(*) $\operatorname{Im}(\tau) \geq \frac{1}{2}\sqrt{3}$ (equivalently, $|q| \leq e^{-\pi\sqrt{3}} = 0.00433342\ldots$),

(**) $0 \leq \alpha \leq \frac{1}{2}$ (equivalently, $1 \geq |u| \geq |q|^{1/2}$).

Lemma 5.1. *Let $t \in \mathbf{C}$ satisfy $|qt| < 1$. Then*

$$\frac{-|qt|}{(1-|q|)(1-|qt|)} \leq \sum_{n\geq 1}\log|1-q^nt| \leq \frac{|qt|}{1-|q|}.$$

Proof. For any $w \in \mathbf{C}$ with $|w| < 1$ we have the elementary bounds

$$\frac{|w|}{1-|w|} \leq \log|1-w| \leq |w|.$$

Substituting $w = q^nt$ and summing over $n \geq 1$ immediately gives the desired upper bound; for the lower bound we need merely note that

$$\sum_{n\geq 1}\log|1-q^nt| \geq \sum_{n\geq 1}\frac{|q^nt|}{1-|q^nt|} \geq \frac{1}{1-|qt|}\sum_{n\geq 1}|q^nt|. \quad \square$$

Next we prove some estimates relating the modular j-function $j(\tau)$, the modular discriminant $\Delta(\tau)$, and the parameter q.

Lemma 5.2. *Assume that* $(*)$ *is true. Then*

(a) $$-5.7538 \le \log^+ |j(\tau)| + \log\left|\frac{1}{(2\pi)^{12}}\Delta(\tau)\right| \le 2.2;$$

(b) $$-5.6795 \le \log^+ |j(\tau)| + \log|q| \le 2.304;$$

(c) $$-0.105 \le \log\left|\frac{1}{(2\pi)^{12}}\frac{\Delta(\tau)}{q}\right| \le 0.1045.$$

Proof. (a) To avoid powers of π in our calculations, we let

$$\Gamma(\tau) = \frac{12}{(2\pi)^4} g_2(\tau) = 1 + 240\sum_{n\ge 1}\frac{n^3 q^n}{1-q^n},$$

$$D(\tau) = \frac{1}{(2\pi)^{12}}\Delta(\tau) = q\prod_{n\ge 1}(1-q^n)^{24}.$$

Then $j(\tau) = (12g_2(\tau))^3/\Delta(\tau) = \Gamma(\tau)^3/D(\tau)$, so

$$\log|j(\tau)D(\tau)| = 3\log|\Gamma(\tau)|.$$

As in [5, Lemma 2.2], it is easy to get an upper bound for $\Gamma(\tau)$:

$$|\Gamma(\tau)| \le 1 + \frac{240}{1-|q|}\sum_{n\ge 1} n^3|q^n| = 1 + 240|q|\frac{1+4|q|+|q|^2}{(1-|q|)^5} \le 2.0813.$$

The last inequality uses $(*)$. Hence,

$$\begin{aligned}\log^+ |j(\tau)| + \log|D(\tau)| &\le \log|j(\tau)D(\tau)| \\ &= 3\log|\Gamma(\tau)| \le 3\log(2.0813) \le 2.2.\end{aligned}$$

To prove the other inequality, we must bound $\Gamma(\tau)$ away from 0. As above, we have

$$|\Gamma(\tau)| \ge 1 - \frac{240}{1-|q|}\sum_{n\ge 1} n^3|q^n| = 1 - 240|q|\frac{1+4|q|+|q|^2}{(1-|q|)^5}. \tag{19}$$

Notice if we use the trivial estimate $|q| \le e^{-\pi\sqrt{3}}$, then the lower bound (19) is negative. This reflects the fact that $j((1+\sqrt{-3})/2) = 0$. We also need the following estimate for $D(\tau)$, which follows immediately from Lemma 5.1 with $t = 1$:

$$\log|D(\tau)| \ge \log|q| - 24\frac{|q|}{(1-|q|)^2}. \tag{20}$$

Using (19) and (20), we find

$$\begin{aligned}&\log^+ |j(\tau)| + \log|D(\tau)| \\ &= \max\{\log|j(\tau)D(\tau)|, \log|D(\tau)|\} = \max\{3\log|\Gamma(\tau)|, \log|D(\tau)|\} \\ &\ge \max\left\{3\log\left(1 - 240|q|\frac{1+4|q|+|q|^2}{(1-|q|)^5}\right), \log|q| - 24\frac{|q|}{(1-|q|)^2}\right\}.\end{aligned} \tag{21}$$

To find a lower bound for this maximum, we equate the two quantities in the right-hand side of (21) and solve numerically for $|q|$. This gives $|q| = 0.003446\ldots$ and a lower bound of $-5.75377\ldots$, which completes the proof of (a).

(b) The upper bound is [5, Lemma 2.2a]; the proof of the lower bound is similar to (a), so we only briefly sketch it. In place of (21) we find, after some calculation,

$$\begin{aligned}&\log^+|j(\tau)| + \log|q| \\ &\geq \max\left\{3\log\left(1 - 240|q|\frac{1+4|q|+|q|^2}{(1-|q|)^5}\right) - 24\frac{|q|}{1-|q|}, \log|q|\right\}.\end{aligned} \tag{22}$$

Now one can verify numerically that the minimum of the right-hand side of (22) occurs at $|q| = 0.0034153\ldots$, giving a lower bound of $-5.67948\ldots$.

(c) Using Lemma 5.1 with $t = 1$ gives

$$-24\frac{|q|}{(1-|q|)^2} \leq \log\left|\frac{1}{(2\pi)^{12}}\frac{\Delta(\tau)}{q}\right| = 24\sum_{n\geq 1}\log|1-q^n| \leq 24\frac{|q|}{1-|q|}.$$

Since $|q| \leq e^{-\pi\sqrt{3}}$, we obtain the stated bounds. □

Next we estimate the Weierstrass $\wp$-function and the local height λ in terms of the parameters u and q.

Lemma 5.3. *Assume that* (*) *and* (**) *are valid. Then*

(a) $$\left|\frac{1}{(2\pi i)^2}\wp(z,\tau) - \frac{u}{(1-u)^2}\right| < 0.1682;$$

(b) $$\begin{aligned}-1.0506 \leq \log^+\left|\frac{1}{(2\pi i)^2}\wp(z,\tau)\right| + 2\log|1-u| \\ \leq 2\log(1+|q|^{\alpha});\end{aligned}$$

(c) $$-0.0665 \leq \lambda(z) + \tfrac{1}{2}B_2(\alpha)\log|q| + \log|1-u| \leq 0.0711.$$

Proof. (a) The Weierstrass $\wp$-function has the q-expansion

$$\begin{aligned}\frac{1}{(2\pi i)^2}\wp(z,\tau) = \frac{u}{(1-u)^2} + \frac{1}{12} \\ + \sum_{n\geq 1}\left\{\frac{q^n u}{(1-q^n u)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - 2\frac{q^n}{(1-q^n)^2}\right\}.\end{aligned}$$

(Cf. [7, Chapter 4, §2 or 10, Appendix C, Proposition 12.6].)

For any $t \in \mathbf{C}$ with $|qt| < 1$ we have the elementary estimate

$$\left|\sum_{n\geq 1}\frac{q^n t}{(1-q^n t)^2}\right| \leq \frac{1}{(1-|qt|)^2}\sum_{n\geq 1}|q^n t| = \frac{|qt|}{(1-|q|)(1-|qt|)^2}. \tag{23}$$

Using (23) three times, with $t = u$, $t = u^{-1}$, and $t = 1$, we find

$$\left|\frac{1}{(2\pi i)^2}\wp(z,\tau) - \frac{u}{(1-u)^2}\right| \leq \frac{1}{12} + \frac{1}{1-|q|}\left\{\frac{|q|^{1+\alpha}}{(1-|q|^{1+\alpha})^2} + \frac{|q|^{1-\alpha}}{(1-|q|^{1-\alpha})^2} + \frac{2|q|}{(1-|q|)^2}\right\}.$$

In the range $0 \leq \alpha \leq \frac{1}{2}$ allowed by $(**)$, the quantity in braces has a maximum at $\alpha = \frac{1}{2}$. Combined with $(*)$, this gives the desired bound

$$\left|\frac{1}{(2\pi i)^2}\wp(z,\tau) - \frac{u}{(1-u)^2}\right| \leq \frac{1}{12} + 0.08482\ldots \leq 0.1682.$$

(b) Letting

$$F = F(z,\tau) = \frac{1}{(2\pi i)^2}\wp(z,\tau) - \frac{u}{(1-u)^2},$$

we have

$$\log^+\left|\frac{1}{(2\pi i)^2}\wp(z,\tau)\right| + 2\log|1-u| = \log\max\{|u+(1-u)^2F|, |1-u|^2\}. \tag{24}$$

From (a), $|F| \leq 0.1682$, so

$$|u+(1-u)^2F| \leq |u| + 0.1682(1+|u|)^2 \leq (1+|u|)^2.$$

Since also $|1-u|^2 \leq (1+|u|)^2$, we immediately obtain the desired upper bound. (Remember that $|u| = |q|^\alpha$.)

For the lower bound we use the estimate

$$\begin{aligned}|u+(1-u)^2F| &\geq 1 - |1-u| - |1-u|^2F \\ &\geq 1 - |1-u| - 0.1682|1-u|^2\end{aligned}$$

to obtain

$$\begin{aligned}&\max\{|u+(1-u)^2F|, |1-u|^2\} \\ &\quad\geq \max\{1-|1-u|-0.1682|1-u|^2, |1-u|^2\} \geq 0.34976.\end{aligned}$$

The minimum value of the middle expression occurs at $|1-u| = 0.5914\ldots$. Substituting into (24) completes the proof of (b).

(c) The local height $\lambda(z)$ is given by the formula

$$\lambda(z) = -\tfrac{1}{2}B_2(\alpha)\log|q| - \log|1-u| \cdot - \sum_{n\geq 1}\log|(1-q^nu)(1-q^nu^{-1})|. \tag{25}$$

(Cf. [6, Chapter I, Theorem 8.1].) Applying Lemma 5.1 twice, once with $t = u$ and once with $t = u^{-1}$, gives

$$-\frac{1}{1-|q|}\left\{\frac{|q|^{1+\alpha}}{1-|q|^{1+\alpha}}+\frac{|q|^{1-\alpha}}{1-|q|^{1-\alpha}}\right\}$$
$$\le \sum_{n\ge 1}\log|(1-q^n u)(1-q^n u^{-1})| \le \frac{1}{1-|q|}\{|q|^{1+\alpha}+|q|^{1-\alpha}\}.$$

For $0 \le \alpha \le \frac{1}{2}$, both sides of this inequality are extreme at $\alpha = \frac{1}{2}$, which gives the estimate

$$-0.0711 \le \sum_{n\ge 1}\log|(1-q^n u)(1-q^n u^{-1})| \le 0.0665. \tag{26}$$

Combining (25) and (26) gives the desired inequalities and completes the proof of (c). □

We next estimate the difference of the local heights for the classical Weierstrass equation.

Proposition 5.4. *We have*

$$-0.973 - \frac{1}{8}\log^+|j(\tau)| \le \lambda(z) - \frac{1}{2}\log^+\left|\frac{\wp(z,\tau)}{\Delta(\tau)^{1/6}}\right| \le 1.07 + \frac{1}{12}\log^+|j(\tau)|.$$

Proof. Since $j(\tau)$ and $\wp(z,\tau)^6/\Delta(\tau)$ are $\mathrm{SL}_2(\mathbf{Z})$ invariant, we can apply a linear fractional transformation to τ to ensure that it satisfies the condition $(*)$. We then choose z modulo $\mathbf{Z}\tau + \mathbf{Z}$ so that

$$-\frac{1}{2} \le \alpha(z) = \frac{\operatorname{Im} z}{\operatorname{Im}\tau} \le \frac{1}{2}.$$

Since $\lambda(-z) = \lambda(z)$ and $\wp(-z,\tau) = \wp(z,\tau)$, we can replace z by $-z$, if necessary, to ensure that $0 \le \alpha \le \frac{1}{2}$. Thus we may assume that $(**)$ also holds.

We begin by applying Lemma 3.1 with

$$a = \left|\frac{1}{(2\pi i)^{12}}\wp(z,\tau)^6\right| \quad \text{and} \quad b = \left|\frac{1}{(2\pi)^{12}}\Delta(\tau)\right|.$$

Note that Lemma 5.2(c) and $(*)$ give the estimate

$$\log b \le \log|q| + 0.1045 \le -\pi\sqrt{3} + 0.1045 < 0, \quad \text{i.e., } |b| < 1,$$

so in this case Lemma 3.1 says that

$$0 \le \log^+\frac{a}{b} - \log^+ a \le -\log b.$$

Multiplying this by $-\frac{1}{12}$ gives

$$\frac{1}{12}\log\left|\frac{1}{(2\pi)^{12}}\Delta(\tau)\right| \le -\frac{1}{12}\log^+\left|\frac{\wp(z,\tau)^6}{\Delta(\tau)}\right| + \frac{1}{2}\log^+\left|\frac{1}{(2\pi i)^2}\wp(z,\tau)\right| \le 0. \tag{27}$$

Now add (27) to the estimate in Lemma 5.3(c), and then subtract half of the estimate in Lemma 5.3(b). Many of the terms cancel, and after a little bit of algebra we are left with

$$\begin{aligned} &-0.0665 - \log(1+|q|^{\alpha}) + \frac{1}{12}\log\left|\frac{1}{(2\pi)^{12}}\Delta(\tau)\right| \\ &\quad \le \lambda(z) - \frac{1}{12}\log^{+}\left|\frac{\wp(z,\tau)^6}{\Delta(\tau)}\right| + \frac{1}{2}B_2(\alpha)\log|q| \le 0.5964. \end{aligned}$$

Next subtract the B_2 term and, in the lower bound, use Lemma 5.2(c) to replace $\frac{1}{12}\log|\Delta(\tau)/q(2\pi)^{12}|$ by -0.105. This finally gives

$$\begin{aligned} &-0.1715 + \frac{\alpha(1-\alpha)}{2}\log|q| - \log(1+|q|^{\alpha}) \\ &\quad \le \lambda(z) - \frac{1}{12}\log^{+}\left|\frac{\wp(z,\tau)^6}{\Delta(\tau)}\right| \le 0.5964 - \frac{1}{2}B_2(\alpha)\log|q|. \end{aligned} \tag{28}$$

We first deal with the upper bound. Using Lemma 5.2(b) and $B_2(\alpha) \le \frac{1}{6}$, valid for $0 \le \alpha \le 1$, we find

$$\begin{aligned} 0.5964 - \tfrac{1}{2}B_2(\alpha)\log|q| &\le 0.5964 - \tfrac{1}{12}\log|q| \\ &\le 1.0697 + \tfrac{1}{12}\log^{+}|j(\tau)|. \end{aligned}$$

This and (28) complete the proof of the upper bound in Proposition 5.4.

To prove the lower bound, we use Lemma 5.2(b) and $(*)$, respectively, to obtain

$$\begin{aligned} \frac{\alpha(1-\alpha)}{2}\log|q| &\ge -2.8898\alpha(1-\alpha) - \frac{1}{8}\log^{+}|j(\tau)|, \\ -\log(1+|q|^{\alpha}) &\ge -\log(1+e^{-\pi\sqrt{3}\alpha}). \end{aligned}$$

Substituting these into (28) gives the lower bound

$$-0.1715 - \tfrac{1}{8}\log^{+}|j(\tau)| - 2.8898\alpha(1-\alpha) - \log(1+e^{-\pi\sqrt{3}\alpha}). \tag{29}$$

Now we reap the reward of keeping track of α in our estimates. Since the quantities $\alpha(1-\alpha)$ and $\log(1+|q|^{\alpha})$ cannot both be large, we gain (a bit) on the final estimate by considering them together. Precisely, one can check that

$$2.8898\alpha(1-\alpha) + \log(1+e^{-\pi\sqrt{3}\alpha}) \le 0.8010883\ldots \quad \text{for all } \alpha \in \mathbf{R},$$

the supremum occurring at $\alpha = 0.407582\ldots$. Substituting this into (29) completes the proof of Proposition 5.4. □

It remains to use the change-of-variable formula to go from a classical Weierstrass equation to a general equation.

Theorem 5.5. *Let $E/\mathbf{C}$ be an elliptic curve given by a Weierstrass equation*

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{30}$$

Let Δ, j, b_2, and 2^* be as in the statement of Theorem 1.1. Then for all $P \in E(\mathbf{C})$,

$$\begin{aligned} -\tfrac{1}{12}\log^+|\Delta| - \tfrac{1}{8}\log^+|j| - \tfrac{1}{2}\log^+|b_2/12| - \tfrac{1}{2}\log 2^* - 0.973 \\ \le \lambda(P) - \tfrac{1}{2}\log^+|x(P)| \\ \le \tfrac{1}{12}\log^+|\Delta^{-1}| + \tfrac{1}{12}\log^+|j| + \tfrac{1}{2}\log^+|b_2/12| + \tfrac{1}{2}\log 2^* + 1.07. \end{aligned}$$

Proof. Choose a τ with $j(\tau) = j(E)$, and let E' be given by the equation

$$E': Y^2 = 4X^3 - g_2(\tau)X - g_3(\tau).$$

Thus there is an isomorphism

$$\frac{\mathbf{C}}{\mathbf{Z}\tau + \mathbf{Z}} \xrightarrow{\sim} E'(\mathbf{C}), \qquad z \mapsto (\wp(z, \tau), \wp'(z, \tau)).$$

Choose $c \in \mathbf{C}^*$ and $r, s, t \in \mathbf{C}$ so that the map

$$x = c^2X + r, \qquad y = \tfrac{1}{2}c^3Y + sc^2X + t$$

gives an isomorphism $E'(\mathbf{C}) \cong E(\mathbf{C})$. Let $z \in \mathbf{C}/(\mathbf{Z}\tau + \mathbf{Z})$ be the point corresponding to $P \in E(\mathbf{C})$. Then

$$\lambda(P) - \tfrac{1}{2}\log^+|x(P)| = \lambda(z) - \tfrac{1}{2}\log^+|c^2\wp(z, \tau) + r|.$$

The usual change-of-variable formulas [10, Chapter III, §1] give $b_2 + 12r = c^2b_2' = 0$ and $\Delta = c^{12}\Delta(\tau)$. Hence,

$$\lambda(P) - \frac{1}{2}\log^+|x(P)| = \lambda(z) - \frac{1}{2}\log^+\left|\Delta^{1/6}\frac{\wp(z, \tau)}{\Delta(\tau)^{1/6}} - \frac{b_2}{12}\right|. \tag{31}$$

It is easy to check that

$$\begin{aligned} &\frac{\max\{|\wp(z, \tau)/\Delta(\tau)^{1/6}|, 1\}}{\max\{|\Delta^{-1/6}|, 1\} \cdot 2^* \cdot \max\{|b_2/12|, 1\}} \\ &\quad \le \max\left\{\left|\Delta^{1/6}\frac{\wp(z, \tau)}{\Delta(\tau)^{1/6}} - \frac{b_2}{12}\right|, 1\right\} \\ &\quad \le \max\left\{\left|\frac{\wp(z, \tau)}{\Delta(\tau)^{1/6}}\right|, 1\right\} \cdot \max\{|\Delta^{1/6}|, 1\} \cdot 2^* \cdot \max\left\{\left|\frac{b_2}{12}\right|, 1\right\}. \end{aligned}$$

Taking logarithms and substituting into (31) gives

$$\begin{aligned} -\frac{1}{12}\log^+|\Delta| - \frac{1}{2}\log 2^* - \frac{1}{2}\log^+\left|\frac{b_2}{12}\right| \\ \le \left\{\lambda(P) - \frac{1}{2}\log^+|x(P)|\right\} - \left\{\lambda(z) - \frac{1}{2}\log^+\left|\frac{\wp(z, \tau)}{\Delta(\tau)^{1/6}}\right|\right\} \\ \le \frac{1}{12}\log^+|\Delta^{-1}| + \frac{1}{2}\log 2^* + \frac{1}{2}\log^+\left|\frac{b_2}{12}\right|. \end{aligned}$$

Now applying Proposition 5.4 gives the desired result. □

6. Proof of the main theorems

In this section we add up our local estimates to prove the global theorems stated in §1.

Proof of Theorem 1.1. The canonical height $\hat{h}(P)$ is equal to the weighted sum of the local heights over all absolute values:

$$\hat{h}(P) = \frac{1}{[K:\mathbf{Q}]} \sum_{v \in M_K} n_v \lambda_v(P).$$

Similarly, for any $t \in K$, the ordinary height is

$$h(t) = \frac{1}{[K:\mathbf{Q}]} \sum_{v \in M_K} n_v \log^+ |t|_v.$$

In the lower bound in Theorem 5.5, we split the $\frac{1}{8}\log^+|j|$ as

$$\tfrac{1}{8}\log^+|j| = \tfrac{1}{24}\log^+|j| + \tfrac{1}{12}\log^+|j|.$$

Summing the estimates provided by Theorems 4.1(a) and 5.5 then gives

$$-\tfrac{1}{24}h(j) - \mu(E) - 0.973 \le \hat{h}(P) - \tfrac{1}{2}h(x(P)) \le \mu(E) + 1.07.$$

In the lower bound, note that $h_\infty(\Delta) = h(\Delta)$, since by assumption Δ is contained in the ring of integers of K. Likewise, in the upper bound we have used the identity $h(\Delta) = h(\Delta^{-1})$. This completes the proof of Theorem 1.1. □

Proof of Theorem 1.3. For equation (7) we have

$$b_2 = 0, \quad c_4 = -2^4 3A, \quad \Delta = -2^4(4A^3 + 27B^2), \quad j = 12^3 \frac{4A^3}{4A^3 + 27B^2}.$$

The conditions on A and B ensure that c_4 and the denominator of j are relatively prime; and the denominator of j is square-free. In other words, for every prime $p \in \mathbf{Z}$ dividing $4A^3 + 27B^2$ we have

$$\operatorname{ord}_p(j) = -1.$$

This means that in adding up these non-Archimedean local heights, we can use part (b) of Theorem 4.1 instead of part (a). We obtain the estimate

$$\tfrac{1}{12}\log|4A^3 + 27B^2| \le \sum_p (\lambda_p(P) - \tfrac{1}{2}\log^+|x(P)|_p).$$

Next we look at the unique Archimedean place. We apply Theorem 5.5 directly, which yields

$$\begin{aligned} &-\tfrac{1}{12}\log^+|16(4A^3 + 27B^2)|_\infty - \tfrac{1}{8}\log^+|j|_\infty - 0.973 \\ &\quad \le \lambda_\infty(P) - \tfrac{1}{2}\log^+|x(P)|_\infty. \end{aligned}$$

Adding the last two estimates then gives

$$-\tfrac{1}{8}\log^+|j| - 1.205 \le \hat{h}(P) - \tfrac{1}{2}h(x(P)).$$

This completes the proof of the first inequality in Theorem 1.3.

We suppose now in addition that $A > 0$. Then the above formula for j shows that $|j|_\infty \le 1728$. The second inequality in Theorem 1.3 is then immediate from the first. □

7. An application: Generators for the Mordell-Weil group

It is still an open problem to give an effective algorithm for computing generators of the Mordell-Weil group of an elliptic curve. The proof of the Mordell-Weil theorem falls into two parts. In the first part, if one is lucky, one finds generators for the quotient $E(K)/mE(K)$ for some small integer m (typically $m = 2$). It is then possible to refine this set into a set of generators for $E(K)$ itself; and this refinement process is effective. However, in practice one needs an effective estimate for the difference $\hat{h} - \frac{1}{2}h(x)$. We will illustrate this process for the three elliptic curves described in Examples 2.4, 2.5, and 2.6. For other examples, see [1, 3].

Example 7.1. Let $E/\mathbf{Q}$ be the elliptic curve

$$E : y^2 = x^3 - x + 1$$

considered in Example 2.4. Since $\#E(\mathbf{F}_3) = 7$ and $\#E(\mathbf{F}_5) = 8$, we see that $E(\mathbf{Q})$ has no torsion. A standard descent (cf. [2]) shows that the rank is at most 1, and a brief search for rational points turns up

$$(-1, 1),\ (0, 1),\ (1, 1),\ (3, 5),\ (5, 11). \tag{32}$$

Hence $E(\mathbf{Q})$ has rank 1, and it remains to find a generator.

Using the algorithm in [11], we compute the canonical height of these five points. The point $P = (1, 1)$ has the smallest height, $\hat{h}(P) = 0.0249\ldots$, and one can then check that the five listed points are (in order) $2P$, $-3P$, P, $-4P$, $5P$. We would like to show that P generates $E(\mathbf{Q})$.

Suppose not. Then $P = nR$ for some $n \ge 2$ and some $R \in E(\mathbf{Q})$. Further, since $x(P) \in \mathbf{Z}$, we see that also $x(R) \in \mathbf{Z}$. If such an R exists, then its height satisfies

$$\hat{h}(R) = \frac{1}{n^2}\hat{h}(P) \le \frac{1}{4}\hat{h}(P) = 0.0061\ldots.$$

Now we use the estimate (15) from Example 2.4, which says that

$$h(x(R)) \le 2\hat{h}(R) + 3.84 \le 3.86.$$

Hence, if R exists, then it satisfies $x(R) \in \mathbf{Z}$, and $|x(R)| \le e^{3.86} < 48$. Now it is a simple matter to check all integer values for x between -1 and 48. (If $x \le -2$, then $x^3 - x + 1 < 0$.) The only points which appear are the five points in (32). Therefore R does not exist, which completes the proof that

$$E(\mathbf{Q}) = \mathbf{Z}(1, 1).$$

Notice our computation uncovered all points with integral coordinates and canonical height less than 0.0061. In particular, it would have found any torsion points, which gives an alternative proof that $E(\mathbf{Q})$ is torsion-free.

The computation in Example 7.1 proceeded especially smoothly because $E(\mathbf{Q})$ had rank 1. When the rank is greater than 1, the following (unpublished) observation of Don Zagier is often helpful.

Proposition 7.2 (Zagier). *Let K be a number field and E/K an elliptic curve. For any real number B, let*

$$S(B) = \{P \in E(K) : \hat{h}(P) \le B\}.$$

Suppose that there is an integer $m \ge 2$ such that $S(B)$ surjects onto the group $E(K)/mE(K)$. Then $S(B)$ generates $E(K)$.

Proof. Let $G = \operatorname{Span}_{\mathbf{Z}} S(B)$. If $G \ne E(K)$, choose a $Q \in E(K) \setminus G$ with minimal height. This is possible, since $\hat{h}(E(K))$ is a discrete subset of $\mathbf{R}$. Since $Q \notin S(B)$, we have a strict inequality $\hat{h}(Q) > B$.

Choose a $P \in S(B)$ so that P and Q have the same image in $E(K)/mE(K)$, and write $P = Q + mR$ with $R \in E(K)$. Note that $R \notin G$. We will show that $\hat{h}(R) < \hat{h}(Q)$, which will contradict the choice of Q having minimal height, thereby proving that $G = E(K)$:

$$\begin{aligned}
\hat{h}(R) &= \frac{1}{m^2}\hat{h}(P - Q) \le \frac{2}{m^2}(\hat{h}(P) + \hat{h}(Q)) \\
&\le \frac{2}{m^2}(B + \hat{h}(Q)) \quad (\text{since } P \in S(B)) \\
&< \frac{4}{m^2}\hat{h}(Q) \quad (\text{since } Q \notin S(B)) \\
&\le \hat{h}(Q) \quad (\text{since } m \ge 2). \quad \square
\end{aligned}$$

Example 7.3. Let $E/\mathbf{Q}$ be the elliptic curve

$$E: y^2 = x^3 - x + 15$$

considered in Example 2.5. Since $\#E(\mathbf{F}_3) = 4$ and $\#E(\mathbf{F}_5) = 8$, we see that $E(\mathbf{Q})$ has at most 2-torsion; it is easy to check that $E(\mathbf{Q})[2] = 0$. Hence $E(\mathbf{Q})$ is torsion-free.

A standard descent (cf. [2]) should show that the rank is at most 2 (although I have not actually done the calculation), and a brief search for rational points turns up

$$P = (6, 15) \quad \text{and} \quad Q = (-2, 3). \tag{33}$$

We also note that

$$P + Q = \left(-\frac{7}{4}, -\frac{27}{8}\right).$$

Using [11], we compute the heights $\hat{h}(P) = 1.0217\ldots$, $\hat{h}(Q) = 0.7229, \ldots,$ and $\hat{h}(P+Q) = 1.4092\ldots$, and then the height regulator

$$\det \begin{pmatrix} \langle P, P\rangle & \langle P, Q\rangle \\ \langle P, Q\rangle & \langle Q, Q\rangle \end{pmatrix} = 0.7105\ldots.$$

Since the regulator is nonzero, P and Q are linearly independent.

Using the same procedure as in Example 7.1, it is easy to check that P, Q and $P+Q$ are not in $2E(\mathbf{Q})$. Hence the map

$$\{O, P, Q, P+Q\} \to E(\mathbf{Q})/2E(\mathbf{Q})$$

is surjective, assuming, as always, that $E(\mathbf{Q})$ has rank 2. Incidentally, this surjectivity proves anew that P and Q are independent.

We now apply Proposition 7.2, which says that $E(\mathbf{Q})$ is generated by the set

$$S = \{R \in E(\mathbf{Q}) : \hat{h}(R) \le \hat{h}(P+Q) = 1.4092\ldots\}.$$

From (16), any point in S satisfies

$$h(x(R)) \le 2\hat{h}(R) + 2.444 \le 5.27.$$

So if $R \in S$, and if we write $x(R) = a/d^2$ in lowest terms, then

$$\max\{|a|, d^2\} \le e^{5.27} < 195.$$

So finally we see that $E(\mathbf{Q})$ is generated by the set

$$S' = \left\{ \left(\frac{a}{d^2}, \frac{b}{d^3} \right) \in E(\mathbf{Q}) : |a| \le 194,\ 1 \le d \le 13,\ b \ge 0 \right\}.$$

Using a microcomputer, one finds that

$$\begin{aligned} S' &= \left\{ (-2, 3), (6, 15), \left(\frac{-7}{4}, \frac{27}{8}\right), \left(\frac{17}{16}, \frac{249}{64}\right) \right\} \\ &= \{Q, P, -P-Q, -P+Q\}. \end{aligned}$$

This completes the proof that

$$E(\mathbf{Q}) = \mathbf{Z}(-2, 3) \oplus \mathbf{Z}(6, 15),$$

subject to the assumption that rank $E(\mathbf{Q}) = 2$.

Example 7.4. We conclude by considering the curve

$$E: y^2 = x^3 - 28x - 48 = (x+4)(x+2)(x-6)$$

from Example 2.6. It is proven in [10, Chapter X, Example 1.5] that the group $E(\mathbf{Q})/2E(\mathbf{Q})$ is generated by the three points

$$P = (-3, 3), \quad Q_1 = (-2, 0), \quad Q_2 = (-4, 0).$$

Here, Q_1 and Q_2 are points of order 2, and P has infinite order. We wish to show that P, Q_1, Q_2 actually generate $E(\mathbf{Q})$.

Suppose that they do not generate $E(\mathbf{Q})$. Since Q_1, Q_2 have order 2 and since P, Q_1, Q_2 do generate $E(\mathbf{Q})/2E(\mathbf{Q})$, it follows that

$$P = mR \quad \text{for some } \textit{odd} \text{ integer } m \geq 3.$$

(That is, we must have $P + T = mR$ for some $T \in E[2]$ and some odd m, and then $P = m(R + T)$.) Hence,

$$\hat{h}(R) = \frac{1}{m^2}\hat{h}(P) = \frac{0.7222\ldots}{m^2} \leq 0.080\ldots.$$

It then follows from (17) that

$$h(x(R)) \leq 2\hat{h}(R) + 6.54 \leq 6.7.$$

Since also $x(R) \in \mathbf{Z}$, we must look for all points $R \in E(\mathbf{Q})$ with $x(R) \in \mathbf{Z}$ and $|x(R)| \leq e^{6.7} < 813$. A computer search finds all such points, namely

$$\begin{aligned}&\{(-4, 0), (-3, 3), (-2, 0), (6, 0), (14, 48), (16, 60)\}\\ &= \{Q_2, P, Q_1, Q_1 + Q_2, P + Q_1, -P + Q_2\}.\end{aligned}$$

This concludes the proof that

$$E(\mathbf{Q}) = \mathbf{Z}(-3, 3) \oplus \mathbf{Z}(-4, 0) \oplus \mathbf{Z}(-2, 0) \cong \mathbf{Z} \oplus \frac{\mathbf{Z}}{2\mathbf{Z}} \oplus \frac{\mathbf{Z}}{2\mathbf{Z}}.$$

Acknowledgment

I would like to thank Don Zagier for suggesting, both verbally and in his joint paper [3], that it would be worthwhile to improve the known estimates for the difference of heights on elliptic curves.

Bibliography

1. A. Bremner and J. W. S. Cassels, *On the equation* $Y^2 = X(X^2 + p)$, Math. Comp. **42** (1982), 257–264.
2. A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715–743.
3. J. P. Buhler, B. H. Gross, and D. B. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank* 3, Math. Comp. **44** (1985), 473–481.
4. V. A. Dem′janenko, *An estimate of the remainder term in Tate's formula*, Mat. Zametki **3** (1968), 271–278. (Russian)
5. M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), 419–450.
6. S. Lang, *Elliptic curves: Diophantine analysis*, Springer-Verlag, New York, 1978.
7. ——, *Elliptic functions*, 2nd ed., Springer-Verlag, New York, 1987.
8. ——, *Conjectured Diophantine estimates on elliptic curves*, Progr. Math. **35** (1983), 155–171.
9. J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211.
10. ——, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, New York, 1986.
11. ——, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), 339–358.

12. D. B. Zagier, *Large integral points on curves*, Math. Comp. **48** (1987), 425–436.
13. H. Zimmer, *On the difference of the Weil height and the Néron-Tate height*, Math. Z. **174** (1976), 35–51.

Department of Mathematics, Brown University, Providence, Rhode Island 02912
E-mail address: ma420000@brownvm.bitnet