New York Journal of Mathematics

New York J. Math. **6** (2000) 331–342.

The Canonical Height of an Algebraic Point on an Elliptic Curve

G. Everest and T. Ward

Abstract. We use elliptic divisibility sequences to describe a method for estimating the global canonical height of an algebraic point on an elliptic curve. This method requires almost no knowledge of the number field or the curve, is simple to implement, and requires no factorization. The method is ideally suited to searching for algebraic points with small height, in connection with the elliptic Lehmer problem. The accuracy of the method is discussed.

Contents

1. Introduction

Let K denote an algebraic number field, with ring of algebraic integers O_K, and E an elliptic curve defined over K, given by a generalized Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

with coefficients $a_1, \dots, a_6 \in O_K$. Let $Q = (x, y)$ denote a K-rational point of E, $Q \in E(K)$. The *global canonical height* is a function $\hat{h} : E(K) \to \mathbb{R}$ with the properties:

1. $\hat{h}(Q) = 0$ if and only if Q is a torsion point of $E(K)$.
2. $\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$ for all $P, Q \in E(K)$.

Received November 27, 2000.
Mathematics Subject Classification. 11G07.
Key words and phrases. Canonical heights, Elliptic divisibility sequences, Elliptic curves, Number fields, Elliptic Lehmer problem.

ISSN 1076-9803/00

The second property is known as the *parallelogram law*. The global canonical height is of fundamental importance in the arithmetic of elliptic curves, due in part to its functoriality. The height appears in basic conjectures such as Birch-Swinnerton-Dyer and there is a deep conjecture known as the *elliptic Lehmer problem*, see [HS90], concerning lower bounds for the height. Besides theoretical considerations however, it sometimes happens that one really wishes to compute the value of the height (for example, to compute the determinant of the height-regulator matrix in searching for curves of large rank).

Silverman [Sil88] described an algorithm for computing the global height, which can be made arbitrarily accurate. In the rational case, this is implemented in Pari-GP (see [GP]). The algorithm in [Sil88] requires the discriminant of the curve to be completely factored; computing the height when the discriminant cannot be factored in reasonable time is considered in [Sil97]. Silverman's method requires much less than the full factorization of the discriminant but still requires some factorization. In principle, the method extends to the general algebraic case, though there is currently no implementation of Silverman's algorithm in the general case. When it is implemented, it is likely to enjoy the same high accuracy it does in the rational case. However there seems to be a small class of curves for which it is vulnerable (see Examples 7 and 10 in Section 4).

Tate's definition of the global height gives a factorization-free approach to computing the global height. Let M_K denote the set of valuations of K, each one corresponding to an absolute value $|\cdot|_v$ (see [Wei74] for background). For each valuation $v \in M_K$, let K_v denote the corresponding completion of K. The *naive height* $h(\alpha)$ of $\alpha \in K$ is

$$h(\alpha) = \frac{1}{d} \sum_{v \in M_K} \log \max\{1, |\alpha|_v\}. \tag{2}$$

For a finite point $Q \in E(K)$, set $h(Q) = h(x(Q))$, and for Q the point at infinity set $h(Q) = 0$. Tate's definition of the global canonical height is

$$\hat{h}(Q) = \frac{1}{2} \lim_{n \to \infty} 4^{-n} h(2^n Q). \tag{3}$$

Knowledge of the naive height is essentially equivalent to knowledge of the minimal polynomial.

Tate's definition is not usually considered to be a very useful method for actually computing the height. In principle it is accurate: However, it requires the computation of large integers and this not only slows it down but makes high accuracy impossible in practice. On the other hand, it does always give an answer because no factorization is needed.

The aim of this note is to exhibit an alternative factorization-free method for computing the global height of an algebraic point on an elliptic curve which stands somewhere between the two algorithms above. Like the method in (3), ours is extremely simple, requiring almost no knowledge of the number field or the elliptic curve and it does not require the curve to be in minimal form. However, our method gives more information than (3) since it also yields the archimedean and non-archimedean parts of the height separately. (If the factorization of the discriminant is known then it will give a complete decomposition of the global height as a sum of local heights.) Our method can also be made much quicker. It gives less accuracy than Silverman's algorithm but high accuracy is not always required. In certain cases, our method can be used in tandem with Silverman's algorithm: see Example 9 in Section 4.

An example of a calculation which does not require great accuracy is the search for algebraic points with small height. This requires an accuracy of only 3 or 4 significant figures together with an easy way of handling algebraic number fields. Calculations such as these would shed light on the elliptic Lehmer problem. In the classical Lehmer problem and its derivatives (see [EW99]) there are many numerical examples. Up to now, there is very little data for the elliptic Lehmer problem outside the rational case. To illustrate our method, we give a couple of examples of small height points found with an easy search: See Examples 11 and 12 in Section 4. Our method uses *elliptic divisibility sequences*, which are sequences associated to the division points on the curves. At the conclusion of the paper, we will make the point that our methodology not only gives a simple way of handling elliptic curves over algebraic number fields; it also throws up the possibility that small height points might be found more efficiently by searching for growth rates of elliptic divisibility sequences.

2. Elliptic divisibility sequences

The essential ingredient in the approach taken here is the sequence of *elliptic division polynomials*. For background on elliptic curves see [Sil86] and [Sil94].

Definition 1. With the notation of (1), define

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1 a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2. \end{aligned}$$

Define a sequence (ψ_n) of polynomials in $O_K[x,y]$ as follows: $\psi_0 = 0, \psi_1 = 1$,

$$\begin{aligned} \psi_2 &= 2y + a_1 x + a_3, \\ \psi_3 &= 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8, \text{ and} \\ \psi_4 &= \psi_2(2x^6 + b_2 x^5 + 5b_4 x^4 + 10b_6 x^3 + 10b_8 x^2 + (b_2 b_8 - b_4 b_6)x + b_4 b_8 - b_6^2). \end{aligned}$$

Now define inductively for $n \geq 2$

$$\begin{aligned} \psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \text{ and} \\ \psi_{2n}\psi_2 &= \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2). \end{aligned}$$

It is straightforward to check that each $\psi_n \in O_K[x,y]$. It is known that ψ_n^2 is a polynomial in x alone having degree $n^2 - 1$ and leading coefficient n^2. The zeros of ψ_n^2 are the x-coordinates of the points on E with order dividing n. Write $\psi_n(Q)$ for ψ_n evaluated at the point $Q = (x,y)$. The sequence $\psi_n(Q)$ is known as an *elliptic divisibility sequence*: Writing $u_n = \psi_n(Q)$ gives the elliptic recurrence relation

$$u_{m+n}u_{m-n} = u_{m+1}u_{m-1}u_n^2 - u_{n+1}u_{n-1}u_m^2 \tag{4}$$

for all $m \geq n \geq 0$. These elliptic divisibility sequences were studied in an abstract setting by Morgan Ward in a series of papers—see [War48] for the details. Shipsey's thesis [Shi00] contains more recent applications of these sequences, which satisfy the same recursion formulæ as the division polynomials. If Q is not a torsion point then the terms of the sequence $(\psi_n(Q))$ are always non-zero. The single relation (4) gives rise to the two relations

$$u_{2n+1} = u_{n+2}u_n^3 - u_{n-1}u_{n+1}^3, \quad \text{and} \tag{5}$$

$$u_{2n}u_2 = u_{n+2}u_n u_{n-1}^2 - u_n u_{n-2}u_{n+1}^2. \tag{6}$$

For computational purposes, it is useful to notice that the two relations (5) and (6) can be subsumed into the single relation

$$u_n u_{\lfloor n/\lfloor (n+1)/2\rfloor\rfloor} = u_{\lfloor (n+4)/2\rfloor}u_{\lfloor n/2\rfloor}u_{\lfloor (n-1)/2\rfloor}^2 - u_{\lfloor (n+1)/2\rfloor}u_{\lfloor (n-3)/2\rfloor}u_{\lfloor (n+2)/2\rfloor}^2,$$

where $\lfloor\cdot\rfloor$ denotes, as usual, the integer part.

Write

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \in O_K \tag{7}$$

for the discriminant of the curve E. The valuations v with $|\Delta|_v < 1$ are precisely the valuations corresponding to primes at which E reduces to a singular curve. Let $D = N_{K|\mathbb{Q}}(\Delta)$ and write T for the set of rational primes which divide D. Given an algebraic integral point $Q \in E(K)$, let

$$E_n = |N_{K|\mathbb{Q}}(\psi_n(Q))| \text{ and } F_n = |E_n| \prod_{p\in T} |E_n|_p.$$

Our method comes from the following theorem.

Theorem 2. *Let Q denote an algebraic integral point on $E(K)$. Then*

$$\hat{h}(Q) = \frac{1}{d}\lim_{n\to\infty}\frac{1}{n^2}\log F_n. \tag{8}$$

The total archimedean contribution is the limit

$$h_\infty(Q) = \frac{1}{d}\lim_{n\to\infty}\frac{1}{n^2}\log E_n. \tag{9}$$

The formula (8) is independent of the equation defining the curve. It might appear that a factorization of the discriminant is required but that is not so. Later we discuss the practicalities of implementing the method. The method extends to rational points provided one knows the valuations at which the x-coordinate is not integral. The denominator can be cleared to obtain an integral point on a curve isomorphic to the starting curve, so the height is unchanged. The proof of Theorem 2 follows in the next section. It uses some detailed knowledge of local heights. For readers interested only in the application of the formula, the next section can be skipped.

3. Local and global heights

The global height is known to be expressible as a sum of local heights, one for each element of M_K. There is a function, continuous away from infinity, $\lambda_v : E(\mathbb{Q}_v) \to \mathbb{R}$ which satisfies the *local parallelogram law*

$$\lambda_v(P+Q) + \lambda_v(P-Q) = 2\lambda_v(Q) + 2\lambda_v(P) - \log|x(Q)-x(P)|_v. \tag{10}$$

Let $n_v = [K_v : \mathbb{Q}_w]/[K : \mathbb{Q}]$ denote the usual local normalizing constants, where v lies above w on $\mathbb{Q}$. Then

$$\hat{h}(Q) = \sum_{v \in M_K} n_v \lambda_v(Q). \tag{11}$$

The fundamental observation behind our method is the *elliptic Jensen formula* from [EF96]. If G is a compact group containing Q, with normalized Haar measure μ_G, then

$$\lambda_v(Q) = 2 \int_G \log |x(P) - x(Q)|_v \, d\mu_G(P) \tag{12}$$

by integrating and cancelling three terms in (10).

If it is required that the expression $\lambda_p(Q) - \frac{1}{2} \log |x(Q)|_p$ be bounded as $Q \longrightarrow 0$, then there is only one such map, the *canonical local height*. It is important to note that in [Sil94], local heights are normalized to make them invariant under isomorphisms. This involves adding a constant which depends on the discriminant of E. The local heights in [Sil94] satisfy a different form of (10).

There are explicit formulæ for each of the local heights (see [Sil86] and [Sil94], or [Eve99] for an alternative approach). For non-archimedean valuations v where Q has good reduction,

$$\lambda_v(Q) = \tfrac{1}{2} \log \max\{1, |x(Q)|_v\}. \tag{13}$$

Notice in particular that if $x(Q)$ is integral at v and Q has good reduction at v then $\lambda_v(Q) = 0$. The bad reduction case is more involved but we need to deal only with *split multiplicative reduction* (see [Sil94, p. 362] for details on this). This is because we may pass to an extension field where the reduction becomes of this type—the local height is functorial in the sense that it respects this passage. In the split multiplicative case, the points on the curve are isomorphic to the points on the Tate curve $K_v^*/q^{\mathbb{Z}}$, where $q \in K_v^*$ has $|q|_v < 1$. The explicit formulæ for the x and y coordinates of a non-identity point are given in terms of the uniformizing parameter $u \in K_v^*$ by

$$\begin{aligned} x = x_u &= \sum_{n \in \mathbb{Z}} \frac{q^n u}{(1 - q^n u)^2} - 2 \sum_{n \geq 1} \frac{n q^n}{(1 - q^n)^2}, \\ y = y_u &= \sum_{n \in \mathbb{Z}} \frac{q^{2n} u^2}{(1 - q^n u)^3} + \sum_{n \geq 1} \frac{n q^n}{(1 - q^n)^2}. \end{aligned}$$

It is clear that $x_u = x_{uq}$ and $x_u = x_{u^{-1}}$. Suppose Q corresponds to the point $u \in K_v^*$ and assume, by invariance under multiplication by q, that u lies in the fundamental domain $\{u \mid |q|_v < |u|_v \leq 1\}$. Then (by [Eve99] or [Sil94]), writing $\rho = \log |u|_v / \log |q|_v$,

$$\lambda_v(Q) = \begin{cases} -\log |1 - u|_v & \text{if } |u|_v = 1, \\ \frac{1}{2}(\rho - \rho^2) \log |q|_v & \text{if } |u|_v < 1. \end{cases}$$

Notice that for $|u|_v = 1$, the local height is non-negative, while if $|u|_v < 1$ the local height is negative.

Theorem 3. *Let Q denote a non-torsion integral point. Suppose $v|\infty$ or v corresponds to a prime of singular reduction. In the latter case, assume equation* (1) *is* *in minimal form. Then there are positive constants A and $B < 2$ such that*

$$\frac{1}{n^2}\log|\psi_n(Q)|_v = \lambda_v(Q) + \begin{cases} O((\log n)^A/n^2) & \text{if } v|\infty, \\ O(1/n^B) & \text{otherwise.} \end{cases} \tag{14}$$

Proof. If $v|\infty$, we claim first that

$$\lim_{n\to\infty} n^{-2}\log|\psi_n(x(Q))|_v = \lambda_\infty(Q). \tag{15}$$

Formula (15) was proved in the rational case in [EW99, Theorem 6.18]; the proof is sketched here in the general case. The height is functorial in the sense that it respects field extensions. Thus we may assume v corresponds to an embedding of K into $\mathbb{C}$. Take $G = E(\mathbb{C})$ in the elliptic Jensen formula (12). The points of n-torsion are dense and uniformly distributed in $E(\mathbb{C})$ as $n \to \infty$, so the limit sum over the torsion points will tend to the integral when the integrand is continuous. Note that the torsion points occur in pairs usually. Working with $\psi_n(Q)$ they only occur with multiplicity 1, hence the formula differs from the usual elliptic Jensen formula in this respect. The only potential problem arises from torsion points close to Q: by [Dav95], for $x = x(Q)$ with $nQ = 0$, $|x - x(Q)|_v > n^{-C}$ for some $C > 0$ which depends on E and Q only. This inequality is enough to imply that the Riemann sum given by the n-torsion points for $\log|x - x(Q)|_v$ converges, which gives (15), and the explicit error term gives the estimate in (14).

Assume now that v is non-archimedean, corresponding to a prime of singular reduction. Let Ω_v denote any complete, algebraically closed field containing K_v. Assume Q is integral, $|x(Q)|_v \le 1$. Now use the parametrisation of the curve described before. The points of order dividing n on the Tate curve are precisely those of the form $\zeta^i q^{j/n}$, $1 \le i, j \le n$, where $\zeta \in \Omega_v$ denotes a fixed, primitive nth root of unity in Ω_v. We claim that

$$\lim_{n\to\infty} n^{-2}\log|\psi_n(x(Q))|_v = \lambda_v(Q). \tag{16}$$

Let G denote the closure of the torsion points: G is not compact, so the v-adic elliptic Jensen formula cannot be used. Instead we use a variant of the Shnirelman integral: for $f : E(\Omega_v) \to \mathbb{R}$ define the elliptic Shnirelman integral to be

$$\int_G f(Q)\mathrm{d}Q = \lim_{n\to\infty} n^{-2}\sum_{n\tau=0} f(\tau)$$

whenever the limit exists.

We claim firstly that for any $P \in E(\mathbb{Q}_p)$, the Shnirelman integral

$$\int_G \lambda_v(P+Q)\mathrm{d}Q = S(E) \text{ exists and is independent of } P. \tag{17}$$

First assume that P is the identity. Using the explicit formula for the local height gives

$$-n^{-2}\sum_{i=1}^{n-1}\log|1-\zeta^i|_v - n^{-2}\sum_{i=0}^{n-1}\sum_{j=1}^{n-1}\frac{k}{2}\left(\frac{j}{n} - \left(\frac{j}{n}\right)^2\right)\log|q|_v. \tag{18}$$

The first sum is bounded by $\log|n|_v/n$, which vanishes in the limit; the second sum converges to $-\frac{k}{12}$. For the general case, let P correspond to the point u on the multiplicative Tate curve. If for some large n no j has $|q^{j/n}u|_v = 1$ then the analogous sum to (18) is close to $-\frac{k}{12}$ by the same argument. Assume therefore that there is a j with this property. Then the first sum in (18) is replaced by

$$-n^{-2}\sum_{i=0}^{n-1}\log|1-q^{j/n}u\zeta^i|_v - n^{-2}\log|1-(q^r u)^n|_v, \tag{19}$$

where $r = j/n$ only depends on u. By v-adic elliptic transcendence theory (see [Dav95]), there is a lower bound for $\log|1-(q^r u)^n|_v$ of the form $-(\log n)^A$, where A depends on E and $u = u(P)$ only. It follows that the first sum vanishes in the limit as before. The second sum in (18) is simply rearranged under rotation by u, so converges to $-\frac{k}{12}$ as before. This proves (17).

The claimed limit (16) now follows by taking the elliptic Shnirelman integral of both sides of the parallelogram law (10) and noting that we count torsion points in pairs. Equation (17) shows that three terms cancel to leave the required limit. The error term in (14) comes from the lower bound used above. □

These estimates are enough to prove the main formula.

Proof of Theorem 2. It will be convenient to use normalized heights, so define

$$\nu_v(Q) = \lambda_v(Q) - \tfrac{1}{12}\log|\Delta|_v.$$

Then ν_v is invariant under isomorphism (see [Sil94]). By the product formula,

$$\hat{h}(Q) = \sum_v n_v\nu_v(Q) = \sum_v n_v\lambda_v(Q).$$

Also, by Theorem 3,

$$\lim_{n\to\infty}\frac{1}{n^2}\log|\psi_n(Q)\Delta^{-n^2/12}|_v = \nu_v(Q). \tag{20}$$

For any $\alpha \in K$, $|N_{K|\mathbb{Q}}(\alpha)| = \prod_{v|\infty}|\alpha|_v$. Therefore, using the product formula again,

$$\log|F_n| = \sum_{v|\infty}\log|\psi_n(Q)\Delta^{-n^2/12}|_v + \sum_{|\Delta|_v<1}|\psi_n(Q)\Delta^{-n^2/12}|_v.$$

The reason for introducing the factor $\Delta^{-n^2/12}$ is to take account of the possibility that the equation (1) is not in minimal form at some non-archimedean v corresponding to a prime of singular reduction. The change of coordinates to put the equation into minimal form is an isomorphism, so it leaves the local height $\nu_v(Q)$ invariant. Now Theorem 2 follows directly from Theorem 3. □

4. Examples

It appears as though we need to factor $D = N_{K|\mathbb{Q}}(\Delta)$ in order to apply Theorem 2. However, Theorem 3 says that for a prime $p \in T$, $|E_n|_p$ is approximately l^{n^2} where l is the total contribution to the height from the valuations which extend $|\cdot|_p$. Therefore, asymptotically, it suffices to compute the gcd of E_n with a suitably high power of D. Since the local height is $t\log|\Delta|_v$ for some $0 \le t \le 1$, the power of D can be n^2. This is likely to be a huge number and there are ways to avoid making this computation. In practice, it is often sufficient to find the gcd of E_n and E_{n+1}. In other words:

$$\hat{h}(Q) = \frac{1}{d} \lim_{n\to\infty} \frac{1}{n^2} \log \left(\frac{E_n}{\gcd(E_n, E_{n+1})} \right). \tag{21}$$

In the last section of the paper, we will discuss other ways to speed up the calculations.

The following examples were calculated using Pari-GP, see [GP], simply applying the basic formula (21). In the main we have only exhibited calculations which were executed within a few seconds at most. We begin by applying our method to examples in the literature—the first two examples come from [Sil88].

Example 4. Let the curve be

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

the field $K = \mathbb{Q}(\sqrt{-2})$, and $Q = (2 + \sqrt{-2}, 1 + 2\sqrt{-2})$. Taking $n = 100$ gives $\hat{h}(Q) \sim .45744\ldots$ to be compared with Silverman's accurate value of $.45754\ldots$. When $n = 200$, we obtain the better approximation $\hat{h}(Q) \sim .45753\ldots$.

Example 5. Let $K = \mathbb{Q}(i)$, let the curve be

$$E : y^2 + 4y = x^3 + 6ix,$$

and $Q = (0, 0)$. Taking $n = 200$ gives $\hat{h}(Q) \sim .33688\ldots$ to be compared with Silverman's accurate value of $.33689\ldots$ The archimedean height is $\sim .51016\ldots$

The next example illustrates that the curve does not need to be in minimal form for the method to work.

Example 6. Let the curve be

$$E : y^2 = x^3 - 16x + 16,$$

and let $Q = (0, 4)$. Taking $n = 150$ gives a value $\hat{h}(Q) \sim .02549\ldots$ with a value $\sim .7186\ldots$ for the archimedean component. The calculation speeds up if we notice that E is isomorphic to the curve $y^2 + y = x^3 - x$, with Q mapping to $P = (0, 0)$ under the isomorphism. Taking $n = 150$ gives $\hat{h}(P) = \hat{h}(Q) \sim .02555\ldots$ which is more accurate, and quicker, due to the slower growth rate of the sequence E_n.

The next examples are manufactured to highlight one of the strengths of our approach: It always gives an answer even if a tricky factorization appears to be necessary. Silverman's approach in [Sil97] computes all the local heights then sums these to give the global height. To compute a local non-archimedean height, the curve needs to be in minimal form for that valuation. If the factorization of Δ is known then the curve can easily be rendered in minimal form for each valuation corresponding to the prime factors of Δ. Even if the factorization is not known, it is usually possible to proceed. With our earlier notation, define

$$c_4 = b_2^2 - 24b_4 \text{ and } c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

In [Sil97], working over $\mathbb{Q}$, Silverman shows that if the factorization of $c = \gcd(c_4, c_6)$ is known then the curve can be put in global minimal form so the local heights can all be computed. Over a number field with class number greater than 1, a global minimal equation will not always exist. Presumably the same kind of argument would work nonetheless. Therefore, the next example is chosen to highlight a potential difficulty: c may have a large gcd with the discriminant. In this case, factorizing c is not much easier than factorizing the discriminant.

Example 7. Let $K = \mathbb{Q}$ and let $m \in \mathbb{N}$ denote an integer that is not factorizable in reasonable time. Consider the curve

$$E : y^2 = x^3 + mx + m^2.$$

Let Q denote the point $(0, m) \in E(K)$. For this curve, $m|c$ and Silverman's algorithm now requires auxiliary arguments (see Remark 8 below). Let $m = pq$ where p and q denote the next primes after 10^{30} and 10^{40}. With $n = 50$, within a minute, our method gave $\hat{h}(Q) \sim 13.657\ldots$ with an archimedean height $\sim 53.936\ldots.$ We also used a floating point for the archimedean contribution: with $n = 300$ we obtained $\sim 53.956\ldots.$ The Pari-GP routine for computing heights returned a warning that the calculation would take several hours. This is all due to the difficulty of factorizing m.

Remark 8. The referee pointed out to us that Silverman's method can be made to work in this example because it can be checked that no 4th power of a prime divides m.

The next example shows how our method can be used in tandem with Silverman's algorithm.

Example 9. With E as in the previous example, let Q denote an algebraic point with $x(Q) = 1$. Even a small value of n shows the total non-archimedean contribution is zero. Thus one may revert immediately to a general algebraic version of Silverman's method to obtain a very accurate value for the global height, which is entirely concentrated at the archimedean valuation. Using our method, with $n = 300$ and with floating point arithmetic on the two archimedean valuations, we obtained the value $\sim 53.956\ldots$ for the total archimedean contribution. Note the value is close to the previous example—this is no real surprise, as the archimedean heights are continuous.

Our next example is an algebraic version of Example 7.

Example 10. Let $f(x) = x^{17} + x + 996$ and let $K = \mathbb{Q}(\rho)$ where ρ denotes any root of $f(x)$. Let $\theta = 1 - 1728\rho^2$, and consider the curve

$$E : y^2 = x^3 + \theta x + \theta^2.$$

Let Q denote the point $(0, \theta) \in E(K)$. With $n = 35$, in under one minute our method gives $\hat{h}(Q) \sim 15.595\ldots.$ The archimedean height is $\sim 50.732\ldots.$ As in the previous example, $\theta|c$. It took Pari-gp 30 minutes to find the factorization

$$C = 11978293086538309 \times 90441402774074985639455903784497233593419557 1$$

of $C = |N_{K|\mathbb{Q}}(\theta)|$; it would have taken at least as long to factor the ideal (c).

Finally, we give two examples of small height points over algebraic number fields. Our method is simple to apply and can be used to search for small height points in connection with the elliptic Lehmer problem. There is very little data associated with this problem beyond the rational case. We hope our paper might inspire an attempt to gather some data.

Example 11. Let w denote a non-trivial cube root of unity and $K = \mathbb{Q}(w)$. Let E be the elliptic curve

$$y^2 = x^3 - 243x + 3726 + 10368w.$$

The point $Q = (3 - 12w, -108w^2)$ has global height $\hat{h}(Q) \sim .01032\ldots$. This was found taking $n = 512 = 2^9$ and using Shipsey's algorithm from the next section. Although the coefficients of the curve might seem large, this example arises from a simple elliptic divisibility sequence. Starting from the sequence $0, 1, 1 + w, 1 + w, 1+w, \ldots$ we used Morgan Ward's formulæ (see [War48, p. 50]) to obtain a point on a curve with coefficients in K whose denominators can be cleared to give E as above.

Example 12. Let $u = (1 + \sqrt{5})/2$ and $K = \mathbb{Q}(u)$. The curve E is

$$y^2 = x^3 + (-2214 + 1215u)x + 40878 - 23328u$$

and the point is $Q = (3 - 9u, 108 - 108u)$. Taking $n = 512$ as before gives $\hat{h}(Q) \sim .00971\ldots$. This example came from the elliptic divisibility sequence which begins in the modest way $0, 1, 1-u, -2+u, 5-3u, \ldots$ Inverting this sequence gives a point on a curve over K and clearing the denominators gives E as above.

Two comments need to be made about these examples. Firstly, although these heights are small, no records have been broken. The elliptic Lehmer problem predicts a lower bound for $d\hat{h}(Q)$ where d is the degree of the number field. Multiplying both the above by 2 shows these values are not smaller than the height ($\sim .01028$) of the rational point $Q = (13, 33)$ on the curve $y^2 + xy + y = x^3 - x^2 - 48x + 147$, which appears in [Sil94, p. 480]. Secondly, these examples hint at an interesting possibility concerning the search for small height points. Perhaps restricting to elliptic divisibility sequences represents an efficiency gain in the sense that small height points will arise from sequences whose first few terms are arithmetically simple.

5. Accuracy

In (14), the error term is estimated using methods from elliptic transcendence theory. In [EEW], we investigated the error in practice and found it to be about $O(1/n^2)$, even for quite modest values of n. For small values of n, the values of E_n can be computed easily using Pari-GP. Several options for achieving greater accuracy are listed below. However, we stress again that there are certain physical limits to this method which go beyond computational considerations: Accuracy of 80 significant figures would involve computing a number with approximately 10^{40} decimal digits. Even storing such numbers is beyond the capabilities of any computer.

1. The archimedean and non-archimedean contributions can be computed separately and this allows the computations to be speeded up. For the archimedean contribution, we can use floating point arithmetic which greatly enhances the speed. For the non-archimedean contribution, we only have to keep a running total of the gcd so big integer arithmetic can be avoided. If the factorization of the discriminant is known then p-adic arithmetic may be used.

2. Since the computation of the height involves big numbers, it is useful to use a package which allows these to be handled efficiently. We are grateful to

John Cannon for implementing our algorithm in Magma [Mag] which gave greater accuracy.

3. Memory is clearly an issue with the method we are describing since it involves the calculation of huge numbers. Storage can be maximized by computing E_n for special n, without needing to know all E_m for $m < n$. Shipsey [Shi00] gives an algorithm that computes E_n in $O(\log n)$ arithmetic operations. Note the distinction between arithmetic operations and bit operations: By arithmetic operation is meant one of the familiar operations of adding or multiplying. The special case where $n = 2^N$ is especially easy to implement and we describe it below. We are grateful to Rachel Shipsey for her permission to include it here.

Now follows Shipsey's algorithm for computing E_n when $n = 2^N$: Given Q and E, find $\psi_i(Q)$ for $i = 2, 3, \ldots, 7$ using the formulae given before. Let

$$T_1 = 1, \quad U_1 = \psi_2(Q), \quad V_1 = \psi_3(Q), \quad W_1 = \psi_4(Q),$$
$$X_1 = \psi_5(Q), \quad Y_1 = \psi_6(Q), \quad Z_1 = \psi_7(Q),$$

and then inductively

$$\begin{aligned} T_{n+1} &= W_n U_n^3 - V_n^3 T_n, \\ U_{n+1} &= (V_n/\psi_2(Q))(X_n U_n^2 - T_n W_n^2), \\ V_{n+1} &= X_n V_n^3 - W_n^3 U_n, \\ W_{n+1} &= (W_n/\psi_2(Q))(Y_n V_n^2 - U_n X_n^2), \\ X_{n+1} &= Y_n W_n^3 - X_n^3 V_n, \\ Y_{n+1} &= (X_n/\psi_2(Q))(Z_n W_n^2 - V_n Y_n^2), \\ Z_{n+1} &= Z_n X_n^3 - Y_n^3 W_n. \end{aligned}$$

After $N - 2$ iterations the value of W is $\psi_n(Q)$, and $E_n = |N_{K|\mathbb{Q}}(\psi_n(Q))|$.

Computing E_n requires $O(\log n)$ arithmetic operations. The operations required for (3) satisfy the same bound. However, our method can be speeded up in two ways. Firstly, by using floating point arithmetic for the archimedean contribution. Secondly, the homogeneity of the formulæ make it possible to keep a running total for the gcd computation, yielding the non-archimedean contribution. By successively factoring out the gcd, the calculations proceed with smaller integers, making the method much faster.

References

[Dav95] Sinnou David, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France (N.S.) (1995), no. 62, MR 98f:11078, Zbl 859.11048.

[EEW] M. Einsiedler, G. Everest and T. Ward. *Primes in elliptic divisibility sequences*, preprint.

[EF96] G. R. Everest and Bríd Ní Fhlathúin, *The elliptic Mahler measure*, Math. Proc. Cambridge Philos. Soc. **120** (1996), no. 1, 13–25, MR 97e:11064, Zbl 865.11068.

[Eve99] Graham Everest, *Explicit local heights*, New York J. Math. **5** (1999), 115–120, MR 2000g:11050.

[EW99] Graham Everest and Thomas Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics*, Springer-Verlag London Ltd., London, 1999, MR 2000e:11087, Zbl 919.11064.

[HS90] Marc Hindry and Joseph H. Silverman, *On Lehmer's conjecture for elliptic curves*, Séminaire de Théorie des Nombres, Paris 1988–1989, Prog. Math. **91** (1990), 103–116, MR 92e:11062, Zbl 741.14013.

[GP] Pari-GP, `http://www.parigp-home.de`.

[Mag] Magma, `http://www.maths.usyd.edu.au:8000/u/magma`.

[Shi00] Rachel Shipsey. *Elliptic Divisibility Sequences.* PhD thesis, University of London (Goldsmiths), 2000.

[Sil86] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, no. 106, Springer-Verlag, New York, 1986, MR 87g:11070, Zbl 585.14026.

[Sil88] Joseph H. Silverman, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), no. 183, 339–358, MR 89d:11049, Zbl 656.14016.

[Sil94] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, no. 151, Springer-Verlag, New York, 1994, MR 96b:11074, Zbl 911.14015.

[Sil97] Joseph H. Silverman, *Computing canonical heights with little (or no) factorization*, Math. Comp. **66** (1997), no. 218, 787–805, MR 97f:11040, Zbl 898.11021.

[War48] Morgan Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31–74, MR 9,332j, Zbl 035.03702.

[Wei74] André Weil, *Basic Number Theory*, third ed., Springer-Verlag, New York, 1974, Die Grundlehren der Mathematischen Wissenschaften, Band 144, MR 55 #302, Zbl 326.12001.

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK.
g.everest@uea.ac.uk http://www.mth.uea.ac.uk/~h090/

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK.
t.ward@uea.ac.uk http://www.mth.uea.ac.uk/~h720/

This paper is available via http://nyjm.albany.edu:8000/j/2000/6-16.html.