MATHEMATICS OF COMPUTATION
Volume 66, Number 218, April 1997, Pages 787–805
S 0025-5718(97)00812-0

COMPUTING CANONICAL HEIGHTS WITH LITTLE (OR NO) FACTORIZATION

JOSEPH H. SILVERMAN

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve with discriminant Δ, and let $P \in E(\mathbb{Q})$. The standard method for computing the canonical height $\hat{h}(P)$ is as a sum of local heights $\hat{h}(P) = \hat{\lambda}_\infty(P) + \sum_p \hat{\lambda}_p(P)$. There are well-known series for computing the archimedean height $\hat{\lambda}_\infty(P)$, and the non-archimedean heights $\hat{\lambda}_p(P)$ are easily computed as soon as all prime factors of Δ have been determined. However, for curves with large coefficients it may be difficult or impossible to factor Δ. In this note we give a method for computing the non-archimedean contribution to $\hat{h}(P)$ which is quite practical and requires little or no factorization. We also give some numerical examples illustrating the algorithm.

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

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

The *canonical height* on E is a quadratic form

$$\hat{h} : E(K) \longrightarrow \mathbb{R}.$$

The canonical height is an extremely important theoretical and computational tool in the arithmetic study of elliptic curves. See [18, Chapter VIII, Section 9] for the definition and basic properties of $\hat{h}$, and [20], [21], and [23] for some discussion of how to compute $\hat{h}$ in practice. In this paper, which may be considered as a continuation of our earlier note [20], we will discuss the computation of the canonical height for curves E whose coefficients $a_1, \dots, a_6$ are large. We note that this is not a mere intellectual exercise, since curves with huge integer coefficients have already made their appearance in the search for curves whose Mordell-Weil group $E(\mathbb{Q})$ has large rank [5], [11], [12], [13], [14], and the standard tool for proving that a set of points $P_1, \dots, P_r \in E(\mathbb{Q})$ is linearly independent is to check the non-vanishing of the height regulator matrix $\det\big(\langle P_i, P_j\rangle\big)$. Here the height pairing $\langle \cdot, \cdot \rangle$ is defined (up to a normalizing factor) by the formula

$$\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

Tate's definition $\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h\big(x(2^nP)\big)$ of the canonical height is not practical for numerical computations. Instead, one uses the Néron-Tate decomposition of the canonical height into a sum of local heights, one for each distinct

Received by the editor October 24, 1995.
1991 *Mathematics Subject Classification.* Primary 11G05, 11Y50.
Key words and phrases. Elliptic curve, canonical height.
Research partially supported by NSF DMS-9424642.

absolute value v on K:

$$\hat{h}(P) = \sum_v n_v \hat{\lambda}_v(P). \tag{2}$$

See [19, Chapter VI] for the definition and existence of the $\hat{\lambda}_v$'s, as well as the choice of the n_v multiplicities.

In order to explain the purpose of this article, we briefly recall the existing methods for computing the $\hat{\lambda}_v$'s. (A more detailed account will be given in Section 1.) To ease notation, we will take $K = \mathbb{Q}$ and will assume that E is given by a minimal Weierstrass equation (1) with discriminant Δ. Let $P \in E(\mathbb{Q})$ be a rational point on E, and write the coordinates of P as $P = (a/d^2, b/d^3)$. Then the decomposition of $\hat{h}(P)$ can be written as the finite sum

$$\hat{h}(P) = \hat{\lambda}_\infty(P) + \log(d) + \sum_{p|\Delta,\ p\nmid d} \hat{\lambda}_p(P). \tag{3}$$

The archimedean local height $\hat{\lambda}_\infty(P)$ is easily computed using a rapidly convergent series, so it poses no problem. Further, for any given prime p, it is extremely easy to calculate the local height $\hat{\lambda}_p(P)$. However, and it is this caveat which motivates the present article, in order to use the sum (3) to compute $\hat{h}(P)$, one must first find all of the prime divisors of Δ. As is well known, factorization of large integers is a time-consuming process. In this article we will explain how to compute $\hat{h}(P)$ without factoring Δ, essentially by grouping together terms in (3) whose $\hat{\lambda}_p$'s have the same form. Our method is not completely factorization free, since it does require the prime factorization of the quantity $\gcd(c_4, c_6)$; but in practice, it is usually feasible to factor $\gcd(c_4, c_6)$ even when Δ is far too large to be effectively factored.

1. Description of the algorithm

Let K be a number field, E/K an elliptic curve given by a Weierstrass equation (1), and let $P \in E(K)$. We begin by briefly reviewing how to compute the local heights $\hat{\lambda}_v(P)$ whose sum is the canonical height (2). See [20] for details. First, if v is an archimedean absolute value v, there are two standard methods for computing $\hat{\lambda}_v(P)$. One method, due to Tate (for real absolute values, with a modification for complex absolute values by the author) can be found in [20]. It expresses $\hat{\lambda}_v(P)$ as an easily computed series which converges geometrically. An alternative series, which is somewhat more complicated but much faster converging, can be found in [3, Algorithm 7.5.7]. It uses the original formulas of Néron and Tate to express $\hat{\lambda}_v(P)$ in terms of a theta function attached to E. The necessary elliptic integrals can be rapidly computed using the AGM. Using either method, the numerical computation of $\hat{\lambda}_v(P)$ for archimedean v is easily accomplished.

Next suppose that v is non-archimedean. The first step in computing $\hat{\lambda}_v(P)$ is to replace the Weierstrass equation (1) by an equation which is minimal at v. (See [18, Chapter VIII, Section 1].) For any given v, this is easily accomplished using any one of a variety of methods [3, Section 7.5.1], [19, Chapter IV, Section 9], [4, Section 3.2], [9]. Having done this, one computes certain (explicitly given) polynomials in terms of the a_i coefficients of (1) and the coordinates of P, and then one takes the ord_v of these values to obtain certain integers N, A, B, C. (See [20, Section 5] for details.)

The local height, up to an appropriate scaling factor, is then given by the following simple algorithm:

- (Good Reduction)
  If $\min\{A, B\} \leq 0$, then $\hat{\lambda}_v(P) = \max\{0, -\frac{1}{2}\operatorname{ord}_v(x_P)\}$.
- (Multiplicative Reduction)
  Else if $\operatorname{ord}_v(c_4) = 0$, let $n = \min\{B, \frac{1}{2}N\}$, then $\hat{\lambda}_v(P) = -n(N-n)/2N$.
- (Additive Reduction)
  Else if $C \geq 3B$, then $\hat{\lambda}_v(P) = -\frac{1}{3}B$. Else $\hat{\lambda}_v(P) = -\frac{1}{8}C$.

What, then, are the computational difficulties which one encounters in computing the canonical height $\hat{h}(P)$? Recall that attached to a Weierstrass equation (1) are certain quantities which we list here for the convenience of the reader:

$$
\begin{gathered}
b_2 = a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6 \\
b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\
c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6, \\
\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.
\end{gathered} \tag{4}
$$

We may assume that the coefficients of the Weierstrass equation lie in the ring of integers of K. Then the procedure in [20] as described above can be used to rapidly compute $\hat{h}(P)$ as soon as one knows exactly which absolute values v contribute non-zero local terms $\hat{\lambda}_v(P)$. More precisely, it suffices to determine exactly which prime ideals of K divide the discriminant Δ. So if the prime factorization of (Δ) can be accomplished, we have nothing to add to [20].

However, if the coefficients of E are of even moderate size, then the discriminant Δ may be quite large and difficult to factor. Further, even if it is feasible to factor Δ using current techniques, it would still be preferable to compute $\hat{h}(P)$ without that factorization, since the time required to perform the factorization is likely to be orders of magnitude larger than the time required for the rest of the computation.

Unfortunately, we are not able to give an entirely "factorization-free" algorithm, but we will discuss various techniques to reduce the amount of factorization required to a minimum. In principle, our techniques would be factorization free if one had an a priori way of verifying that a given Weierstrass equation is minimal; but in practice we have found that it is most efficient to combine our method with a small amount of factorization. And since we do not know a non-factorization way to check a Weierstrass equation for minimality, our algorithm must begin with a factorization of $\gcd(c_4, c_6)$. In practice, this quantity tends to be quite small compared to Δ.

Remark. It is worth noting that the algorithm described in this paper (with a few minor modifications) does give a factorization-free method for computing the canonical height of points on elliptic curves defined over function fields such as $\mathbb{F}_q(T)$ or $\mathbb{Q}(T)$. The reason is that in such a function field, it is possible to efficiently write any element $f \in k[T]$ as a product $f_1f_2^2f_3^3\cdots f_r^r$, where the f_i's are squarefree. This is done by the standard method of taking derivatives and gcd's. If it were possible to perform a similar decomposition in number fields, the algorithm for $\hat{h}$ over number fields would also become completely factorization free.

Remark. We should also mention that the local heights which we compute in this paper are non-normalized heights. For theoretical work, it is usually preferable to

work with normalized heights, so the reader should be aware that in the literature the symbol "$\hat{\lambda}_v$" may differ from our $\hat{\lambda}_v$ by $v(\Delta)$. (See [19], for example.) Of course, the extra $v(\Delta)$ will cancel out when the local heights are summed to form the global height.

For the remainder of this paper, we will restrict attention to $K = \mathbb{Q}$. This has the advantage of greatly simplifying our exposition, while covering the situation most commonly encountered in the literature. The ideas which we use can easily be adapted to other number (or function) fields by the interested reader. We now describe, step-by-step, our algorithm for computing $\hat{h}(P)$, with an explanation of why each step works. In section 2 we will give a concise summary of the algorithm suitable for implementation, and section 3 contains some numerical examples.

Step 1. Initial Data. The algorithm requires an elliptic curve $E/\mathbb{Q}$ given by a Weierstrass equation (1) with coefficients $a_i \in \mathbb{Z}$, and a rational point $P = (x_1, y_1) \in E(\mathbb{Q})$. No assumption is made concerning the minimality of the equation (1).

Step 2. Compute Associated Quantities. Compute the quantities $b_2, b_4, b_6, b_8, c_4, c_6, \Delta$ listed in (4).

Step 3. Find Minimal Equation. Factor $\gcd(c_4, c_6)$ completely. Use this factorization to find a minimal Weierstrass equation for E over $\mathbb{Z}$. The fastest way to do this is a short algorithm of Connell and Kraus [4, Section 3.2] which has superceded an earlier method of Laska [9]. (Remark. In the Connell-Kraus algorithm as presented in [4], one of the steps asks for all prime factors of the quantity $6\gcd(c_6^2, \Delta)$. This is the same as the set of primes dividing $6\gcd(c_4, c_6)$.) An alternative algorithm of Tate [3, Section 7.5.1][19, Chapter IV, Section 9] is more complicated, but has the advantage of also computing the conductor and reduction types for E. Regardless of the method chosen, make the appropriate change of coordinates to the point P and recompute the associated quantities (4). We now have a minimal Weierstrass equation (1), a point $P = (x_1, y_1) \in E(\mathbb{Q})$, and a factorization of the quantity $\gcd(c_4, c_6)$.

Step 4. Archimedean Height. Compute the height $\hat{\lambda}_\infty(P)$ corresponding to the archimedean absolute value on $\mathbb{Q}$. This can be done using either Tate's series [20] or theta functions [3, Algorithm 7.5.7]. Set $H \leftarrow \hat{\lambda}_\infty(P)$. We will use H to accumulate the pieces of the canonical height $\hat{h}(P)$.

Step 5. Formal Group Contributions. The primes p for which $P = (x_1, y_1)$ lies in the formal group $E_1(\mathbb{Q}_p)$ contribute to the canonical height, but luckily we don't need to know exactly which primes these are, since all of the required information is contained in the (denominator) of the rational number x_1. So we augment H by

$$H \leftarrow H + \frac{1}{2}\log(\text{denominator of } x_1).$$

Step 6. Contributions From Small Primes. The only remaining non-zero local heights $\hat{\lambda}_p(P)$ are for primes p which divide the discriminant Δ. Our goal is to try to avoid factoring Δ, but it makes sense to do a little bit of factoring at this point. So we choose some bound p_0 and find all primes $p < p_0$ dividing Δ. In principle, it will suffice to take $p_0 = 5$. However, if Δ is divisible by large powers, later portions of the algorithm may be inefficient, so it is probably better to take

at least $p_0 = 100$. Alternatively, one can just take $p_0 = 5$, and if a later part of the algorithm bogs down, one can return to this step and search for additional small primes dividing Δ to high powers. In any case, for each $p < p_0$ dividing Δ, use the algorithm in [20] to compute $\hat{\lambda}_p(P)$ and add it onto the accumulating total, while also removing these primes from Δ:

$$H \leftarrow H + \sum_{\substack{p|\Delta \\ p<p_0}} \hat{\lambda}_p(P), \qquad \Delta \leftarrow \Delta \prod_{p<p_0} p^{-\operatorname{ord}_p(\Delta)}.$$

Step 7. Additive Reduction Contributions. For primes $p \geq 5$, so in particular for $p \geq p_0$, the primes of additive reduction are precisely the primes dividing both c_4 and c_6. We already found these primes in step (2) when we factored $\gcd(c_4, c_6)$, so we can use the algorithm [20] to compute the $\hat{\lambda}_p(P)$'s and add them onto the total, while also removing them from Δ:

$$H \leftarrow H + \sum_{\substack{p|\gcd(c_4,c_6) \\ p\geq p_0}} \hat{\lambda}_p(P), \qquad \Delta \leftarrow \Delta \prod_{\substack{p|\gcd(c_4,c_6) \\ p\geq p_0}} p^{-\operatorname{ord}_p(\Delta)}.$$

Step 8. Additional "Good Reduction" Contributions. Here "good reduction" means primes for which the point P has good reduction, or in fancier terminology, primes p for which the point P lies in the identity component $E_0(\mathbb{Q}_p)$ of the Néron model of $E/\mathbb{Q}_p$. (See [18, Chapter VII] and [19, Chapter IV] for details.) We can determine these primes and remove them from Δ with no factorization. First we compute

$$A_1 = (\text{numerator of } 3x_1^2 + 2a_2x_1 + a_4 - a_1y_1),$$
$$B_1 = (\text{numerator of } 2y_1 + a_1x_1 + a_3),$$

where recall that $P = (x_1, y_1)$. Then P lies in $E_0(\mathbb{Q}_p)$ if and only if $\gcd(A_1, B_1)$ is prime to p. Further, since we already took care of the formal group contributions in Step (5), the primes with $P \in E_0(\mathbb{Q}_p)$ contribute nothing further to $\hat{h}(P)$. (This follows from [19, Theorem VI.4.1].) Hence we may remove from Δ that part which is prime to A_1 and B_1. In other words, we may replace Δ by

$$\Delta_1 \leftarrow \gcd(\Delta, A_1^\infty, B_1^\infty).$$

Remark. For any integers M and N, the notation $\gcd(M, N^\infty)$ is an abbreviation for the quantity

$$\gcd(M, N^\infty) \stackrel{\text{def}}{=} \max_{n\geq 1} \gcd(M, N^n) = \prod_{p|N} p^{\operatorname{ord}_p(M)}.$$

In other words, it is that part of M composed of primes which also divide N. In practice, we want to be able to compute $\gcd(M, N^\infty)$ without factoring N. This can be accomplished by computing $\gcd(M, N^n)$ for $n = 0, 1, 2, \ldots$ until reaching an n satisfying

$$\gcd(M, N^n) = \gcd(M, N^{n+1}).$$

(A more efficient method is described in section 2.) This gcd is then equal to $\gcd(M, N^\infty)$. We define $\gcd(M, N_1^\infty, N_2^\infty)$ similarly.

It follows from general principles that Δ_1 is a powerful number; that is, every prime which divides Δ_1 will divide it to at least the second power. In particular,

the square-free part of the discriminant Δ has been eliminated. It turns out that many of the large curves which have appeared in the literature have a discriminant which is mostly squarefree. (We will discuss some examples in section 3.) So it will frequently happen that $\Delta_1 = 1$, especially if p_0 in Step (6) was chosen to be of reasonable size. If $\Delta_1 = 1$, the algorithm terminates and we have $H = \hat{h}(P)$. In any case, we have avoided the necessity of factoring the square-free part of Δ, which is generally a big savings.

Step 9. Multiplicative Reduction Contributions. If $\Delta_1 > 1$, then E has multiplicative reduction of type I_{N_p} for each prime p dividing Δ_1, where $N_p = \operatorname{ord}_p(\Delta_1) \geq 2$. The algorithm described in [20] says that the local height is given by

$$\hat{\lambda}_p(P) = \frac{-n_p(N_p - n_p)}{2N_p} \log p = -\frac{1}{2} \cdot \frac{n_p}{N_p} \left(1 - \frac{n_p}{N_p}\right) \log p^{N_p},$$

where

$$n_p = \min\left\{\operatorname{ord}_p(B_1), N_p/2\right\}.$$

(Recall that $B_1 = 2y_1 + a_1x_1 + a_3$.) Of course, in practice we won't know the prime divisors of Δ_1. However, we can exploit this formula by considering the multiples $2P, 3P, \ldots$, since it turns out that the map

$$t_p : E(\mathbb{Q}) \longrightarrow \mathbb{Q}, \qquad Q \longmapsto \frac{n_p(Q)}{N_p},$$

(more or less) satisfies

$$t_p(mQ) \equiv m t_p(Q) \pmod{\{\pm 1\}\mathbb{Z}}.$$

We illustrate the procedure for $2P$. The first step is to compute $2P = (x_2, y_2)$. However, we should note that as we take larger multiples, the size of the coordinates will become unwieldy. So instead all that we really need to do is to compute

$$2P \equiv (x_2, y_2) \bmod \Delta_1,$$

and similarly for higher multiples. There is, of course, a slight chance that as we attempt to compute $2P \bmod \Delta_1$, we will run into a problem because we are required to compute an inverse $z^{-1} \bmod \Delta_1$ for some z with $\gcd(z, \Delta_1) > 1$. If this happens, it will almost certainly lead to a factorization of Δ_1, and we can then deal with each factor of Δ_1 separately. (The reader will undoubtedly recognize that this "unusual situation" is the underlying basis for Lenstra's elliptic curve factorization method [10].) Assuming now that we are able to compute $2P \bmod \Delta_1$, we set

$$B_2 = 2y_2 + a_1x_2 + a_3 \pmod{\Delta_1}.$$

We then define

$$\Delta_2 = \gcd(\Delta_1, B_2^\infty) \qquad \text{and} \qquad \Delta_2' = \Delta_1/\Delta_2.$$

These last two partial discriminants have the following interpretation:

$$p|\Delta_2 \iff P \notin E_0(\mathbb{Q}_p) \text{ and } 2P \notin E_0(\mathbb{Q}_p),$$
$$p|\Delta_2' \iff P \notin E_0(\mathbb{Q}_p) \text{ and } 2P \in E_0(\mathbb{Q}_p).$$

This enables us to deal with the primes dividing Δ_2', since for those primes we have $n_p/N_p = 1/2$. Hence the local height for such primes is

$$\hat{\lambda}_p(P) = -(1/8) \operatorname{ord}_p(\Delta_2') \log(p),$$

and adding them all up means that we have no need to determine the actual primes dividing Δ_2'. In other words, at this step of the algorithm we augment our running total H by

$$H \leftarrow H - \frac{1}{8}\log \Delta_2'.$$

It remains to deal with the primes dividing Δ_2. Of course, if we're lucky, then $\Delta_2 = 1$ and we're done. Otherwise we repeat the process using $3P, 4P, \ldots$. Here are the next few steps of the algorithm:

- Compute $3P \equiv (x_3, y_3) \pmod{\Delta_2}$. Let $B_3 = 2y_3 + a_1x_3 + a_3$.
  Let $\Delta_3 = \gcd(\Delta_2, B_3^\infty)$ and $\Delta_3' = \Delta_2/\Delta_3$.
  Augment $H \leftarrow H - \frac{1}{9}\log \Delta_3'$.
  If $\Delta_3 = 1$, then stop, otherwise continue.
- Compute $4P \equiv (x_4, y_4) \pmod{\Delta_3}$. Let $B_4 = 2y_4 + a_1x_4 + a_3$.
  Let $\Delta_4 = \gcd(\Delta_3, B_4^\infty)$ and $\Delta_4' = \Delta_3/\Delta_4$.
  Augment $H \leftarrow H - \frac{3}{32}\log \Delta_4'$.
  If $\Delta_4 = 1$, then stop, otherwise continue.
- Compute $5P \equiv (x_5, y_5) \pmod{\Delta_4}$. Let $B_5 = 2y_5 + a_1x_5 + a_3$.
  Let $\Delta_5 = \gcd(\Delta_4, B_5^\infty)$ and $\Delta_5' = \Delta_4/\Delta_5$.
  It is tempting to write "and so on," but a new phenomenon occurs here!

To describe this new phenomenon, we first explain the contributions from $3P$ and $4P$. The primes p dividing Δ_3' are those primes for which $P, 2P \notin E_0(\mathbb{Q}_p)$ and $3P \in E_0(\mathbb{Q}_p)$. It follows for these primes that $n_p/N_p = 1/3$, so $\hat{\lambda}_p(P) = -(1/9)\operatorname{ord}_p(\Delta_3')\log(p)$, and adding them up gives the specified contribution of $-(1/9)\log\Delta_3'$. Similarly, if p divides Δ_4', then $P, 2P, 3P \notin E_0(\mathbb{Q}_p)$ and $4P \in E_0(\mathbb{Q}_p)$, from which we deduce that $n_p/N_p = 1/4$, yielding a contribution of $-(3/32)\log\Delta_4'$.

Next consider a prime p dividing Δ_5'. Then $P, 2P, 3P, 4P \notin E_0(\mathbb{Q}_p)$ and $5P \in E_0(\mathbb{Q}_p)$, but now there are two possibilities for n_p/N_p, namely $1/5$ and $2/5$. So we need to separate Δ_5' into two parts without, of course, performing a full factorization. Here is the procedure. From the definition of the n_p's, we see that

$$\gcd(\Delta_5', B_1) = \alpha_1\alpha_2^2,$$

where the primes dividing α_1 correspond to $n_p/N_p = 1/5$ and the primes dividing α_2 correspond to $n_p/N_p = 2/5$. If we replace P by $2P$, we find that the roles are reversed,

$$\gcd(\Delta_5', B_2) = \alpha_1^2\alpha_2.$$

Thus we can recover α_1 and α_2 merely by computing some gcd's,

$$\alpha_1^3 = \frac{\gcd(\Delta_5', B_2)^2}{\gcd(\Delta_5', B_1)} \qquad \text{and} \qquad \alpha_2^3 = \frac{\gcd(\Delta_5', B_1)^2}{\gcd(\Delta_5', B_2)}.$$

Having computed α_1 and α_2, we get the local heights for primes dividing Δ_5',

$$H \leftarrow H - \frac{2}{25}\log\gcd(\Delta_5', \alpha_1^\infty) - \frac{3}{25}\log\gcd(\Delta_5', \alpha_2^\infty).$$

Of course, if $\Delta_5 = 1$, we're done, and if not, we continue in a similar vein.

For completeness, we describe how to deal with the primes which arise when we consider the multiple mP. So suppose that we have dealt with all primes p for which one of the multiples $P, 2P, \ldots, (m-1)P$ lies in $E_0(\mathbb{Q}_p)$, and we are left with a

piece of the discriminant Δ_{m-1} divisible by the remaining primes of multiplicative reduction. As before, we compute

$$mP \equiv (x_m, y_m) \pmod{\Delta_{m-1}} \qquad \text{and} \qquad B_m = 2y_m + a_1x_m + a_3,$$

and we divide the remaining discriminant into the two pieces

$$\Delta_m = \gcd(\Delta_{m-1}, B_m^\infty) \qquad \text{and} \qquad \Delta'_m = \Delta_{m-1}/\Delta_m.$$

The primes p dividing Δ'_m are those with $mP \in E_0(\mathbb{Q}_p)$ and no lower multiple of P in $E_0(\mathbb{Q}_p)$. This means that there is a factorization

$$\gcd(\Delta'_m, B_1) = \alpha_1\alpha_2^2\alpha_3^3\cdots\alpha_r^r,$$

where $r = \lfloor m/2 \rfloor$, $\alpha_i = 1$ if $\gcd(i,m) > 1$, and the primes dividing α_i are the primes for which $n_p/N_p = i/m$. As before, we want to determine the α_i's without performing a factorization, since once we know the α_i's, we know the appropriate amount to add onto H, namely

$$H \leftarrow H - \frac{1}{2}\sum_{i=1}^{\lfloor m/2 \rfloor} \frac{i(m-i)}{m^2} \log \gcd(\Delta'_m, \alpha_i^\infty).$$

(In the sum, it's only necessary to take i's with $\gcd(i,m) = 1$.)

In order to find the α_i's, we consider also the multiples of P. We have already computed the quantities $B_1, B_2, \ldots, B_r$, and if we were to factor $\gcd(\Delta'_m, B_k)$, we would find that it equals

$$\gcd(\Delta'_m, B_k) = \alpha_1^{\{k\}_m}\alpha_2^{\{2k\}_m}\alpha_3^{\{3k\}_m}\cdots\alpha_r^{\{rk\}_m},$$

where

$$\{A\}_m = \bigl\{\min|A - mK| \,:\, K \in \mathbb{Z}\bigr\}.$$

In other words, $\{A\}_m$ is the magnitude of the least residue of A modulo m, where the least residue is taken between $-m/2$ and $m/2$. Taking $k = 1, 2, \ldots, r$, we obtain r equations for the r variables $\alpha_1, \ldots, \alpha_r$. More precisely, consider the matrix

$$M_m = \begin{pmatrix} \{1\}_m & \{2\}_m & \cdots & \{i\}_m & \cdots & \{r\}_m \\ \{2\}_m & \{4\}_m & \cdots & \{2i\}_m & \cdots & \{2r\}_m \\ \vdots & & \ddots & & & \vdots \\ \{j\}_m & \{2j\}_m & \cdots & \{ij\}_m & \cdots & \{rj\}_m \\ \vdots & & & & \ddots & \vdots \\ \{r\}_m & \{2r\}_m & \cdots & \{ri\}_m & \cdots & \{r^2\}_m \end{pmatrix}.$$

It is likely that M_m is invertible for all m, but in any case we have checked that it is invertible for all $m \le 50$, which should suffice for most applicaitons. (We will discuss M_m further below.) Write the adjoint matrix of M_m as

$$M_m^{\text{adj}} = \bigl(t_m(i,j)\bigr)_{1\le i,j\le r}.$$

That is, M_m^{adj} has integer coefficients and $M_m M_m^{\text{adj}} = (\det M_m) I_r$. We can then recover the α_i's from the relation

$$\alpha_i^{\det M_m} = \prod_{k=1}^{r} \gcd(\Delta'_m, B_k)^{t_m(i,k)}. \tag{5}$$

There are two remarks to make concerning this formula. First, it follows from the general theory that the product is a perfect $\det(M_m)^{\text{th}}$-power, so all operations can be performed using integer arithmetic.

Second, it is unfortunately true that $\det(M_m)$ may be too large for these computations to be performed in practice. For m's of moderate size, there are various ways to simplify the computations. Thus it sometimes happens that every entry of the adjoint matrix has a factor in common with the determinant, in which case the appropriate root can be extracted from both sides of (5). Another way to simplify is to work instead with the matrix M'_m whose entries are the $\{ij\}_m$'s with $\gcd(i,m) = \gcd(j,m) = 1$. The M'_m's are smaller matrices than the M_m's, so their adjoint entries and determinants tend to be smaller integers. If one also cancels common factors from the entries of M'^{adj}_m and $\det(M'_m)$, then one finds that the exponents in (5) are at most 18 for all $m \leq 10$, and in that range they are at most 8 except for $m = 7$. However, when $m = 11$, the left-hand side of the analogue of (5) will be α_i^{2325}, and the exponents on the right-hand side will be as large as 391. Further, we should mention that although it appears that the matrix M_m is invertible for all m, it also appears that M'_m fails to be invertible for precisely those m's satisfying $4|m$ and $m \geq 16$.

This concludes our description of the "factorization-free" canonical height algorithm. In the next section we will give pseudo-code implementing the algorithm.

Remark. Although it is not of immediate use in calculating the canonical height, we should mention that the partial discriminant Δ'_m will be a perfect m^{th} power. However, it need not be true that $\sqrt[m]{\Delta'_m}$ is squarefree.

Remark. There is one additional strategy which may be employed as one computes the multiples of P. At each stage one can compute

$$\gcd(\Delta_m, B_1, B_2, \ldots, B_m).$$

It is possible that at some point this number will become small enough to factor completely, thereby yielding all of the remaining primes of bad reduction.

Remark. The matrices M_m and M'_m which appear above would seem to have some relation to the Demjanenko matrices used by Folz and Zimmer [6] in studying torsion points on elliptic curves and used by other authors ([7], [16], [17]) to investigate the class number of (abelian) number fields.

2. Programming the algorithm

In this section we give pseudo-code to implement the algorithm described in section 1. After giving the main algorithm, we briefly explain how to compute some of the subsidiary quantities which it requires.

PROGRAM to Compute the Canonical Height of $P \in E(\mathbb{Q})$

DATA required by the algorithm

$a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, Weierstrass coefficients for $E/\mathbb{Q}$

$x_1, y_1 \in \mathbb{Q}$, coordinates for $P = (x_1, y_1) \in E(\mathbb{Q})$

$p_0 \geq 4$, a quantity for which one can easily find prime factors $< p_0$

ALGORITHM

Compute the quantities c_4, c_6, Δ given in (4).

`Factor` completely $\gcd(c_4, c_6)$.

If necessary, replace the given equation with a `Minimal Weierstrass Equation`, making the appropriate coordinate change to $P = (x_1, y_1)$.

Compute the `Archimedean Height` $\hat{\lambda}_\infty(P)$ of P.
Set

$$H \leftarrow \hat{\lambda}_\infty(P) + \frac{1}{2}\log(\text{denominator of } x_1).$$

Compute

$$\begin{aligned} A_1 &\leftarrow (\text{numerator of } 3x_1^2 + 2a_2x_1 + a_4 - a_1y_1),\\ B_1 &\leftarrow (\text{numerator of } 2y_1 + a_1x_1 + a_3),\\ \Delta_1 &\leftarrow \gcd(\Delta, A_1^\infty, B_1^\infty). \end{aligned}$$

IF $\Delta_1 = 1$ **THEN EXIT RETURNING** H
Find the set $\mathcal{P}$ of all `Small Primes` $p < p_0$ which divide Δ_1 and all primes which divide $\gcd(c_4, c_6, \Delta_1)$. For each prime $p \in \mathcal{P}$, compute the `Non-archimedean Local Height` $\hat{\lambda}_p(P)$. Set

$$H \leftarrow H + \sum_{p\in\mathcal{P}} \hat{\lambda}_p(P) \qquad \text{and} \qquad \Delta_1 \leftarrow \Delta \prod_{p\in\mathcal{P}} p^{-\operatorname{ord}_p(\Delta_1)}.$$

IF $\Delta_1 = 1$ **THEN EXIT RETURNING** H
DO $m = 2$ **TO** $m = 4$
Compute $mP \equiv (x_m, y_m) \pmod{\Delta_{m-1}}$.
Set $B_m \leftarrow 2y_m + a_1x_m + a_3$.
Set $\Delta_m \leftarrow \gcd(\Delta_{m-1}, B_m^\infty)$ and $\Delta'_m \leftarrow \Delta_{m-1}/\Delta_m$.
Set $H \leftarrow H - \dfrac{m-1}{2m^2}\log \Delta'_m$.
IF $\Delta_m = 1$ **THEN EXIT RETURNING** H
END DO m **LOOP**
DO $m = 5$ **TO** $m = 10$
Compute $mP \equiv (x_m, y_m) \pmod{\Delta_{m-1}}$.
Set $B_m \leftarrow 2y_m + a_1x_m + a_3$.
Set $\Delta_m \leftarrow \gcd(\Delta_{m-1}, B_m^\infty)$ and $\Delta'_m \leftarrow \Delta_{m-1}/\Delta_m$.
Form the matrix M whose dimensions are $\frac{1}{2}\phi(m)$-by-$\frac{1}{2}\phi(m)$ and whose entries are given by

$$M_{ij} = \{ij\}_m \qquad \text{with } 1 \le i, j < m/2 \text{ and } \gcd(i,m) = \gcd(j,m) = 1.$$

Here $\{k\}_m$ is defined as follows. First write $k = mq + r$ with $0 \le r < m$. Then $\{k\}_m = \min\{r, m-r\}$.
Compute the adjoint matrix M^{adj}. Let

$$\begin{aligned} \mu_1 &\leftarrow \text{content}(M^{\mathrm{adj}}) = \text{gcd of the entries of } M^{\mathrm{adj}},\\ \mu_2 &\leftarrow \gcd\bigl(\mu_1, \det(M)\bigr),\\ M' &\leftarrow \mu_2^{-1} M^{\mathrm{adj}},\\ \mu &\leftarrow \mu_2^{-1}\det(M). \end{aligned}$$

DO $i = 1$ **TO** $\lfloor m/2 \rfloor$ **WITH** $\gcd(i,m) = 1$
Set

$$\alpha_i \leftarrow \left(\prod_{\substack{1\le k<m/2\\ \gcd(k,m)=1}} \gcd(\Delta'_m, B_k)^{M'_{ik}} \right)^{1/\mu}$$

(Note: The α_i's will be integers.)

END DO i **LOOP**
Set

$$H \leftarrow H - \frac{1}{2} \sum_{\substack{1 \le i < m/2 \\ \gcd(i,m)=1}} \frac{i(m-i)}{m^2} \log \gcd(\Delta'_m, \alpha_i^\infty).$$

IF $\Delta_m = 1$ **THEN EXIT RETURNING** H
END DO m **LOOP**
EXIT RETURNING MESSAGE "Numbers Too Large"
END OF PROGRAM

Remarks. (1) The program for computing $\hat{h}(P)$ given above refers to a number of subsidiary algorithms. We have listed these required subroutines below, with appropriate references or pseudo-code.

(2) Depending on the particular implementation, it is permissible to have the last m-loop go up to $m = 15$. However, this may require the computation of numbers with a tremendous number of digits.

(3) The last m-loop will certainly fail for $m = 16$, because the associated matrix M turns out to be non-invertible. The larger matrix

$$\big(\{ij\}\big)_{1 \le i,j \le m/2}$$

is invertible, at least for $m \le 50$, and it can be used in place of M. However, the powers necessary for computing the α_i's will probably be too large to make this a practical alternative.

(4) In the unlikely event that the algorithm fails with $\Delta_{10} > 1$, it will be true that every prime dividing Δ_{10} divides it to at least the 11^{th} power. This may be helpful in trying to factor Δ_{10}. Of course, if one can effect a complete factorization of Δ_{10}, then the computation of the canonical height of P is completed by computing

$$H \leftarrow H + \sum_{p \mid \Delta_{10}} \hat{\lambda}_p(P).$$

We now list the subroutines needed to implement the canonical height algorithm as described above.

SUBROUTINE: Compute $\gcd(M, N^\infty) = \sup_{k \ge 1} \gcd(M, N^k)$
$N_2 \leftarrow \gcd(M, N)$
IF $N_2 = 1$ **THEN EXIT RETURNING** 1
$N_1 \leftarrow 1$
WHILE $N_1 \ne N_2$
$N_1 \leftarrow N_2$
$N_2 \leftarrow \gcd(M, N_2^2)$
END WHILE
EXIT RETURNING N_1
SUBROUTINE: Minimal Model
INPUT: $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, Weierstrass coefficients for $E/\mathbb{Q}$
OUTPUT:
$u, r, s, t \in \mathbb{Z}$ so that a minimal Weierstrass equation is obtained by the change of variables $u^2 x' = x + r$ and $u^3 y' = y + sx + t$

ALGORITHM: There are a number of efficient algorithms in the literature for finding a minimal model, although they all require a complete factorization of $\gcd(c_4, c_6)$. The quickest is due to Connell and Kraus, see [4, Section 3.2] and [8]

SUBROUTINE: Archimedean local height $\hat{\lambda}_\infty(P)$

INPUT:

$a_1, a_2, a_3, a_4, a_6 \in \mathbb{R}$, Weierstrass coefficients for $E/\mathbb{R}$

$x_1, y_1 \in \mathbb{R}$, coordinates for $P = (x_1, y_1) \in E(\mathbb{R})$

OUTPUT: The archimedean local height $\hat{\lambda}_\infty(P)$ of P (non-normalized)

ALGORITHM: There are two standard algorithms for computing archimedean local heights. The most efficient uses theta functions and q-expansions. It is described in [3, Algorithm 7.5.7] and is especially good when high precision output is desired and when computing the heights of several points on a single elliptic curve. The second algorithm, given by a series of Tate, is described in [20] and [4].

SUBROUTINE: Non-archimedean local height $\hat{\lambda}_p(P)$

INPUT:

$a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, Weierstrass coefficients for a minimal equation for $E/\mathbb{Q}$

$x_1, y_1 \in \mathbb{Q}$, coordinates for $P = (x_1, y_1) \in E(\mathbb{Q})$

a prime p

OUTPUT: The non-archimedean local height $\hat{\lambda}_p(P)$ of P (non-normalized)

ALGORITHM: There is a short efficient algorithm for computing $\hat{\lambda}_p(P)$ due to the author. See [3, Algorithm 7.5.6], [4], or [20].

SUBROUTINE: Find Small Prime Factors

INPUT: An integer $N > 0$ to factor and a bound p_0

OUTPUT: A list of small prime factors of N, including all primes $\leq p_0$

ALGORITHM: There are many algorithms currently in use for finding prime factors of a given number N, some of which are especially efficient at finding small prime factors. We refer the reader to [3, Chapters 8 and 10] and [15] and to the additional references cited in those works.

SUBROUTINE: Compute mP Modulo D on E

INPUT:

$a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, Weierstrass coefficients for $E/\mathbb{Q}$

$x_1, y_1 \in \mathbb{Q}$, coordinates for $P = (x_1, y_1) \in E(\mathbb{Q})$

The multiple m and the modulus $D > 0$

OUTPUT: Integers $0 \leq x_m, y_m < D$ so that $mP_1 \equiv (x_m, y_m) \pmod{D}$ (or a non-trivial factorization of D)

ALGORITHM: Using the standard addition formulas on E, together with any favorite tricks for speeding the computation of a multiple of an element of an abelian group, one computes mP_1 modulo D. For small values of m, this will almost always be possible. In rare instances, there may be a problem due to the necessity of inverting a number $d \bmod D$ with $\gcd(d, D) > 1$. In this case, it will almost always be true that $\gcd(d, D) < D$, yielding a non-trivial factorization of D. For further discussion, see [3, Section 10.3] or [10].

3. Numerical examples

The examples in this section are designed to illustrate the algorithm described in this paper. In order to keep the numbers to a manageable size for exposition, we give examples which can in principle be computed via a complete factorization of the discriminant using existing factorization techniques. However, even when such a factorization is possible, the time spent performing the factorization will generally far exceed the time required for the remainder of the algorithm. Further, as the search for curves of ever higher rank continues, it is quite likely that people will want to compute canonical heights on curves for which a complete factorization of the discriminant is beyond current methods. All computations in this section were performed using PARI-GP [1].

Example 1. For our first example we will take the curve with Mordell-Weil rank ≥ 21 discovered by Nagao and Kouya [14],

$$E : y^2 + xy + y = x^3 + x^2 - 215843772422443922015169952702159835x \\ - 19474361277787151947255961435459054151501792241320535.$$

We will compute the height of the first point in their list of 21 independent points,

$$P = (x_1, y_1) = (800843008889340065933/16, \\ 22662214190910903990783584765347/64) \in E(\mathbb{Q}).$$

We first compute

$$c_4 = 10360501076277308256728157729703672081,$$
$$c_6 = 16825848144008099204725392608156810861436365523723401479,$$
$$\Delta = 47973775404376774653692377\ldots500948985175040000 \approx 4.8 \times 10^{107}.$$

Since $\gcd(c_4, c_6) = 1$, we know that the given Weierstrass equation is minimal at all primes. Further, 2 and 3 are the only possible primes of additive reduction, and since $\gcd(c_4, 6) = 1$, even they are not primes of additive reduction.

We will accumulate the canonical height in the variable H, starting with the contribution from the archimedean local height and the denominator of the coordinates. (The latter can be thought of as the piece coming from primes for which P lies in the formal group.)

$$H \leftarrow \hat{\lambda}_\infty(P) + \frac{1}{2}\log(\text{denominator of } x_1) = 23.37537990122540238111.$$

This value was computed using 50 terms of the modified Tate series [20] with 28 digits of accuracy for all intermediate calculations.

The next step is to compute the quantities

$$A_1 = (\text{numerator of } 3x_1^2 + 2a_2x_1 + a_4 - a_1y_1)$$
$$= 19239933185644058332109370142185711516121 75,$$
$$B_1 = (\text{numerator of } 2y_1 + a_1x_1 + a_3) = 22662214192512590008562264897245,$$
$$\Delta_1 = \gcd(\Delta, A_1^\infty, B_1^\infty) = 2561980729714144375.$$

We are not done, since $\Delta_1 \neq 1$, but at least we are able to discard the 108 digit discriminant Δ and work instead with the 19 digit partial discriminant Δ_1.

As noted above, $\gcd(c_4, c_6) = 1$, so at this stage we do a brief search for small primes dividing Δ_1. Even the briefest of searches leads to a complete factorization,

$$\Delta_1 = 5^4 \cdot 7^4 \cdot 13^4 \cdot 17^3 \cdot 23^3.$$

It is now a simple matter to use the algorithm in [20] to compute the local heights $\hat{\lambda}_p(P)$ for each of the primes dividing Δ_1. Thus setting

$$N_p = \operatorname{ord}_p(\Delta_1) \quad \text{and} \quad n_p = \min\{\operatorname{ord}_p(B_1), N_p/2\},$$

we have the formula

$$\hat{\lambda}_p(P) = -\frac{n_p(N_p - n_p)}{2N_p} \log p.$$

Using the values

$$\begin{array}{lllll} n_5 = 1 & n_7 = 1 & n_{13} = 2 & n_{17} = 1 & n_{23} = 1 \\ N_5 = 4 & N_7 = 4 & N_{13} = 4 & N_{17} = 3 & N_{23} = 3 \end{array}$$

we compute

$$\begin{aligned} H &\leftarrow H - \frac{3}{8}\log 5 - \frac{3}{8}\log 7 - \frac{1}{2}\log 13 - \frac{1}{3}\log 17 - \frac{1}{3}\log 23 \\ &= 18.77008051277431529284. \end{aligned}$$

This value is the canonical height, $\hat{h}(P) = 18.77008051277431529284$.

Example 2. For our second example we will use the following curve constructed by Mark van Hoeij (private communication):

$$\begin{aligned} y^2 = x^3 &- 4076083021652228852170062877062961491179952x \\ &+ 4091000816808637826375202064853265315925248411524553675846823296. \end{aligned}$$

He constructs 12 points on this curve and asks how many of them are independent. Before listing the points, we observe that the given equation is not minimal, since $\gcd(c_4, c_6) = 20736 = 2^8 \cdot 3^4$. Using the Connell-Kraus algorithm (or simply asking PARI [1]), we find that the change of variables

$$x = 12^2 X + 12 \qquad \text{and} \qquad y = 12^3 Y + 6 \cdot 12^2 X$$

leads to the minimal equation

$$\begin{aligned} Y^2 + XY = X^3 &- 19657036176949406115789269275959497932 0X \\ &+ 13700678961470114462523205310522221718867909730928893584 00. \end{aligned}$$

With these new coordinates, van Hoeij's 12 points are

$$\begin{aligned}
P_1 &= (-15382802087488234960, -27455949782890791352389030520),\\
P_2 &= (-16733492223754210, -37058834305478910033970898770),\\
P_3 &= (14181468265809374240, -37874845955500053287677993720),\\
P_4 &= (8829512271896634740, 17966601929235299971063379480),\\
P_5 &= (9754615013879173610, -19513478328652166909182739470),\\
P_6 &= (14239349028193298690, 38186266384267741536181276580),\\
P_7 &= (-774866341119340293535/256,\\
&\qquad 1802854594834706356157442212337 05/4096),\\
P_8 &= (12010508378700149540, 27234197525885990193801702980),\\
P_9 &= (333708543266811281840, 60908144535003077791088868414 80),\\
P_{10} &= (1846561087864399790, 31833710066236063558369500980),\\
P_{11} &= (32244843999188965160, -16898999307382748203046913 7720),\\
P_{12} &= (-14047442794238129440, 36869876653997578860733393160).
\end{aligned}$$

Happily, we now find that $\gcd(c_4, c_6) = 1$ and $\gcd(c_4, 6) = 1$, so there are no primes of additive reduction. Searching for small prime factors ($< 10^4$) of the discriminant, we obtain

$$\Delta = -2^{13} \cdot 3^{10} \cdot 5^7 \cdot 29^2 \cdot 59^2 \cdot \Delta',$$

where $\Delta' \approx 3 \cdot 10^{96}$ is not prime. However, it turns out that for all of the P_i's, and hence also for all of the $P_i + P_j$'s, the quantity

$$B_P = (\text{numerator of } 2Y_P + X_P)$$

is relatively prime to Δ', so the primes dividing Δ' contribute nothing to the sum of local heights. Hence for each of these points we have

$$\hat{h}(P) = \hat{\lambda}_\infty(P) + \hat{\lambda}_2(P) + \hat{\lambda}_3(P) + \hat{\lambda}_5(P) + \hat{\lambda}_{29}(P) + \hat{\lambda}_{59}(P).$$

We have computed the archimedean heights using Tate's series [20]. Setting $N_p = \operatorname{ord}_p(\Delta)$, the non-archimedean heights are easily computed using the formulas

$$n_p(P) = \min\{\operatorname{ord}_p(B_P), N_p/2\} \quad \text{and} \quad \hat{\lambda}_p(P) = -\frac{n_p(P)\big(N_p - n_p(P)\big)}{2N_p} \log p.$$

For example, for the point P_1 we find

$$n_2 = 6, \quad n_3 = 5, \quad n_5 = 3, \quad n_{29} = 0, \quad n_{59} = 1,$$

and so

$$\begin{aligned}
\hat{h}(P_1) &= \hat{\lambda}_\infty(P_1) - \frac{21}{13}\log 2 - \frac{5}{4}\log 3 - \frac{6}{7}\log 5 - 0 \cdot \log 29 - \frac{1}{4}\log 59\\
&= 17.43328753223294397933.
\end{aligned}$$

In a similar fashion we can compute the height pairings

$$\langle P_i, P_j \rangle = \hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j)$$

and find the (approximate) rank of the resulting height regulator matrix. Using only the first nine points gives

$$\det\bigl(\langle P_i, P_j\rangle\bigr)_{1\le i,j\le 9} \approx 515284729781.21216435,$$

so these nine points are independent. On the other hand, the 10×10 matrices obtained using $P_1, \dots, P_9$ together with any one of P_{10}, P_{11}, or P_{12} all have determinant $< 10^{-14}$ (i.e., approximately 0). Hence the 12 points $P_1, \dots, P_{12}$ (probably) generate a subgroup of rank 9 in $E(\mathbb{Q})$. Indeed, using the LLL-lattice reduction algorithm on the height regulator matrix, it is not hard to find the dependencies

$$P_{10} = P_3 - P_4 + P_5, \quad P_{11} = P_8 + P_9 - P_{10}, \quad P_{12} = -P_3 + P_4 + P_9,$$

which proves that the P_i's generate a group of exact rank 9.

Example 3. In this example we want to illustrate all of the facets of the height algorithm, while at the same time using numbers of only moderate size. For this reason we will make the (unrealistic) assumption that it is impractical to factor a number if all of its prime divisors are greater than 1000. The reader desiring a more realistic example is free to replace the 4 digit primes which we use by 100 digit primes of their choice.

We will consider the elliptic curve

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

with Weierstrass coefficients

$$\begin{aligned} a_1 &= 1, \qquad a_2 = 8072861327939044382, \qquad a_3 = 0, \\ a_4 &= 10275316809363556795461766523 1, \\ a_6 &= 256120501093228007479884477351888442326880235693 7732. \end{aligned}$$

The associated c_4, c_6, and Δ are

$$\begin{aligned} c_4 &= 10427374353899879488732857757 1671661 4753, \\ c_6 &= -33673711670912972520736651177974292415915897253548519625009, \\ \Delta &= -86242445247101430848\dots 289502959078997005043 \approx 10^{110}. \end{aligned}$$

We are going to compute the height of the point

$$P = (x_1, y_1) = (2006053, 506083492215689671260102 05).$$

The first step is to compute

$$\gcd(c_4, c_6) = 9 = 3^2.$$

This immediately implies that the given Weierstrass equation is minimal, since any non-minimal prime p would satisfy $p^4|c_4$ and $p^6|c_6$.

We now begin the computation of $\hat{h}(P)$, building up the value in the variable H. The coordinates of P have no denominators, so we start with the archimedean local height

$$H \leftarrow \hat{\lambda}_\infty(P) = 20.41170720883318698063.$$

This value was computed using 100 terms of the modified Tate series [20] with 100 digits of accuracy for all intermediate calculations.

Next we compute the values

$$\begin{aligned}
A_1 &= 3x_1^2 + 2a_2x_1 + a_4 - a_1y_1 = 10273494891978500326783685994 5,\\
B_1 &= 2y_1 + a_1x_1 + a_3 = 10121669844313793425402646 3,\\
\Delta_1 &= \gcd(\Delta, A_1^\infty, B_1^\infty)\\
&= 14553325197808847254470055095771266571313\\
&\qquad 650144949187250718607370958224 14 \approx 10^{74}.
\end{aligned}$$

Notice we have already saved ourselves the necessity of factoring the quantity

$$\Delta/\Delta_1 = -592596152940264934942419702225524379.$$

This is a considerable savings, since although it turns out that

$$\Delta/\Delta_1 = -3^3 \cdot 2221 \cdot 251056780425667 \cdot 39361763713243511,$$

it took a Power Macintosh 7100/80 using Lenstra's algorithm [2] more than 24 minutes to find the last two prime factors.

Since $\gcd(c_4, c_6, \Delta_1) = 1$ and Δ_1 is not divisible by any primes less than 1000 (which is our assumed maximum factoring capability), we do not need to compute any local heights for small primes or for additive reduction primes.

It's time to take multiples of our point.

$$\begin{aligned}
2P &= (x_2, y_2) = (-8072861327942025248, -5060014719445977599221 4442),\\
B_2 &= 2y_2 + a_1x_2 + a_3 = -10120030246178087992645 4132,\\
\Delta_2 &= \gcd(\Delta_1, B_2^\infty) = \Delta_1,\\
\Delta_2' &= \Delta_1/\Delta_2 = 1.
\end{aligned}$$

So $2P$ contributes nothing to the height. We move on to $3P$. (Note that although in principle we can compute the multiple mP modulo Δ_{m-1}, these first few multiples are computed exactly because their coordinates are smaller than Δ_{m-1}.)

$$\begin{aligned}
3P &= (x_3, y_3) = (1414560438036121/9, -13664786315107345322555457702/27),\\
B_3 &= (\text{numerator of } 2y_3 + a_1x_3 + a_3) = -27329572630172253837968070 41,\\
\Delta_3 &= \gcd(\Delta_2, B_3^\infty)\\
&= 37288283068467913271619929304342047747913129462215843,\\
\Delta_3' &= \Delta_2/\Delta_3 = 3902921776013756462819.
\end{aligned}$$

This gives a local contribution

$$H \leftarrow H - \frac{1}{9}\log \Delta_3' = 14.88770583118239162330.$$

(Remark. As predicted, $\Delta_3' = 15744539^3$ is a perfect cube, but note that we have computed the associated local contribution without using the factorization $15744539 = 3571 \cdot 4409$.)

In a similar fashion we compute $4P$, $5P$, and $6P$, and we find that $\Delta_3 = \Delta_4 = \Delta_5 = \Delta_6$. (These computations may be performed modulo Δ_3.) Finally, when we

compute $7P$, we make some progress. Thus we find

$$\begin{aligned}
7P &\equiv (x_7, y_7) \pmod{\Delta_6} \quad \text{with} \\
x_7 &= 33246232589947480078789732387854093328224250415808504, \\
y_7 &= 36461933382309843791454573060870589714095785205742589, \\
B_7 &\equiv 2y_7 + a_1x_7 + a_3 \equiv 31593533217631341118459019900911 \\
&\qquad\qquad 177260589561902861996 \pmod{\Delta_6}, \\
\Delta_7 &= \gcd(\Delta_6, B_7^\infty) = 1, \\
\Delta_7' &= \Delta_6/\Delta_7 = \Delta_6.
\end{aligned}$$

Next we form the 3×3 matrix M whose entries are $\{ij\}_7$ and compute its adjoint,

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \qquad M^{\mathrm{adj}} = \begin{pmatrix} 5 & -1 & -7 \\ -1 & -7 & 5 \\ -7 & 5 & -1 \end{pmatrix}.$$

The matrix M has determinant $\det(M) = -18$, and its adjoint has content 1. We also need the three quantities

$$\begin{aligned}
\gcd(\Delta_7', B_1) &= 6428686063347928717, \\
\gcd(\Delta_7', B_2) &= 902252202074987, \\
\gcd(\Delta_7', B_3) &= 198562664231.
\end{aligned}$$

From these we obtain three integers $\alpha_1, \alpha_2, \alpha_3$ using the formulas

$$\begin{aligned}
\alpha_1 &= \bigl(\gcd(\Delta_7', B_1)^5 \cdot \gcd(\Delta_7', B_2)^{-1} \cdot \gcd(\Delta_7', B_3)^{-7}\bigr)^{-1/18} = 1, \\
\alpha_2 &= \bigl(\gcd(\Delta_7', B_1)^{-1} \cdot \gcd(\Delta_7', B_2)^{-7} \cdot \gcd(\Delta_7', B_3)^{5}\bigr)^{-1/18} = 5279, \\
\alpha_3 &= \bigl(\gcd(\Delta_7', B_1)^{-7} \cdot \gcd(\Delta_7', B_2)^{5} \cdot \gcd(\Delta_7', B_3)^{-1}\bigr)^{-1/18} = 6133.
\end{aligned}$$

It happens that 5279 and 6133 are primes, but we don't need to know this, since the α_i's alone are sufficient to compute the associated local heights,

$$\begin{aligned}
H &\leftarrow H - \frac{1}{2}\sum_{i=1}^{3} \frac{i(7-i)}{49} \log \gcd(\Delta_7', \alpha_i^\infty) \\
&= H - \frac{3}{49}\log\gcd(\Delta_7', 1) - \frac{5}{49}\log\gcd(\Delta_7', 5279^\infty) - \frac{6}{49}\log\gcd(\Delta_7', 6133^\infty) \\
&= 1.28962916577182254773.
\end{aligned}$$

Since $\Delta_7 = 1$, the algorithm terminates, returning the value

$$\hat{h}(P) = 1.28962916577182254773.$$

Acknowledgement

I would like to thank John Cremona for his helpful comments and Mark van Hoeij for sending me the curve and points used in Example 2.

References

1. C. Batut, D. Bernardi, H. Cohen, M. Olivier, *PARI-GP*, Version 1.3.7.
2. D. Bernardi, *Décomprime*, Version 1.0, un program de décomposition des nombres en facteurs premiers utilisant les courbes elliptiques.
3. H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math., vol. 138, Springer Verlag, Berlin, 1993. MR **94i:**11105
4. J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1992. MR **93m:**11053
5. S. Fermiger, *Un exemple de courbe elliptique definie sur* $\mathbb{Q}$ *de rang* ≥ 19, C.R. Acad. Sci. Paris **315** (1992), 719–722.
6. H.G. Folz and H.G. Zimmer, *What is the rank of the Demjanenko matrix?*, J. Symbolic Computation **4** (1987), 53–67. MR **88k:**11038
7. F. Hazama, *Demjanenko matrix, class numbers, and Hodge group*, J. Number Theory **34** (1990), 174–177. MR **90m:**11090
8. A. Kraus, *Quelques remarques a propos des invariants* c_4, c_6, *et* Δ *d'une courbe elliptique*, Acta Arith. **54** (1989), 75–80. MR **90j:**11045
9. M. Laska, *An algorithm for finding a minimal Weierstrass equation for an elliptic curve*, Math. Comp. **38** (1982), 257–260. MR **84e:**14033
10. H. Lenstra Jr., *Factoring integers with elliptic curves*, Annals of Math. **126** (1987), 649–673. MR **89g:**11125
11. J.-F. Mestre, *Construction de courbes elliptique sur* $\mathbb{Q}$ *de rang* ≥ 12, C.R. Acad. Sci. Paris **295** (1982), 643–644. MR **84b:**14019
12. ———, *Un exemple de courbes elliptique definie sur* $\mathbb{Q}$ *de rang* ≥ 15, C.R. Acad. Sci. Paris **314** (1992), 453–455. MR **93b:**11071
13. K. Nagao, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* ≥ 20, Proc. Japan Acad. **69** (1993), 291–293. MR **95a:**11052
14. K. Nagao and T. Kouya, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* ≥ 21, Proc. Japan Acad. **70** (1994), 104–105. MR **95e:**11063
15. H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985. MR **88k:**11002
16. J. Sands and W. Schwarz, *A Demjanenko matrix for abelian fields of prime power conductor*, J. Number Theory **52** (1995), 85–97. MR **96b:**11141
17. W. Schwarz, *Demjanenko matrix and 2-divisibility of class numbers*, Arch. Math. **60** (1993), 154–156. MR **94g:**11095
18. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1986. MR **87g:**11070
19. ———, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 151, Springer-Verlag, Berlin and New York, 1994. MR **96b:**11074
20. ———, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), 339–358. MR **89d:**11049
21. H.M. Tschöpe and H.G. Zimmer, *Computation of the Néron-Tate height on elliptic curves*, Math. Comp. **48** (1987), 351–370. MR **87m:**14025
22. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variable IV (B.J. Birch and W.Kuyk, eds.), (Antwerp, 1972, Lect. Notes in Math. 272, Springer-Verlag, Berlin, 1975. MR **52:**13850
23. H. Zimmer, *A limit formula for the canonical height of an elliptic curve and its application to height computations.*, Number Theory (R.A. Mollin, ed.), Walter de Gruyter, Berlin–New York, 1990, pp. 641–659. MR **93d:**11060

Mathematics Department, Box 1917, Brown University, Providence, Rhode Island 02912

E-mail address: jhs@gauss.math.brown.edu