CANONICAL HEIGHTS ON THE JACOBIANS OF CURVES OF GENUS 2 AND THE INFINITE DESCENT

E.V. FLYNN AND N.P. SMART

Abstract. We give an algorithm to compute the canonical height on a Jacobian of a curve of genus 2. The computations involve only working with the Kummer surface and so lengthy computations with divisors in the Jacobian are avoided. We use this height algorithm to give an algorithm to perform the "infinite descent" stage of computing the Mordell-Weil group. This last stage is performed by a lattice enlarging procedure.

1. Introduction

The theory of the canonical height for abelian varieties is very well understood in the theoretical literature, see for instance [10]. However the only situation where the understanding is full enough to admit a method to actually compute such objects is the theory of elliptic curves, see [16] and [18]. One of the main reasons for wanting to be able to compute the canonical height is to perform efficiently the infinite descent and hence compute a basis for the Mordell-Weil group of an elliptic curve given representatives for E/mE. To do this one needs to bound the difference between the canonical and the naive heights. A naive way of doing this is explained in [3] and [17], however a much more efficient algorithm has recently been given by Siksek, [14].

In this paper we shall explain how using a direct analogue of Siksek's method one can perform, for some examples, an infinite descent on Jacobians of curves of genus 2. In other words we compute explicit generators for their Mordell-Weil groups. To perform such a step we hence require an algorithm to compute the canonical height on such Jacobians and a method to bound the difference between the two height functions.

The authors would like to thank S. Siksek, M. Stoll, E. Schaefer and an anonymous referee for many helpful comments. The second author would like to acknowledge the support of an EPSRC grant which aided the research described in this paper.

2. Definitions

We shall assume throughout that C is a curve of genus 2, defined over $\mathbb{Q}$, given by an equation of the form

$$C : Y^2 = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0,$$

where, without loss of generality, we shall assume that the f_i are all in $\mathbb{Z}$. Let $J(\mathbb{Q})$ denote the Mordell-Weil group of the Jacobian of C. This is given by unordered pairs of points, $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, which are fixed (as a pair) by the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, following the notation in [2][Chapter 8]. We assume that our

pairs could include the points ∞_+ and ∞_-. We have to blow down pairs of the form $\{(x,y),(x,-y)\}$ to the canonical divisor $\mathcal{O}$, which forms the zero of the group law on $J(\mathbb{Q})$. Let $K \subset \mathbb{P}^3$ denote the Kummer surface of $J(\mathbb{Q})$. This surface is given by the quartic equation in $\mathbb{P}^3$,

$$R(k_1,k_2,k_3)k_4^2 + S(k_1,k_2,k_3)k_4 + T(k_1,k_2,k_3) = 0, \tag{1}$$

where R, S, T are given by:

$$\begin{aligned}
R(k_1,k_2,k_3) &= k_2^2 - 4k_1k_3,\\
S(k_1,k_2,k_3) &= -2\left(2k_1^3f_0 + k_1^2k_2f_1 + 2k_1^2k_3f_2 + k_1k_2k_3f_3 + 2k_1k_3^2f_4\right.\\
&\quad \left. + k_2k_3^2f_5 + 2k_3^3f_6\right),\\
T(k_1,k_2,k_3) &= -4k_1^4f_0f_2 + k_1^4f_1^2 - 4k_1^3k_2f_0f_3 - 2k_1^3k_3f_1f_3 - 4k_1^2k_2^2f_0f_4\\
&\quad + 4k_1^2k_2k_3f_0f_5 - 4k_1^2k_2k_3f_1f_4 - 4k_1^2k_3^2f_0f_6 + 2k_1^2k_3^2f_1f_5\\
&\quad - 4k_1^2k_3^2f_2f_4 + k_1^2k_3^2f_3^2 - 4k_1k_2^3f_0f_5 + 8k_1k_2^2k_3f_0f_6 - 4k_2^4f_0f_6\\
&\quad - 4k_1k_2^2k_3f_1f_5 + 4k_1k_2k_3^2f_1f_6 - 4k_1k_2k_3^2f_2f_5 - 2k_1k_3^3f_3f_5\\
&\quad - 4k_2^3k_3f_1f_6 - 4k_2^2k_3^2f_2f_6 - 4k_2k_3^3f_3f_6 - 4k_3^4f_4f_6 + k_3^4f_5^2.
\end{aligned}$$

We have a map

$$\kappa : \left\{ \begin{array}{ccc} J(\mathbb{Q}) & \to & K \\ P=\{P_1,P_2\} & \mapsto & \mathbf{k}_P = (1,k_2,k_3,k_4) \\ P=\{P_1,\infty_\pm\} & \mapsto & \mathbf{k}_P = (0,1,k_3,k_4) \\ P=\{\infty_\pm,\infty_\pm\} & \mapsto & \mathbf{k}_P = (0,0,1,k_4) \\ P=\{\infty_+,\infty_-\}=\mathcal{O} & \mapsto & \mathbf{k}_P = (0,0,0,1) \end{array} \right. .$$

Throughout this paper we shall assume, unless otherwise stated, that every point on the Kummer surface is normalized so that the first non-zero coordinate is equal to one.

In the case where the pair $\{P_1,P_2\}$ does not contain a point at infinity and $P_1 \neq P_2$ we have: $k_1 = 1, k_2 = x_1 + x_2, k_3 = x_1x_2$ and k_4 given by

$$k_4 = \left(\begin{array}{l} 2f_0 + f_1x_1 + f_1x_2 + 2f_2x_1x_2 + f_3x_1^2x_2 + f_3x_1x_2^2 \\ +2f_4x_1^2x_2^2 + f_5x_1^3x_2^2 + f_5x_1^2x_2^3 + 2f_6x_1^3x_2^3 - 2y_1y_2 \end{array} \right) /(x_1-x_2)^2.$$

In the case where the pair $\{P_1,P_2\}$ does not contain a point at infinity and $P_1 = P_2$ we have k_1,k_2,k_3 as before, but now k_4 is uniquely determined by equation (1). In the case where the pair is $\{(x_1,y_1),\infty_\pm\}$, we have $k_1 = 0, k_2 = 1, k_3 = x_1$ and $k_4 = f_5x_1^2 + 2f_6x_1^3 - (\pm\sqrt{f_6}2y_1)$. Finally when the pair consists of two equal points at infinity then the value of k_4 can be determined from equation (1). By abuse of notation we shall also refer to the point $(0,0,0,1)$ on the Kummer as $\mathcal{O}$.

The map κ is analogous to the map

$$f : \left\{ \begin{array}{ccc} E & \to & \mathbb{P}^1 \\ (x,y) & \mapsto & x \end{array} \right.$$

on an elliptic curve as it is $2:1$ mapping P and $-P$ to the same element except on the points of order 2 and $\mathcal{O}$, where it is injective.

Following Gross, [9], we define the naive height and canonical height on $J(\mathbb{Q})$ by

$$h_K(\{P_1,P_2\}) = h(\mathbf{k}_P)\ ,\ \hat{h}(\{P_1,P_2\}) = \lim_{n\to\infty} \frac{1}{n^2} h([n]\mathbf{k}_P)$$

where h denotes the standard height on projective space and $[n]$ denotes the map on the Kummer surface induced by the multiplication by $[n]$ map on the Jacobian.

We shall also refer to this induced map as multiplication by $[n]$ on the Kummer. All the standard properties of a canonical height can then be derived. The proofs are analogous to the elliptic case explained in Silverman, [15][Pages 228-231], upon noting the following fact which is shown in [7]:

$$h_K(P+Q)+h_K(P-Q)=2h_K(P)+2h_K(Q)+O(1).$$

Our goal is to compute $\hat{h}$. By general theory, see for instance [10], there exist local height functions:

$$\hat{\lambda}_p : J(\mathbb{Q}_p) \to \mathbb{R}$$

such that

$$\hat{h}(P)=\sum_p \hat{\lambda}_p(P),$$

where the sum is over all finite and infinite primes. We shall follow this approach of breaking the canonical height into local components in this paper. We assume throughout that all the absolute values are normalized so that the product formula holds.

3. Multiplication By Two

In this section we look at the induced multiplication by two map on the Kummer. We need to find for which primes such a map becomes "degenerate" (that is, primes p for which there exists a point $\mathbf{k}$ in projective space over $\mathbb{F}_p$, such that the duplication formula applied to $\mathbf{k}$ evaluates to 0 in $\mathbb{F}_p$ at every coordinate) and for each such prime what is the minimum power of the prime one needs for it to stop being "degenerate". This will be used later to bound the difference between the canonical and the naive heights.

Let $\mathbf{k}=(k_1,k_2,k_3,k_4)$ be a point on K; then we denote by $\delta(\mathbf{k})$ the point on K such that $[2]\mathbf{k}=\delta(\mathbf{k})=(\delta_1,\delta_2,\delta_3,\delta_4)$, where $[2]$ denotes the induced multiplication by 2 map, $\delta(\mathbf{k})$ is given by the formulae in [5]. It is these formulae for $\delta(\mathbf{k})$ that we shall use in our main algorithm. The formulae for $\delta(\mathbf{k})$ are too long to reproduce here but are at: www.maths.ox.ac.uk/~flynn/genus2/kummer/duplication

We wish to study the function

$$E_p(\mathbf{k})=\frac{\max\left(|\delta_1|_p,|\delta_2|_p,|\delta_3|_p,|\delta_4|_p\right)}{\max\left(|k_1|_p,|k_2|_p,|k_3|_p,|k_4|_p\right)^4},$$

which does not depend on the choice of normalization of the k_i which we make. The main result we shall need is

Lemma 1. *If $J(\mathbb{Q})$ has good reduction at an odd prime p, then $E_p(\mathbf{k})=1$.*

Proof. Let $P \in J(\mathbb{Q}_p)$ and choose coordinates $(k_1,\ldots,k_4)$ for $\kappa(P)$ such that $\max(|k_1|_p,\ldots,|k_4|_p)=1$. Reduction mod p of these coordinates gives coordinates for the image of $\tilde{P}$ on the Kummer $\tilde{K}$ belonging to the reduced Jacobian $\tilde{J}$. Since δ is well-defined on $\mathbb{P}^3$ and reduction mod p commutes with everything, we must have $\max(|\delta_1|_p,\ldots,|\delta_4|_p)=1$. □

There is another description of the multiplication by 2 map in terms of a composition of linear and quadratic maps, [2][Chapter 12] and [7]. We recap on this here. Consider the curve

$$C : Y^2=F(X)$$

where $F(X)$ is a sextic polynomial. We extend the ground field to a number field M, if necessary, so we can write C in the form

$$C : Y^2 = q_1(X)q_2(X)q_3(X) = (\alpha_1X^2+\beta_1X+\gamma_1)(\alpha_2X^2+\beta_2X+\gamma_2)(\alpha_3X^2+\beta_3X+\gamma_3).$$

We then set

$$\Delta = \Delta(q_1, q_2, q_3) = \begin{vmatrix} \gamma_1 & \beta_1 & \alpha_1 \\ \gamma_2 & \beta_2 & \alpha_2 \\ \gamma_3 & \beta_3 & \alpha_3 \end{vmatrix}.$$

Lemma 2. *Let C be a curve of genus 2 in the form $Y^2 = F(X)$, where $F(X)$ is a sextic with nonzero discriminant. Then it is always possible, over the algebraic closure, to write $F(X) = q_1(X)q_2(X)q_3(X)$, so that $\Delta = \Delta(q_1, q_2, q_3) \neq 0$.*

Proof. Write $F(X) = f_6(X - \alpha_1)\dots(X - \alpha_6)$ over the algebraic closure, with $\alpha_1, \dots, \alpha_6$ distinct and $f_6 \neq 0$. Take $q_1(X) = f_6(X - \alpha_1)(X - \alpha_2)$, $q_2(X) = (X - \alpha_3)(X - \alpha_4)$, $q_3(X) = (X - \alpha_5)(X - \alpha_6)$. Note that a fractional linear transformation $X \mapsto (aX + b)/(cX + d)$, $Y \mapsto Y/(cX + d)^3$, where $ad - bc \neq 0$, maps C to an isomorphic curve of genus 2, of the form $Y^2 =$ quintic or sextic in X; furthermore, Δ of the new curve is a nonzero constant times that of the original curve. Now choose a, b, c, d so that $\alpha_1, \alpha_2, \alpha_3$ are mapped to $\infty, 0, 1$, respectively, and let β, γ, δ denote the images of $\alpha_4, \alpha_5, \alpha_6$, respectively. This gives $D : Y^2 = X(X - 1)(X - \beta)(X - \gamma)(X - \delta)$ as the image curve of genus 2. Suppose that it is never possible to write $F(X)$ as described in the Lemma. Then Δ of q_1, q_2, q_3 above must be zero, and so Δ of $X, (X-1)(X-\beta), (X-\gamma)(X-\delta)$, namely $\beta-\gamma\delta$, must be zero also. Repeating the same argument, but with $\alpha_4, \alpha_5, \alpha_6$ permuted, gives that $\gamma - \beta\delta = 0$ and $\delta - \beta\gamma = 0$. These three equations in β, γ, δ imply either that at least one of them is zero, or that two of them are equal, contradicting the fact that the curve D is of genus 2. □

We shall always make the choice of q_1, q_2, q_3 of the above Lemma. This will allow us to decompose the multiplication by 2 map into a composition of linear and quadratic maps, as we shall now explain.

Using the short hand $[p, q] = p'q - q'p$ we define

$$\hat{q}_1(X) = [q_2, q_3] \ , \ \hat{q}_2(X) = [q_3, q_1] \ , \ \hat{q}_3(X) = [q_1, q_2].$$

The Jacobian of C is isogenous via the Richelot isogeny to the Jacobian of the following curve

$$\hat{C} : \Delta Y^2 = \hat{q}_1(X)\hat{q}_2(X)\hat{q}_3(X).$$

The point is that we can decompose the duplication map as the composition of the Richelot isogeny and its dual. Then setting

$$b_{i,j} = R(q_i, q_j) \ , \ \hat{b}_{i,j} = R(\hat{q}_i, \hat{q}_j),$$

where $R(f, g)$ denotes the resultant of two polynomials, we define

$$b_i = b_{i,j}b_{i,k} \ , \ \hat{b}_i = \hat{b}_{i,j}\hat{b}_{i,k} \ \text{ where } \{i, j, k\} = \{1, 2, 3\}.$$

We can find three matrices W_1, W_2, W_3 with coefficients in $L = M(\sqrt{b_1}, \sqrt{b_2}, \sqrt{\hat{b}_1}, \sqrt{\hat{b}_2})$ such that the duplication map can be written

$$\delta(\mathbf{k}) = [2]\mathbf{k} = W_1\tau W_2\tau W_3\mathbf{k},$$

where τ is the map which sends (v_i) to (v_i^2).

The p-adic matrix norm of a matrix, $A = (a_{i,j})$, is defined by

$$|A|_p = \max_{i,j} |a_{i,j}|_p,$$

where $|a_{i,j}|_p$ is some arbitrarily chosen extension of the p-adic valuation to the field L. This norm satisfies the inequality $|A\mathbf{x}|_p \leq |A|_p|\mathbf{x}|_p$. Using this norm we define $w_i(p)$ by

$$p^{w_i(p)} = |W_i^{-1}|_p \text{ for } i \in \{1,2,3\}.$$

¿From the explicit definitions of the W_i in [7][pages 3011-3012] we know that $w_i(p) = 0$ for all p such that $|2\Delta D_F|_p = 1$, where D_F is the discriminant of $F(X)$. We can now give upper and lower bounds on the function $E_p(\mathbf{k})$, for a finite prime p, using this decomposition of the multiplication by [2] map.

Lemma 3. *Let p denote a finite prime and define v by*

$$v = w_1(p) + 2w_2(p) + 4w_3(p)$$

then

$$p^{-v} \leq E_p(\mathbf{k}) \leq 1.$$

Proof. We can assume, as the δ_i are expressed as quartic forms in the k_i, that we have

$$|\mathbf{k}|_p = \max\left(|k_1|_p, |k_2|_p, |k_3|_p, |k_4|_p\right) = 1.$$

We shall assume that

$$|\delta(\mathbf{k})|_p < p^{-v}$$

and try and deduce a contradiction. But we have

$$\mathbf{k} = W_3^{-1}\tau^{-1}W_2^{-1}\tau^{-1}W_1^{-1}\delta(\mathbf{k}).$$

Hence

$$|\mathbf{k}|_p < p^{w_3+w_2/2+w_1/4-v/4} = 1$$

which contradicts $|\mathbf{k}|_p = 1$.

The upper bound on $E_p(\mathbf{k})$ follows trivially from the definition of $E_p(\mathbf{k})$ as it does not depend on the choice of the normalization for the k_i, hence we can normalize so that the k_i are all coprime integers. In which case all the δ_i are also integers. The upper bound is then immediate. □

¿From the above Lemma we can find a lower bound for $E_p(\mathbf{k})$ directly. Usually it is more practical to use a computational technique rather like [14][Section 2.4] to produce a lower bound. We shall return to this in the examples below.

4. Multiplication By N On The Kummer and Jacobian

For any P on the Jacobian, let $\mathbf{k}_P = \big(k_1(P), k_2(P), k_3(P), k_4(P)\big)$ denote the image on the Kummer surface. Recall from equation (3.4.1) on p.23 of [2] that there are polynomials B_{ij}, biquadratic in the $k_i(P), k_i(Q)$ such that the 4×4 matrix $\big(B_{ij}(\mathbf{k}_P, \mathbf{k}_Q)\big)$ is projectively equal to

$$\big(k_i(P+Q)k_j(P-Q) + k_i(P-Q)k_j(P+Q)\big).$$

These can be obtained by anonymous ftp, from the same site and directory as described near the beginning of Section 3. Suppose now that we are given $\big(k_i(P)\big) = \mathbf{k}_P$ and $\big(k_i(Q)\big) = \mathbf{k}_Q$, but that we do not know P, Q. Then we only know P up to $\pm P$, and Q up to $\pm Q$, and so there are two possibilities for the image on the Kummer surface of the sum, namely $\mathbf{k}_{P+Q}$ and $\mathbf{k}_{P-Q}$. Suppose further that we

are given (m_1, m_2, m_3, m_4), equal to a choice of either $\mathbf{k}_{P+Q}$ or $\mathbf{k}_{P-Q}$. Then the remaining 'companion' choice is given by

$$(n_i) = \big(2m_j B_{ij}(\mathbf{k}_P, \mathbf{k}_Q) - m_i B_{jj}(\mathbf{k}_P, \mathbf{k}_Q)\big),$$

where j is fixed and chosen so that $m_j \neq 0$. In summary, given the image of P, Q on the kummer surface, and given (m_i), one choice of $\mathbf{k}_{P+Q}$ or $\mathbf{k}_{P-Q}$, we can find the 'companion' choice, (n_i), working only on the Kummer surface. Let us say that

$$(n_i) = \text{pseudo-add}\big(\mathbf{k}_P, \mathbf{k}_Q\big) \text{ companion to } (m_i).$$

Note that $(m_i) = (n_i)$ precisely when either P or Q is a point of order 1 or 2.

Now, let $\mathbf{k} = (k_1, k_2, k_3, k_4)$ be some point on the Kummer surface for which we want to find the multiple $[N]\mathbf{k}$. Initialize

$$\mathbf{x} = (0,0,0,1), \quad \mathbf{y} = (k_1, k_2, k_3, k_4), \quad \mathbf{z} = (k_1, k_2, k_3, k_4), \quad M = N.$$

Now perform the following four steps.

IF M is odd THEN replace $\mathbf{x}$ by pseudo-add$(\mathbf{x}, \mathbf{z})$ companion to $\mathbf{y}$.

IF M is even THEN replace $\mathbf{y}$ by pseudo-add$(\mathbf{y}, \mathbf{z})$ companion to $\mathbf{x}$.

Replace $\mathbf{z}$ by its double $\delta(\mathbf{z})$.

Replace M by the integer part of $M/2$.

The δ of the third step is as described in Section 3. On repeating the above four steps until $M = 0$, we see that the final value of $\mathbf{x}$ is guaranteed to be the required $[N]\mathbf{k}$. Only $\mathrm{O}(\log(N))$ steps are required, and only computations on the Kummer surface (as opposed to the Jacobian) are required. This is the natural generalization of the method for elliptic curves, using the projective x-coordinate, described on p.128 of [1].

For performing multiplication, or even general additions, on the Jacobian, it is possible to work entirely with divisors; but then most of the time is spent on the radical simplification steps for the (possibly quadratic) points on the support. Given $P = \{P_1, P_2\}$ and $Q = \{Q_1, Q_2\}$ in the Mordell-Weil group, we can work entirely over $\mathbb{Q}$ by using a $\mathbb{P}^{15}$ embedding of the Jacobian: $\mathbf{z}(P) = \big(z_i(P)\big)$, where $z_0, \ldots, z_{15}$ are as described on p.8 of [2]. The members of the Mordell-Weil group are represented by points in $\mathbb{P}^{15}(\mathbb{Q})$. Recall from Lemma 3.9.1 of [2] that there is a 4×4 matrix of bilinear forms ϕ_{ij}, such that, projectively

$$\big(k_i(P-Q)k_j(P+Q)\big) = \big(\phi_{ij}(\mathbf{z}(P), \mathbf{z}(Q))\big).$$

For at least one value of i, we have $k_i(P-Q) \neq 0$, and for this fixed value of i, the row $\big(k_i(P-Q)k_j(P+Q)\big)$ gives the image of $P+Q$ on the Kummer surface, and so determines two possible choices, say $\mathbf{v}, \mathbf{w}$, as candidates for $\mathbf{z}(P+Q)$. One of these will be $\mathbf{z}(P+Q)$ and the other will be $-\mathbf{z}(P+Q)$. Now apply the bilinear forms to $\mathbf{v}$ and $\mathbf{z}(-P)$ and check whether the result is the same as $(k_i(Q))$; further, apply the bilinear forms to $\mathbf{v}$ and $\mathbf{z}(-Q)$ and check whether the result is the same as $(k_i(P))$. If both of the checks are positive, then we know in total three facts about $\mathbf{v}$, namely:

$$\pm\mathbf{v} = \mathbf{z}(P) + \mathbf{z}(Q), \quad \pm\mathbf{z}(Q) = \mathbf{v} - \mathbf{z}(P), \quad \pm\mathbf{z}(P) = \mathbf{v} - \mathbf{z}(Q).$$

These imply that $\mathbf{v} = \mathbf{z}(P) + \mathbf{z}(Q)$. Note that the first two checks are sufficient unless $\mathbf{z}(P)$ is a point of order 2; the first and third checks are sufficient unless $\mathbf{z}(Q)$ is a point of order 2. If any of the checks fail, then $\mathbf{w} = \mathbf{z}(P) + \mathbf{z}(Q)$. This gives a procedure for a general addition on the Jacobian, from which a fast multiplication-by-N procedure can be easily derived.

5. Decomposing the Canonical Height into Local Components

First we define a naive local height function:

$$\lambda_p : \begin{cases} K(\mathbb{Q}_p) & \to & \mathbb{R} & \\ (k_1,k_2,k_3,k_4) & \mapsto & \log\left(\max\left(1,|k_2/k_1|_p,|k_3/k_1|_p,|k_4/k_1|_p\right)\right) & \text{If } k_1 \neq 0 \\ (0,k_2,k_3,k_4) & \mapsto & \log\left(\max\left(1,|k_3/k_2|_p,|k_4/k_2|_p\right)\right) & \text{If } k_2 \neq 0 \\ (0,0,k_3,k_4) & \mapsto & \log\left(\max\left(1,|k_4/k_3|_p\right)\right) & \text{If } k_3 \neq 0 \\ (0,0,0,k_4) & \mapsto & 0 & \text{Otherwise.} \end{cases}$$

Note that the naive global height is given as the sum of the naive local heights. We also wish to decompose the canonical height into a sum of local height functions. Therefore we will need to modify the naive local height function above.

We define the following local error function which measures the difference between the naive local height and the local height function we wish to define. For $\mathbf{k}_P \in K$ we set

$$\epsilon_p(\mathbf{k}_P) = \begin{cases} \lambda_p([2]\mathbf{k}) - 4\lambda_p(\mathbf{k}) + \log|\delta_1| & \text{If } \delta_1 \neq 0 \\ \lambda_p([2]\mathbf{k}) - 4\lambda_p(\mathbf{k}) + \log|\delta_2| & \text{If } \delta_1 = 0 \text{ and } \delta_2 \neq 0 \\ \lambda_p([2]\mathbf{k}) - 4\lambda_p(\mathbf{k}) + \log|\delta_3| & \text{If } \delta_1 = 0, \delta_2 = 0 \text{ and } \delta_3 \neq 0 \\ \lambda_p([2]\mathbf{k}) - 4\lambda_p(\mathbf{k}) + \log|\delta_4| & \text{If } \delta_1 = 0, \delta_2 = 0 \text{ and } \delta_3 = 0. \end{cases}$$

The above definition depends on the choice of normalization of the point $\mathbf{k}$. As mentioned before we have made the choice such that the first non-zero coordinate of $\mathbf{k}$ is equal to 1. With this choice of normalization we see that another equivalent way of defining $\epsilon_p(\mathbf{k})$ is by $\epsilon_p(\mathbf{k}) = \log E_p(\mathbf{k})$, where

$$E_p(\mathbf{k}) = \frac{\max\left(|\delta_1|_p,|\delta_2|_p,|\delta_3|_p,|\delta_4|_p\right)}{\max\left(|k_1|_p,|k_2|_p,|k_3|_p,|k_4|_p\right)^4}.$$

¿From Lemma 3 we can deduce upper and lower bounds on $E_p(\mathbf{k})$ and hence on $\epsilon_p(\mathbf{k})$ for all finite primes. For the infinite prime we can produce approximate upper and lower bounds by using some well known techniques from Numerical Analysis and Optimization, such as steepest descent.

Hence we can conclude that we have two positive constants, $c_1^{(p)}$ and $c_2^{(p)}$, such that for all $\mathbf{k} \in K(\mathbb{Q}_p)$,

$$-c_1^{(p)} \leq \epsilon_p(\mathbf{k}) \leq c_2^{(p)}.$$

We now apply Tate's method to ϵ_p. Define the following function

$$\mu_p : \begin{cases} K(\mathbb{Q}_p) & \to & \mathbb{R} \\ \mathbf{k} & \mapsto & \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \epsilon_p([2^n]\mathbf{k}) \end{cases}.$$

Since ϵ_p is absolutely bounded the sum defining μ_p converges. Hence μ_p is well defined. As multiplication by m and $\epsilon_p(\mathbf{k}) = \log E_p(\mathbf{k})$ are continuous we see that μ_p gives a bounded continuous function on all of $K(\mathbb{Q}_p)$.

Finally using Tate's telescoping series trick we have

$$4\mu_p(\mathbf{k}) - \mu_p([2]\mathbf{k}) = \sum_{n=0}^{\infty} \frac{1}{4^n}\epsilon_p([2^n]\mathbf{k}) - \sum_{n=0}^{\infty} \frac{1}{4^{n+1}}\epsilon_p([2^{n+1}]\mathbf{k}) = \epsilon_p(\mathbf{k}).$$

We then define the local height function to be

$$\hat{\lambda}_p(P) = \lambda_p(\mathbf{k}_P) + \mu_p(\mathbf{k}_P).$$

In particular this function satisfies

$$\begin{aligned}\hat{\lambda}_p([2]P) &= \lambda_p([2]\mathbf{k}_P) + \mu_p([2]\mathbf{k}_P) \\ &= 4\lambda_p(\mathbf{k}_P) + \epsilon_p(\mathbf{k}_P) - \log|\delta_i|_p + 4\mu_p(\mathbf{k}_P) - \epsilon_p(\mathbf{k}_P) \\ &= 4(\lambda_p(\mathbf{k}_P) + \mu_p(\mathbf{k}_P)) - \log|\delta_i|_p \\ &= 4\hat{\lambda}_p(P) - \log|\delta_i|_p.\end{aligned}$$

As noted above the naive height function is equal to the sum of the naive local height functions. Also we noted above that for almost all finite primes we have that the naive local height and the local height functions are equal. Indeed we can determine the finite set of primes where this does not hold. Hence the local height is also zero except at finitely many places.

We have two positive constants $c_1^{(p)}, c_2^{(p)}$ such that

$$-c_1^{(p)} \leq \epsilon_p(\mathbf{k}) \leq c_2^{(p)}$$

and for almost all primes we have $c_1^{(p)} = c_2^{(p)} = 0$. Hence the following sums are well defined

$$c_1 = \sum_p c_1^{(p)} \ , \ c_2 = \sum_p c_2^{(p)}.$$

Using this we can prove:

Theorem 4. *For all $P \in J(\mathbb{Q})$ we have*

$$\hat{h}(P) = \sum_p \hat{\lambda}_p(P)$$

and

$$-c_1/3 \leq \hat{h}(P) - h_K(P) \leq c_2/3.$$

Proof. Define

$$L : \left\{ \begin{array}{ccc} J(\mathbb{Q}) & \rightarrow & \mathbb{R} \\ P & \mapsto & \sum_p \hat{\lambda}_p(P) \end{array} \right.$$

We also have, as

$$L(P) - h_K(P) = \sum_p \left(\sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \epsilon_p([2^n]\mathbf{k}_P) \right)$$

and $-c_1^{(p)} \leq \epsilon_p(\mathbf{k}_Q) \leq c_2^{(p)}$ for all $Q \in J(Q)$, that

$$-c_1/3 \leq L(P) - h_K(P) \leq c_2/3. \tag{2}$$

Now let $P \in J(\mathbb{Q})$, then we have

$$L([2]P) = \sum 4\hat{\lambda}_p(P) = 4\sum \hat{\lambda}_p(P) = 4L(P).$$

So for all P we have that (2) holds as does $L([2]P) = 4L(P)$. But $\hat{h}(P)$ is the unique function which satisfies these properties, hence $\hat{h}(P) = L(P)$. □

6. Computing The Canonical Height

Having decomposed the canonical height into local factors we therefore need only compute each local factor and sum to produce the desired result. The only trouble with this is dealing with the primes for which the local non-archimedian error functions are non-zero. We would also like to be able to compute the canonical height without performing any integer factorization which is very expensive. To see how to do this in the elliptic curve case see [19].

For the infinite prime we can use the series for μ_p to compute the local height. Computing a rough estimate for $c_1^{(\infty)}$ and $c_2^{(\infty)}$, using say steepest descent on the function $\epsilon_\infty(P)$, will tell us how many terms to take to obtain the desired accuracy.

For the finite primes with non-zero error functions we could proceed as in [16]. However the rather large number of possibilities of bad reduction of a Jacobian makes this method look unpromising. We hence add P to itself until we obtain a point, Q, for which all error functions are zero. We can then compute the non-archimedian contribution as this is just the sum of the naive local heights.

Note in the following algorithm we do not need to determine which primes give non-trivial error functions or anything else which may depend on integer factorization. We will need to determine such primes however to compute the constant c_1 above for use later on in performing the infinite descent.

Algorithm For The Canonical Height.

- **Determine Q.**
  Compute $\kappa(Q) = \kappa([m]P)$ with $m \geq 1$ such that $E_p(\mathbf{k}_Q) = 1$ for all primes p. Note this does not require the determination of the primes p at all and that the multiplication by $[m]$ can be done on the Kummer, on the Jacobian or with divisor classes.
- **Compute Non-Archimedian Component of $\hat{h}(Q)$.**
  This is nothing but the sum of the naive local heights of Q. It is the logarithm of the least common multiple of the denominators of the point $\kappa(Q)$, where we have chosen the normalization, as before, to be the one where the first non-zero coordinate is equal to one.
- **Compute Archimedian Component of $\hat{h}(Q)$.**
  This can be computed to the desired accuracy using the definition of $\hat{\lambda}_p$ and the series defining $\mu_\infty(\mathbf{k}_Q)$.
- **Compute Canonical Height Of P**
  Sum the results from the previous two steps and divide by m^2.

The only thing that remains is to be discussed is how to compute the number m. This is accomplished with the following algorithm.

Algorithm To Find m.

- Set $m = 1$
- Compute $\mathbf{k} = \kappa([m]P)$. Normalize $\mathbf{k}$ so that it contains entries which are integers with gcd equal to 1. Then compute $\delta(\mathbf{k})$.
- If the gcd of the entries of $\delta_1, \ldots, \delta_4$ is not equal to 1 then set $m = m + 1$ and repeat.

Note that, for any choice of m, and for any prime p such that $|2D_F|_p = 1$, it is immediate from Lemma 1 that p does not divide all of $\delta_1, \ldots, \delta_4$. For any p in the finite set of primes for which $|2D_F|_p \neq 1$, there exists an m_p such that $[m_p]P$

lies in the kernel of reduction (see p.71 of [2]); in this case, for any n, $[m_p n]P$ will have p dividing all of κ_i, δ_i, for $i = 1, 2, 3$, but not κ_4, δ_4. Clearly, $m = \mathrm{lcm}(m_p)$, where the least common multiple is taken over all p with $|2D_F|_p \neq 1$, gives an m satisfying the first step of our Algorithm for the Canonical Height. This guarantees the existence of such an m; in practice, we have found that in fact it is sufficient to take a value of m much smaller than $\mathrm{lcm}(m_p)$.

7. The Infinite Descent : Bounding the Index

In this section we show how, given a way to compute the canonical heights of points on the Jacobian, we can compute the index of a subgroup of finite index in $J(\mathbb{Q})$. This uses the ideas in [14].

Let $\hat{J}$ denote the group $J(\mathbb{Q})/J(\mathbb{Q})_{Tors}$, i.e. the free part of $J(\mathbb{Q})$. We assume that we are given independent generators, $P_1, \ldots, P_r$, of a sublattice of $\hat{J}$ of full rank. For example $P_1, \ldots, P_r$ could be a basis of $\hat{J}/m\hat{J}$ for some $m \geq 2$, which do not correspond to points of order dividing m. We let n denote the index of our sublattice in the full lattice. Hence if $n = 1$ then we have generators of the free part of the full Mordell-Weil group of $J(\mathbb{Q})$.

We define the standard height pairing matrix, R, of $P_1, \ldots, P_r$ by:

$$R = (< P_i, P_j >)_{1 \leq i,j \leq r}$$

where for all $P, Q \in J(\mathbb{Q})$ we have

$$< P, Q >= \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right).$$

We call $\mathrm{Reg}(P_1, \ldots, P_r) = \det(R)$ the regulator of the sublattice generated by $P_1, \ldots, P_r$. If the sublattice has index one then this is the regulator of $J(\mathbb{Q})$, which we denote by Reg_J. It follows that

$$\mathrm{Reg}_J = \frac{1}{n^2}\mathrm{Reg}(P_1, \ldots, P_r).$$

We wish to compute a lower bound on Reg_J. To accomplish this we first enumerate all $P \in \hat{J}$ with

$$0 < \hat{h}(P) \leq \lambda$$

with some choice of λ which makes that above enumeration possible. Ideally λ will be chosen as large as possible. The enumeration will be accomplished by searching for all points on the Kummer with naive height less than

$$\lambda + c_1/3.$$

In practice we have found that a value of less than 7 for $\lambda + c_1/3$ seems well within present computing power. However if the value of $c_1/3$ is larger than 7 then our method will only work either through an advance in theory or by using more powerful computing equipment and techniques.

Call the resulting set of points on $\hat{J}$ with $\hat{h}(P) \leq \lambda$, S_1. We then define S_i and M_i by the following rule:

- If $S_i \neq \emptyset$ then let Q_i denote an element of S_i with minimal canonical height. Let $M_i = \hat{h}(Q_i)$ and let
$$S_{i+1} = S_i \setminus < Q_1, \ldots, Q_i > .$$
- If $S_i = \emptyset$ then set $M_i = \lambda$.

Hence if t is the largest integer with $S_t \neq \emptyset$ then $M_1, \ldots, M_t$ are the first t successive minima of $\hat{h}$ and $\lambda = M_{t+1} = \ldots = M_r$ are lower bounds on the other successive minima. A standard result in the Geometry of Numbers, [11][Lemma 3.34], gives us

$$M_1 \ldots M_r \leq \gamma_r^r \mathrm{Reg}_J,$$

where γ_r^r denotes "Hermite's Constants" which are given, for $r \leq 8$, by

$$\begin{array}{llll} \gamma_1^1 = 1, & \gamma_2^2 = \frac{4}{3}, & \gamma_3^3 = 2, & \gamma_4^4 = 4, \\ \gamma_5^5 = 8, & \gamma_6^6 = \frac{64}{3}, & \gamma_7^7 = 64, & \gamma_8^8 = 256, \end{array}$$

but for $r \geq 9$ only upper bounds are known, the best being given by

$$\gamma_r^r \leq \left(\frac{2}{\pi}\right)^r \Gamma\left(\frac{r+4}{2}\right)^2.$$

Given this lower regulator bound we can find an upper bound on the index of our sublattice by

$$n \leq \sqrt{\frac{\mathrm{Reg}(P_1, \ldots, P_r)\gamma_r^r}{M_1 \ldots M_r}}.$$

8. Lattice Enlargement

We now have the problem of either reducing the upper bound on the index to a value less than 2. To do this we again adapt the methods of Siksek, [14].

We suppose we are given a basis $P_1, \ldots, P_r$ of a sublattice of $\hat{J}$. By the previous section we can assume that we also have an upper bound, N, on the index of this sublattice in $\hat{J}$. If $N < 2$ then we clearly can go no further. If our basis was obtained from a 2-descent say via the methods of Schaefer, [12], then if we reduce N to a number less than 3 we have also finished.

We need then to only check for each prime p less than N whether the index of our sublattice is divisible by p. In other words we need to determine if we can find a $Q \in \hat{J}$ and $x_1, \ldots, x_r \in \mathbb{Z}$ with $\gcd(x_1, \ldots, x_r) = 1$ such that

$$\sum_{i=1}^{r} x_i P_i = pQ.$$

It is clear we can assume that $|x_i| \leq (p-1)/2$ hence we have only a finite number of cases to check. However a naive search would be grossly inefficient, hence following Siksek we perform a sieve:

Let $P_{r+1}, \ldots, P_{r+s}$ denote a basis for $J(\mathbb{Q})_{Tors}/pJ(\mathbb{Q})_{Tors}$. Note that $s = 0$ unless there is rational p-torsion present. We define the following $\mathbb{F}_p$ subspace of ${\mathbb{F}_p}^{r+s}$

$$V_p = \left\{ \widetilde{\mathbf{x}} \in {\mathbb{F}_p}^{r+s} : \exists \mathbf{x} \in \mathbb{Z}^{r+s} \text{ with } \widetilde{\mathbf{x}} \equiv \mathbf{x} \pmod{p} \text{ and } \sum_{i=1}^{r+s} x_i P_i \in pJ(\mathbb{Q}) \right\}.$$

The aim of the sieve is to find linear dependencies which reduce the a priori upper bound on the dimension of V_p to something rather small (hopefully 0). We therefore perform the following steps for a moderately sized number of primes q (at least $r+s$).

(1) Find a prime q such that
   - $J(\mathbb{Q})$ has good reduction at q.
   - $|\widetilde{J}(\mathbb{F}_q)|$ is divisible by p but not by p^2.

This second condition could be troublesome especially if there is rational p^2 torsion. We could in this case just revert to a simple search instead of a sieve or use the p-Sylow subgroup of $\widetilde{J}(\mathbb{F}_q)$ as Siksek suggests in the elliptic curve case.

(2) Define l by $lp = |\widetilde{J}(\mathbb{F}_q)|$ and define $\widetilde{P}_i \equiv [l]P_i \pmod q$. If $\widetilde{P}_i \equiv \widetilde{\mathcal{O}}$ for $i = 1, \ldots, r+s$ we reject this value of q and choose another one.

(3) Suppose that $\widetilde{P_j}$ is a non-trivial element of $\widetilde{J}(\mathbb{F}_q)$. By our choice of q it is then clear that $\widetilde{P_j}$ generates $l\widetilde{J}(\mathbb{F}_q)$.

(4) We find m_i such that $\widetilde{P}_i \equiv m_i\widetilde{P_j} \pmod q$. So we obtain the following equation for elements in V_p

$$\sum_{i=1}^{r+s} m_i \widetilde{x}_i \equiv 0 \pmod p. \tag{3}$$

So after a few such steps we can compute the subspace of $\mathbb{F}_p^{r+s}$ defined by our relations (3). This subspace will contain V_p. Hopefully we obtain $V_p = \{0\}$ and we can deduce that p does not divide the index and so pass on to the next prime p.

We are then only left with one problem, which arises when we cannot deduce that $V_p = \{0\}$: given an explicit value of $P \in \hat{J}$ and a prime p determine if there is a $Q \in J(\mathbb{Q})$ such that

$$[p]Q = P.$$

In none of the examples considered did this problem arise, however we shall explain a solution to this problem for completeness.

The difficult and potentially time-consuming situation is when there does in fact exist such a Q, in which case we wish to search for it. First search for a prime q which satisfies:
(a) q is of good reduction.
(b) The p-torsion subgroup of $\widetilde{J}(\mathbb{F}_q)$ is the same as that of $J(\mathbb{Q})$.
(c) The torsion order m of $\widetilde{P}$ (the reduction of P mod q) in $\widetilde{J}(\mathbb{F}_q)$ is coprime to p.
Assuming that such a q has been found, the following gives what seems to be a good technique for searching for Q. One first computes

$$S = [m]P,$$

which is in the kernel of reduction modulo q. Note that, from property (b), $[m]Q$ is in the kernel of reduction for precisely one value of Q satisfying $[p]Q = P$. Let $R = [m]Q$, where Q is taken to be fixed as this choice of Q. Then R is the unique member of the kernel of reduction satisfying

$$[p]R = S.$$

Let $\mathbf{a} = \mathbf{z}(R)$ and $\mathbf{b} = \mathbf{z}(S)$ be the members of $\mathbb{P}^{15}(\mathbb{Q})$ corresponding to R and S, respectively, as described in Section 4. Let $s_i = a_i/a_0$ and $t_i = b_i/b_0$ for $i = 0, \ldots, 15$. The fact that $\mathbf{a}, \mathbf{b}$ are in the kernel of reduction corresponds to the fact that s_i, t_i are divisible by q for $i = 1, \ldots, 15$. Our situation is that we know the values of the t_i and we wish to find the values of the s_i. It is straightforward to solve for the s_i modulo q^2, and then proceed in a Henselian manner to solve for the s_i modulo any desired power of q. Note that, having found the s_i modulo q^r, it is a quick computation to improve this to modulo q^{r+1}.

¿From condition (c), we know that there are λ, μ such that $\lambda m + \mu p = 1$, so that

$$[\lambda]R + [\mu]P = Q.$$

Therefore, we can quickly compute the ratios of the coordinates of $\mathbf{z}(Q)$, modulo any desired power of q. These ratios are in $\mathbb{Q}$, and so the problem of finding Q is reduced to that of deducing each of these members of $\mathbb{Q}$ from their q-adic expansions, which can be done by computing the convergents of the corresponding q-adic continued fractions.

9. Searching For Points On The Kummer

The main bottleneck in our method is searching for points with small naive height on the Kummer surface. We wish to find all $\mathbf{k}$ satisfying equation (1) for which $h(\mathbf{k}) \leq C$. We can obviously assume that the k_i are normalized to be rational integers and to have greatest common divisor equal to one.

However we are not interested in all such $\mathbf{k}$, only those which correspond to a rational point on the Jacobian. Examining the equations of the Jacobian given in [4], we see that the following two functions (at least) should be rational squares;

$$\begin{aligned} t_1(k_1,k_2,k_3,k_4) &= k_3k_4k_1^2 + f_0k_1^4 + f_4k_3^2k_1^2 + f_5k_3^2k_2k_1 + f_6k_3^2k_2^2, \\ t_2(k_1,k_2,k_3,k_4) &= (k_3^2k_4 + f_0k_2^2k_1 + f_1k_2k_3k_1 + f_2k_3^2k_1)k_1 + f_6k_3^4, \end{aligned}$$

where $F(X) = f_6X^6 + \ldots + f_0$. ¿From the defining equation of the Kummer, (1), we know the following function must also be a square

$$t_3(k_1,k_2,k_3) = S(k_1,k_2,k_3)^2 - 4R(k_1,k_2,k_3)T(k_1,k_2,k_3).$$

To search for small points we therefore use a sieve. We choose a prime p and find all possible k_1, k_2, k_3 such that $t_3(k_1,k_2,k_3)$ is a square modulo p. We then solve equation (1) modulo p to find the two possible values of k_4 modulo p. Using the values of $k_1, \ldots, k_4$ we then determine whether $t_1(k_1, \ldots, k_4)$ and $t_2(k_1, \ldots, k_4)$ are both squares. After sieving modulo a few primes we check the remaining cases using exact integer arithmetic.

This is completely analogous to the elliptic curve case. There one uses a quadratic sieve type method to determine which possible x-coordinates in our range could correspond to rational points on the elliptic curve. However unlike the elliptic curve case which is a two parameter sieve we have a three parameter sieving interval. This leads to a much worse runtime behaviour of the search for points of small height.

10. Example One

In this first example we consider the curve of rank one which occurred in the paper by Flynn, Poonen and Schaefer, [8]. They showed that the curve

$$Y^2 = F(X) = X^6 + 8X^5 + 22X^4 + 22X^3 + 5X^2 + 6X + 1$$

has a Jacobian of rank one. The Jacobian has the divisor $P = \{\infty_+, \infty_+\}$ as a point of infinite order, which is also a non-trivial coset representative of $J(\mathbb{Q})/2J(\mathbb{Q})$.

The discriminant of $F(X)$ is divisible only by the primes 2 and 3701. It is far too expensive to apply Lemma 3 directly to deduce lower bounds on $E_p(P)$ for $p = 2$ and 3701, however a simple computer program shows that

$$c_1^{(2)} = 6\log 2 \ , \ c_1^{(3701)} = \log 3701.$$

The program justs finds all p-adic points, $\mathbf{k}$, on the Kummer such that $|\mathbf{k}|_p = 1$ and $E_p(\mathbf{k}) \neq 1$. We hence find, after computing the constants at $p = \infty$ using steepest descent on the function $E_\infty(\mathbf{k})$, that

$$h(P) \leq \hat{h}(P) + 5.599$$

for all $P \in J(\mathbb{Q})$. We find that

$$\kappa(P) = \mathbf{k} = (0, 0, 1, -6)$$

and that

$$\delta(\mathbf{k}) = (-64, 192, 0, 128).$$

Hence we certainly see that we need to take a multiple of P to compute the canonical height as the gcd of the last four numbers is 64. We find that the point $Q = [19]P$ is the first point such that $E_p(\mathbf{k}_Q) = 1$ for all primes p. In particular we see

$$\kappa(Q) = \kappa([19]P) = [19]\mathbf{k} = (-6171, 19716, -1937, 21855)$$

and then

$$\delta([19]\mathbf{k}) = \left(\begin{array}{ll} 25340357118287540, & -62762674467369936, \\ 109810743817017600, & -501849187931653423 \end{array} \right).$$

We find $\hat{h}(Q) = 10.2390242$ and so the canonical height of the point $\{\infty_+, \infty_+\}$ is given by $10.239/19^2 = 0.028$.

We search for all points on the Kummer with naive height less than $5.599 + 0.029 = 5.628$. We find 10 such points (not including the image of $\mathcal{O}$). These points are given by

$$\begin{array}{lll} (0, 0, 1, -6) & (0, 1, -3, 20) & (0, 1, -3, 16) \\ (0, 1, 0, 2) & (0, 1, 0, -2) & (1, -6, 9, 46) \\ (1, -3, 0, -2) & (1, 0, 0, 4) & (3, -12, 1, -6) \\ (9, -27, 0, -14) & & \end{array}$$

We find that all of these points on the Kummer correspond to points on the Jacobian with canonical height greater than or equal to 0.028. Hence the full Mordell-Weil group is generated by $\{\infty_+, \infty_+\}$. To deduce this we do not need the index bounding techniques mentioned in this paper. We are in a rank one case so we need only note that P has been shown to be the smallest point of non-zero canonical height.

11. Example Two

Here we look at the curve

$$Y^2 = X^5 + 16X^4 - 274X^3 + 817X^2 + 178X + 1.$$

In [13], Schaefer has shown that the Jacobian of this curve has rank 7, a set of coset representatives of $J(\mathbb{Q})/2J(\mathbb{Q})$ being given by

$$\begin{array}{ll} \{(-17, 1223), \infty_+\} & \{(-9, 557), \infty_+\} \\ \{(-6, 317), \infty_+\} & \{(-2, 73), \infty_+\} \\ \{(0, 1), \infty_+\} & \{(4, 37), \infty_+\} \\ \{(\beta_1/2, 191), (\beta_2/2, 191)\} & \end{array}$$

where $\beta_1 = (5 - \sqrt{177})$ and $\beta_2 = (5 + \sqrt{177})$. However we require a curve whose coefficient of X^6 is non-zero. Hence we make the change of variable $X \to 1/X$ to obtain the curve

$$C : Y^2 = X^6 + 178X^5 + 817X^4 - 274X^3 + 16X^2 + X$$

which has discriminant $D_C = 191^2 941^4$. The above generators of $J(\mathbb{Q})/2J(\mathbb{Q})$ become

$$P_1 = \{(-1/17, 1223/4913), (0,0)\} \quad P_2 = \{(-1/9, 557/729), (0,0)\}$$
$$P_3 = \{(-1/6, 317/216), (0,0)\} \quad P_4 = \{(-1/2, 73/8), (0,0)\}$$
$$P_5 = \{(0,0), \infty_+\} \quad P_6 = \{(1/4, 37/64), (0,0)\}$$
$$P_7 = \{(-\beta_1/76, \gamma_1), (-\beta_2/76, \gamma_2)\}$$

where $\gamma_1 = (132745 - 12033\sqrt{177})/109744$ and $\gamma_2 = (132745 + 12033\sqrt{177})/109744$. For this curve Lemma 1 tells us that the only primes for which the non-archimedian error functions could be non-zero are $p = 2, 191$ and 941. For these primes it is easy to compute the value of $c_1^{(p)}$ namely:

$$c_1^{(2)} = 4\log(2)\ ,\ c_1^{(191)} = 2\log(191)\ ,\ c_1^{(941)} = 2\log(941).$$

For the infinite prime we compute $c_1^{(\infty)}$ using a numerical method (hence this is only an approximation) to obtain

$$c_1^{(\infty)} \approx 0.$$

Hence we find that

$$c_1 \approx \log(2^4 191^2 941^2),$$

and so for any divisor class P on the Jacobian we have

$$h_K(P) \leq \hat{h}(P) + c_1/3 \leq \hat{h}(P) + 8.9903.$$

It is easy to see that $c_2^{(\infty)} \leq 20.595$, hence if we take the infinite series for the local height at ∞ and truncate it at the N^{th} term then the error will be less than

$$\max(c_1^{(\infty)}, c_2^{(\infty)}) \sum_{i=N+1}^{\infty} \frac{1}{4^{i+1}} = 20.595 \sum_{i=N+1}^{\infty} \frac{1}{4^{i+1}} = \frac{6.865}{4^{N+1}}.$$

Using the algorithm given earlier one can then compute that the regulator of our 7 points is given by 463.4175.

To perform the infinite descent we therefore need to search for points on the Kummer with small height. We have tried various techniques for this, however none has yet been successful enough to enumerate enough points to bound the index of our set of 7 independent points in the full group. We need to be able to find all points on the Kummer with coordinates less than

$$\exp(8.9903 + \epsilon) \approx 10000$$

in absolute value. Hence this example seems to be out of range of the present methods.

12. Example Three

Here we consider the curve

$$C : Y^2 = (X^2 + 6X + 7)(X^2 + 4X + 1)(X^2 + 2X + 3).$$

This was studied by Flynn, [6], where the rank was determined to be 2. Generators of the free part modulo $2J(\mathbb{Q})$ were found to be given by

$$P_1 = \{(-2,3), (-2,3)\}\ ,\ P_2 = \{(-1+\sqrt{6}, 16+8\sqrt{6}), (-1-\sqrt{6}, 16-8\sqrt{6})\}.$$

The discriminant of the sextic is given by $-2^{30}3^3$. We find that

$$c_1^{(\infty)} = 2.6836\ ,\ c_2^{(\infty)} = 18.974.$$

Now Lemma 3 gives us

$$c_1^{(2)} \leq 97 \log 2 \ , \ c_1^{(3)} \leq 3 \log 3,$$

and all other $c_1^{(p)}$ for finite p are zero. However again using a simple computer program we can deduce

$$c_1^{(2)} = 16 \log 2 \ , \ c_1^{(3)} = 2 \log 3.$$

We then find the regulator of P_1 and P_2 is given by 1.343. Indeed $\hat{h}(P_1) = 3.055$ and $\hat{h}(P_2) = 1.002$. We find

$$c_1 = c_1^{(2)} + c_1^{(3)} + c_1^{(\infty)} = 16 \log(2) + 2 \log(3) + 2.6836 = 15.97118.$$

Hence we have that

$$h(P) \leq \hat{h}(P) + c_1/3 = \hat{h}(P) + 5.3237.$$

To bound the index we enumerated all points on the Jacobian with canonical height less than $\lambda = 0.206$. This means we needed to find all points on the Kummer with naive height less than $5.529 = 5.323 + 0.206$; this took around 10 hours. Of the 8 such points all have canonical height greater than 1.002. Hence we know that there are no points on the Jacobian with canonical height less than 0.206. Hence we derive the following upper bound on the index of the two points P_1, P_2 in the whole group:

$$n \leq \sqrt{\frac{\frac{4}{3} 1.343}{\lambda^2}} = 6.5.$$

It follows that the only primes which we need to check to possibly enlarge the subgroup are 3 and 5. This is because the subgroup of finite index arose by a descent via Richelot isogeny, [6], and hence 2 cannot divide the index.

We first consider the prime 3. We wish to determine whether the equation

$$x_1 P_1 + x_2 P_2 = [3] Q$$

is satisfied for some $Q \in J(\mathbb{Q})$ and $a_i \in \{-1, 0, 1\}$ not both zero. Note that $\widetilde{J}(\mathbb{F}_5)$ has order 60 and hence we find, setting

$$[20]P_1 \equiv \widetilde{P_1} \equiv \widetilde{\mathcal{O}} \pmod 5 \text{ and } [20]P_2 \equiv \widetilde{P_2} \not\equiv \widetilde{\mathcal{O}} \pmod 5$$

that we must have $x_2 = 0$. Then looking at $\widetilde{J}(\mathbb{F}_{17})$, which has order 336, we see that

$$\widetilde{P_1} \equiv [112]P_1 \equiv [112]P_2 \equiv \widetilde{P_2} \not\equiv \widetilde{\mathcal{O}} \pmod{17}.$$

¿From this we conclude that $x_1 \equiv -x_2 \pmod 3$ and hence $x_1 = x_2 = 0$. Hence we cannot find a subgroup of index 3.

We finally see if we can find a subgroup of index 5. This means determining whether the following equation has any solutions:

$$x_1 P_1 + x_2 P_2 = [5] Q$$

where $Q \in J(\mathbb{Q})$ with $x_i \in \{-2, -1, 0, 1, 2\}$ not both zero. Using again $\widetilde{J}(\mathbb{F}_5)$ we find

$$\widetilde{P_1} \equiv [12]P_1 \equiv [12]P_2 \equiv \widetilde{P_2} \not\equiv \widetilde{\mathcal{O}} \pmod 5.$$

Hence $x_1 \equiv -x_2 \pmod 5$. We then look at $\widetilde{J}(\mathbb{F}_{13})$ which has order 180. Here we see, setting

$$\widetilde{P_1} \equiv [36]P_1 \pmod{13} \text{ and } \widetilde{P_2} \equiv [36]P_2 \pmod{13},$$

that $\widetilde{P_2} = 4\widetilde{P_1} \neq \widetilde{\mathcal{O}}$ and so $x_1 \equiv x_2 \pmod 5$. Hence $x_1 = x_2 = 0$ and the group has no subgroups of index 5.

Hence the free part of the Mordell-Weil group of $J(\mathbb{Q})$ is generated by P_1 and P_2.

References

[1] J.W.S. Cassels. *Lectures on Elliptic Curves*. LMS Student Texts, Cambridge University Press, 1991.

[2] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*. Cambridge University Press, 1996.

[3] J.E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1992.

[4] E.V. Flynn. The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. *Proc. Camb. Phil. Soc.*, Vol 107, pp 425–441, 1990.

[5] E.V. Flynn. The group law on the Jacobian of a curve of genus 2. *J. reine. angew. Math.*, Vol 439, pp 45–69, 1993.

[6] E.V. Flynn. Descent via isogeny in dimension 2. *Acta. Arith.*, Vol 66, pp 23–43, 1994.

[7] E.V. Flynn. An explicit theory of heights. *Trans. AMS*, Vol 347, pp 3003–3015, 1995.

[8] E.V. Flynn, B. Poonen, and E.F. Schaefer. Cycles of quadratic polynomials and rational points on a genus 2 curve. *Preprint*, 1996.

[9] B. Gross. Local heights on curves. In *Arithmetic Geometry*, Ed. Cornell and Silverman, pages 327–339. Springer-Verlag, 1986.

[10] S. Lang. *Fundamentals of Diophantine Geometry*. Springer-Verlag, 1983.

[11] M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory*. Cambridge University Press, 1989.

[12] E.F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. *J. Number Theory*, Vol 51, pp 219–232, 1995.

[13] E.F. Schaefer. Class groups and Selmer groups. *J. Number Theory*, Vol 56, pp 79–114, 1996.

[14] S. Siksek. Infinite descent on elliptic curves. *Rocky Mountain Journal of Maths*, Vol 25, pp 1501–1538, 1995.

[15] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.

[16] J.H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, Vol 51, pp 339–358, 1988.

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

[18] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.

[19] J.H. Silverman. Computing canonical heights with little (or no) factorization. *Preprint*, 1996.

Mathematical Institute, University of Oxford, Oxford OX1 3LB
E-mail address: flynn@maths.ox.ac.uk

Institute Of Maths and Stats, University of Kent at Canterbury, Canterbury, Kent, CT2 7NF
E-mail address: N.P.Smart@ukc.ac.uk