Compositio Mathematica **105:** 79–94, 1997.

A flexible method for applying Chabauty's Theorem

E. V. FLYNN
Department of Pure Mathematics, University of Liverpool, P.O. Box 147, Liverpool, L69 3BX, England. e-mail: evflynn@liv.ac.uk

Received 13 March 1995; accepted in final form 20 November 1995

Abstract. A strategy is proposed for applying Chabauty's Theorem to hyperelliptic curves of genus > 1. In the genus 2 case, it shown how recent developments on the formal group of the Jacobian can be used to give a flexible and computationally viable method for applying this strategy. The details are described for a general curve of genus 2, and are then applied to find $\mathcal{C}(\mathbb{Q})$ for a selection of curves. A fringe benefit is a more explicit proof of a result of Coleman.

Key words: Jacobians, curves, rational points, Chabauty, formal groups.

0. Introduction

We recall the following result of Chabauty [4], which gives a way of deducing information about the K-rational points on a curve from its Jacobian.

PROPOSITION 0.1. *Let $\mathcal{C}$ be a curve of genus g defined over a number field K, whose Jacobian has Mordell–Weil rank $\leqslant g-1$. Then $\mathcal{C}$ has only finitely many K-rational points.*

This is a weaker result than Faltings' Theorem; however, when applicable, Chabauty's method can often be used to give good bounds for the number of points on a curve. For example, McCallum in [14], [15] obtains conditional bounds on the number of rational points on the Fermat curves, and Coleman [5] has given the following conditional genus 2 applications.

PROPOSITION 0.2. *Let $\mathcal{C}$ be a curve of genus 2 defined over $\mathbb{Q}$, and $p \geqslant 4$ be a prime of good reduction. If the Jacobian of $\mathcal{C}$ has rank at most 1 and $\tilde{\mathcal{C}}$ is the reduction of $\mathcal{C}$ mod p then $\#\mathcal{C}(\mathbb{Q}) \leqslant \#\tilde{\mathcal{C}}(\mathbb{F}_p) + 2$.* □

PROPOSITION 0.3. *Let $\mathcal{C}$ be the curve of genus 2:*

$$\mathcal{C}: Y^2 = X(X^2-1)(X-1/\lambda)(X^2+aX+b),$$

with $\lambda, a, b \in \mathbb{Z}$. Suppose $3^{2r} \| \lambda$, for some $r > 0$, and 3 does not divide $b(1-a+b)(1+a+b)$, and that the Jacobian of $\mathcal{C}$ has rank at most 1. Then

$\mathcal{C}(\mathbb{Q})$ contains precisely the points $(0,0),(1,0),(-1,0),(1/\lambda,0)$ and the 2 rational points at infinity. □

The only non-trivial application of Proposition 0.2 in the literature is due to Gordon and Grant [11], [13].

EXAMPLE 0.4. Let $\mathcal{C}$ be the curve $Y^2 = X(X-1)(X-2)(X-5)(X-6)$ defined over $\mathbb{Q}$. Then $\mathcal{J}(\mathbb{Q})$ has rank 1 and $\#\mathcal{C}(\mathbb{Q}) = \#\tilde{\mathcal{C}}(\mathbb{F}_7) + 2 = 10$. □

It seems likely that it will be hard to find many other direct applications of Proposition 0.2 which will resolve $\#\mathcal{C}(\mathbb{Q})$ completely, since one requires the bound $\#\tilde{\mathcal{C}}(\mathbb{F}_p) + 2$ to be attained. However, there have recently been applications of Proposition 0.3 in [10], such as the following examples.

EXAMPLE 0.5. The Jacobian of the curve: $Y^2 = X(X^2-1)(X-\frac{1}{9})(X^2 - 18X + 1)$ has rank 1 over $\mathbb{Q}$. Hence, by Proposition 0.3, there are no $\mathbb{Q}$-rational points on the curve apart from the points $(0,0),(1,0),(-1,0),(1/9,0)$ and the 2 rational points at infinity. Similarly, the Jacobian of the curve: $Y^2 = X(X^2-1)(X+\frac{1}{9})(X^2 - 4X - 1)$ has rank 1 over $\mathbb{Q}$. Hence, by Proposition 0.3, there are no $\mathbb{Q}$-rational points on the curve apart from the points $(0,0),(1,0),(-1,0),(-1/9,0)$ and the 2 rational points at infinity. □

The above 3 examples are the only non-trivial applications of these methods so far which have resolved $\mathcal{C}(\mathbb{Q})$ entirely. For a typical curve, apart from the above special cases, it would be desirable to have a direct method of exploiting the arithmetic information specific to the curve. Chabauty's general strategy [4] in the genus 2 case can be described as follows. Let us suppose that the curve $Y^2 = (\text{sextic in } X)$ of genus 2 is defined over a number field K, and that $\mathcal{J}(K)$, the group of K-rational points on the Jacobian, has been shown to have rank 1, generated by the torsion group and the non-torsion generator D. Let v be any place of good reduction, K_v be the completion of K with respect to v, and k_v be the residue field. Further, let $\tilde{D}$ be the image of D under the reduction map from $\mathcal{J}(K_v)$ to $\mathcal{J}(k_v)$, and let M be the torsion order of $\tilde{D}$ (such an M must exist, since $\mathcal{J}(k_v)$ is a finite group). It follows that $D' = M \cdot D$ is in the kernel of reduction, and that any member of $\mathcal{J}(K)$ can be written in the form: $A + N \cdot D'$ for some $N \in \mathbb{Z}$, and some divisor A in the finite set:

$$S = \{B + i \cdot D : B \in \mathcal{J}_{\text{tors}}(K) \text{ and } 0 \leqslant i \leqslant M-1\}.$$

That is to say, $S + D'\mathbb{Z} = \mathcal{J}(K)$. If we now let E and L represent the formal exponential and logarithm maps on the formal group of $\mathcal{J}$, then

$$G = \{A + E(N \cdot L(D')) : A \in S, N \in K_v, |N|_v \leqslant 1\}$$

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

is a one dimensional analytic subgroup of $\mathcal{J}(K_v)$ which contains $\mathcal{J}(K)$. We have a natural map $\mathcal{C} \to \mathcal{J}$ which takes a point P on $\mathcal{C}$ to the class of the divisor $2P - \infty^+ - \infty^-$ (note that the role of ∞^+, ∞^- could be performed by any two distinct points on $\mathcal{C}$ conjugate under the hyperelliptic involution). Let Υ denote the image of $\mathcal{C}$ under this map. The map $\mathcal{C} \to \Upsilon$ is bijective outside the Weierstrass points of $\mathcal{C}$. Following Chabauty, we observe that $\mathcal{C}(K) \subseteq \mathcal{C}(K_v) \cap G$ and the latter set is finite.

Our main aim in this paper is to make this explicit. We shall embed $\mathcal{J}$ into $\mathbb{P}^{15}$ and identify $\Upsilon(K)$, the image of $\mathcal{C}(K)$, as an explicit quadric section of $\mathcal{J}$; $\{j \in \mathcal{J}(K) : q(j) = 0\}$ for some q. Let $h_A(N) = A + N \cdot D'$. Then $\mathcal{C}(K_v) \cap G$ is in one-to-one correspondence with the disjoint union over $A \in S$ of the sets

$$\{N \in K_v : q(h_A(N)) = 0, |N|_v \leqslant 1\}.$$

By using bilinear forms relating to the group law, and an explicit construction of the terms of the formal group, we can construct, for each $A \in S$ a power series

$$\theta(N) = \theta_A(N) = c_0 + c_1 N + c_2 N^2 + \cdots \in K_v[[N]]$$

whose coefficients tend to 0 in K_v, and whose zeroes include all zeroes of $q(h_A(N))$. We shall show how to compute the coefficients $c_i = c_i(A)$ to any desired degree of accuracy, and then use a version of Newton's lemma deduce a bound on the number of zeroes of $\theta_A(N)$. Adding these bounds over all $A \in S$ gives a bound on the size of $\mathcal{C}(K)$, which we hope to be the same as the number of members of $\mathcal{C}(K)$ already known. Note that the bound obtained can differ from the true value of $\mathcal{C}(K)$ when there exist values of $N \in K_v$ with $|N|_v \leqslant 1$ such that N satisfies θ and $N \notin \mathbb{Z}$. In this case, we have the option of trying a new place of good reduction v at which the above process can be repeated; each choice of v gives a new chance that $\mathcal{C}(K)$ will be determined completely. It is not claimed that this is guaranteed to terminate, but we shall see that in practice it seems either to resolve $\mathcal{C}(K)$ completely, or at least to give a very sharp bound. There is also the advantage that, when there is a suspected missing point in $\mathcal{C}(K)$ still to be found, the above process will impose congruence conditions on the possible value of N, speeding the search for the missing point.

The above strategy, and the mechanical details to be presented in Sections 1 and 2, can in principle easily be generalised to hyperelliptic curves of higher genus $g > 2$ for which $\mathcal{J}(K)$ has rank $r < g$, with non-torsion generators $D_1, \ldots, D_r$. The above argument is unchanged, except the M is replaced by $M_1, \ldots, M_r$, and θ replaced by a set of g power series. One would then combine finite resultant computations with Strassman's Theorem to bound the possible values of $N_1, \ldots, N_r$.

Most of the work in implementing the above strategy is contained in the derivation of the power series θ. There are two requirements: the ability to compute arbitrarily many coefficients of θ up to any required degree of accuracy in K_v, and an explicit sequence $d_n \to 0$ such that $|c_n|_v \leqslant d_n$ for all n. In Sections 1

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

and 2 we shall use the formal group, and its associated formal exponential and logarithm maps, to show how both of these can be done for an arbitrary curve of genus 2. We also demonstrate a time-saving refinement which often allows the use of generators of $\mathcal{J}(K)/2\mathcal{J}(K)$, even when generators of $\mathcal{J}(K)$ are not known. In Section 3, we use the technique to compute $\mathcal{C}(\mathbb{Q})$ completely for a selection of curves of genus 2, and give a brief indication of how the technical details might in future be generalised to hyperelliptic curves of genus > 2.

1. The Jacobian variety and formal group

In this section we briefly summarise some of the explicit structures which have been developed in [6], [7], and fix notation. A general curve $\mathcal{C}$ of genus 2, over a ground field K of characteristic not equal to 2, 3 or 5, may be taken to have the form

$$\mathcal{C}: Y^2 = F(X) = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0, \quad (1)$$

with $f_0, \ldots, f_6$ in K, $f_6 \neq 0$, and the discriminant $\Delta(F) \neq 0$. We let $\mathrm{Pic}^0_{\bar{K}}(\mathcal{C})$ denote the Picard group of $\mathcal{C}$ over the algebraic closure $\bar{K}$ of K; that is, the group of divisors of $\mathcal{C}$ of degree 0 modulo linear equivalence ([14], p. 32). We represent [1] any element of $\mathrm{Pic}^0_{\bar{K}}(\mathcal{C})$ by an unordered pair of points $\{(x_1, y_1), (x_2, y_2)\}$ on $\mathcal{C}$, where we also allow ∞^+ and ∞^- (the 2 branches of the singularity of $\mathcal{C}$ at infinity) to appear in the unordered pair. The notation $\{(x_1, y_1), (x_2, y_2)\}$ is shorthand for the divisor: $(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-$. This representation gives a one-to-one correspondence except that we must identify all pairs of the form $\{(x, y), (x, -y)\}$ to give the canonical equivalence class, which we denote by $\mathcal{O}$. Generically, three such elements will sum to $\mathcal{O}$ if there is a function of the form Y – (cubic in X) which meets $\mathcal{C}$ at all 6 component points. The Mordell–Weil group, $\mathrm{Pic}^0_K(\mathcal{C})$, is the subgroup of $\mathrm{Pic}^0_{\bar{K}}(\mathcal{C})$ invariant under Galois action. In our representation, it consists of pairs of points which are either both defined over K, or are conjugate over K and quadratic.

As a group, $\mathrm{Pic}^0_{\bar{K}}(\mathcal{C})$ may be identified with the $\bar{K}$ valued points on the Jacobian of $\mathcal{C}$. Jacobian of $\mathcal{C}$. The Jacobian may be given the structure of a smooth projective variety in $\mathbf{P}$ of dimension 2 using the following basis [2].

DEFINITION 1.1. Let the map $J: \mathrm{Pic}^0_{\bar{K}}(\mathcal{C}) \to \mathbf{P}^{15}$ take $D = \{(x_1, y_1), (x_2, y_2)\} \in \mathrm{Pic}^0_{\bar{K}}(\mathcal{C})$ to $\mathbf{a} = (a_0, \ldots a_{15})$, where $a_0, \ldots a_{15}$ are as follows:

$$\begin{aligned} a_{15} &= (x_1 - x_2)^2, a_{14} = 1, a_{13} = x_1 + x_2, a_{12} = x_1x_2, a_{11} \\ &= x_1x_2(x_1 + x_2), a_{10} = (x_1x_2)^2, \end{aligned}$$

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

$$\begin{aligned}
a_9 &= (y_1 - y_2)/(x_1 - x_2),\ a_8 = (x_2y_1 - x_1y_2)/(x_1 - x_2), a_7 \\
&= (x_2^2y_1 - x_1^2y_2)/(x_1 - x_2), \\
a_6 &= (x_2^3y_1 - x_1^3y_2)/(x_1 - x_2), a_5 = (F_0(x_1, x_2) - 2y_1y_2)/(x_1 - x_2)^2, \\
a_4 &= (F_1(x_1, x_2) - (x_1 + x_2)y_1y_2)/(x_1 - x_2)^2, a_3 = (x_1x_2)a_5, \\
a_2 &= (G_0(x_1, x_2)y_1 - G_0(x_2, x_1)y_2)/(x_1 - x_2)^3, \\
a_1 &= (G_1(x_1, x_2)y_1 - G_1(x_2, x_1)y_2)/(x_1 - x_2)^3, a_0 = a_5^2,
\end{aligned}$$

where

$$\begin{aligned}
F_0(x_1, x_2) &= 2f_0 + f_1(x_1 + x_2) + 2f_2(x_1x_2) + f_3(x_1x_2)(x_1 + x_2) \\
&\quad +2f_4(x_1x_2)^2 + f_5(x_1x_2)^2(x_1 + x_2) + 2f_6(x_1x_2)^3, \\
F_1(x_1, x_2) &= f_0(x_1 + x_2) + 2f_1(x_1x_2) + f_2(x_1x_2)(x_1 + x_2) \\
&\quad +2f_3(x_1x_2)^2 + f_4(x_1x_2)^2(x_1 + x_2) + 2f_5(x_1x_2)^3 \\
&\quad +f_6(x_1x_2)^3(x_1 + x_2), \\
G_0(x_1, x_2) &= 4f_0 + f_1(x_1 + 3x_2) + f_2(2x_1x_2 + 2x_2^2) + f_3(3x_1x_2^2 + x_2^3) \\
&\quad +4f_4(x_1x_2^3) + f_5(x_1^2x_2^3 + 3x_1x_2^4) + f_6(2x_1^2x_2^4 + 2x_1x_2^5), \\
G_1(x_1, x_2) &= f_0(2x_1 + 2x_2) + f_1(3x_1x_2 + x_2^2) + 4f_2(x_1x_2^2) \\
&\quad +f_3(x_1^2x_2^2 + 3x_1x_2^3) + f_4(2x_1^2x_2^3 + 2x_1x_2^4) \\
&\quad +f_5(3x_1^2x_2^4 + x_1x_2^5) + 4f_6(x_1^2x_2^5).
\end{aligned}$$

The canonical divisor class $\mathcal{O}$ is mapped by J to $(1, 0, \ldots, 0)$, and the Mordell–Weil group $\mathrm{Pic}^0_K(\mathcal{C})$ is mapped into $\mathbf{P}^{15}(K)$. There is a simpler embedding into $\mathbf{P}^8$ described in [12] for the special case when $\mathcal{C}$ has a rational Weierstrass point. However, we wish our final power series to provide arithmetic information about any curve of genus 2, regardless of whether it has a rational Weierstrass point, and so we shall use structures based only on the general $\mathbf{P}^{15}$ embedding. The above 16 functions are a basis for the space of functions symmetric in (x_1, y_1) and (x_2, y_2), which may have a pole of any order at $\mathcal{O}$ and are at worst the order of $x_1^2x_2^2$ at infinity, but have no other poles; see [2] for more details. The following result from [6] gives the structure of the Jacobian variety.

THEOREM 1.2. *Let $\mathbb{Z}_\mathbf{f}$ denote $\mathbb{Z}[f_0, \ldots, f_6]$. The 72 quadratic forms over $\mathbb{Z}_\mathbf{f}$ given in the file ~ftp/pub/genus2/jacobian.variety/defining.equations available from the machine ftp.liv.ac.uk by anonymous ftp. are a set of defining equations for the Jacobian variety, denoted $\mathcal{J} = \mathcal{J}(\mathcal{C})$, induced by the embedding of Definition* 1.1. □

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

The map J of Definition 1.1 gives a group isomorphism between $\mathrm{Pic}^0_{\bar{K}}(\mathcal{C})$ and $\mathcal{J}(\bar{K})$, the $\bar{K}$-rational points of $\mathcal{J}$. The restriction of J to $\mathrm{Pic}^0_K(\mathcal{C})$ gives a group isomorphism with $\mathcal{J}(K)$.

The *localised* coordinates: $s_i = a_i/a_0$ for $i = 1, \ldots, 15$ include a pair of local parameters: s_1, s_2. A process of recursive substitution (as described in [6], p. 429) then allows each s_i to be written as formal power series in s_1, s_2 over $\mathbb{Z}_{\mathbf{f}}$.

$$s_i = \sigma_i(s_1, s_2) \in \mathbb{Z}_{\mathbf{f}}[[s_1, s_2]]. \tag{2}$$

It was shown in [6], p. 433, that the formal group induced by the local parameters s_1, s_2 is defined over the same ring as the coefficients of $\mathcal{C}$.

THEOREM 1.3. *Suppose that the ground field K is a non-Archimedean field with valutaion v and that $f_0, \ldots, f_6$ all lie in the valuation ring of K. Let $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathcal{J}(K_v)$ be such that $\mathbf{c} = \mathbf{a} + \mathbf{b}$, where $\mathbf{a} + \mathbf{b}$ is addition in $\mathcal{J}(K_v)$. Further, let $s_1 = a_1/a_0, s_2 = a_2/a_0, t_1 = b_1/b_0, t_2 = b_2/b_0, u_1 = c_1/c_0, u_2 = c_2/c_0$ (the local parameters of $\mathbf{a}, \mathbf{b}, \mathbf{c}$, respectively). Then there is a formal group law $\mathcal{F} = \begin{pmatrix} \mathcal{F}_1 \\ \mathcal{F}_2 \end{pmatrix}$ where $\mathcal{F}_1, \mathcal{F}_2$ are power series in s_1, s_2, t_1, t_2 defined over $\mathbb{Z}_{\mathbf{f}}$, which contain terms only of odd degree. If $\mathbf{a}, \mathbf{b}$ both lie in the kernel of reduction:*

$$\mathcal{N} = \{\mathbf{a} \in \mathcal{J}(K_v) : |s_i(\mathbf{a})|_v < 1, \text{ for } 1 \leqslant i \leqslant 15\}, \tag{3}$$

then $\mathcal{F}_1, \mathcal{F}_2$ converge on $\mathcal{N} \times \mathcal{N}$, and $u_1 = \mathcal{F}_1(s_1, s_2, t_1, t_2)$, $u_2 = \mathcal{F}_2(s_1, s_2, t_1, t_2)$. □

It is described in [6], [7] how the terms of the formal group may be computed up to terms of any given degree. Up to cubic terms the formal group is:

$$\begin{aligned} \mathcal{F}_1 &= s_1 + t_1 + 2f_4 s_1^2 t_1 + 2f_4 s_1 t_1^2 - f_1 s_2^2 t_2 - f_1 s_2 t_2^2 + \cdots, \\ \mathcal{F}_2 &= s_2 + t_2 + 2f_2 s_2^2 t_2 + 2f_2 s_2 t_2^2 - f_5 s_1^2 t_1 - f_5 s_1 t_1^2 + \cdots. \end{aligned} \tag{4}$$

We can therefore describe the group law locally up to any desired degree of accuracy. We shall also require explicit equations which relate to the image of the global group law on the Kummer surface. An embedding of the Kummer surface is given by the functions: $a_5, a_{12}, a_{13}, a_{14}$. For convenience, we introduce the labeling: $k_1 = a_{14}, k_2 = a_{13}, k_3 = a_{12}, k_4 = a_5$, so that:

$$k_1 = 1,\ k_2 = x_1 + x_2,\ k_3 = x_1 x_2,\ k_4 = (F_0(x_1, x_2) - 2y_1 y_2)/(x_1 - x_2)^2, \tag{5}$$

where $F_0(x_1, x_2)$ is as defined in 1.1. For any field L containing K, we let $\mathcal{K}(L)$ represent the image of the map κ on $\mathcal{J}(L)$ which takes $(a_0, \ldots, a_{15})$ to (k_1, k_2, k_3, k_4). The map κ identifies $\pm$; that is to say, $\kappa(\mathbf{a}) = \kappa(-\mathbf{a})$ for any $\mathbf{a} \in \mathcal{J}(L)$.

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

THEOREM 1.4. *Let* $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathcal{J}(L)$ *be such that* $\mathbf{c} = \mathbf{a}+\mathbf{b}$, *where* L *is any field containing* K. *Then the* 4×4 *matrix, given in the file ~ftp/pub/genus 2/jacobian.variety/bilinear.forms available from the machine ftp.liv.ac.uk by anonymous ftp, of bilinear forms* $(\phi_{ij}(\mathbf{a}, \mathbf{b}))$ *defined over* $\mathbb{Z}_\mathbf{f}$ *is projectively equal to the matrix* $(k_i(\mathbf{a} - \mathbf{b})k_j(\mathbf{a} + \mathbf{b}))$. *That is, there exists a constant* $\rho \in L$ *such that* $\rho \neq 0$ *and* $\phi_{ij}(\mathbf{a}, \mathbf{b}) = \rho \cdot k_i(\mathbf{a} - \mathbf{b})k_j(\mathbf{a} + \mathbf{b})$ *for all* i, j. □

For our purposes here, we shall usually only require $(\phi_{41}, \phi_{42}, \phi_{43})$, which projectively give the triple (k_1, k_2, k_3), where $\mathbf{k} = \kappa(\mathbf{c})$, provided that $k_4(\mathbf{a} - \mathbf{b}) \neq 0$. The initial terms of these are as follows.

$$\begin{aligned}
\phi_{41}(\mathbf{a}, \mathbf{b}) &= b_0a_5 + 2a_2b_2 + a_0b_5 + \cdots, \\
\phi_{42}(\mathbf{a}, \mathbf{b}) &= 2a_0b_4 + 2b_1a_2 + 2a_1b_2 + 2b_0a_4 + \cdots, \\
\phi_{43}(\mathbf{a}, \mathbf{b}) &= a_0b_3 + 2a_1b_1 + b_0a_3 + \cdots.
\end{aligned} \tag{6}$$

Note that, in the exceptional situations where $k_4(\mathbf{a} - \mathbf{b}) = 0$, there must always exists an i such that $k_i(\mathbf{a} - \mathbf{b}) = 0$, in which case the above can be replaced by $(\phi_{i1}, \phi_{i2}, \phi_{i3})$.

2. Finding the Strassman bound

In order to obtain information about the series $\theta(N)$, mentioned in the introduction, it is helpful first to derive coefficients of the standard exponential and logarithm of the formal group $\mathcal{F}$.

DEFINITION 2.1. Let $\mathcal{F}$ be the formal group defined over $\mathbb{Z}_\mathbf{f}$ as described in Theorem 1.3. Let $\mathbf{s}$ be a shorthand notation for the pair of variables $\begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$; similarly $\mathbf{t}$ for $\begin{pmatrix} t_1 \\ t_2 \end{pmatrix}$. Define the *formal exponential of* $\mathcal{F}$ as $E = \begin{pmatrix} E_1 \\ E_2 \end{pmatrix}$, where E_1, E_2 are power series in $\mathbf{s}$ over the field of fractions of $\mathbb{Z}_\mathbf{f}$, by: $E(\mathbf{s}) = \mathbf{s} +$ terms of higher degree, and $E(\mathbf{s} + \mathbf{t}) = \mathcal{F}(E(\mathbf{s}), E(\mathbf{t}))$. Similarly define the *formal logarithm of* $\mathcal{F}$ as $L = \begin{pmatrix} L_1 \\ L_2 \end{pmatrix}$, where L_1, L_2 are power series in $\mathbf{s}$ over the field of fractions of $\mathbb{Z}_\mathbf{f}$, by: $L(E(\mathbf{s})) = \mathbf{s}$. Equivalently: $L(\mathbf{s}) = \mathbf{s} +$ terms of higher degree, and $L(\mathcal{F}(\mathbf{s}, \mathbf{t})) = L(\mathbf{s}) + L(\mathbf{t})$.

These power series give the formal isomorphism, defined over the field of fractions of $\mathbb{Z}_\mathbf{f}$, between the formal group $\mathcal{F}$ and the additive formal group: $\mathbf{s} + \mathbf{t}$. The following lemma describes what denominators can occur in the coefficients.

LEMMA 2.2. *Let* $\mathcal{F}$, E, L *be as in Definition* 2.1. *Then each of* E_1,E_2,L_1,L_2 *can be written in the form:* $\sum(a_{ij}/i!j!)s_1^i s_2^j$, *where* $a_{ij} \in \mathbb{Z}_\mathbf{f}$ *and* $a_{ij} = 0$ *when* $i + j$ *is even.*

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

Proof. Let $E'(\mathbf{s})$ denote the 2×2 matrix $(\partial E_i/\partial s_j)$. Similarly, let $\mathcal{F}_{\mathbf{s}} = (\partial \mathcal{F}_i/\partial s_j)$ and $\mathcal{F}_{\mathbf{t}} = (\partial \mathcal{F}_i/\partial t_j)$. Differentiating both sides of the equation $E(\mathbf{s}+\mathbf{t}) = \mathcal{F}(E(\mathbf{s}), E(\mathbf{t}))$ with respect to $\mathbf{t}$, and then evaluating at $\mathbf{t} = \mathbf{0}$, gives:

$$E'(\mathbf{s}) = \mathcal{F}_{\mathbf{t}}(E(\mathbf{s}), \mathbf{0}) \cdot E'(\mathbf{0}) = \mathcal{F}_{\mathbf{t}}(E(\mathbf{s}), \mathbf{0}),$$

since $E'(\mathbf{0})$ is the identity matrix. Now, taking derivatives with respect to $\mathbf{s}$ and evaluating at $\mathbf{s} = \mathbf{0}$ gives, by induction on r, that $\partial^r E_k/\partial s_1^i \partial s_2^j \in \mathbb{Z}_{\mathbf{f}}$ and is 0 when r is even. A similar argument on the equation $L(E(\mathbf{s})) = \mathbf{s}$ gives the same result on L_1, L_2. □

Note that the above proof provides an inductive technique for deriving coefficients of $s_1^i s_2^j$ in E, L for all i, j up to any any desired value of $i + j$. For the rest of this section, we assume that the curve $\mathcal{C}$ of equation (1) is defined over a number field K. Without loss of generality, we also assume that the coefficients of the sextic $F(X)$ are algebraic integers. Let v denote a place of good reduction of $\mathcal{C}$, lying above the rational prime p (so that $|p|_v = p^{-1}$). Let K_v be the completion of K with respect to v. The following standard theorem follows from the theory of Newton polygons, as described on p. 62 of [3].

THEOREM 2.3 (Strassman). *Let* $\theta(X) = c_0 + c_1 X + c_2 X^2 + \cdots \in K_v[[X]]$ *satisfy* $c_n \to 0$ *in* K_v. *Define* k *uniquely by:* $|c_k|_v \geqslant |c_i|_v$ *for all* $i \geqslant 0$, *and* $|c_k|_v > |c_i|_v$ *for all* $i > k$. *Then there are at most* k *values of* $x \in K_v$ *such that* $\theta(x) = 0$ *and* $|x|_v \leqslant 1$. □

Note that, when c_k has been identified, it is a finite amount of work to determine the exact number of such solutions (which may be less than k), using the Weierstrass Preparation Theorem [3], p. 107. The following definition will help to keep track of bounds on the valuations of the coefficients of the subsequent power series.

DEFINITION 2.4.

$$\mathcal{P}_m^{(n)}(\mathbf{s}) = \left\{ \phi = \sum_{i+j \geqslant m} b_{ij} s_1^i s_2^j \in K_v[[\mathbf{s}]] : |b_{ij}|_v \leqslant p^{(i+j-n)/(p-1)} \right\}.$$

EXAMPLE 2.5. $E_1, E_2, L_1, L_2 \in \mathcal{P}_1^{(1)}(\mathbf{s})$ since, for $i + j = r$, $|i!j!|_v \geqslant |r!|_v \geqslant p^{-(r-1)/(p-1)}$.

LEMMA 2.6. *Let* $\phi \in \mathcal{P}_m^{(n)}$, $\phi' \in \mathcal{P}_{m'}^{(n')}$. *Then* $\phi \circ \phi' \in \mathcal{P}_{mm'}^{(nn')}$, $\phi + \phi' \in \mathcal{P}_{\min(m,m')}^{(\min(n,n'))}$ *and* $\phi\phi' \in \mathcal{P}_{m+m'}^{(n+n')}$. □

When $\mathbf{s}$ is the vector of local parameters for some $\mathbf{a} \in \mathcal{J}(K_v)$, we let $N \cdot \mathbf{s}$ denote the vector of local parameters for $N \cdot \mathbf{a}$. We are now in a position to develop $N \cdot \mathbf{s}$ as

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

a power series in N, with a sharp bound on the v-adic effect of the denominators. The following is an immediate application.

LEMMA 2.7. *Define* $[N, \mathbf{s}] = E(N \cdot L(\mathbf{s})) = \tau_1(\mathbf{s})N + \tau_3(\mathbf{s})N^3 + \cdots$, *where each* τ_i *represents a* 2×1 *vector whose entries are power series in* s_1, s_2 *over* K_v, *and only odd powers of* N *occur. Then, for all* i, *each component of* $\tau_i(\mathbf{s})$ *lies in* $\mathcal{P}_i^{(1)}(\mathbf{s})$, *and contains only terms of odd degree in* $\mathbf{s}$. □

The first few terms of τ_1 and τ_3 are as follows.

$$\tau_1(\mathbf{s}) = \begin{pmatrix} s_1 - \frac{2}{3}f_4 s_1^3 + \frac{1}{3}f_1 s_2^3 + \cdots \\ s_2 + \frac{1}{3}f_5 s_1^3 - \frac{2}{3}f_2 s_2^3 + \cdots \end{pmatrix}, \ \tau_3(\mathbf{s}) = \begin{pmatrix} \frac{2}{3}f_4 s_1^3 - \frac{1}{3}f_1 s_2^3 + \cdots \\ -\frac{1}{3}f_5 s_1^3 + \frac{2}{3}f_2 s_2^3 + \cdots \end{pmatrix}. \quad (7)$$

In general, a divisor in $\mathrm{Pic}_K^0(\mathcal{C})$ has the special form $\{P, P\}$ precisely when $k_2^2 - 4k_1k_3 = 0$, where k_1, k_2, k_3 are as in equation (5). Let $A, B \in \mathrm{Pic}_K^0(\mathcal{C})$ and $\mathbf{a}, \mathbf{b} \in \mathcal{J}(K)$ be the images of A, B respectively, under the embedding J into $\mathbf{P}^{15}(K)$ described in Definition 1.1. By Theorem 1.4, if the divisor $A + B$ has this special form then $\phi_{i2}(\mathbf{a}, \mathbf{b})^2 - 4\phi_{i1}(\mathbf{a}, \mathbf{b})\phi_{i3}(\mathbf{a}, \mathbf{b}) = 0$ for any value for $i = 1, \ldots 4$. We shall only make use to the case $i = 4$, but it is worth bearing in mind that one obtains a variation of the following for each choice of i. We are now in a position to compose these power series to obtain the $\theta(N)$ mentioned in the introduction.

DEFINITION 2.8. For $\mathbf{t} = \begin{pmatrix} t_1 \\ t_2 \end{pmatrix}$, let $\sigma(\mathbf{t})$ denote $(\sigma_i(\mathbf{t})) \in \mathbb{P}^{15}(\mathbb{Z}_{\mathbf{f}}[[\mathbf{t}]])$, where the σ_i are as described in equation (2). Let $A \in \mathrm{Pic}_K^0(\mathcal{C})$, with associated $\mathbf{a} \in \mathbf{P}^{15}(K)$. Define $\psi_{\mathbf{a}}(\mathbf{t}) = \phi_{42}(\mathbf{a}, \sigma(\mathbf{t}))^2 - 4\phi_{41}(\mathbf{a}, \sigma(\mathbf{t}))\phi_{43}(\mathbf{a}, \sigma(\mathbf{t}))$, and let m be the degree of the lowest degree term in $\mathbf{t}$ with a non-vanishing coefficient. Define:

$$\theta_{\mathbf{a}}^{(\mathbf{s})}(N) = \psi_{\mathbf{a}}([N, \mathbf{s}]) = c_m(\mathbf{s})N^m + c_{m+1}(\mathbf{s})N^{m+1} + \cdots \in K[[\mathbf{s}]][[N]].$$

For the motivation for defininining the power series $\theta_{\mathbf{a}}^{(\mathbf{s})}(N)$, the reader can look ahead to Proposition 2.10. In the special case when $A = \mathcal{O}$, we have $m = 6$, and only terms of even degree in N and $\mathbf{s}$ occurring. The initial term of $c_6(\mathbf{s})$ then has the simple form:

$$c_6(\mathbf{s}) = 4(f_0 s_2^6 + \cdots + f_6 s_1^6) + \cdots = 4s_2^6 F(s_1/s_2) + \cdots, \quad (8)$$

where F is the sextic of equation (1).

In general, we wish to ensure that the evaluation of each coefficient $c_j(\mathbf{s})$ for a specific $\mathbf{a} \in \mathcal{J}(K)$ at a pair of local parameters, converges to some $c_j \in K_v$, and that $|c_j|_v \to 0$. It is clearly sufficient for the extension $[K_v, \mathbb{Q}_p]$ to be unramified (so that we merely have to avoid an additional finite set of places in addition to those of bad reduction). In fact, this condition can be slightly relaxed to the following

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

bound on the ramification index.

THEOREM 2.9. *Let A, $\mathbf{a}$, m and $\theta_{\mathbf{a}}^{(\mathbf{s})}(N) = \sum_{j \geqslant m} c_j(\mathbf{s}) N^j$ be as in Definition* 2.8. *Then $c_j(\mathbf{s}) \in \mathcal{P}_j^{(m)}(\mathbf{s})$, for all j. Suppose that the ramification index e of the extension $[K_v, \mathbb{Q}_p]$ satisfies $e < p-1$. Let $D' \in \mathrm{Pic}_K^0(\mathcal{C})$ lie in the kernel of reduction, with its associated pair of local parameters denoted by $\mathbf{s}^{D'} = \begin{pmatrix} s_1^{D'} \\ s_2^{D'} \end{pmatrix}$, and with δ denoting $\max(|s_1^{D'}|_v, |s_2^{D'}|_v)$. Then each $c_j(\mathbf{s}^{D'})$ converges to some $c_j \in K_v$, and $|c_j|_v \leqslant d_j$, where $d_j = \delta^j p^{(j-m)/(p-1)} \to 0$.*

Proof. The fact that $c_j(\mathbf{s}) \in \mathcal{P}_j^{(m)}(\mathbf{s})$ follows from Lemma 2.6. Since D' lies in the kernel of reduction, it follows that $|s_1^{D'}|_v, |s_2^{D'}|_v \leqslant p^{-1/e}$. Hence any term in $c_j(\mathbf{s}^{D'})$ of degree r in $\mathbf{s}^{D'}$ must have valuation at most $d_r < p^{-r/e} p^{(r-m)/(p-1)} \to 0$, since $e < p-1$. It follows that each $c_j(\mathbf{s}^{D'})$ converges in K_v, and that the limit has valuation at most d_j, as required. □

The proposed strategy to try to determine $\mathcal{C}(K)$ may therefore be described as follows. Suppose that $\mathcal{J}(K)$ has been shown to have rank 1, and that the torsion group and infinite generator D have been found (using the methods in [1], [8], [16]). Suppose also that all of the Weierstrass points $(x, 0)$ in $\mathcal{C}(K)$ have been found by factorising F over K, which is straightforward. It remains to try to find all of the non-Weierstrass points, and to prove that they have all been found.

Step 1. Choose a place v, lying above some rational prime p, which is of good reduction for $\mathcal{C}$, and for which the ramification index of $[K_v : \mathbb{Q}_p]$ is less than $p-1$. Note that this only excludes a finite number of choices of v.

Step 2. Find M such that $D' = M \cdot D$ lies in the kernel of the reduction map from K_v to the residue field k_v. Let S be the finite set $\{B + i \cdot D : B \in \mathcal{J}_{\mathrm{tors}}(K)$ and $0 \leqslant i \leqslant M-1\}$.

Step 3. For each $A \in S$, let $\mathbf{a}$ be the corresponding member of $\mathbf{P}^{15}(K)$ under the embedding of Definition 1.1. Determine m, the degree of the lowest degree term in $\mathbf{t}$ for the power series $\psi_{\mathbf{a}}(\mathbf{t})$ of Definition 2.8.

At this point, we can appeal to the following proposition which follows from the discussion in this section.

PROPOSITION 2.10. *Let S, D', A, $\mathbf{a}$ be as in steps* $1, 2, 3$ *above, and $\mathbf{s}^{D'}$ be the vector of local parameters corresponding to D'. Let $\Upsilon(K)$ denote the image of $\mathcal{C}(K)$ under the map which takes $P \in \mathcal{C}(K)$ to $\{P, P\} \in \mathcal{J}(K)$. Then the set of $N \in K_v, |N|_v \leqslant 1$ such that $\theta_{\mathbf{a}}^{(\mathbf{s}^{D'})}(N) = 0$ contains the set of $N \in \mathbb{Z}$ such that $A + N \cdot D' \in \Upsilon(K)$.* □

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

Step 4. Approximate the coefficients $c_j = c_j(\mathbf{s}^{D'})$ of the power series $\theta_{\mathbf{a}}^{(\mathbf{s}^{D'})}(N) \in K_v[[N]]$ up to sufficiently high degree in $\mathbf{s}$ so that k is determined, where k is defined by: $|c_k|_v \geqslant |c_i|_v$ for all $i \geqslant 0$, and $|c_k|_v > |c_i|_v$ for all $i > k$. Apply Strassman's Theorem (Theorem 2.3) to find the number of $N \in K_v$ with $|N|_v \leqslant 1$ which satisfy the power series. This gives an upper bound for the number of such N for which $N \in \mathbb{Z}$. This in turn is precisely the number of values of $N \in \mathbb{Z}$ for which the divisor $A + N \cdot D'$ either satisfies $k_4(A - N \cdot D') = 0$ or is of the form $\{P, P\}$ (or is $\mathcal{O}$ in the special case $A = \mathcal{O}$, $N = 0$).

Step 5. The sum of these bounds over all $A \in S$ gives a bound on the total number of non-Weierstrass points in $\mathcal{C}(K)$. If this is larger than the number of known points, then one can repeat the above steps with new places v. If the resulting bounds are persistently too high, and one suspects the existence of a further member of $\mathcal{C}(K)$ then one can search to see whether $A + N \cdot D'$ is of the form $\{P, P\}$, assisted by v-adic information of step 4, which will give congruence conditions on N.

There are two possible enhancements to the above strategy. The first is to take the product $\theta_{\mathbf{a}}^{(\mathbf{s}^{D'})}\theta_{-\mathbf{a}}^{(\mathbf{s}^{D'})}$, which can be described entirely on the Kummer surface (being invariant under negation), and allows both $\mathbf{a}$ and $-\mathbf{a}$ to be dealt with simultaneously. In practice, we have not found that this significantly reduces the computations, and we shall not refer to it in the worked examples. The second enhancement is more significant. Suppose that only $\mathcal{J}(K)/2\mathcal{J}(K)$ and the torsion group of $\mathcal{J}(K)$ have been determined, with the rank shown to be 1. This is the situation after a successful 2-descent, for which recent methods are becoming quite fast [1], [8], [10], [16]. In this case, a divisor D of infinite order will be known, but it will not be known whether D and the torsion group give a set of generators. There is an effective procedure for deducing a set of generators for $\mathcal{J}(K)$, which has even been made workable in practice [9], but is very slow. Let $v, p, D' = M \cdot D, S$ be as in steps 1 and 2. Then there must exist a $W \in \mathbb{Z}$ and divisor D_0 such that $D = W \cdot D_0$ and D_0 is the missing generator. The value of W will not be known, but it may be that one can show by a finite field argument in k_v that $M \cdot D_0$ lies in the kernel of reduction. We further try to show that W is not divisible by p; this can be done either by a further finite field argument, or by looking at the valuations of the local parameters in $\mathbf{s}^{D'}$. It then follows that any K-rational divisor can still be written in the form $A + N \cdot D'$, but where N is now in $\mathbb{Q}$, with denominator W. It remains true that $N \in K_v$ and $|N|_v \leqslant 1$, and so the remaining steps are as usual with the Strassman bounds still applicable.

3. Worked examples

We shall illustrate the ideas of Section 2 by computing $\mathcal{C}(\mathbb{Q})$ completely for two specific curves, giving a more direct proof of Coleman's result (Proposition 0.3), and deriving a conditional result for a further family of curves,

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

EXAMPLE 3.1. Let $\mathcal{C}$ be the curve $Y^2 = (X^2+1)(X^2+2)(X^2+2X+2)$. Then $\mathcal{C}(\mathbb{Q})$ consists only of the six points: ∞^+, ∞^-, $(0, \pm 2)$ and $(-1/2, \pm 15/8)$.

Proof. It has already been shown in [9] that $\mathcal{J}(\mathbb{Q})$ has rank 1 and is generated by the torsion group (which consists of $\mathcal{O}$ and the 3 elements of order 2), and the divisor $D = \{\infty^+, \infty^+\}$. There are no $\mathbb{Q}$-rational Weierstrass points, since the 3 quadratic factors are irreducible. We take $v = p = 3$ as our place of good reduction, since 3 does not divide the discriminant of $\mathcal{C}$. Then $D' = 5 \cdot D = \{(-1/2, 15/8), (-1/2, 15/8)\}$ lies in the kernel of the reduction map from $\mathcal{J}(\mathbb{Q}_3)$ to $\mathcal{J}(\mathbb{F}_3)$. The local parameters associated to D' are: $s_1^{D'} = 6225/22472$ and $s_2^{D'} = -555/11236$. Let S be the finite set $\{B + i \cdot D : B \in \mathcal{J}_{\text{tors}}(\mathbb{Q}) \text{ and } 0 \leqslant i \leqslant 4\}$, which has 20 members. For each $A \in S$ we wish to find all N such that $A + N \cdot D'$ is a divisor of the special form $\{P, P\}$. But we can immediately discard any A whose reduction $\tilde{A}$ is not of this type in $\mathcal{J}(\mathbb{F}_3)$. This leaves only the 5 divisors: $\{\infty^+, \infty^+\}$, $\{\infty^-, \infty^-\}$, $\{(0,2),(0,2)\}$, $\{(0,-2),(0,-2)\}$ and $\mathcal{O}$ as the possibilities for A.

For $A = \{\infty^+, \infty^+\}$, we have that the lowest degree term of $\psi_{\mathbf{a}}(\mathbf{t})$ has degree $m = 1$. From Theorem 2.9, it follows that $\theta_{\mathbf{a}}^{(\mathbf{s})}(N) = c_1(\mathbf{s})N + c_2(\mathbf{s})N^2 + \cdots \in K[[\mathbf{s}]][[N]]$, where $c_j(\mathbf{s}) \in \mathcal{P}_j^{(1)}(\mathbf{s})$, for all $j \geqslant 1$. The coefficient $c_1(\mathbf{s}) = -128 s_2 +$ terms of degree $\geqslant 1$ in $\mathbf{s}$. Evaluating at $\mathbf{s} = \mathbf{s}^{D'}$, Theorem 2.9 gives that terms of degree $j \geqslant 1$ in $\mathbf{s}$ all have valuation $\leqslant 3^{-(j+1)/2} < 3^{-1}$. Working modulo 9 (which only requires the evaluation of the single linear term $-128 s_2$ above) gives that: $\theta_{\mathbf{a}}^{(\mathbf{s}^{D'})}(N) \equiv 3N \pmod 9$. In summary, $|c_1|_3 = 3^{-1}$ and $|c_j|_3 < 3^{-1}$ for all $j > 1$ so that, by Strassman's Theorem $N = 0$ is the only solution in $\mathbb{Z}_3$ and so is the only solution in $\mathbb{Z}$. Therefore, the only case when $A + N \cdot D'$ is of the form $\{P, P\}$ is $N = 0$. Similarly, when A is the divisor $\{\infty^-, \infty^-\}$, $\{(0,2),(0,2)\}$, or $\{(0,-2),(0,-2)\}$, then $\theta_{\mathbf{a}}^{(\mathbf{s}^{D'})}(N)$ is congruent (mod 9) to $-3N$, $3N$ and $-3N$, respectively. In each case it follows that $N = 0$ is the only solution.

Finally, in the case $A = \mathcal{O}$, the lowest degree term has degree 6 with only even powers of N occurring, so that: $\theta_{\mathbf{a}}^{(\mathbf{s})}(N) = c_6(\mathbf{s})N^6 + c_8(\mathbf{s})N^8 + \cdots \in K[[\mathbf{s}]][[N]]$, where $c_j(\mathbf{s}) \in \mathcal{P}_j^{(6)}(\mathbf{s})$, for all $j \geqslant 6$. Evaluating at $\mathbf{s} = \mathbf{s}^{D'}$, up to terms of degree 8 in $\mathbf{s}$, gives that: $\theta_{\mathbf{a}}^{(\mathbf{s}^{D'})}(N) \equiv 2187N^6 + 4372N^8 (\text{mod } 3^8)$. Therfore, $|c_6|_3 = |c_8|_3 = 3^{-7}$ and $|c_j|_3 < 3^{-7}$ for all $j > 8$, so that $N = 0, 1, -1$ are the only solutions.

The only possible divisors in $\mathcal{J}(\mathbb{Q})$ of the form $\{P, P\}$ are therefore those where P is one of the known six $\mathbb{Q}$-rational points, and so these must give all of the $\mathbb{Q}$-rational non-Weierstrass points, as required. □

COMMENT 3.2. Let $\mathcal{C}$, D, D' and S be as in Example 3.1, and suppose that we initially only know that $\mathcal{J}_{\text{tors}}(\mathbb{Q})$ consists of $\mathcal{O}$ and the 3 points of order 2, that $\mathcal{J}(\mathbb{Q})$ has rank 1, and that D has infinite order, but do not know whether $\mathcal{J}_{\text{tors}}(\mathbb{Q})$ and D actually generate $\mathcal{J}(\mathbb{Q})$. This is the situation after performing the descent

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

via isogeny in [8], but before the time consuming height computation in [9]. Then there must exist a $W \in \mathbb{Z}$ and D_0 such that $D = W \cdot D_0$ and $\mathcal{J}_{\text{tors}}(\mathbb{Q}), D_0$ generate $\mathcal{J}(\mathbb{Q})$. We now pursue the strategy described at the end of Section 2. In $\mathcal{J}(\mathbb{F}_3)$, whatever is the value of W, it is always true that $5 \cdot \widetilde{D_0} = \tilde{\mathcal{O}}$, so that $D_0' = 5 \cdot D_0$ is in the kernel of reduction. Furthermore, if $3 | W$ then $(5W/3) \cdot D_0$ would lie in the kernel of reduction and $D' = 3(5W/3) \cdot D_0$; this would force the local parameters of D' to have valuation $\leqslant 3^{-2}$, contradicting the fact that they in fact have valuation 3^{-1}. Therefore, $3 \not| W$ (a fact which we might also have tried to show by considering $\mathcal{J}(\mathbb{F}_p)$ for some other prime p of good reduction). It follows that everything in $\mathcal{J}(\mathbb{Q})$ may be expressed as $A + N_0 \cdot D_0'$, where $A \in S$, $N_0 \in \mathbb{Z}$, as usual, which can formally be written as $A + N \cdot D'$, where $N = N_0/W$. The proof of Example 3.1 now carries through unchanged, even without knowing D_0, since it found all possible solutions of $N \in \mathbb{Z}_3$, which includes any $N = N_0/W$, with $3 \not| W$.

The above strategy also allows us to deal easily with quadratic fields which embed into $\mathbb{Q}_3$.

COROLLARY 3.3. *Let $\mathcal{C}$ be as in Example* 3.1 *and let $K = \mathbb{Q}(\sqrt{d})$, where $d \equiv 1 \pmod 3, d \neq -2$. If $\mathcal{J}(K)$ has rank* 1 *then $\mathcal{C}(K)$ consists only of the six $\mathbb{Q}$-rational points described in Example* 3.1.

Proof. If d is a quadratic residue mod 7, then $\#\mathcal{J}_{\text{tors}}(\mathbb{Q})$ divides the gcd of $\#\mathcal{J}(\mathbb{F}_3) = 20$, $\#\mathcal{J}(\mathbb{F}_7) = 96$, and so consists only of $\mathcal{O}$ and the 3 divisors of degree 2. If d is a quadratic non-residue mod 7, then $\#\mathcal{J}_{\text{tors}}(\mathbb{Q})$ divides the gcd of $\#\mathcal{J}(\mathbb{F}_3) = 20, \#(\mathbb{F}_{49}) = 3072$, giving the same result. Embedding K into $\mathbb{Q}_3$, which is possible since d is a square in $\mathbb{Q}_3$, the proof as described in comment 3.2 now carries through unchanged, to show that the 6 known points in $\mathcal{C}(\mathbb{Q})$ are also the only non-Weierstrass points in $\mathcal{C}(K)$. There are also no new Weierstrass points, since the 3 quadratic factors remain irreducible. In the omitted case $d = -2$, there are the 2 new Weierstrass points $(\pm\sqrt{-2}, 0)$. □

The same strategy gives a more direct proof of Coleman's result, Proposition 0.3, as follows. Let $\mathcal{C}, \lambda, a, b$ be as in Proposition 0.3, so that $\lambda = 3^{2r}\mu$, where $r > 0$ and $3 \not| \mu$. Then $\mathcal{C}$ is $\mathbb{Q}$-birationally equivalent to: $Y^2 = X(X^2 - 1)(3^{2r}\mu^2 X - \mu)(X^2 + aX + b)$. We can take $D' = \{\infty^+, \infty^+\}$, which is in the kernel of reduction from $\mathcal{J}(\mathbb{Q}_3)$ to $\mathcal{J}(\mathbb{F}_3)$. Assume for the moment that $D' \notin 3\mathcal{J}(\mathbb{Q})$. Arguing as in comment 3.2 gives that we need only find what values of N make $N \cdot D'$ a divisor of the type $\{P, P\}$. The local parameters of D' have valuations: $|S_1^{D'}|_3 = 3^{-r}$ and $|s_2^{D'}|_3 = 3^{-3r}$. Working modulo 3^{8r} all terms disappear except:

$$\theta_{\mathcal{O}}^{\mathbf{s}^{D'}}(N) \equiv \tfrac{4}{3}(s_1^{D'})^8\mu^2N^6 - \tfrac{1}{3}(s_1^{D'})^8\mu^2N^8$$

so that $|c_6|_3 = |c_8|_3 = 3^{-8r+1}$, whereas $|c_j|_3 \leqslant 3^{8r}$ for all $j > 8$. Therefore, $N = 0, \pm 1$ are the only solutions, giving that the only non-Weierstrass points on

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

$\mathcal{C}$ are ∞^+ and ∞^-, as required. Finally, if $D' \in 3\mathcal{J}(\mathbb{Q})$ then let t be the largest integer, $1 < t < r$, such that $D' \in 3^t\mathcal{J}(\mathbb{Q})$ and let D'' be such that $D' = 3^tD''$. Then $|s_1^{D''}|_3 = 3^{-r+t}$ and $|s_2^{D''}|_3 = 3^{-3r+t}$. The above argument can be applied to D'', but working modulo $3^{8(r-t)}$, to show that $N = 0, \pm 3^t$ are the only solutions to $\theta_{\mathcal{O}}^{\mathbf{s}^{D''}}(N)$, as required.

A similar argument applies to the following family of curves.

EXAMPLE 3.4. Let $\mathcal{C}$ be the curve: $Y^2 = (X - a)(X^4 + b)$, where $a, b \in \mathbb{Q}$, $a, b \equiv 1 \pmod 3$. If $\mathcal{J}(\mathbb{Q})$ has rank 1 then $\mathcal{C}(\mathbb{Q})$ contains only ∞, $(1, 0)$ and at most 1 pair of non-Weierstrass points: (x, y) and $(x, -y)$.

Proof. If there is a pair of non-Weierstrass $\mathbb{Q}$-rational points, then by a $\mathbb{Q}_3$ argument it must be of one of the forms: $(1 + 3^{2r}k, \pm 3^r\ell)$, where $r > 0, k, l \in \mathbb{Q}$, and $|k|_3 = |\ell|_3 = 1$ or $((1 + 3m)/3^{2r}, \pm(1 + 3n)/3^r)$, where $r > 0$, $m, n \in \mathbb{Z}_3$. In the first case, take $D' = \{(1 + 3^{2r}k, 3^r\ell), (1 + 3^{2r}k, 3^r\ell)\}$, and in the second case $D' = \{((1+3m)/3^{2r}, (1+3n)/3^r), ((1+3m)/3^{2r}, \pm(1+3n)/3^r)\}$. Either of these is in the kernel of reduction from $\mathcal{J}(\mathbb{Q}_3)$ to $\mathcal{J}(\mathbb{F}_3)$, and one can show in the usual way that $N \cdot D'$ is a divisor of the type $\{P, P\}$ exactly when $N = 0, \pm 1$. □

All of the above examples were shown using 3-adic arguments, which are somewhat special in that denominators of 3 can occur in coefficients of $\theta(N)$ as early as terms of degree 2 higher than the lowest degree term in N. This fact was relevant in all of the above examples. For variety, we give a final example which has 3 as a prime of bad reduction, but for which a 5-adic argument is sufficient to resolve $\mathcal{C}(\mathbb{Q})$.

EXAMPLE 3.5. Let $\mathcal{C}$ be the curve: $Y^2 = X(X - 1)(X^2 - 3)(X^2 - 9)$. Then $\mathcal{C}(\mathbb{Q})$ consists of the 4 Weierstrass points: $(0, 0)$, $(1, 0)$, $(3, 0)$, $(-3, 0)$ and the pair of non-Weierstrass points: ∞^+, ∞^-.

Proof. A $\mathbb{Q}$-birationally equivalent curve (the curve $\widehat{\mathcal{C}}^{(2)}$ in Example 3.3 of [8]) was shown to have Jacobian of rank 1, with $\mathcal{J}_{\text{tors}}(\mathbb{Q})$ consisting only of the 2-torsion group of size 8, and so the same is true of $\mathcal{C}$. Take $D = \{(0, 0), \infty^+\} + \{(1, 0), (-3, 0)\}$ and $D' = 3D$, which lies in the kernel of the reduction map from $\mathcal{J}(\mathbb{Q}_5)$ to $\mathcal{J}(\mathbb{F}_5)$. The local parameters corresponding to D' both have 5-adic valuation 5^{-1}. As usual, we can ignore those divisors A for which $\tilde{A}$ is not of the form $\{P, P\}$ in $\mathcal{J}(\mathbb{F}_5)$. This leaves only $\{\infty^+, \infty^+\}, \{\infty^-, \infty^-\}$ and $A = \mathcal{O}$ to be considered. In the case $A = \{\infty^+, \infty^+\}$, we may work modulo 5^2 which only requires the computation of the linear terms in $\mathbf{s}$. This gives: $\theta_{\mathbf{a}}^{\mathbf{s}^{D'}}(N) \equiv 20N \pmod{5^2}$, so that $N = 0$ is the only case where $A + N \cdot D'$ is of the type $\{P, P\}$. Similarly for $A = \{\infty^-, \infty^-\}$. In the final case $A = \mathcal{O}$, we can work modulo 5^8 to see that $\theta_{\mathbf{a}}^{\mathbf{s}^{D'}}(N) \equiv 5^7 \cdot N^6 \pmod{5^8}$, so that $N = 0$ is again the only solution. Note that this is an easier computation than in the previous examples, since only the terms

https://doi.org/10.1023/A:1000111601294 Published online by Cambridge University Press

of degree 6 in **s** (that is, the expression given in equation (8)) were required; the earliest non-integral denominators can only occur at terms of degree 10 in **s**, and all term of degree $\geqslant 8$ in **s** are guaranteed to be 0 (mod 5^8). We finally conclude that ∞^+ and ∞^- are the only non-Weierstrass points in $\mathcal{C}(\mathbb{Q})$, as required. □

So far, the recent techniques available for finding ranks by 2-descent have not been applied to compute ranks over number fields. This is the only reason why we have not included an example which completely resolves $\mathcal{C}(K)$ where K is a number field (since we must first know that $\mathcal{J}(K)$ has rank 1). However, we have taken the trouble in Section 2 to work through our Chabauty method for a general number field on the grounds that such ranks should soon be forthcoming (for example, the approach to 2-descent in [10], [16] looks easily applicable to number fields), at which time the material of Section 2 will be immediately available to try to compute $\mathcal{C}(K)$ when $\mathcal{J}(K)$ has been shown to have rank 1. Corollary 3.3 gives an advance indication of this.

For hyperelliptic curves of higher genus there are already techniques available for computing the rank of the Jacobian; there is a genus 3 example in [16]. In principle, the mechanical details of Section 2 will also carry over, but with g local parameters, and with an embedding of the Jacobian into $\mathbb{P}^{4^g-1}$. In practice, it would be well worth bypassing the computation of the complete bilinear forms $\phi_{ij}(\mathbf{a}, \mathbf{b})$, which will become large as the genus increases. We observe, however, that in computing the above examples only a small portion of these expressions were required to compute the final power series to the required degree of accuracy. The main step of Example 3.5 only used the initial (degree 6) terms of $\theta_{\mathcal{O}}^{(\mathbf{s}^{D'})}$, which required only substitution into equation (8), an equation which looks highly amenable to generalisation to higher genus.

References

1. Cassels, J. W. S.: The Mordell-Weil group of curves of genus 2. Arithmetic and Geometry papers dedicated to I. R. Shafarevich on the occasion of his sixtieth birthday, Vol. 1. Arithmetic, 29–60, Birkhäuser, Boston (1983).
2. Cassels, J. W. S.: Arithmetic of curves of genus 2. Number Theory and Applications (ed. R.A. Mollin), 27–35. NATO ASI Series C, 265. Kluwer Academic Publishers, 1989.
3. Cassels, J. W. S.: Local Fields. *London Mathematical Society Student Texts* 3. Cambridge University Press, 1986.
4. Chabauty C.: Sur les points rationels des variétés algébriques dont l'irregularité et supérieur á la dimension. *Comptes Rendus, Paris* 212 (1941), 882–885.
5. Coleman, R. F.: Effective chabauty. *Duke Math. J.* 52 (1985), 765–780.
6. Flynn, E. V.: The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. *Math. Proc. Camb. Phil. Soc.* 107 (1990), 425–441.
7. Flynn, E. V.: The group law on the Jacobian of a curve of genus 2. *J. Reine Angew. Math.* 439 (1993), 45–69.
8. Flynn, E. V.: Descent via isogeny on the Jacobian of a curve of genus 2. *Acta Arithmetica LXVII.1* (1994), 23–43.
9. Flynn, E. V.: An explicit theory of heights in dimension 2. To appear in Trans. *Amer. Math. Soc.*.
10. Flynn, E. V.: On a theorem of Coleman. Preprint, January 1995.

11. Gordon, D. M. and Grant, D.: Computing the Mordell–Weil rank of Jacobians of curves of genus 2. *Trans. A.M.S.*, 337, Number 2, (1993), 807–824.
12. Grant, D.: Formal groups in genus 2. *J. Reine Angew. Math*. 411 (1990), 96–121.
13. Grant, D.: A curve for which Coleman's Chabauty bound is sharp. Preprint, 1993.
14. McCallum, W. G.: On the Shafarevich–Tate group of the Jacobian of a quotient of the Fermat curve. *Invent. Math*. 93 (1988), 637–666.
15. McCallum, W. G.: The arithmetic of Fermat curves. *Math. Ann*. 294 (1992), 503–511.
16. Schaefer, E. F.: 2-descent on the Jacobians of hyperelliptic curves. *J. Number Theory* (to appear).
17. Silverman, J. H.: The Arithmetic of Elliptic Curves. Springer-Verlag, New York (1986).