THE HASSE PRINCIPLE AND THE BRAUER-MANIN OBSTRUCTION FOR CURVES

E.V. FLYNN

ABSTRACT. We discuss a range of ways, extending existing methods, to demonstrate violations of the Hasse principle on curves. Of particular interest are curves which contain a rational divisor class of degree 1, even though they contain no rational point. For such curves we construct new types of examples of violations of the Hasse principle which are due to the Brauer-Manin obstruction, subject to the conjecture that the Tate-Shafarevich group of the Jacobian is finite.

1. Introduction

Let K be a number field and let $\mathbb{A}_K$ denote the adèles of K. Suppose that $\mathcal{X}$ is a smooth projective variety over K violating the Hasse principle; that is, $\mathcal{X}(K) = \emptyset$ even though $\mathcal{X}(\mathbb{A}_K) \neq \emptyset$. Global reciprocity applied to the Brauer-Grothendieck group $\mathrm{Br}(\mathcal{X})$ defines a certain subset $\mathcal{X}(\mathbb{A}_K)^{\mathrm{Br}} \subset \mathcal{X}(\mathbb{A}_K)$ which contains the diagonal image of $\mathcal{X}(K)$ (see [27], p.101). When $\mathcal{X}(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$ we say that the violation of the Hasse principle is explained by the Brauer-Manin obstruction. When $\mathcal{X}$ is a surface, examples have been constructed (see [27], §8) where $\mathcal{X}$ violates the Hasse principle in a way not explained by the Brauer-Manin obstruction.

When $\mathcal{X}$ is a curve $\mathcal{C}$ it is an open question whether the Brauer-Manin obstruction is the only obstruction to the Hasse principle. When $\mathcal{X}$ is of genus 1, we have the following result of Manin (see [27], p.114).

Lemma 1. *Let $\mathcal{C}$ be a smooth proper curve of genus 1 defined over K, with Jacobian $\mathcal{E}$. Suppose that the Tate-Shafarevich group $\text{Ш}(\mathcal{E})$ is finite. Then the Brauer-Manin obstruction is the only obstruction to the Hasse principle for $\mathcal{C}$. That is, if $\mathcal{C}(K) = \emptyset$ and $\mathcal{C}(\mathbb{A}_K) \neq \emptyset$ then $\mathcal{C}(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.*

Regardless of the genus of $\mathcal{C}$, we also have the following result (see [27], Cor. 6.2.5).

Lemma 2. *Let $\mathcal{C}$ be a smooth proper curve defined over K, with Jacobian $\mathcal{J}$, and suppose that $\text{Ш}(\mathcal{J})$ is finite. If $\mathcal{C}$ has no K-rational divisor class of degree 1 then the Brauer-Manin obstruction is the only obstruction to the Hasse principle for $\mathcal{C}$.*

For simplicity throughout, we shall write our curves in affine form, but will always mean the corresponding smooth projective curve. Isolated examples of Lemma 2 are known: there are three such curves over $K = \mathbb{Q}$, including $X^4 + Y^4 = 241^2$, given in [9], and a curve over $K = \mathbb{Q}(\sqrt{-13})$ given in [26]. All of these are of genus 3 and have reducible Jacobians, with maps to elliptic curves. There is also the genus 2 curve $Y^2 = -37(X^2+1)(5X^2-32)(32X^2-5)$, given in Prop. 28 of [22], which has reducible Jacobian $\mathcal{J}$; it

Date: February 16, 2004.
1991 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14H40.
Key words and phrases. Hasse Principle, Jacobians, Brauer-Manin Obstruction.
The author was supported by EPSRC grant GR/R82975/01.

has points everwhere locally, but $\mathrm{Pic}^1_{\mathcal{C}}$ is nontrivial in $Ш(\mathcal{J})$. The previous rarity of genus 2 examples is explained by the following result (see [24]).

Lemma 3. *Let $\mathcal{C}$ be a smooth proper curve of genus g defined over $\mathbb{Q}$ with points everywhere locally. Let $\mathcal{J}$ be the Jacobian of $\mathcal{C}$, and suppose that $Ш(\mathcal{J})[p] = 0$ for each prime $p \leq 2g-2$. Then $\mathcal{C}$ has a $\mathbb{Q}$-rational divisor class of degree* 1.

Proof Since $\mathcal{C}$ has points everywhere locally, $\mathrm{Pic}^1_{\mathcal{C}}$ represents an element of $Ш(\mathcal{J})$. If $\mathcal{C}$ does not have a rational divisor class of degree 1, then this element is nonzero. On the other hand, this element is killed by $2g-2$, since the canonical class makes $\mathrm{Pic}^{2g-2}_{\mathcal{C}}$ a trivial homogeneous space for $\mathcal{J}$. □

In genus 2, this means that any potential example of Lemma 2 must have nontrivial 2-part of $Ш(\mathcal{J})$. Since, as we shall see, the main available technique for testing whether there exists a rational divisor class of degree 1 requires an initial computation of the rank of $\mathcal{J}(\mathbb{Q})$, and since there are currently no methods of second descent available, it is difficult to find such an example. One conceivable method is to try to show analytically that the rank is 0 or 1 assuming the conjectures of Birch and Swinnerton-Dyer; a 2-descent could then give examples with nontrivial 2-torsion in $Ш(\mathcal{J})$. However, we shall instead shortly explain an alternative and unconditional way this can be overcome in the case where the Jacobian admits a rational Richelot isogeny.

When such a divisor class exists, we can embed the curve in its Jacobian and gain some insight into the Brauer-Manin obstruction. Note that all of the curves we shall consider here have points everywhere locally; for such curves, every K-rational divisor class contains a K-rational divisor, by the local-global principle for the Brauer group [13]; therefore, in the statement of the following theorem (which is a consequence of Proposition 6.2.4 of [27]; see also p.36 of [23]), the existence of a K-rational divisor class R of degree 1 is sufficient.

Theorem 1. *Let $\mathcal{C}$ be a smooth proper curve defined over K, with Jacobian $\mathcal{J}$. Suppose that $Ш(\mathcal{J})$ is finite and that $\mathcal{C}$ has a K-rational divisor A of degree 1. Define the embedding $\zeta : \mathcal{C} \to \mathcal{J} : P \mapsto [P] - R$, where $R = [A]$ and where $[\ ]$ denotes class modulo linear equivalence.*[1] *Then inside the group $\prod_{\mathfrak{p}} H^0(K_{\mathfrak{p}}, \mathcal{J})$ we have*

$$\mathcal{C}(K) \cong \zeta\Big(\prod_{\mathfrak{p}} \mathcal{C}(K_{\mathfrak{p}})\Big) \cap \mathcal{J}(K) \subset \zeta\Big(\prod_{\mathfrak{p}} \mathcal{C}(K_{\mathfrak{p}})\Big) \cap \overline{\mathcal{J}(K)} \cong \mathcal{C}(\mathbb{A}_K)^{Br}, \tag{1}$$

where the product is taken over the set of all places of K, and $\overline{\mathcal{J}(K)}$ denotes the topological closure of $\mathcal{J}(K)$.

For the special case when $\mathcal{J}(K)$ has rank 0, we have that $\mathcal{J}(K)$ is finite and so $\mathcal{J}(K) = \overline{\mathcal{J}(K)}$. This forces the above to be an equality, giving the following result of Scharaschkin (see p.37 of [23] or p. 127 of [27]).

[1] We shall typically use the letter A to denote a divisor, and D, E, R to denote divisor classes.

Corollary 1. *Let $\mathcal{C}$ be a smooth proper curve over K, with Jacobian $\mathcal{J}$, and suppose that $\text{Ш}(\mathcal{J})$ is finite. If $\mathcal{C}$ has a K-rational divisor class R of degree 1 and $\mathcal{J}(K)$ is finite then the Brauer-Manin obstruction is the only obstruction to the Hasse principle for $\mathcal{C}$.*

Only a few examples have been computed where there exists a rational divisor class of degree 1, such as the curve $3X^4 + 4Y^4 = 19$ (discussed in [3], on p.48 of [23], and on p.128 of [27]), which again has reducible Jacobian, with maps to elliptic curves; the arguments are only applicable to this special situation. Similarly, the discussion in [13] and [25], which considers the genus 2 curve $Y^2 = 2(X^3+7)(X^3-7)$, is only applicable to curves with reducible Jacobians and maps to elliptic curves, as are the techniques in [2].

The aim here is to contribute to work on these themes in several ways. First, in Section 2 we present a straightforward way of deciding whether a genus 2 curve has a rational divisor class of degree 1, once generators for $\mathcal{J}(\mathbb{Q})$ are known; this allows the computation of many violations of the Hasse principle due to the Brauer-Manin obstruction in the case where there does not exists such a divisor class, with a style of proof more widely applicable than those for the isolated examples mentioned above. Second, in Sections 3,4, we shall extend the range of techniques available for proving that a given curve has no $\mathbb{Q}$-rational points, by combining the 'flat' and 'deep' information rather than the standard procedure of considering each separately, and – when available – by using a rational divisor class of degree 1 to embed the curve in its Jacobian; we shall derive some associated algebra to assist others who may wish to perform similar computations. Furthermore, we shall present examples (again due to the Brauer-Manin obstruction) of a new type, where the Jacobian is simple (the previous literature having concentrated on cases where the Jacobian is reducible, with maps to elliptic curves) and where there does exist such a divisor class; we shall include cases when $\mathcal{J}(\mathbb{Q})$ is finite (and so are automatically due to to the Brauer-Manin obstruction), and cases when $\mathcal{J}(\mathbb{Q})$ has nonzero rank (when our new techniques must be applied). In all cases, the proofs that $\mathcal{C}(\mathbb{Q}) = \emptyset$ are unconditional, but the results that they are due to the Brauer-Manin obstruction are subject to the conjecture that the Tate-Shafarevich group of the Jacobian is finite. Finally, as the techniques presented here are amenable to the mass production of examples, we take the opportunity to perform some rather heavy computations on a large number of curves. This should be viewed as a first step towards gaining statistical insight as to the rarity of any violations of the Hasse principle that might not be due to the Brauer-Manin obstruction.

Theorem 1 gives rise to the computational procedure which will be used in our examples, as follows. Note that, if we project from $K_\mathfrak{p}$ to the residue field $k_\mathfrak{p}$ in (1) then we are led to consider $\tau^{-1}\big(\zeta(\prod'_\mathfrak{p} \mathcal{C}(k_\mathfrak{p}))\big) \cap \overline{\mathcal{J}(K)}$, where $\prod'_\mathfrak{p}$ is over primes $\mathfrak{p}$ of good reduction and τ is the natural map from $\mathcal{J}(\mathbb{A}_K)$ to $\prod'_\mathfrak{p}(\mathcal{J}(k_\mathfrak{p}))$. For computational purposes, it is helpful to use the fact that $\overline{\mathcal{J}(K)}$ is the same as the profinite completion of $\mathcal{J}(K)$. Suppose we have found generators $D_1, \ldots, D_r$ of the free part of $\mathcal{J}(K)$ so that any member of $\mathcal{J}(K)$ can be written as $D = T + n_1 D_1 + \ldots n_r D_r$, for some $T \in \mathcal{J}(K)_{\text{tors}}$ and $n_1, \ldots, n_r \in \mathbb{Z}$. Then, for each $\mathfrak{p}$, the mod $\mathfrak{p}$ component of the requirement that $\tau^{-1}\big(\zeta(\prod'_\mathfrak{p} \mathcal{C}(k_\mathfrak{p}))\big) \cap \overline{\mathcal{J}(K)} \neq \emptyset$ induces congruence conditions on $(n_1, \ldots, n_r)$ modulo $(N_1^{(\mathfrak{p})}, \ldots, N_r^{(\mathfrak{p})})$, where each $N_i^{(\mathfrak{p})}$ is the order of the reduction of D_i modulo $\mathfrak{p}$. This is the 'flat' information which will be used in the majority of our examples; when (for each T) the information for several $\mathfrak{p}$ give contradictory congruences, then we have a proof that $\mathcal{C}(K)=\emptyset$. We shall also illustrate in Example 7 how the deeper $\mathfrak{p}$-adic part of the obstruction can be used.

Each of our test curves was of genus 2 with coefficients in $\mathbb{Z}$,

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

Let $\mathcal{J}$ denote the Jacobian of $\mathcal{C}$. We first ran through all such curves for which f_0 was in the range $-3,\ldots,2$, and each of $f_1,\ldots,f_6$ was in the range $-2,\ldots,2$. We then ran through all curves for which f_6 was in the range $-2,\ldots,2$, each of $f_2,\ldots,f_5$ was in the range $-5,\ldots,5$, and $f_1=f_3-f_5+2, f_0=f_6-f_4+2$, ensuring that the point $(i,1+i)$ was on the curve. This was with the idea of encouraging the rank upwards while having control over one of the members of $\mathcal{J}(\mathbb{Q})$, namely $[(i,1+i)+(-i,1-i)-\infty^+-\infty^-]$, where ∞^+,∞^- denote the points on the non-singular curve that lie over the singular point at infinity. Similarly, we ran through all curves for which f_6 was in the range $-2,\ldots,2$, each of $f_2,\ldots,f_5$ was in the range $-5,\ldots,5$, and $f_1=-4f_5-2f_3, f_0=-8f_6-4f_4-2f_2+1$, ensuring that the point $(\sqrt{2},1)$ was on the curve. This gave 210878 curves in total. We concentrated on the curves which had points everywhere locally, but had no $\mathbb{Q}$-rational points with x-coordinate n/d for n,d in the range $-1000,\ldots,1000$. We then, over several months, tried to compute the rank of $\mathcal{J}(\mathbb{Q})$ in each case, using the *magma* [20] routines written by Michael Stoll [30]. For some of the curves, even after 4 hours of computer time per curve on a Sparcstation, we were unable to compute the Selmer bound or were unable to find sufficient independent members of $\mathcal{J}(\mathbb{Q})$ to achieve the rank bound; such cases were discarded. These could be due either to the Selmer bound not equalling the rank, or to the generators of $\mathcal{J}(\mathbb{Q})$ being large in height. After checking for birational equivalence over $\mathbb{Q}$, we were finally left with a selection of 134 inequivalent curves, which we proved to have points everywhere locally, and for which the rank of $\mathcal{J}(\mathbb{Q})$ was found; of these, $10,38,73,13$ were of rank $0,1,2,3$, respectively. For each of these curves the known generators of $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ were shown to be actual generators of $\mathcal{J}(\mathbb{Q})$ using the methods of [29],[31]. These curves are listed in the appendix, indexed by a number and a letter, the number indicating the rank of $\mathcal{J}(\mathbb{Q})$; for example, the curve $\mathcal{C}_{3a}$ has $\mathcal{J}_{3a}(\mathbb{Q})$ of rank 3. One of the curves, $\mathcal{C}_{2T}$ has reducible Jacobian; all of the other 133 curves were shown to have absolutely simple Jacobian, using the method in [28].

Since these 134 examples have no nontrivial 2-part of $\text{Ш}(\mathcal{J})$, they must each have a $\mathbb{Q}$-rational divisor class of degree 1, and so Lemma 3 tells us that none are examples of Lemma 2. In order to construct examples of Lemma 2, we require curves where $\text{Ш}(\mathcal{J})[2]\neq 0$. Even though generally applicable second descent techniques have not been developed in genus 2, there remains the option (suggested by Nils Bruin) of using a Richelot isogeny and comparing the ranks obtained for the Jacobians of the original curve and that of the Richelot isogenous curve. We remind the reader of the type of curve to which this applies.

$$\mathcal{C}: Y^2 = G_1G_2G_3 = (g_{12}X^2+g_{11}X+g_{10})(g_{22}X^2+g_{21}X+g_{20})(g_{32}X^2+g_{31}X+g_{30}). \tag{3}$$

The curve with 4-isogenous Jacobian (see [1] for a description of the isogeny) is

$$\mathcal{D}: \Delta Y^2 = (G_2'G_3-G_2G_3')(G_3'G_1-G_3G_1')(G_1'G_2-G_1G_2'), \tag{4}$$

where $\Delta = \det(g_{ij})$. If one obtains differing 2-Selmer bounds on the $\mathbb{Q}$-ranks of the Jacobians of $\mathcal{C}$ and $\mathcal{D}$, then this demonstrates members of the 2-part of Ш, giving potential examples of Lemma 2. We have included 11 examples of this type in our list. Since these few curves were specifically hand picked and constructed to provide examples of this type, we shall not include them in our final summary.

The author acknowledges the helpful advice of Nils Bruin, Victor Scharaschkin and Michael Stoll.

2. Constructing a rational divisor class of degree 1 or proving its non-existence

Let $\mathcal{C}$ be a curve of genus 2 of the form (2), with Jacobian $\mathcal{J}$. We shall adopt the customary shorthand notation $\{P_1, P_2\}$ to denote the divisor class $[P_1 + P_2 - \infty^+ - \infty^-]$, which is in $\mathcal{J}(K)$ when P_1, P_2 are points on $\mathcal{C}$ and either P_1, P_2 are both K-rational or P_1, P_2 are quadratic over K and conjugate. We regard $\infty^+, \infty^- \in \mathcal{C}(K)$ when the coefficient of X^6 is a square in K. Suppose that we have found the rank of $\mathcal{J}(K)$ and generators for $\mathcal{J}(K)/2\mathcal{J}(K)$, using the methods described in [30]. Let $F(X) = F_1(X) \dots F_m(X)$ be the factorisation of $F(X)$ into irreducible polynomials over K; for each i, let θ_i be a root of $F_i(x)$ and let $L_i = K(\theta_i)$. Following p.49 of [10], we define the homomorphism

$$\begin{aligned} \mu \quad &: \mathcal{J}(K) \to \Big(L_1^*/(L_1^*)^2 \times \dots \times L_m^*/(L_m^*)^2\Big)/\tilde{}, \\ &: \{(x_1, y_1), (x_2, y_2)\} \mapsto [(x_1 - \theta_1)(x_2 - \theta_1), \dots, (x_1 - \theta_m)(x_2 - \theta_m)], \end{aligned} \tag{5}$$

where the equivalence relation $\tilde{}$ is defined by

$$[a_1, \dots, a_m]\tilde{}[b_1, \dots, b_m] \iff a_1 = wb_1, \dots, a_m = wb_m, \text{ for some } w \in K^*. \tag{6}$$

Since μ is a map to a Boolean group, its kernel clearly contains $2\mathcal{J}(K)$. It also contains members of $\mathcal{W}$ given by the following definition (see p.58 of [10]).

Definition 2. Let $\mathcal{C} : Y^2 = F(X)$ be as in (2) defined over K, with Jacobian $\mathcal{J}$, and let $\mathcal{O}$ denote the canonical divisor class on $\mathcal{C}$, which is of degree 2. Let $\mathcal{W}$ denote the set of elements $\{P_1, P_2\}$ in $\mathcal{J}(K)$ with the following property: there is an effective divisor A_0 of degree 3 which is either defined over K or defined over a quadratic extension of K and linearly equivalent to its conjugate A_0' and such that $P_1 + P_2 + A_0 + A_0' \in 4\mathcal{O}$.

The following lemma is also from [10], pp.53–55, and describes the kernel of μ.

Lemma 4. *Let μ be as in (5) and $\mathcal{C}, \mathcal{J}, \mathcal{W}$ be as in Definition 2. The difference of any two members of $\mathcal{W}$ is in $2\mathcal{J}(K)$ and the kernel of μ consists precisely of the union of $2\mathcal{J}(K)$ and $\mathcal{W}$. The index of $2\mathcal{J}(K)$ in the kernel of μ is either 1 or 2. Suppose that $\mathcal{W}$ is not empty. Then $\mathcal{W} \subset 2\mathcal{J}(K)$ precisely when at least one of the following holds:*

(i) *$F(X)$ has a root $\theta \in K$.*

(ii) *The roots of $F(X)$ can be divided into two sets of three roots, where the sets are either defined over K (as wholes) or defined over a quadratic extension and conjugate over K.*

It is easy to decide whether Criterion (i) of Lemma 4 is satisfied. There is a useful method for deciding whether the more subtle Criterion (ii) is satisfied; namely, to construct the polynomial (see p.56 of [10])

$h(X) = \prod(X - \theta_i\theta_j\theta_k - \theta_\ell\theta_m\theta_n)$, where the product is taken over the ten unordered partitions of the six roots $\theta_1, \ldots, \theta_6$ of $F(X)$ into two sets of three. Provided that $h(X)$ is square free, Criterion (ii) of Lemma 4 is satisfied exactly when $h(X)$ has a root in K. If $h(X)$ is not square free, then one can compute $F(x+c)$ for some $c \in \mathbb{Z}$ and derive the resulting new $h(X)$; for some $c = 1, \ldots 45$ this guarantees to give at least one instance where $h(X)$ is square free. It is therefore straightforward in practice to determine whether Criterion (i) or (ii) is satisfied (see p.258 of [30]).

We now wish to establish a connection between the above theory and K-rational divisor classes of degree 1. We first consider the easiest case, when Criterion (i) or (ii) of Lemma 4 is satisfied.

Lemma 5. *Let $\mathcal{C} : Y^2 = F(X)$ be as in (2) defined over K, with Jacobian $\mathcal{J}$, and suppose that either Criterion (i) or (ii) of Lemma 4 is satisfied. Then there exists a K-rational divisor class of degree 1 on $\mathcal{C}$.*

Proof If Criterion (i) is satisfied then $[(\theta, 0)]$ is a K-rational divisor class of degree 1. If Criterion (ii) is satisfied, then we can divide the roots of $F(X)$ into $\{\theta_1, \theta_2, \theta_3\}$ and $\{\theta_4, \theta_5, \theta_6\}$, where either both sets are defined over K or they are defined over a quadratic extension $K(\sqrt{d})$ and conjugate. On the former case, the divisor $(\theta_1, 0)+(\theta_2, 0)+(\theta_3, 0)$ is defined over K, as must therefore be the divisor class $[(\theta_1, 0)+(\theta_2, 0)+(\theta_3, 0)]$. In the latter case, the divisors $(\theta_1, 0) + (\theta_2, 0) + (\theta_3, 0)$ and $(\theta_4, 0) + (\theta_5, 0) + (\theta_6, 0)$ are linearly equivalent, since their difference is $(\theta_1, 0) + (\theta_2, 0) + (\theta_3, 0) + (\theta_4, 0) + (\theta_5, 0) + (\theta_6, 0) - 2(\theta_4, 0) - 2(\theta_5, 0) - 2(\theta_6, 0)$, which is linearly equivalent to $(\theta_1, 0) + (\theta_2, 0) + (\theta_3, 0) + (\theta_4, 0) + (\theta_5, 0) + (\theta_6, 0) - 3\mathcal{O}$, which is the divisor of the function Y; hence $[(\theta_1, 0) + (\theta_2, 0) + (\theta_3, 0)]$ is equal to its $K(\sqrt{d}) : K$-conjugate $[(\theta_4, 0) + (\theta_5, 0) + (\theta_6, 0)]$, and so again $[(\theta_1, 0) + (\theta_2, 0) + (\theta_3, 0)]$ is defined over K. In either case, $[(\theta_1, 0) + (\theta_2, 0) + (\theta_3, 0)] - \mathcal{O}$ is then a K-rational divisor class of degree 1. □

Example 1. *The curves $\mathcal{C}_{0j} : Y^2 = (X^3 + X + 1)(2X^3 - 1)$ and $\mathcal{C}_{1b} : Y^2 = -(X^3 + X + 1)(X^3 + 2X^2 - 2)$ have $\mathbb{Q}$-rational divisor class of degree 1 given by*

(7) $R = [(\theta_1, 0) + (\theta_2, 0) + (\theta_3, 0) - \infty^+ - \infty^-]$, *where $\theta_1, \theta_2, \theta_3$ are the roots of $X^3 + X + 1$.*

Since $\mathcal{J}_{0j}(\mathbb{Q})$ has rank 0 and no nontrivial torsion, we have that $\mathcal{C}_{0j}$ violates the Hasse principle.

Proof If there existed $P \in \mathcal{C}_{0j}(\mathbb{Q})$, then $[P] - R$ would give a member of $\mathcal{J}_{0j}(\mathbb{Q})$ distinct from the identity element, a contradiction. □

The same argument applies to any of the 10 curves $\mathcal{C}_{0a}, \ldots, \mathcal{C}_{0j}$ listed at the beginning of Table 1 in the appendix. Already we therefore have examples of Corollary 1.

Corollary 2. *There exist, in genus > 1, absolutely simple examples of Corollary 1. Specifically, there exist curves $\mathcal{C}$ of genus 2 defined over $\mathbb{Q}$, which violate the Hasse principle, which have $\mathbb{Q}$-rational divisor classes of degree 1, and whose Jacobians $\mathcal{J}$ are absolutely simple and of $\mathbb{Q}$-rank 0. If Ш$(\mathcal{J})$ is finite then $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$ and so the Brauer-Manin obstruction explains the violations of Hasse principle for these curves.*

We shall see in Sections 3,4 how to deal with curves like $\mathcal{C}_{1b}$, where the Jacobian has nonzero $\mathbb{Q}$-rank.

When neither (i) nor (ii) is satisfied, the existence or otherwise of a K-rational divisor class of degree 1 is determined by whether or not the kernel of μ is larger than $2\mathcal{J}(K)$.

Lemma 6. *Let $\mathcal{C} : Y^2 = F(X)$ be as in (2) defined over K, with Jacobian $\mathcal{J}$, and suppose that neither Criterion (i) nor (ii) of Lemma 4 is satisfied. If the kernel of μ is $2\mathcal{J}(K)$ then there does not exist a K-rational divisor class of degree 1 on $\mathcal{C}$. In particular, $\mathcal{C}(K) = \emptyset$.*

Proof Imagine there were a K-rational divisor class R of degree 1 on $\mathcal{C}$. Then $R + R - \mathcal{O} \in \mathcal{J}(K)$ is clearly in the kernel of μ. However, the 16 members S of $\mathcal{J}(\overline{K})$ satisfying $2S = R + R - \mathcal{O}$ are of the form $R + [(\theta_i, 0)] - \mathcal{O}$ or $R + [(\theta_i, 0) + (\theta_j, 0) + (\theta_k, 0)] - 2\mathcal{O}$, where $\theta_i, \theta_j, \theta_k$ are distinct roots of $F(X)$. Neither of these can be defined over K since neither Criterion (i) nor (ii) is satisfied; this gives that $R + R - \mathcal{O}$ is not in $2\mathcal{J}(K)$ even though it is in the kernel of μ, a contradiction. □

The above gives a slick way of showing in many cases that $\mathcal{C}(K) = \emptyset$, once generators for $\mathcal{J}(K)/2\mathcal{J}(K)$ have been found. One merely has to run through all members of the finite set $\mathcal{J}(K)/2\mathcal{J}(K)$ and check whether any are in the kernel of μ (it is described in [30] how to check whether a given member of $\mathcal{J}(K)$ is in the kernel of μ). If only the identity element is in the kernel of μ then we can immediately deduce the nonexistence of a K-rational divisor class of degree 1 and that $\mathcal{C}(K) = \emptyset$; if $\mathcal{C}(K)$ also has points everywhere locally, then we can further deduce a violation of the Hasse principle which is due to the Brauer-Manin obstruction – subject, as usual, to the finiteness of $Ш(\mathcal{J})$.

Example 2. *The curve $\mathcal{C}_{3p} : Y^2 = F_{3p}(X) = -3(2X^2 - 19)(2X^2 + 4X + 5)(X^2 + 8)$ has no $\mathbb{Q}$-rational divisor class of degree 1 and so $\mathcal{C}_{3p}(\mathbb{Q}) = \emptyset$. The Jacobian $\mathcal{J}_{3p}$ has $\mathbb{Q}$-rank 3.*

Proof First note that, after performing a 2-descent directly on $\mathcal{J}_{3p}$, one merely obtains a 2-Selmer bound of 5 for the rank of $\mathcal{J}_{3p}(\mathbb{Q})$, and one finds

$$\begin{aligned} T_1 &= \{(\sqrt{\tfrac{19}{2}}, 0), (-\sqrt{\tfrac{19}{2}}, 0)\},\ T_2 = \{(\sqrt{-8}, 0), (-\sqrt{-8}, 0)\}, \\ D_1 &= \{(i, 42 + 21i), (-i, 42 - 21i)\},\ D_2 = \{(\sqrt{2}, 60 + 15\sqrt{2}), (-\sqrt{2}, 60 - 15\sqrt{2})\}, \\ D_3 &= \{(\sqrt{\tfrac{11}{3}}, \tfrac{70}{3} + 35\sqrt{\tfrac{11}{3}}), (-\sqrt{\tfrac{11}{3}}, \tfrac{70}{3} - 35\sqrt{\tfrac{11}{3}})\}, \end{aligned} \tag{8}$$

where T_1, T_2 generate the torsion group of $\mathcal{J}_{3p}(\mathbb{Q})$, and D_1, D_2, D_3 are independent points of infinite order in $\mathcal{J}_{3p}(\mathbb{Q})$, giving that $3 \leq$ rank of $\mathcal{J}_{3p}(\mathbb{Q}) \leq 5$. On the other hand, applying (4) to $\mathcal{C}_{3p}$ gives the curve $\mathcal{D}_{3p} : Y^2 = 3 \cdot 840^2 X(2X^2 + 24X + 19)(2X^2 - 11X - 16)$; applying a 2-descent gives a 2-Selmer bound of 3 for the $\mathbb{Q}$-rank of the Jacobian of $\mathcal{D}_{3p}$. Since this is Richelot-isogenous over $\mathbb{Q}$ to $\mathcal{J}_{3p}$, the rank of $\mathcal{J}_{3p}$ must also be 3 (and so $\#Ш(\mathcal{J}_{3p})[2] > 1$), with T_1, T_2, D_1, D_2, D_3 generating all of $\mathcal{J}_{3p}(\mathbb{Q})/2\mathcal{J}_{3p}(\mathbb{Q})$. Applying the map μ of (5) to $n_1T_1 + n_2T_2 + n_3D_1 + n_4D_2 + n_5D_3$, for all 32 choices of $n_i = 0, 1$, we find that only the case $n_1 = n_2 = \ldots = n_5 = 0$ is mapped by μ to the identity, and so the kernel of μ is $2\mathcal{J}_{3p}(\mathbb{Q})$. Since clearly the roots of $F_{3p}(X)$ satisfy neither Criterion (i) nor (ii) of Lemma 4, we can deduce from Lemma 6 that there does not exist a $\mathbb{Q}$-rational divisor class of degree 1 on $\mathcal{C}_{3p}$, and so $\mathcal{C}_{3p}(\mathbb{Q}) = \emptyset$. □

The same argument applies to all of the rank 1 cases $\mathcal{C}_{1M}, \mathcal{C}_{1N}, \mathcal{C}_{1O}, \mathcal{C}_{1P}$, the rank 2 cases $\mathcal{C}_{2\varphi}, \mathcal{C}_{2\chi}, \mathcal{C}_{2\psi}, \mathcal{C}_{2\omega}$, and the rank 3 cases $\mathcal{C}_{3n}, \mathcal{C}_{3o}, \mathcal{C}_{3p}$, given at the end of Tables $1, 3, 4$ in the appendix. As with all of our curves, these have been checked to have points everywhere locally. This gives us nontrivial examples of Lemma 2.

Corollary 3. *There exist, in genus > 1, absolutely simple examples of Lemma 2. Specifically, there exist curves $\mathcal{C}$ of genus 2 defined over $\mathbb{Q}$, which violate the Hasse principle, which do not have $\mathbb{Q}$-rational divisor classes of degree 1, and whose Jacobians $\mathcal{J}$ are absolutely simple and of $\mathbb{Q}$-ranks $1, 2$ and 3. If $\text{Ш}(\mathcal{J})$ is finite then $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$ and so the Brauer-Manin obstruction explains the violations of the Hasse principle for these curves.*

The reverse direction of Lemma 6 is also straightforward.

Lemma 7. *Let $\mathcal{C} : Y^2 = F(X)$ be as in (2) with Jacobian $\mathcal{J}$, and suppose that neither Criterion (i) nor (ii) of Lemma 4 is satisfied. If the kernel of μ is larger than $2\mathcal{J}(K)$ then there exists a K-rational divisor class of degree 1 on $\mathcal{C}$.*

Proof Let $D \in \mathcal{J}(K)$ be in the kernel of μ, but not in $2\mathcal{J}(K)$. It follows from Lemma 4 that $D \in \mathcal{W}$, where $\mathcal{W}$ is as described in Definition 2, and so there must exist an an effective divisor A_0 of degree 3 which is either defined over K or defined over a quadratic extension of K and linearly equivalent to its conjugate A_0'. Then $R = [A_0] - \mathcal{O}$ is a K-rational divisor class of degree 1. □

In practice, given D in the kernel of μ but not in $2\mathcal{J}(K)$, finding A_0 is quite hard, and so the above proof does not tell us how to find R, a K-rational divisor class of degree 1. Suppose that $D = \{P_0, P_0'\}$, where $P_0, P_0' \in \mathcal{C}(K(\sqrt{d}))$ for some quadratic extension $K(\sqrt{d})$ of K, and where P_0 and P_0' are conjugates over K. In this case, it is helpful first to consider the twist

$$\mathcal{C}^{\mathrm{tw}} : Y^2 = dF(X), \quad \text{with Jacobian } \mathcal{J}^{\mathrm{tw}}. \tag{9}$$

Then there is the map

$$\mathrm{tw} : \mathcal{C} \to \mathcal{C}^{\mathrm{tw}} : (x, y) \mapsto (x, y)^{\mathrm{tw}} = (x, \sqrt{d}\, y) \tag{10}$$

and the induced map on the Jacobian

$$\mathrm{tw} : \mathcal{J} \to \mathcal{J}^{\mathrm{tw}} : \{(x_1, y_1), (x_2, y_2)\} \mapsto \{(x_1, y_1), (x_2, y_2)\}^{\mathrm{tw}} = \{(x_1, \sqrt{d}\, y_1), (x_2, \sqrt{d}\, y_2)\}. \tag{11}$$

We note in passing that, for any $D \in \mathcal{J}(K(\sqrt{d}))$, we have $(D+D', (D-D')^{\mathrm{tw}}) \in \mathcal{J}(K) \times \mathcal{J}^{\mathrm{tw}}(K)$. Conversely, for any $(E_1, E_2) \in \mathcal{J}(K) \times \mathcal{J}^{\mathrm{tw}}(K)$ we have $E_1 + E_2^{\mathrm{tw}^{-1}} \in \mathcal{J}(K(\sqrt{d}))$. Since the composition of these, in either order, is duplication, we have that

$$\mathrm{rank}\big(\mathcal{J}(K(\sqrt{d}))\big) = \mathrm{rank}\big(\mathcal{J}(K)\big) + \mathrm{rank}\big(\mathcal{J}^{\mathrm{tw}}(K)\big). \tag{12}$$

In order to compute the divisor class R, the following version of Lemma 7 was pointed out by Michael Stoll, which gives a construction, provided that $\mathcal{J}(K)/2\mathcal{J}(K)$ has been found and $\#\mathcal{J}(K)[2] = 1$.

Lemma 8. *Let $\mathcal{C} : Y^2 = F(X)$ be as in (2) defined over K, with Jacobian $\mathcal{J}$. Suppose that $\#\mathcal{J}(K)[2] = 1$ and that there exists D which is in the kernel of μ but is not in $2\mathcal{J}(K)$. When $D = \{P_1, P_2\}$, where $P_1, P_2 \in \mathcal{C}(K)$, then $R = [P_1]$ or $[P_2]$ is a K-rational divisor class of degree 1. Otherwise $D = \{P_0, P_0'\}$, where $P_0, P_0' \in \mathcal{C}(K(\sqrt{d}))$ for some quadratic extension $K(\sqrt{d})$ of K, and where P_0 and P_0' are conjugates. In this case, $\{P_0^-, P_0'\}^{\mathrm{tw}} \in 2\mathcal{J}^{\mathrm{tw}}(K)$ and $\{P_0^-, P_0'\}^{\mathrm{tw}} = 2E_0$ for some $E_0 \in \mathcal{J}^{\mathrm{tw}}(K)$, where P_0^- denotes the image of P_0 under the hyperelliptic involution $(x, y) \mapsto (x, -y)$. Let $D_0 = E_0^{\mathrm{tw}^{-1}}$. Then $R = [P_0] + D_0$ is a K-rational divisor class of degree 1.*

Proof The case $D = \{P_1, P_2\}$, where $P_1, P_2 \in \mathcal{C}(K)$, is trivial. Suppose now that we are in the second situation $D = \{P_0, P_0'\}$, where $P_0, P_0' \in \mathcal{C}(K(\sqrt{d}))$ and are conjugates over K. It follows from Lemma 4 that $D \in \mathcal{W}$, where $\mathcal{W}$ is as described in Definition 2, and so $D \in \mathcal{W}_d$, where $\mathcal{W}_d$ is the same as $\mathcal{W}$ but for the field $K(\sqrt{d})$. Also, $\{P_0, P_0\} \in \mathcal{W}_d$ and so, again by Lemma 4, the difference $\{P_0, P_0'\} - \{P_0, P_0\} = \{P_0^-, P_0'\} \in 2\mathcal{J}(K(\sqrt{d}))$. Hence $\{P_0^-, P_0'\} = 2D_0$ for some $D_0 \in \mathcal{J}(K(\sqrt{d}))$. Now,

$$(\{P_0^-, P_0'\}^{\mathrm{tw}})' = \{((P_0^-)^{\mathrm{tw}})', ((P_0')^{\mathrm{tw}})'\} = \{(P_0')^{\mathrm{tw}}, (P_0^-)^{\mathrm{tw}}\} = \{P_0^-, P_0'\}^{\mathrm{tw}}, \tag{13}$$

so that $\{P_0^-, P_0'\}^{\mathrm{tw}}$, and so also $E_0 = D_0^{\mathrm{tw}}$, are in $\mathcal{J}^{\mathrm{tw}}(K)$, given that $\#\mathcal{J}^{\mathrm{tw}}(K)[2] = \#\mathcal{J}(K)[2] = 1$ and $\{P_0^-, P_0'\}^{\mathrm{tw}} = 2E_0$. Now, let $R = [P_0] + D_0$. Then $D_0' = (E_0^{\mathrm{tw}^{-1}})' = -(E_0')^{\mathrm{tw}^{-1}} = -D_0$, so that

$$R' = [P_0'] + D_0' = [P_0'] - D_0 = [P_0'] - 2D_0 + D_0 = [P_0'] - \{P_0^-, P_0'\} + D_0 = R, \tag{14}$$

so that R is defined over K, as required. □

Example 3. *The curve $\mathcal{C}_{2U} : Y^2 = F_{2U}(X) = -2X^6 - 2X^5 + 2X^4 + X^3 - 2X^2 - X + 2$ has a $\mathbb{Q}$-rational divisor class of degree 1 given by*

$$R = [P_0 + (0, \sqrt{2}) - (-1, -\sqrt{2})], \text{ where } P_0 = (\frac{7}{17} + \frac{4}{17}\sqrt{2}, -\frac{1888}{4913} + \frac{3465}{4913}\sqrt{2}). \tag{15}$$

Proof The Jacobian $\mathcal{J}_{2U}$ has no nontrivial torsion over $\mathbb{Q}$, and has $\mathbb{Q}$-rank 2, with $\mathcal{J}_{2U}(\mathbb{Q})$ generated by

$$\begin{aligned} D_1 &= \{(-\tfrac{1}{6} + \tfrac{1}{6}\sqrt{13}, -\tfrac{7}{54} + \tfrac{19}{54}\sqrt{13}), (-\tfrac{1}{6} - \tfrac{1}{6}\sqrt{13}, -\tfrac{7}{54} - \tfrac{19}{54}\sqrt{13})\}, \\ D_2 &= \{(-\tfrac{3}{2} + \tfrac{1}{6}\sqrt{-3}, -\tfrac{13}{6} - \tfrac{13}{18}\sqrt{-3}), (-\tfrac{3}{2} - \tfrac{1}{6}\sqrt{-3}, -\tfrac{13}{6} + \tfrac{13}{18}\sqrt{-3})\}. \end{aligned} \tag{16}$$

Applying the map μ of (5) to $D_1, D_2, D_1 + D_2$, one finds that the kernel of μ contains $D = D_1 + D_2 = \{P_0, P_0'\}$, where P_0 is as in (15). Following the proof of Lemma 8, we define the curve $\mathcal{C}_{2U}^{\mathrm{tw}} : Y^2 = 2F_{2U}(X)$, with Jacobian $\mathcal{J}_{2U}^{\mathrm{tw}}$, and the maps $\mathrm{tw} : \mathcal{C}_{2U} \to \mathcal{C}_{2U}^{\mathrm{tw}}$ and $\mathrm{tw} : \mathcal{J}_{2U} \to \mathcal{J}_{2U}^{\mathrm{tw}}$ as given in (9),(11) with $d = 2$. Then $\{P_0^-, P_0'\}^{\mathrm{tw}} \in 2\mathcal{J}_{2U}^{\mathrm{tw}}(\mathbb{Q})$ and one can either use a search or the inverse image of the morphism of multiplication by 2 to obtain $E_0 = \{(0, 2), (-1, 2)\} \in \mathcal{J}_{2U}^{\mathrm{tw}}(\mathbb{Q})$ which satisfies $\{P_0^-, P_0'\}^{\mathrm{tw}} = 2E_0$. Furthermore, $E_0 = D_0^{\mathrm{tw}}$, where $D_0 = \{(0, \sqrt{2}), (-1, \sqrt{2})\} \in \mathcal{J}_{2U}(\mathbb{Q}(\sqrt{2}))$ satisfies $\{P_0^-, P_0'\} = 2D_0$. Then, by (14) we see that $R = [P_0] + D_0$ is defined over $\mathbb{Q}$. Finally, $R = [P_0] + D_0 = [P_0 + (0, \sqrt{2}) + (-1, \sqrt{2}) - \infty^+ - \infty^-]$, which is the same divisor class as $[P_0 + (0, \sqrt{2}) - (-1, -\sqrt{2})]$. □

If we are able to find $\mathcal{J}(K)/2\mathcal{J}(K)$ and if $\#\mathcal{J}(K)[2] = 1$, then the above discussion gives an effective procedure which either finds a K-rational divisor class of degree 1 or proves its nonexistence. First, one checks whether Criterion (i) or (ii) of Lemma 4 is satisfied, in which case one easily constructs a K-rational divisor class of degree 1 using the roots $F(X)$. If neither criterion is satisfied and the kernel of μ is the same as $2\mathcal{J}(K)$, then there is no such divisor class by Lemma 6. If neither criterion is satisfied and the kernel of μ is larger than $2\mathcal{J}(K)$, then there is such a divisor class, and Lemma 8 gives a way of constructing it. Note that the step of the above proof where one finds $E_0 \in \mathcal{J}^{\text{tw}}(K)$ such that $\{P_0^-, P_0'\}^{\text{tw}} = 2E_0$, can clearly be effectively performed, either by finding the inverse images of E_0 under the morphism of multiplication by 2, or by using the explicit theory of heights in [14],[16],[29],[31]. We suppose that a modification of the proof of Lemma 8 can be made to deal with the existence of nontrivial 2-torsion, but this was not required for any of our examples.

3. The map $P \mapsto \{P, P\} = [P + P - \infty^+ - \infty^-]$

Given a genus 2 curve $\mathcal{C}$ of the form (2) which is a suspected violation of the Hasse principle, one option is to use the map $P \mapsto \{P, P\} = [P+P-\infty^+ - \infty^-]$ from $\mathcal{C}$ to its Jacobian $\mathcal{J}$. This is not quite an embedding, since all Weierstrass points are mapped to the identity; one first needs to perform a straightforward check that $F(X)$ has no roots in K. If so, then determining $\mathcal{C}(K)$ is the same as finding all members of $\mathcal{J}(K)$ of the form $\{P, P\}$. In the context of Chabauty's Theorem (see [11],[12],[21]), where the rank of $\mathcal{J}(K)$ is 1, this is discussed in [15]. We shall briefly discuss here the generalisation in arbitrary rank. Suppose that $\mathcal{J}(K)$ has rank r with generators $D_1, \ldots, D_r$ of the free part of $\mathcal{J}(K)$, so that any $D \in \mathcal{J}(K)$ can be written

$$D = T + n_1 D_1 + \ldots + n_r D_r, \tag{17}$$

for some $T \in \mathcal{J}(K)_{\text{tors}}$, the torsion group of $\mathcal{J}(K)$. First, fix a place of good reduction $\mathfrak{p}$ and let $k_{\mathfrak{p}}$ be the residue field of $K_{\mathfrak{p}}$; further, let $\widetilde{\mathcal{J}}$ and $\widetilde{D}_i$ represent, respectively, the reductions mod $\mathfrak{p}$ of $\mathcal{J}$ and D_i. Define

$$N_i^{(\mathfrak{p})} = \text{order of } \widetilde{D}_i \text{ in } \widetilde{\mathcal{J}}(k_{\mathfrak{p}}), \quad E_i^{(\mathfrak{p})} = N_i^{(\mathfrak{p})} D_i, \quad i = 1, \ldots r, \tag{18}$$

so that each $E_i^{(\mathfrak{p})} \in \mathcal{J}(K)$ is in the kernel of the reduction map from $\mathcal{J}(K)$ to $\widetilde{\mathcal{J}}(k_{\mathfrak{p}})$. Suppose there exists $D = \{(x_1, y_1), (x_2, y_2)\}$ in the image of our map, so that $D = \{P, P\}$, for some $P \in \mathcal{J}(K)$. Then the elements $x_1 + x_2, x_1 x_2 \in K$ satisfy

$$(x_1 + x_2)^2 - 4x_1 x_2 = 0, \tag{19}$$

as do the $\tilde{x}_1, \tilde{x}_2$ of $\widetilde{D}$. For each $T \in \mathcal{J}(K)_{\text{tors}}$, one can then see when this is satisfied for all possibilities of $(n_1, \ldots, n_r)$ modulo $(N_1^{(\mathfrak{p})}, \ldots, N_r^{(\mathfrak{p})})$, giving a set of congruence conditions of the form

$$(n_1, \ldots, n_r) \in \{(b_{1_j}^{(\mathfrak{p})}, \ldots, b_{r_j}^{(\mathfrak{p})}) : \ j = 1, \ldots, J^{(\mathfrak{p})}\} \bmod (N_1^{(\mathfrak{p})}, \ldots, N_r^{(\mathfrak{p})}). \tag{20}$$

If it turns out, for every $T \in \mathcal{J}(K)_{\text{tors}}$, that there exists a set of places $\mathfrak{p}$ such that these congruences are contradictory, then we can conclude that $\mathcal{C}(K) = \emptyset$

Example 4. *The curve $\mathcal{C}_{2\zeta} : Y^2 = 2X^6 - 2X^4 - X^3 + X^2 + X - 2$ violates the Hasse principle and has Jacobian $\mathcal{J}_{2\zeta}$ of $\mathbb{Q}$-rank 2.*

Proof There is no nontrivial torsion in $\mathcal{J}_{2\zeta}(\mathbb{Q})$, and generators of $\mathcal{J}_{2\zeta}(\mathbb{Q})$ are given by

$$\begin{aligned} D_1 &= \{(-\tfrac{1}{2} - \tfrac{1}{2}i, \tfrac{3}{2}i), (-\tfrac{1}{2} + \tfrac{1}{2}i, -\tfrac{3}{2}i)\}, \\ D_2 &= \{(\tfrac{19}{34} + \tfrac{1}{34}\sqrt{-217}, -\tfrac{435}{4913} - \tfrac{639}{9826}\sqrt{-217}), (\tfrac{19}{34} - \tfrac{1}{34}\sqrt{-217}, -\tfrac{435}{4913} + \tfrac{639}{9826}\sqrt{-217})\}, \end{aligned} \tag{21}$$

so that any $D \in \mathcal{J}_{2\zeta}(\mathbb{Q})$ satisfies $D = n_1 D_1 + n_2 D_2$ for some $n_1, n_2 \in \mathbb{Z}$. Let $\widetilde{\mathcal{C}}_{2\zeta}$ and $\widetilde{\mathcal{J}}_{2\zeta}$ be the reductions of $\mathcal{C}_{2\zeta}$ and $\mathcal{J}_{2\zeta}$ modulo 3. Then D_1 and D_2 reduce modulo 3 to $\widetilde{D}_1 = \widetilde{D}_2 = \{(1+i, 0), (1-i, 0)\} \in \widetilde{\mathcal{J}}_{2\zeta}(\mathbb{F}_3)$. The orders of D_1 and D_2 are therefore $N_1^{(3)} = N_2^{(3)} = 2$. It follows that any $D = n_1 D_1 + n_2 D_2 \in \mathcal{J}_{2\zeta}(\mathbb{Q})$ must reduce modulo 3 either to the identity element when $n_1 + n_2$ is even, or to $\{(1+i,0), (1-i,0)\}$ when $n_1 + n_2$ is odd. Now imagine that there exists $P \in \mathcal{C}_{2\zeta}(\mathbb{Q})$, which must reduce modulo 3 to $\widetilde{P} = (0,1)$ or $\widetilde{P} = (0,2)$, since these are the only members of $\widetilde{\mathcal{C}}_{2\zeta}(\mathbb{F}_3)$. Then $\{P, P\} \in \mathcal{J}_{2\zeta}(\mathbb{Q})$ would have to reduce modulo 3 either to $\{(0,1),(0,1)\}$ or to $\{(0,2),(0,2)\}$ in $\widetilde{\mathcal{J}}_{2\zeta}(\mathbb{F}_3)$, neither of which is the identity element or $\{(1+i,0),(1-i,0)\}$, a contradiction. Hence, no such P exists, giving that $\mathcal{C}_{2\zeta}(\mathbb{Q}) = \emptyset$, as required. □

It was fortunate in the above example that reduction modulo a single prime gave an immediate contradiction (that is, in the notation of (20), the set of congruences corresponding to the prime 3 was the empty set); normally, it is necessary to combine information from different primes. A more typical example will be given in the next section.

When finite field reductions fail to show the nonexistence of rational points on $\mathcal{C}$, we can make use of deeper local information by describing locally the multiples of $E_1^{(\mathfrak{p})}, \ldots, E_r^{(\mathfrak{p})}$. We first write each n_i as $\tilde{n}_i^{(\mathfrak{p})} + m_i^{(\mathfrak{p})} N_i^{(\mathfrak{p})}$, where $\tilde{n}_i^{(\mathfrak{p})}$ denotes the reduction of n_i mod $N_i^{(\mathfrak{p})}$, so that any $D \in \mathcal{J}(K)$ can now be written

$$D = T + \tilde{n}_1^{(\mathfrak{p})} D_1 + \ldots + \tilde{n}_r^{(\mathfrak{p})} D_r + m_i^{(\mathfrak{p})} E_1^{(\mathfrak{p})} + \ldots m_r^{(\mathfrak{p})} E_r^{(\mathfrak{p})}. \tag{22}$$

Since $E_1^{(\mathfrak{p})}, \ldots, E_r^{(\mathfrak{p})}$ are in the kernel of reduction, one can use the formal group (as in [15]) to find, for each choice of $T \in \mathcal{J}(K)_{\mathrm{tors}}$ and $\tilde{n}_1^{(\mathfrak{p})}, \ldots, \tilde{n}_r^{(\mathfrak{p})}$, a triple of power series,

$$(\psi_1^{(\mathfrak{p})}(m_1^{(\mathfrak{p})}, \ldots, m_r^{(\mathfrak{p})}),\ \psi_2^{(\mathfrak{p})}(m_1^{(\mathfrak{p})}, \ldots, m_r^{(\mathfrak{p})}),\ \psi_3^{(\mathfrak{p})}(m_1^{(\mathfrak{p})}, \ldots, m_r^{(\mathfrak{p})})), \tag{23}$$

equal to $(1 : x_1 + x_2 : x_1 x_2)$ for D in (22). Combining this with (19) gives a power series

$$\psi_2^{(\mathfrak{p})}(m_1^{(\mathfrak{p})}, \ldots, m_r^{(\mathfrak{p})})^2 \ - \ \psi_1^{(\mathfrak{p})}(m_1^{(\mathfrak{p})}, \ldots, m_r^{(\mathfrak{p})})\ \psi_3^{(\mathfrak{p})}(m_1^{(\mathfrak{p})}, \ldots, m_r^{(\mathfrak{p})}) = 0, \tag{24}$$

which gives conditions on $m_1^{(\mathfrak{p})}, \ldots, m_r^{(\mathfrak{p})}$ modulo p^s, where $p = \mathrm{char}(k_{\mathfrak{p}})$ is a rational prime. These induce congruence conditions of the form

$$(n_1, \ldots, n_r) \in \{(\ell_{1_j}^{(\mathfrak{p})}, \ldots, \ell_{r_j}^{(\mathfrak{p})}) :\ j = 1, \ldots, J^{(\mathfrak{p})}\} \bmod (p^s, \ldots, p^s), \tag{25}$$

where s can be made arbitrarily large, depending on the accuracy our computations. For $s \geq 1$ we can regard this as 'deep' information for a particular prime, as opposed to the 'flat' information of (20). In the special case when $r = 1$ Chabauty's theorem applies and this gives us a bound on $\#\mathcal{C}(K)$, as described in [15].

It is clear that no two deep conditions of the form (25) can ever give a contradiction for different primes, whereas several flat conditions might do so. A more subtle idea is that the flat and deep information might be usefully combined, when the $N_i^{(\mathfrak{p})}$ for one prime has a prime factor at the place of the deep information. We shall give examples of these types in the next section.

4. The embedding $P \mapsto [P] - R$, where R is a rational divisor class of degree 1

The map of the previous section has clear inefficiencies due to the fact that it is not an embedding. In particular, any set of primes modulo which there are Weierstrass points can never show $\mathcal{C}(K)$ to be empty, since the identity element in $\mathcal{J}(K)$ will be of the form $\{P, P\}$ modulo all such primes. This can often mean that one needs to compute modulo much higher primes than are computationally viable. Furthermore, for the purposes of investigating the Brauer-Manin obstruction and applying Theorem 1, we wish to use an actual embedding of $\mathcal{C}$ in $\mathcal{J}$. Embeddings that have previously been employed in the literature are either of the form $P \mapsto [P] - [P_0]$, for some fixed $P_0 \in \mathcal{C}(K)$ or they rely on $\mathcal{J}$ being reducible and having an elliptic curve as a factor [23]. Neither of these are available in our case, since we wish our methods to apply when $\mathcal{C}(K)$ is empty and when $\mathcal{J}$ is absolutely simple. If the methods in Section 2 establish that there is no K-rational divisor class of degree 1; then, as we have seen, $\mathcal{C}(K)$ is empty and the Brauer-Manin obstruction is the only obstruction to the Hasse principle. Suppose instead that the methods of Section 2 establish that there does exist a K-rational divisor class R of degree 1 and compute it. Then we can use $P \mapsto [P] - R$ to embed $\mathcal{C}$ into $\mathcal{J}$. We mention the following trivial result merely to clarify why such an embedding is guaranteed to be at least as strong as that of the last section.

Lemma 9. *Let R be a K-rational divisor class of degree 1. Suppose that $D \in \mathcal{J}(K_\mathfrak{p})$ is of the form $[P] - R$, for some $P \in \mathcal{C}(K_\mathfrak{p})$. Then $2D + 2R - \mathcal{O}$ is of the form $\{P, P\}$.*

Proof Since $D = [P] - R$, we must have $2D + 2R - \mathcal{O} = [P + P] - \mathcal{O} = \{P, P\}$. □

The above tells us that a genuine embedding like $P \mapsto [P] - R$ will be at least as successful as the methods of the previous section; as we shall soon see, in many cases it is an improvement. We first need to describe the embedding explicitly, which is simply a matter of algebra. One takes a general point $P = (u, v)$ and performs the group law in $\mathcal{J}(K)$ to compute the representative of the degree 0 divisor class $[P] - R$ in the form $D = \{(x_1, y_1), (x_2, y_2)\}$, giving x_1, y_1, x_2, y_2 as functions of u, v. This induces a polynomial relation satisfied between x_1, y_1, x_2, y_2, which will perform the same role as (19) in the previous section.

To give a general idea of the algebra involved, we illustrate this first for the simplest case, when our curve $\mathcal{C} : Y^2 = F(X)$ is such that $F(X)$ is the product of conjugate cubics. In this case, Criterion (ii) of Lemma 4 is satisfied, and so $\mathcal{C}$ has a K-rational divisor class.

Lemma 10. *Let $\mathcal{C}$ be a curve of genus 2 of the form*

$$\mathcal{C} : Y^2 = G(X)H(X) = (g_3X^3 + g_2X^2 + g_1X + g_0)(h_3X^3 + h_2X^2 + h_1X + h_0), \tag{26}$$

where $G(X), H(X)$ are either both defined over K or are quadratic and conjugate over K, so that the divisor class $R = [(\theta_1, 0) + (\theta_2, 0) + (\theta_3, 0) - \infty^+ - \infty^-]$ is K-rational and of degree 1, where $\theta_1, \theta_2, \theta_3$

are the roots of $G(X)$. *Let* ζ *be the embedding of* $\mathcal{C}$ *into* $\mathcal{J}$ *defined by* $(u,v) \mapsto [(u,v)] - R$, *and suppose that* $D = \{(x_1,y_1),(x_2,y_2)\} \in \zeta(\mathcal{C}(K))$. *Then* x_1, x_2 *satisfy*

$$\begin{array}{l} (g_3h_2 - g_2h_3)(x_1x_2)^2 + (g_3h_1 - g_1h_3)x_1x_2(x_1+x_2) + (g_3h_0 - g_0h_3)(x_1+x_2)^2 \\ +(g_2h_1 - g_1h_2 + g_0h_3 - g_3h_0)x_1x_2 + (g_2h_0 - g_0h_2)(x_1+x_2) + (g_1h_0 - g_0h_1) = 0. \end{array} \tag{27}$$

Proof Let $D = \zeta(P)$, where $P = (u,v) \in \mathcal{C}(K)$. Then $D = \{(u,v),(\theta_1,0)\} + \{(\theta_2,0),(\theta_3,0)\}$. First note that the function $G(u)Y - vG(X)$ intersects $\mathcal{C}$ at $(u,v),(\theta_1,0),(\theta_2,0),(\theta_3,0)$, and at the roots x_1,x_2 of the quadratic in X given by $q_2(u)X^2 + q_1(u)X + q_0(u)$, where

$$\begin{array}{ll} q_2(u) & = (g_3h_2 - g_2h_3)u^2 + (g_3h_1 - g_1h_3)u + g_3h_0 - g_0h_3, \\ q_1(u) & = (g_3h_1 - g_1h_3)u^2 + (g_3h_0 - g_0h_3 + g_2h_1 - g_1h_2)u + g_2h_0 - g_0h_2, \\ q_0(u) & = (g_3h_0 - g_0h_3)u^2 + (g_2h_0 - g_0h_2)u + g_1h_0 - g_0h_1. \end{array} \tag{28}$$

From these, we obtain $x_1 + x_2 = -q_1(u)/q_2(u)$ and $x_1x_2 = q_0(u)/q_2(u)$. The relation (27) is then obtained by taking the resultant of $(x_1+x_2)q_2(u) + q_1(u)$ and $(x_1x_2)q_2(u) - q_0(u)$ with respect to u. □

Note that (27) is weaker than the condition that $D \in \zeta(\mathcal{C}(K))$; the condition equivalent to $D \in \zeta(\mathcal{C}(K))$ combines (27) with equations involving y_1, y_2. When the K-rational degree 1 divisor class has been obtained using Lemma 8, the same idea applies for describing the embedding explicitly.

Example 5. *Let* $\mathcal{C}_{2U}$ *and* R *be as in Example 3, and let* $\mathcal{J}_{2U}$ *be the Jacobian of* $\mathcal{C}_{2U}$. *Define the embedding* $\zeta : \mathcal{C}_{2U} \longrightarrow \mathcal{J}_{2U} : P \mapsto [P] - R$. *Then*

$$\begin{array}{rl} \zeta\big((u,v)\big) & = \{(x_1,y_1),(x_2,y_2)\}, \text{ where } x_1,x_2 \text{ are the roots of} \\ & \big(4u^4+8u^3-8u^2-12u+17\big)X^2 + \big(4u^4+2u^3-12u^2+7u-4v+10\big)X - \big(6u^4+10u^3-15u^2+4uv-12u+4v+7\big), \\ & \text{and } y_1 = L(x_1), y_2 = L(x_2), \text{ where} \\ L(X) & = \frac{32u^8+64u^7-24u^5v-40u^5-40u^4v-96u^4+128u^3v+48u^3+88u^2v+48u^2-158uv-122u+50v+62}{16u^8+64u^7-224u^5+8u^4+464u^3-128u^2-408u+289}X \\ & + \frac{-16u^8+32u^7+160u^6+8u^5v-120u^5+20u^4v-284u^4-40u^3v+88u^3+96u^2v-16u^2+198uv-94u-239v+62}{16u^8+64u^7-224u^5+8u^4+464u^3-128u^2-408u+289}. \end{array} \tag{29}$$

Proof Recall that $R = [P_0 + (0,\sqrt{2}) - (-1,-\sqrt{2})]$, where P_0 is as in (15). So, our embedding is given by $\zeta((u,v)) = [(u,v)] - R = \{(u,v),(-1,-\sqrt{2})\} + \{P_0^-,(0,-\sqrt{2})\}$, where as usual P_0^- is the hyperelliptic involute of P_0. One now merely performs the group law on $\mathcal{J}_{2U}$, as follows. Let $\Gamma(X)$ be the unique cubic polynomial such that $Y = \Gamma(X)$ passes through $(u,v),(-1,-\sqrt{2}),P_0^-,(0,-\sqrt{2})$. Then $Y = \Gamma(X)$ and $\mathcal{C}_{2U}$ have six points of intersection, namely $(u,v),(-1,-\sqrt{2}),P_0^-,(0,-\sqrt{2})$ and two further points Q_1,Q_2. The points $(x_1,y_1),(x_2,y_2)$ in (29) are then the hyperelliptic involutes of Q_1,Q_2. □

The techniques available, both for using finite fields to obtain congruence conditions (the flat information) and for working with local power series (the deep information) are now precisely the same as described in the previous section, but adapted so that equations such as (27) now perform the role previously performed by (19). The appendix provides pointers to the programs written to adapt these techniques. Armed with our explicit descriptions of the $\mathbb{Q}$-rational degree 1 divisor class R and the embedding $\zeta : P \mapsto [P] - R$, we are now in a position to perform applications of the Brauer-Manin Obstruction, using the description (1) in Theorem 1. The following example shows how using a genuine embedding of the form $P \mapsto [P] - R$ can strictly improve on the $P \mapsto \{P,P\} = [P + P - \infty^+ - \infty^-]$ map of the previous section.

Example 6. *Let* $\mathcal{C}_{2U}$ *and* R *be as in Example 3, and let* $\mathcal{J}_{2U}$ *be the Jacobian of* $\mathcal{C}_{2U}$. *Then* $\mathcal{J}_{2U}(\mathbb{Q})$ *has rank* 2 *and* $\mathcal{C}_{2U}(\mathbb{Q}) = \emptyset$.

Proof Recall from Example 3 that the Jacobian $\mathcal{J}_{2U}$ has no nontrivial torsion over $\mathbb{Q}$, and has $\mathbb{Q}$-rank 2, with $\mathcal{J}_{2U}(\mathbb{Q})$ generated by the D_1, D_2 given in (16). Let R be the $\mathbb{Q}$-rational degree 1 divisor class given in (15), and as usual define the embedding $\zeta : \mathcal{C}_{2U} \longrightarrow \mathcal{J}_{2U} : P \mapsto [P] - R$. Since ζ is defined over $\mathbb{Q}$, any $P \in \mathcal{C}_{2U}(\mathbb{Q})$ must map to $\zeta(P) \in \mathcal{J}_{2U}(\mathbb{Q})$, and so $\zeta(P) = n_1 D_1 + n_2 D_2$, for some $n_1, n_2 \in \mathbb{Z}$.

First, let $\widetilde{\mathcal{C}}_{2U}, \widetilde{\mathcal{J}}_{2U}, \widetilde{D}_1, \widetilde{D}_2, \widetilde{R}, \tilde{\zeta}$ be the reductions of $\mathcal{C}_{2U}, \mathcal{J}_{2U}, D_1, D_2, R, \zeta$ modulo 3, in particular, the divisor class $\widetilde{R} = [(-1-i,1) + (0,i) - (-1,-i)]$. Then $\widetilde{\mathcal{C}}_{2U}(\mathbb{F}_3)$ contains only the points: $(1,1), (1,-1), \infty^+, \infty^-$, where the points ∞^+, ∞^- refer to the branches at infinity where Y/X^3 is $1, -1$, respectively, modulo 3. Any $P \in \mathcal{C}_{2U}(\mathbb{Q})$ must have $\widetilde{P}$ equal to one of these, and so the possibilities for $\widetilde{\zeta(P)} = \tilde{\zeta}(\widetilde{P}) = [\widetilde{P}] - \widetilde{R}$ can be obtained by computing $\tilde{\zeta}((1,1)), \tilde{\zeta}((1,-1)), \tilde{\zeta}(\infty^+)$ and $\tilde{\zeta}(\infty^-)$. For example, the image of $(1,1)$ can be computed as $\tilde{\zeta}((1,1)) = [(1,1)] - \widetilde{R} = \{(1,1), (-1-i,-1)\} + \{(0,-i), (-1,-i)\}$ in $\widetilde{\mathcal{J}}_{2U}(\mathbb{F}_3)$. We perform this sum in $\widetilde{\mathcal{J}}_{2U}(\mathbb{F}_3)$ by finding $y = -(x^3 + (1+i)x^2 + ix + i)$, defined over $\mathbb{F}_3(i)$, which meets $\widetilde{\mathcal{C}}_{2U}$ at the points $(1,1), (-1-i,-1), (0,-i), (-1,-i)$, together with the additional two points $(1,1), \infty^-$. It follows that $\{(1,1), (-1-i,-1)\} + \{(0,-i), (-1,-i)\} + \{(1,1), \infty^-\}$ is the identity in $\widetilde{\mathcal{J}}_{2U}(\mathbb{F}_3)$ and so $\tilde{\zeta}((1,1)) = -\{(1,1), \infty^-\} = \{(1,-1), \infty^+\}$. Similarly, one can compute $\tilde{\zeta}((1,-1)) = \{(-1+i,1), (-1-i,1)\}$, $\tilde{\zeta}(\infty^+) = \{(1+i,-i), (1-i,i)\}$, and $\tilde{\zeta}(\infty^-) = \{(1,-1), (1,-1)\}$. In summary, any $P \in \mathcal{C}_{2U}(\mathbb{Q})$ must satisfy

$$(30) \qquad \widetilde{\zeta(P)} = \{(1,-1), \infty^+\},\ \{(-1+i,1), (-1-i,1)\},\ \{(1+i,-i), (1-i,i)\} \text{ or } \{(1,-1), (1,-1)\}.$$

Further, the reductions of D_1 and D_2 modulo 3 are $\widetilde{D}_1 = \{(1,1), \infty^+\}$ and $\widetilde{D}_2 = \{\infty^+, \infty^+\}$. On taking multiples of $\widetilde{D}_1, \widetilde{D}_2$, we find that $13\widetilde{D}_1$ and $13\widetilde{D}_2$ are the identity in $\widetilde{\mathcal{J}}_{2U}(\mathbb{F}_3)$, so that the orders of $\widetilde{D}_1$ and $\widetilde{D}_2$ are $N_1^{(3)} = N_2^{(3)} = 13$. The other multiples of $\widetilde{D}_2$ are

$$\begin{array}{lll}
1\widetilde{D}_2 = \{\infty^+, \infty^+\}, & 2\widetilde{D}_2 = \{(-1+i,-1), (-1-i,-1)\}, & 3\widetilde{D}_2 = \{(1,-1), \infty^-\}, \\
4\widetilde{D}_2 = \{(1,-1), \infty^+\}, & 5\widetilde{D}_2 = \{(1+i,i), (1-i,-i)\}, & 6\widetilde{D}_2 = \{(1,1), (1,1)\}, \\
7\widetilde{D}_2 = \{(1,-1), (1,-1)\}, & 8\widetilde{D}_2 = \{(1+i,-i), (1-i,i)\}, & 9\widetilde{D}_2 = \{(1,1), \infty^-\}, \\
10\widetilde{D}_2 = \{(1,1), \infty^+\}, & 11\widetilde{D}_2 = \{(-1+i,1), (-1-i,1)\}, & 12\widetilde{D}_2 = \{\infty^-, \infty^-\}.
\end{array}$$

The only overlap between the above list and (30) are the multiples $4\widetilde{D}_2, 7\widetilde{D}_2, 8\widetilde{D}_2, 11\widetilde{D}_2$. Since we also have $\widetilde{D}_1 = 10\widetilde{D}_2$, we see that $n_1\widetilde{D}_1 + n_2\widetilde{D}_2$ is a member of (30) exactly when $10n_1 + n_2 \equiv 4, 7, 8$ or $11 \pmod{13}$. Since $\zeta(P) = n_1 D_1 + n_2 D_2$ for some $n_1, n_2 \in \mathbb{Z}$, we must also have that $\widetilde{\zeta(P)} = n_1\widetilde{D}_1 + n_2\widetilde{D}_2$, and so we need only consider n_1, n_2 satisfying this condition. Unlike Example 4 we have not shown an immediate contradiction, but we have found congruence conditions which must be satisfied by n_1, n_2.

$$(31) \qquad P \in \mathcal{C}_{2U}(\mathbb{Q}) \Rightarrow \zeta(P) = n_1 D_1 + n_2 D_2, \text{ some } n_1, n_2 \in \mathbb{Z} \text{ with } 10n_1 + n_2 \equiv 4, 7, 8 \text{ or } 11 \pmod{13}.$$

If we now perform the above process, but with reductions modulo 19, we find that $\widetilde{D}_1$ has order 26 and $\widetilde{D}_2$ has order 104, with $\widetilde{D}_1 = 36\widetilde{D}_2$. The only multiples of $\widetilde{D}_2$ which intersect with the possible values of $\widetilde{\zeta(P)}$ are $23\widetilde{D}_2, 44\widetilde{D}_2, 83\widetilde{D}_2, 88\widetilde{D}_2$, so that

$$(32) \quad P \in \mathcal{C}_{2U}(\mathbb{Q}) \Rightarrow \zeta(P) = n_1 D_1 + n_2 D_2, \text{ some } n_1, n_2 \in \mathbb{Z} \text{ with } 36n_1 + n_2 \equiv 23, 44, 83 \text{ or } 88 \pmod{104}.$$

However, reducing this last equation modulo 13 gives that $10n_1 + n_2$ must be 5 or 10 (mod 13), which contradicts (31). Hence $\mathcal{C}_{2U}(\mathbb{Q}) = \emptyset$, as required. □

It is apparent in combining the above sets of congruences that not all of the information is needed, merely the information after reducing all sets of congruences modulo 13, which we refer to as smoothness bound B(13). For example, in Table 3 in the appendix, we summarise the entry for $\mathcal{C}_{2U}$ as: Fl(3, 19), B(13), to indicate that the congruence information obtained at $\widetilde{\mathcal{J}}_{2U}(\mathbb{F}_3)$ and $\widetilde{\mathcal{J}}_{2U}(\mathbb{F}_{19})$ is sufficient, even after further reducing all sets of congruences modulo 13. This can be important for examples such as $\mathcal{C}_{2T}, \mathcal{C}_{2\mu}$ and $\mathcal{C}_{2\phi}$, where five primes are required, and where computing the intersections of the congruence sets would be time consuming without a smoothness bound. In writing the programs associated to these computations, care has been taken to quotient out redundant information iteratively as the sets of congruence conditions are intersected.

Example 6 illustrates how the genuine injection ζ can improve upon the $P \mapsto \{P, P\}$ map of Section 3. Had we applied the technique of Example 4 to the curve $\mathcal{C}_{2U}$ the congruence conditions obtained from $\widetilde{\mathcal{J}}_{2U}(\mathbb{F}_3)$ and $\widetilde{\mathcal{J}}_{2U}(\mathbb{F}_{19})$ would not have been contradictory. Indeed, the collection of congruence conditions using all primes of good reduction below 100 would still be insufficient. Of the 67 curves resolved by this method, the improvement using ζ was computationally crucial for 24 curves, in the sense that their status could be changed from *Unresolved* to *Resolved* using primes of good reduction up to 100. Even for the remaining 43 curves solved by either approach, using ζ reduced the size of the primes required for a further 13 curves.

The same argument as in Example 6 applies to any of the 38 curves $\mathcal{C}_{1a}, \ldots, \mathcal{C}_{1L}$ in Table 1, each with Jacobian of $\mathbb{Q}$-rank 1, the 28 curves $\mathcal{C}_{2T}, \ldots, \mathcal{C}_{2\phi}$ in Table 3, each with Jacobian of $\mathbb{Q}$-rank 2, and the curve $\mathcal{C}_{3m}$ in Table 4 with Jacobian of $\mathbb{Q}$-rank 3, given in the appendix. Since, as always, we have checked that all of these curves have points everywhere locally and have absolutely simple Jacobians, we now have nontrivial examples of Theorem 1.

Corollary 4. *There exist, in genus > 1, absolutely simple examples of Theorem 1 using (1) to show that $\mathcal{C}(\mathbb{Q}) = \emptyset$. Specifically, there exist curves $\mathcal{C}$ of genus 2 defined over $\mathbb{Q}$, which violate the Hasse principle, which have $\mathbb{Q}$-rational divisor classes of degree 1, and whose Jacobians $\mathcal{J}$ are absolutely simple and of $\mathbb{Q}$-rank 1, 2 and 3. If $\text{Ш}(\mathcal{J})$ is finite then $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$ and so the Brauer-Manin obstruction explains the violations of Hasse principle for these curves.*

Note that in Example 6, we have only used the flat information, by which we mean the information obtained from (1) after projecting to the residue fields $k_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$ at the finite places. Of course, useful information can also be obtained p-adically beyond that of merely the projection to the residue fields – that is to say, the deep information. Indeed, one can sometimes combine flat information from one prime and the deep information from another prime. This is done the following example at two primes, where merely the flat information would be insufficient.

Example 7. *Let $\mathcal{C}_{1b}$ and R be as in Example 1, and let $\mathcal{J}_{1b}$ be the Jacobian of $\mathcal{C}_{1b}$. Then $\mathcal{J}_{1b}(\mathbb{Q})$ has rank* 1 *and $\mathcal{C}_{1b}(\mathbb{Q}) = \emptyset$.*

Proof The Jacobian $\mathcal{J}_{1b}$ has no nontrivial torsion over $\mathbb{Q}$, and has $\mathbb{Q}$-rank 1, with $\mathcal{J}_{1b}(\mathbb{Q})$ generated by $D_1 = \{(-\frac{13}{34} + \frac{1}{34}\sqrt{101}, \frac{7207}{9826} + \frac{599}{9826}\sqrt{101}), (-\frac{13}{34} - \frac{1}{34}\sqrt{101}, \frac{7207}{9826} - \frac{599}{9826}\sqrt{101})\}$. Let R be the $\mathbb{Q}$-rational degree 1 divisor class given in (7), and as usual define the embedding $\zeta : \mathcal{C}_{1b} \longrightarrow \mathcal{J}_{1b} : P \mapsto [P] - R$. Since ζ is defined over $\mathbb{Q}$, any $P \in \mathcal{C}_{1b}(\mathbb{Q})$ must map to $\zeta(P) \in \mathcal{J}_{1b}(\mathbb{Q})$, and so $\zeta(P) = n_1 D_1$, for some $n_1 \in \mathbb{Z}$.

First, let $\widetilde{\mathcal{C}}_{1b}, \widetilde{\mathcal{J}}_{1b}, \widetilde{D}_1, \widetilde{R}, \tilde{\zeta}$ be the reductions of $\mathcal{C}_{1b}, \mathcal{J}_{1b}, D_1, R, \zeta$ modulo 3, in particular, the divisor class $\widetilde{R} = [(1,0) + (1+i,0) - (1-i,0)]$. Then $\widetilde{\mathcal{C}}_{1b}(\mathbb{F}_3)$ contains only the point: $(1,0)$; any $P \in \mathcal{C}_{1b}(\mathbb{Q})$ must have $\widetilde{P} = (1,0)$, and so the only possibility for $\widetilde{\zeta(P)} = \tilde{\zeta}(\widetilde{P}) = [\widetilde{P}] - \widetilde{R}$ is $\tilde{\zeta}((1,0)) = \{(1+i,0),(1-i,0)\}$. In summary, any $P \in \mathcal{C}_{1b}(\mathbb{Q})$ must satisfy

$$\widetilde{\zeta(P)} = \{(1+i,0),(1-i,0)\} \text{ in } \widetilde{\mathcal{J}}_{1b}(\mathbb{F}_3). \tag{33}$$

Further, the reduction of D_1 modulo 3 is $\widetilde{D}_1 = \{(-1+i,1-i),(-1-i,1+i)\}$, with multiples given by

$$\begin{aligned} 1\widetilde{D}_1 &= \{(-1+i,1-i),(-1-i,1+i)\}, & 2\widetilde{D}_1 &= \{(1+i,0),(1-i,0)\},\\ 3\widetilde{D}_1 &= \{(-1+i,-1+i),(-1-i,-1-i)\}, & 4\widetilde{D}_1 &= \text{identity}, \end{aligned}$$

so that the order of $\widetilde{D}_1$ is $N_1^{(3)} = 4$. The only overlap between the above list and (33) is $2\widetilde{D}_1$, giving

$$P \in \mathcal{C}_{1b}(\mathbb{Q}) \Rightarrow \zeta(P) = n_1 D_1, \text{ some } n_1 \in \mathbb{Z} \text{ with } n_1 \equiv 2 \pmod 4. \tag{34}$$

If we now perform the above process, but with reductions modulo 37, we find that the reduction of D_1 modulo 37 has order $N_1^{(37)} = 27$, and imitating the above computations gives

$$P \in \mathcal{C}_{1b}(\mathbb{Q}) \Rightarrow \zeta(P) = n_1 D_1, \text{ some } n_1 \in \mathbb{Z} \text{ with } n_1 \equiv 7 \text{ or } 20 \pmod{27}. \tag{35}$$

Unlike Example 6 we do not have a contradiction from the above flat information at our two primes $p = 3, 37$, and indeed no contradiction was ever possible since the orders of the reductions of D_1 are 4 and 27, which are coprime. However, the latter order suggests that we should now go back to the case $p = 3$, and consider the deep information there. From (34), we know that $n_1 = 2 + 4m_1$, for some $m_1 \in \mathbb{Z}$. Let $E_1 = 4D_1$. Then E_1 is in the kernel of reduction modulo 3, and so the formal group of $\mathcal{J}_{1b}$ can be used to describe $n_1 D_1 = (2+4m_1)D_1 = 2D_1 + m_1 E_1$ in terms of power series in m_1 defined over $\mathbb{Z}_3$, using the method in [15]. Computing (23) modulo 3^4 gives the following initial parts of the power series.

$$\begin{array}{l} \text{There exist } \psi_1(m_1),\ \psi_2(m_1),\ \psi_3(m_1) \in \mathbb{Z}_3[[m_1]], \text{ congruent (mod 81), respectively, to} \\ 2 + 72m_1 + 54m_1^2 + 54m_1^3,\ 58 + 27m_1 + 18m_1^2 + 54m_1^3,\ 37 + 45m_1^2, \text{ such that, for all } m_1 \in \mathbb{Z}, \\ (2+4m_1)D_1 = \{(x_1,y_1),(x_2,y_2)\} \Rightarrow (\psi_1(m_1),\ \psi_2(m_1),\ \psi_3(m_1)) = (1, x_1+x_2, x_1x_2). \end{array} \tag{36}$$

To be in $\zeta(\mathcal{C}_{1b}(\mathbb{Q}))$, we know that $(1, x_1+x_2, x_1x_2)$ satisfy (27) which, for our curve $\mathcal{C}_{1b}$ specialises to the equation $-2(x_1x_2)^2 + x_1x_2(x_1+x_2) + 3(x_1+x_2)^2 - x_1x_2 + 2(x_1+x_2) + 2 = 0$, and so our $\psi_i(m_1)$ must satisfy $-2\psi_3(m_1)^2 + \psi_2(m_1)\psi_3(m_1) + 3\psi_2(m_1)^2 - \psi_1(m_1)\psi_3(m_1) + 2\psi_1(m_1)\psi_2(m_1) + 2\psi_1(m_1)^2 = 0$. Substituting (36) into this last equation and reducing modulo 81 gives $27(1 + m_1^2 + m_1^3) \equiv 0 \pmod{81}$. In summary, the deep information at $p = 3$ tells us that

$$P \in \mathcal{C}_{1b}(\mathbb{Q}) \Rightarrow \zeta(P) = n_1 D_1, \text{ some } n_1 = 2 + 4m_1 \text{ with } m_1 \in \mathbb{Z} \text{ and } 27(1 + m_1^2 + m_1^3) \equiv 0 \pmod{81}. \tag{37}$$

Now, this last equation implies $1 + m_1^2 + m_1^3 \equiv 0 \pmod 3$, which is only satisfied when $m_1 \equiv 1 \pmod 3$, and so $n_1 = 2 + 4m_1 \equiv 0 \pmod 3$. But this contradicts (35), and so the deep information at $p = 3$ contradicts the flat information at $p = 37$. Hence $\mathcal{C}_{1b}(\mathbb{Q}) = \emptyset$, as required. □

5. Summary of results

As has been mentioned, an open question (see [27], p.133) in this context is as follows.

Question 1. *Is the Brauer-Manin obstruction the only obstruction to the Hasse principle for smooth projective curves?*

We do not intend to claim any evidence in either direction; our aim here has been methodological: to show how to implement the obstruction in practice, and to find new types of examples with absolutely simple Jacobians, proving Corollaries 2,3,4. However, it is worth making a few general observations based on these experimentations. The use of only flat information (as in Example 6) places us at the mercy of whether there are nontrivial common factors between the orders of the generators modulo different primes; the above Example 7 shows the potential benefit of combining flat and deep information, since there is a guarantee that we can construct sets of congruence conditions whose moduli have nontrivial common factors. In that example, the order of the reduction of D_1 at $p = 37$ was 27, which was guaranteed in advance to have a nontrivial common factor with the modulus of the deep information at $p = 3$. However it should also be confessed that for none of our examples did the use of deep information change the status of the curve; even curve $\mathcal{C}_{1b}$ in Example 7 can be resolved with purely flat information at the prime $p = 5$. This gives rise to an associated question.

Question 2. *Is the flat information of the Brauer-Manin obstruction the only obstruction to the Hasse principle for smooth projective curves?*

By this we mean, when there does exist a rational divisor class of degree 1, is the technique used in Example 6 always sufficient? In our computations, this was certainly the case for all rank 1 examples, and so we can claim some mild evidence for Question 2, at least for genus 2 and rank 1. For these 38 cases, there was a strong bias towards success using small primes, with 34 of the 38 curves requiring only the flat information from primes up to 20. The remaining 4 stubborn curves $\mathcal{C}_{1L}, \mathcal{C}_{1s}, \mathcal{C}_{1y}, \mathcal{C}_{1p}$ then required the information up to $23, 29, 53, 67$, respectively. The rank 2 cases also showed a similar reduced benefit per prime as the size of the primes increase. It is difficult to know to what extent our remaining unresolved examples might constitute evidence against Question 1; the mere fact that we are not able to resolve a given curve using Brauer-Manin obstruction information from primes up to some bound, tells us nothing. It is always possible that the use of a further prime beyond our bounds of computation might show that $\mathcal{C}(\mathbb{Q}) = \emptyset$. It is also possible in principle that $\mathcal{C}(\mathbb{Q}) \neq \emptyset$ for some of our unresolved curves; however, since we know generators for $\mathcal{J}(\mathbb{Q})$ in each case, we were able to run through linear combinations of generators (whose heights increase exponentially in the multiples) and check that these are not in the image of ζ. One can then check that there are no members of $\mathcal{C}(\mathbb{Q})$ up to a much larger naive height bound than a direct search on the curve. In this way, it can easily be checked that none of our unresolved curves have a $\mathbb{Q}$-rational point (x,y), with $x = a/b$, $a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$ and $|a|, |b| < 10^{30}$.

If it turns out that the Brauer-Manin obstruction does not explain all violations of the Hasse principle on curves, then it is natural to ask what other obstructions might be available which are stronger. One possibility is in the covers literature, such as [5],[6],[7], where techniques to try to find all of $\mathcal{C}(\mathbb{Q})$ are described, which involve towers of 2-covers, some abelian and some nonabelian. If, on further more comprehensive experimentations, there seem to arise likely negative examples to Question 1, then the techniques in [5],[6],[7] (also applied in [17],[18],[19]) provide an alternative route for resolving such curves; in such cases, the hard part of the problem would then be to prove that the Brauer-Manin obstruction fails. This contrasts with the literature on diagonal surfaces (such as [4],[32]), where the computation of at least the arithmetic part of the Brauer-Manin obstruction is a finite problem.

Appendix: Tables of curves

The following tables give the current status of our 145 curves of genus 2. For each curve, it was checked directly that there exists a point over $\mathbb{R}$ and $\mathbb{Q}_p$, for every prime $p < 13$ and every prime of bad reduction. For any prime $p \geq 13$ of good reduction, the Hasse-Weil bound $|\#\widetilde{\mathcal{C}}(\mathbb{F}_p) - (p+1)| \leq 2g\sqrt{p}$, where $g = 2$ is the genus [33], shows that there is automatically at least one point over the finite field $\mathbb{F}_p$, which by Hensel's Lemma must lift to a point on $\mathcal{C}$ over $\mathbb{Q}_p$. Therefore, all of the following curves have been checked to have points everywhere locally. Furthermore, all of the curves have been checked not to have any $\mathbb{Q}$-rational point (x,y), with $x = a/b$, $a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$ and $|a|, |b| < 10^{30}$.

The Jacobian of the curve $\mathcal{C}_{2T}$ in Table 3 is not absolutely simple, since there is a map

$$(X,Y) \mapsto (-((X+i)/(X-i))^2, 8Y/(X-i)^3)$$

from $\mathcal{C}_{2T}$ to the elliptic curve $Y^2 = (4-3i)X^3 + (60-23i)X^2 + (60+23i)X + (4+3i)$. The Jacobian of $\mathcal{C}_{2T}$ is isogenous to the Weil restriction of scalars from $\mathbb{Q}(i)$ to $\mathbb{Q}$ of this elliptic curve. For the other curves, the technique in [28] tells us that the Jacobian is absolutely simple if any prime p of good reduction can be found such that $a_p^2 - 4(b_p - 2p)$ is not a square in $\mathbb{Q}$ and $X^4 - \frac{b_p-2p}{p}X^3 + \frac{a_p^2-2b_p+2p}{p}X^2 - \frac{b_p-2p}{p}X + 1 \neq 0$ for all X equal to an nth root of unity, for $n \in \{1,2,3,4,5,6,8,10,12\}$. Here, a_p and b_p represent the standard quantities $a_p = p + 1 - \#\widetilde{\mathcal{C}}(\mathbb{F}_p)$ and $b_p = \frac{1}{2}\#\widetilde{\mathcal{C}}(\mathbb{F}_{p^2}) + \frac{1}{2}(\#\widetilde{\mathcal{C}}(\mathbb{F}_p))^2 - (p+1)\#\widetilde{\mathcal{C}}(\mathbb{F}_p) + p$. We found that, for all curves except $\mathcal{C}_{2T}$, this condition was satisfied for at least one of $p = 3,5,7,11,13,17,19$. Therefore, all curves except $\mathcal{C}_{2T}$ have been proved to have Jacobians which are absolutely simple, that is to say, which are geometrically non-isogenous to the product of elliptic curves.

The tables are sorted in order of increasing rank of $\mathcal{J}(\mathbb{Q})$. In each row, the left hand entry gives the name of the curve; this is followed by the equation of the curve, the rank of $\mathcal{J}(\mathbb{Q})$ and the status of the curve. When the status is listed as *Unresolved* we do not know whether there exists a member of $\mathcal{C}(\mathbb{Q})$. The status $\#\mathcal{J}(\mathbb{Q}) = 1 \Rightarrow \mathcal{C}(\mathbb{Q}) = \emptyset$ means that the rank of $\mathcal{J}(\mathbb{Q})$ is 0 and there is no nontrivial torsion; it can then be shown that $\mathcal{C}(\mathbb{Q}) = \emptyset$, using the same argument given for $\mathcal{C}_{0j}$ in Example 1. The status *No Deg-1-Div-Class*/$\mathbb{Q} \Rightarrow \mathcal{C}(\mathbb{Q}) = \emptyset$, means that $\mathcal{C}(\mathbb{Q})$ has been proved to be empty by showing the nonexistence of a $\mathbb{Q}$-rational divisor class of degree 1, in the style of Example 2. When the status is listed in the form $\mathrm{Fl}(p_1, \ldots, p_k), \mathrm{B}(N) \Rightarrow \mathcal{C}(\mathbb{Q}) = \emptyset$, this means that there does exist a $\mathbb{Q}$-rational divisor class R of degree 1, and that the flat information from $\zeta : P \mapsto [P] - R$ at $p_1, \ldots, p_k$ proves that $\mathcal{C}(\mathbb{Q}) = \emptyset$, in the style of Example 6. The entry $\mathrm{B}(N)$ gives a smoothness bound which eases the computations; it indicates that the combined flat congruence information is sufficient even after reducing all sets of congruences modulo N. Of course, the choice of R is not unique; however, any two $\mathbb{Q}$-rational divisors classes R, R' of degree 1 satisfy $R - R' \in \mathcal{J}(\mathbb{Q})$. Replacing R by R' in the definition of ζ merely translates the computations by a fixed member of $\mathcal{J}(\mathbb{Q})$ and does not affect whether the resulting congruences are contradictory. Therefore, the choice of R does not affect the result of the computation.

More details of the computations have been placed in files available at

www.maths.ox.ac.uk/~flynn/genus2/manin/

These include more information about each curve, such as sets of generators for each $\mathcal{J}(\mathbb{Q})$, and a range of programs written in *magma* [20], which perform computations such as those in Example 6. Some attempts at efficiency have been made in these programs, since a purely naive combining of the sets of congruence information would rapidly explode. In particular, out of our entire set S of congruences, we iteratively focus on the current highest prime power p^r which occurs as a factor of more than one modulus, and combine the associated subset T of congruences (whose moduli are divisible by p^r) into a single congruence modulo m, say; once this has been completed, it is safe to reduce this congruence modulo m/p, since no other modulus will now be divisible by p^r. We then adjust S by replacing all of T by this single congruence. The new version of S will not have congruences with moduli divisible by p^r and so we can repeat the process, but concentrating on the new (and smaller) largest prime power dividing more than one modulus.

There are also independent subroutines available at the above site, which perform the prerequisite processes – for example, computing a $\mathbb{Q}$-rational divisor class R of degree 1, when given $D \in \ker\mu$ which is not in $2\mathcal{J}(\mathbb{Q})$, as in Example 3, and computing the corresponding map ζ, as in (29). Examples are given in the files where the programs are used to show that $\mathcal{C}(\mathbb{Q}) = \emptyset$ by computing the Brauer-Manin information. By imitating these, it should be straightforward for readers to use these programs to compute their own examples. The programs make regular use of routines (such as CosetIntersection) by Nils Bruin, which will appear in Magma 2.11, and are included in the routine library [8].

$\mathcal{C}$	Equation	Rk	Status
$\mathcal{C}_{0a}$	$Y^2 = -(X^3+X^2+1)(2X^3+X-2)$	0	$\#\mathcal{J}_{0a}(\mathbb{Q})=1 \Rightarrow \mathcal{C}_{0a}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{0b}$	$Y^2 = -(X^3+X^2+1)(2X^3-X-2)$	0	$\#\mathcal{J}_{0b}(\mathbb{Q})=1 \Rightarrow \mathcal{C}_{0b}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{0c}$	$Y^2 = -(X^3+X^2+1)(X^3+X^2+X-2)$	0	$\#\mathcal{J}_{0c}(\mathbb{Q})=1 \Rightarrow \mathcal{C}_{0c}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{0d}$	$Y^2 = -(X^3-X-1)(X^3+2X^2+2)$	0	$\#\mathcal{J}_{0d}(\mathbb{Q})=1 \Rightarrow \mathcal{C}_{0d}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{0e}$	$Y^2 = -(X^3+X^2-1)(X^3-X+2)$	0	$\#\mathcal{J}_{0e}(\mathbb{Q})=1 \Rightarrow \mathcal{C}_{0e}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{0f}$	$Y^2 = -(X^3+X^2+1)(X^3-X-2)$	0	$\#\mathcal{J}_{0f}(\mathbb{Q})=1 \Rightarrow \mathcal{C}_{0f}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{0g}$	$Y^2 = (X^3-2X-2)(2X^3-2X^2+2X-1)$	0	$\#\mathcal{J}_{0g}(\mathbb{Q})=1 \Rightarrow \mathcal{C}_{0g}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{0h}$	$Y^2 = (X^3-X^2-1)(2X^3-X+2)$	0	$\#\mathcal{J}_{0h}(\mathbb{Q})=1 \Rightarrow \mathcal{C}_{0h}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{0i}$	$Y^2 = (X^3-X^2-1)(2X^3+X^2-X+1)$	0	$\#\mathcal{J}_{0i}(\mathbb{Q})=1 \Rightarrow \mathcal{C}_{0i}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{0j}$	$Y^2 = (X^3+X+1)(2X^3-1)$	0	$\#\mathcal{J}_{0j}(\mathbb{Q})=1 \Rightarrow \mathcal{C}_{0j}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1a}$	$Y^2 = -(X^2+X-1)(X^4+X^3+X^2+X+2)$	1	$\mathrm{Fl}(3), \mathrm{B}(2) \Rightarrow \mathcal{C}_{1a}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1b}$	$Y^2 = -(X^3+X+1)(X^3+2X^2-2)$	1	$\mathrm{Fl}(5), \mathrm{B}(3) \Rightarrow \mathcal{C}_{1b}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1c}$	$Y^2 = -X^6-X^5-2X^4-2X^3-X^2+2X+2$	1	$\mathrm{Fl}(7,13), \mathrm{B}(77) \Rightarrow \mathcal{C}_{1c}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1d}$	$Y^2 = -X^6-X^5-2X^4-2X^3+X^2-2X+2$	1	$\mathrm{Fl}(3,11), \mathrm{B}(7) \Rightarrow \mathcal{C}_{1d}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1e}$	$Y^2 = -(X^3+X^2+2)(X^3+X-1)$	1	$\mathrm{Fl}(5,7,19), \mathrm{B}(30) \Rightarrow \mathcal{C}_{1e}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1f}$	$Y^2 = -X^6-X^5-X^4+X^2-X+2$	1	$\mathrm{Fl}(11), \mathrm{B}(20) \Rightarrow \mathcal{C}_{1f}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1g}$	$Y^2 = -X^6-X^5-X^3-X^2-X+2$	1	$\mathrm{Fl}(3), \mathrm{B}(2) \Rightarrow \mathcal{C}_{1g}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1h}$	$Y^2 = -X^6-X^5+X^4+X^3+2X^2-X+2$	1	$\mathrm{Fl}(19), \mathrm{B}(11) \Rightarrow \mathcal{C}_{1h}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1i}$	$Y^2 = -X^6-X^4-2X^3-2X^2+X+2$	1	$\mathrm{Fl}(19), \mathrm{B}(11) \Rightarrow \mathcal{C}_{1i}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1j}$	$Y^2 = -(X^3+X-1)(X^3+2)$	1	$\mathrm{Fl}(5,13), \mathrm{B}(3) \Rightarrow \mathcal{C}_{1j}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1k}$	$Y^2 = 2X^6-2X^5-2X^4+X^3+X^2-X-1$	1	$\mathrm{Fl}(5,7), \mathrm{B}(19) \Rightarrow \mathcal{C}_{1k}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1l}$	$Y^2 = (2X^3-2X^2+1)(X^3-X-1)$	1	$\mathrm{Fl}(3,5), \mathrm{B}(4) \Rightarrow \mathcal{C}_{1l}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1m}$	$Y^2 = 2X^6-2X^5-2X^4+X^3+2X^2+2$	1	$\mathrm{Fl}(11,13), \mathrm{B}(3) \Rightarrow \mathcal{C}_{1m}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1n}$	$Y^2 = (X^3-X^2+1)(2X^3-X-2)$	1	$\mathrm{Fl}(3,5), \mathrm{B}(4) \Rightarrow \mathcal{C}_{1n}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1o}$	$Y^2 = 2X^6-2X^5-2X^3+2X^2-2X-2$	1	$\mathrm{Fl}(19), \mathrm{B}(5) \Rightarrow \mathcal{C}_{1o}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1p}$	$Y^2 = 2X^6-2X^5+X^4-2X^3-2X^2-2X-2$	1	$\mathrm{Fl}(67), \mathrm{B}(250) \Rightarrow \mathcal{C}_{1p}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1q}$	$Y^2 = (X^3-X^2-1)(2X^3+X+2)$	1	$\mathrm{Fl}(3,13), \mathrm{B}(8) \Rightarrow \mathcal{C}_{1q}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1r}$	$Y^2 = 2X^6-2X^5+2X^4-2X^3-X^2-X-1$	1	$\mathrm{Fl}(5,11), \mathrm{B}(11) \Rightarrow \mathcal{C}_{1r}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1s}$	$Y^2 = 2X^6-X^5-2X^4-2X^3+2X^2-X-1$	1	$\mathrm{Fl}(29), \mathrm{B}(28) \Rightarrow \mathcal{C}_{1s}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1t}$	$Y^2 = (X^2+X+1)(2X^4-2X^3-X^2+2X-2)$	1	$\mathrm{Fl}(11), \mathrm{B}(10) \Rightarrow \mathcal{C}_{1t}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1u}$	$Y^2 = 2X^6-X^4-X^3+X^2-X-1$	1	$\mathrm{Fl}(13), \mathrm{B}(12) \Rightarrow \mathcal{C}_{1u}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1v}$	$Y^2 = 2X^6+X^4-X^3-2X^2-2X-1$	1	$\mathrm{Fl}(3,5), \mathrm{B}(3) \Rightarrow \mathcal{C}_{1v}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1w}$	$Y^2 = 2X^6-2X^5+2X-3$	1	$\mathrm{Fl}(7), \mathrm{B}(17) \Rightarrow \mathcal{C}_{1w}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1x}$	$Y^2 = 2X^6-X^5-X^2+2X-3$	1	$\mathrm{Fl}(3), \mathrm{B}(1) \Rightarrow \mathcal{C}_{1x}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1y}$	$Y^2 = 2X^6-X^5+2X^4-2X^3-X^2-2X-3$	1	$\mathrm{Fl}(17,53), \mathrm{B}(87) \Rightarrow \mathcal{C}_{1y}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1z}$	$Y^2 = 2X^6-X^4-2X^3-2X^2+2X-3$	1	$\mathrm{Fl}(5), \mathrm{B}(3) \Rightarrow \mathcal{C}_{1z}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1A}$	$Y^2 = 2X^6-2X^3+2X^2-2X-3$	1	$\mathrm{Fl}(3), \mathrm{B}(4) \Rightarrow \mathcal{C}_{1A}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1B}$	$Y^2 = -(X^3+X+1)(2X^3-3X^2-3)$	1	$\mathrm{Fl}(5), \mathrm{B}(3) \Rightarrow \mathcal{C}_{1B}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1C}$	$Y^2 = -(2X^3-2X^2+X-2)(X^3-X^2+X+1)$	1	$\mathrm{Fl}(5), \mathrm{B}(9) \Rightarrow \mathcal{C}_{1C}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1D}$	$Y^2 = -X^6-2X^5-5X^4-4X^3+X^2+5$	1	$\mathrm{Fl}(3,13,17), \mathrm{B}(21) \Rightarrow \mathcal{C}_{1D}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1E}$	$Y^2 = -(X^3+X^2+2X+1)(X^3-X^2+X-3)$	1	$\mathrm{Fl}(7), \mathrm{B}(14) \Rightarrow \mathcal{C}_{1E}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1F}$	$Y^2 = -(X^3-X^2-1)(X^3+X^2+X+3)$	1	$\mathrm{Fl}(7,19), \mathrm{B}(3) \Rightarrow \mathcal{C}_{1F}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1G}$	$Y^2 = -(X^3-2X^2-X-2)(X^3+X+1)$	1	$\mathrm{Fl}(5), \mathrm{B}(15) \Rightarrow \mathcal{C}_{1G}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1H}$	$Y^2 = (X^3-X^2+X+1)(2X^3+2X^2+3X+2)$	1	$\mathrm{Fl}(5), \mathrm{B}(3) \Rightarrow \mathcal{C}_{1H}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1I}$	$Y^2 = (X^3+X^2+X+3)(2X^3-2X^2+3X-2)$	1	$\mathrm{Fl}(5), \mathrm{B}(7) \Rightarrow \mathcal{C}_{1I}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1J}$	$Y^2 = (2X^3+2X-1)(X^3+X^2-X+1)$	1	$\mathrm{Fl}(3,19), \mathrm{B}(2) \Rightarrow \mathcal{C}_{1J}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1K}$	$Y^2 = (X^3+X-1)(2X^3+3X^2+3)$	1	$\mathrm{Fl}(5), \mathrm{B}(7) \Rightarrow \mathcal{C}_{1K}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1L}$	$Y^2 = -(X^3+3)(X^3+X^2-5)$	1	$\mathrm{Fl}(7,11,23), \mathrm{B}(18) \Rightarrow \mathcal{C}_{1L}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1M}$	$Y^2 = -2(X^2+X+1)(X^2+15)(X^2-13)$	1	No Deg-1-Div-Class/$\mathbb{Q}$ $\Rightarrow \mathcal{C}_{1M}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1N}$	$Y^2 = -2(X^2+X+1)(X^2-21)(X^2+23)$	1	No Deg-1-Div-Class/$\mathbb{Q}$ $\Rightarrow \mathcal{C}_{1N}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1O}$	$Y^2 = -2(X^2+X+1)(X^2+40)(X^2-38)$	1	No Deg-1-Div-Class/$\mathbb{Q}$ $\Rightarrow \mathcal{C}_{1O}(\mathbb{Q})=\emptyset$
$\mathcal{C}_{1P}$	$Y^2 = -2(X^2+X+1)(X^2-54)(X^2+56)$	1	No Deg-1-Div-Class/$\mathbb{Q}$ $\Rightarrow \mathcal{C}_{1P}(\mathbb{Q})=\emptyset$

Table 1. All Rank 0 and 1 Examples

$\mathcal{C}$	Equation	Rk	Status
$\mathcal{C}_{2a}$	$Y^2 = -(2X^3+X+2)(X^3+X^2-1)$	2	Unresolved
$\mathcal{C}_{2b}$	$Y^2 = -2X^6-2X^5+X^4-2X^3-X^2+X+2$	2	Unresolved
$\mathcal{C}_{2c}$	$Y^2 = -2X^6-2X^5+X^4-X^3-X^2+X+2$	2	Unresolved
$\mathcal{C}_{2d}$	$Y^2 = -2X^6-2X^5+2X^4-X^3-2X+2$	2	Unresolved
$\mathcal{C}_{2e}$	$Y^2 = -2X^6-X^5-2X^4-2X^3-X+2$	2	Unresolved
$\mathcal{C}_{2f}$	$Y^2 = -2X^6-X^5-X^4+2X^3+X^2+2X+2$	2	Unresolved
$\mathcal{C}_{2g}$	$Y^2 = -X^6-2X^5-2X^4-X^3+X^2-2X+2$	2	Unresolved
$\mathcal{C}_{2h}$	$Y^2 = -X^6-2X^5-X^4-X^3+2$	2	Unresolved
$\mathcal{C}_{2i}$	$Y^2 = -X^6-2X^5-X^4-X^3+X^2-2X+2$	2	Unresolved
$\mathcal{C}_{2j}$	$Y^2 = -X^6-2X^5-2X^3-X+2$	2	Unresolved
$\mathcal{C}_{2k}$	$Y^2 = -X^6-2X^5-X^3-X^2+2$	2	Unresolved
$\mathcal{C}_{2l}$	$Y^2 = -X^6-2X^5+X^4-X^3+X^2-X+2$	2	Unresolved
$\mathcal{C}_{2m}$	$Y^2 = -X^6-2X^5-2X^4-X^3-X+2$	2	Unresolved
$\mathcal{C}_{2n}$	$Y^2 = -X^6-X^5+2X^4-2X^3-X+2$	2	Unresolved
$\mathcal{C}_{2o}$	$Y^2 = -X^6-X^5+2X^4-2X^2-X+2$	2	Unresolved
$\mathcal{C}_{2p}$	$Y^2 = -X^6+2X^4-X^3+X+2$	2	Unresolved
$\mathcal{C}_{2q}$	$Y^2 = 2X^6-2X^5+X^3-X-1$	2	Unresolved
$\mathcal{C}_{2r}$	$Y^2 = 2X^6-2X^5+2X^4-2X^2+X+2$	2	Unresolved
$\mathcal{C}_{2s}$	$Y^2 = 2X^6-X^5-2X^4+2X^3-2X-2$	2	Unresolved
$\mathcal{C}_{2t}$	$Y^2 = 2X^6-2X^4-X^3+X^2-X-1$	2	Unresolved
$\mathcal{C}_{2u}$	$Y^2 = 2X^6-X^3+2X^2+2$	2	Unresolved
$\mathcal{C}_{2v}$	$Y^2 = 2X^6-X^3+2X^2+X-1$	2	Unresolved
$\mathcal{C}_{2w}$	$Y^2 = -2X^6-2X^5-4X^4+4X^3+3X^2+8X+5$	2	Unresolved
$\mathcal{C}_{2x}$	$Y^2 = -2X^6-X^5-5X^4-X^2+3X+2$	2	Unresolved
$\mathcal{C}_{2y}$	$Y^2 = -2X^6-3X^4+4X^2+2X+5$	2	Unresolved
$\mathcal{C}_{2z}$	$Y^2 = -2X^6-3X^4+4X^3+4X^2+6X+5$	2	Unresolved
$\mathcal{C}_{2A}$	$Y^2 = -(X^3-X^2+X-3)(2X^3+2X^2+3X+2)$	2	Unresolved
$\mathcal{C}_{2B}$	$Y^2 = -2X^6+2X^5-4X^4+4X^3+3X^2+4X+5$	2	Unresolved
$\mathcal{C}_{2C}$	$Y^2 = -2X^6+4X^5-3X^4-4X^3+4X^2-6X+5$	2	Unresolved
$\mathcal{C}_{2D}$	$Y^2 = -X^6-2X^5-3X^4-5X^3-X+2$	2	Unresolved
$\mathcal{C}_{2E}$	$Y^2 = -X^6+3X^3+3X^2+5X+2$	2	Unresolved
$\mathcal{C}_{2F}$	$Y^2 = 2X^6-4X^5+X^4+5X^3+5X^2+11X+6$	2	Unresolved
$\mathcal{C}_{2G}$	$Y^2 = 2X^6-2X^5-3X^4-2X^3+3X^2+2X+8$	2	Unresolved
$\mathcal{C}_{2H}$	$Y^2 = 2X^6-2X^5+3X^4-X^3-5X^2+3X-6$	2	Unresolved
$\mathcal{C}_{2I}$	$Y^2 = 2X^6-4X^4+2X^2+2X+8$	2	Unresolved
$\mathcal{C}_{2J}$	$Y^2 = 2X^6+5X^4+3X^3+X^2+5X-2$	2	Unresolved
$\mathcal{C}_{2K}$	$Y^2 = 2X^6+5X^4+4X^3+6X-3$	2	Unresolved
$\mathcal{C}_{2L}$	$Y^2 = 2X^6+4X^5-4X^4+2X^2-2X+8$	2	Unresolved
$\mathcal{C}_{2M}$	$Y^2 = 2X^6+4X^5-3X^4-X^3+X^2-3X+6$	2	Unresolved
$\mathcal{C}_{2N}$	$Y^2 = 2X^6+4X^5+X^3-3X^2-X-1$	2	Unresolved
$\mathcal{C}_{2O}$	$Y^2 = 2X^6+4X^5+X^4+4X^3-3X^2+2X-2$	2	Unresolved
$\mathcal{C}_{2P}$	$Y^2 = (2X^3+2X^2+X+2)(X^3+X^2+X-1)$	2	Unresolved
$\mathcal{C}_{2Q}$	$Y^2 = -X^6-2X^5-2X^4-X^3+X^2+10X+15$	2	Unresolved
$\mathcal{C}_{2R}$	$Y^2 = -X^6-X^5-5X^4-2X^3+4X^2+8X+21$	2	Unresolved
$\mathcal{C}_{2S}$	$Y^2 = -X^6+3X^5+3X^4-4X^3-4X^2-4X+5$	2	Unresolved

Table 2. Unresolved Rank 2 Examples

$\mathcal{C}$	Equation	Rk	Status
$\mathcal{C}_{2T}$	$Y^2 = -2X^6 - 2X^5 - X^3 - 2X + 2$	2	$\mathrm{Fl}(3,13,17,37,41), \mathrm{B}(90) \Rightarrow \mathcal{C}_{2T}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2U}$	$Y^2 = -2X^6 - 2X^5 + 2X^4 + X^3 - 2X^2 - X + 2$	2	$\mathrm{Fl}(3,19), \mathrm{B}(13) \Rightarrow \mathcal{C}_{2U}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2V}$	$Y^2 = -2X^6 - X^5 - 2X^4 - 2X^3 - X^2 + 2X + 2$	2	$\mathrm{Fl}(5), \mathrm{B}(9) \Rightarrow \mathcal{C}_{2V}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2W}$	$Y^2 = -X^6 - 2X^5 + X^4 + 2X^3 + 2X^2 + X + 2$	2	$\mathrm{Fl}(79), \mathrm{B}(80) \Rightarrow \mathcal{C}_{2W}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2X}$	$Y^2 = -(X^2 + 1)(X^4 + 2X^3 + X^2 - X - 2)$	2	$\mathrm{Fl}(3), \mathrm{B}(20) \Rightarrow \mathcal{C}_{2X}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2Y}$	$Y^2 = -X^6 - 2X^5 - 2X^4 + X^3 + 2X^2 - X + 2$	2	$\mathrm{Fl}(3,19,43), \mathrm{B}(30) \Rightarrow \mathcal{C}_{2Y}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2Z}$	$Y^2 = -X^6 - X^5 - 2X^4 - 2X^3 + 2X^2 - X + 2$	2	$\mathrm{Fl}(7), \mathrm{B}(11) \Rightarrow \mathcal{C}_{2Z}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\alpha}$	$Y^2 = -X^6 + 2X^5 - X^3 + X + 2$	2	$\mathrm{Fl}(7), \mathrm{B}(8) \Rightarrow \mathcal{C}_{2\alpha}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\beta}$	$Y^2 = 2X^6 - 2X^5 - X^4 - X^3 - X + 2$	2	$\mathrm{Fl}(5), \mathrm{B}(9) \Rightarrow \mathcal{C}_{2\beta}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\gamma}$	$Y^2 = 2X^6 - 2X^5 - X^3 + X^2 - X - 1$	2	$\mathrm{Fl}(11), \mathrm{B}(17) \Rightarrow \mathcal{C}_{2\gamma}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\delta}$	$Y^2 = 2X^6 - 2X^5 + X^4 - X^3 - X^2 + X - 1$	2	$\mathrm{Fl}(3,5,7,19), \mathrm{B}(15) \Rightarrow \mathcal{C}_{2\delta}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\epsilon}$	$Y^2 = 2X^6 - 2X^5 + 2X^4 - X^3 - X - 1$	2	$\mathrm{Fl}(3), \mathrm{B}(3) \Rightarrow \mathcal{C}_{2\epsilon}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\zeta}$	$Y^2 = 2X^6 - 2X^4 - X^3 + X^2 + X - 2$	2	$\mathrm{Fl}(3), \mathrm{B}(2) \Rightarrow \mathcal{C}_{2\zeta}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\eta}$	$Y^2 = 2X^6 - 2X^3 + 2X^2 + X + 2$	2	$\mathrm{Fl}(5), \mathrm{B}(8) \Rightarrow \mathcal{C}_{2\eta}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\theta}$	$Y^2 = 2X^6 - X^3 - X^2 - X - 1$	2	$\mathrm{Fl}(3), \mathrm{B}(4) \Rightarrow \mathcal{C}_{2\theta}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\iota}$	$Y^2 = -2X^6 + 2X^5 - 2X^4 - 3X^3 + 3X^2 - 3X + 3$	2	$\mathrm{Fl}(29), \mathrm{B}(149) \Rightarrow \mathcal{C}_{2\iota}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\kappa}$	$Y^2 = -X^6 - 2X^5 - 4X^4 + 5X^2 + 4X + 8$	2	$\mathrm{Fl}(7), \mathrm{B}(11) \Rightarrow \mathcal{C}_{2\kappa}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\lambda}$	$Y^2 = -(X^3 - X^2 + X - 2)(X^3 + X^2 + 3X + 1)$	2	$\mathrm{Fl}(3,11,13,37), \mathrm{B}(380) \Rightarrow \mathcal{C}_{2\lambda}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\mu}$	$Y^2 = -(X^3 - X^2 - X - 1)(X^3 + X^2 + X + 2)$	2	$\mathrm{Fl}(7,19,23,53,67), \mathrm{B}(308) \Rightarrow \mathcal{C}_{2\mu}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\nu}$	$Y^2 = -X^6 + 2X^5 - 4X^4 + 4X^3 + 4X + 3$	2	$\mathrm{Fl}(13), \mathrm{B}(16) \Rightarrow \mathcal{C}_{2\nu}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\xi}$	$Y^2 = 2X^6 - 4X^5 - 3X^4 + 6X + 5$	2	$\mathrm{Fl}(53), \mathrm{B}(40) \Rightarrow \mathcal{C}_{2\xi}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\pi}$	$Y^2 = 2X^6 - 4X^5 + X^4 - 4X^3 + 5X^2 + 2X + 6$	2	$\mathrm{Fl}(11), \mathrm{B}(29) \Rightarrow \mathcal{C}_{2\pi}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\rho}$	$Y^2 = 2X^6 - X^5 + 2X^4 + 4X^3 - 3X^2 + 7X - 3$	2	$\mathrm{Fl}(5), \mathrm{B}(3) \Rightarrow \mathcal{C}_{2\rho}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\sigma}$	$Y^2 = 2X^6 + 2X^5 + 2X^4 - 5X^3 + 3X^2 - 5X + 3$	2	$\mathrm{Fl}(11,31,59), \mathrm{B}(6) \Rightarrow \mathcal{C}_{2\sigma}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\varsigma}$	$Y^2 = -X^6 - 3X^5 - 4X^4 + 2X^3 - X^2 + 8X + 27$	2	$\mathrm{Fl}(3,13,41), \mathrm{B}(18) \Rightarrow \mathcal{C}_{2\varsigma}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\tau}$	$Y^2 = -X^6 - 4X^4 - 2X^3 + 5X^2 + 4X + 15$	2	$\mathrm{Fl}(3,19,23), \mathrm{B}(70) \Rightarrow \mathcal{C}_{2\tau}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\upsilon}$	$Y^2 = -X^6 - 3X^4 - 4X^3 + X^2 + 8X + 19$	2	$\mathrm{Fl}(11,13), \mathrm{B}(7) \Rightarrow \mathcal{C}_{2\upsilon}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\phi}$	$Y^2 = -X^6 - 2X^4 - X^3 + 5X^2 + 2X + 7$	2	$\mathrm{Fl}(3,29,43,47,59), \mathrm{B}(396) \Rightarrow \mathcal{C}_{2\phi}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\varphi}$	$Y^2 = -2(X^2 + X + 1)(X^2 - 20)(X^2 + 22)$	2	No Deg-1-Div-Class/$\mathbb{Q} \Rightarrow \mathcal{C}_{2\varphi}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\chi}$	$Y^2 = -(7X^2 + 34)(2X^2 + 4X + 5)(X^2 - 26)$	2	No Deg-1-Div-Class/$\mathbb{Q} \Rightarrow \mathcal{C}_{2\chi}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\psi}$	$Y^2 = -3(4X^2 - 29)(2X^2 + 4X + 5)(X^2 + 12)$	2	No Deg-1-Div-Class/$\mathbb{Q} \Rightarrow \mathcal{C}_{2\psi}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{2\omega}$	$Y^2 = (2X^2 + 4X + 5)(11X^2 + 20)(4X^2 + 13)$	2	No Deg-1-Div-Class/$\mathbb{Q} \Rightarrow \mathcal{C}_{2\omega}(\mathbb{Q}) = \emptyset$

Table 3. Resolved Rank 2 Examples

$\mathcal{C}$	Equation	Rk	Status
$\mathcal{C}_{3a}$	$Y^2 = -2X^6 - 2X^5 - X^4 - X^3 - X + 2$	3	Unresolved
$\mathcal{C}_{3b}$	$Y^2 = -2X^6 - 2X^5 - X^3 + 2X^2 - 2X + 2$	3	Unresolved
$\mathcal{C}_{3c}$	$Y^2 = -2X^6 - X^4 - X^3 - 2X^2 - X + 2$	3	Unresolved
$\mathcal{C}_{3d}$	$Y^2 = -X^6 - 2X^4 - X^3 - 2X^2 + 2$	3	Unresolved
$\mathcal{C}_{3e}$	$Y^2 = -X^6 - X^3 - X^2 - X + 2$	3	Unresolved
$\mathcal{C}_{3f}$	$Y^2 = 2X^6 - 2X^5 - 2X^4 - 2X^3 - 2X^2 - X + 2$	3	Unresolved
$\mathcal{C}_{3g}$	$Y^2 = 2X^6 + 2X^5 + 2X^4 + X^3 - 2X^2 - X + 2$	3	Unresolved
$\mathcal{C}_{3h}$	$Y^2 = 2X^6 - 2X^5 - 2X^4 + 2X^3 - 2X^2 + X - 3$	3	Unresolved
$\mathcal{C}_{3i}$	$Y^2 = 2X^6 - X^5 - 2X^4 + 2X^3 - 2X^2 - 3$	3	Unresolved
$\mathcal{C}_{3j}$	$Y^2 = 2X^6 - X^5 + 2X^3 - 2X^2 - 3$	3	Unresolved
$\mathcal{C}_{3k}$	$Y^2 = 2X^6 - X^5 + 2X^4 - 2X^3 - 2X - 3$	3	Unresolved
$\mathcal{C}_{3l}$	$Y^2 = 2X^6 - X^5 + 2X^4 + 2X^3 - X^2 + 2X - 3$	3	Unresolved
$\mathcal{C}_{3m}$	$Y^2 = 2X^6 - X^4 - X^3 - X^2 - X - 3$	3	$\mathrm{Fl}(3), \mathrm{B}(10) \Rightarrow \mathcal{C}_{3m}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{3n}$	$Y^2 = -2(2X^2 + 4X + 5)(X^2 - 17)(2X^2 + 11)$	3	No Deg-1-Div-Class/$\mathbb{Q} \Rightarrow \mathcal{C}_{3m}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{3o}$	$Y^2 = (2X^2 + 4X + 5)(7X^2 + 16)(2X^2 + 11)$	3	No Deg-1-Div-Class/$\mathbb{Q} \Rightarrow \mathcal{C}_{3o}(\mathbb{Q}) = \emptyset$
$\mathcal{C}_{3p}$	$Y^2 = -3(2X^2 - 19)(2X^2 + 4X + 5)(X^2 + 8)$	3	No Deg-1-Div-Class/$\mathbb{Q} \Rightarrow \mathcal{C}_{3n}(\mathbb{Q}) = \emptyset$

Table 4. All Rank 3 Examples

References

[1] J.-B. Bost and J.-F. Mestre. Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. *Gaz. Math. Soc. France* **38** (1988), 36–64.

[2] A. Bremner. Some interesting curves of genus 2 to 7. *J. Number Theory*, **67** (1997), 277–290.

[3] A. Bremner, D.J. Lewis and P. Morton, Some varieties with points only in a field extension. *Arch. Math.*, **43** (1984), 344–350.

[4] M.J. Bright and H.P.F. Swinnerton-Dyer. Computing the Brauer-Manin obstructions. *Math. Proc. Cam. Phil. Soc.*, **137** (2004), 1–16.

[5] N. Bruin. Chabauty methods using covers on curves of genus 2. http://www.math.leidenuniv.nl/reports/1999-15.shtml

[6] N. Bruin. KASH-based program for performing 2-descent on elliptic curves over number fields. Available from: http://www.math.uu.nl/people/bruin/ell.shar

[7] N. Bruin and E.V. Flynn. Towers of 2-covers of hyperelliptic curves. To appear in *Trans. Amer. Math. Soc.*

[8] N. Bruin. Routines to accompany the article *The primitive solutions to the equation* $x^3 + y^9 = z^2$. Available from: http://www.cecm.sfu.ca/ nbruin/eq239/routines.m

[9] J.W.S. Cassels. The arithmetic of certain quartic curves. *Proc. Royal Soc. Edinburgh*, **100A** (1985), 201–218.

[10] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* LMS–LNS **230**. Cambridge University Press, Cambridge, 1996.

[11] C. Chabauty. Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. *C. R. Acad. Sci. Paris*, **212** (1941), 1022–1024.

[12] R.F. Coleman. Effective Chabauty, *Duke Math. J.*, **52** (1985), 765–780.

[13] D. Coray and C. Manoil. On large Picard groups and the Hasse principle for curves and K3 surfaces. *Acta. Arith.*, **LXXVI.2** (1996), 165–189.

[14] E.V. Flynn. An explicit theory of heights. *Trans. Amer. Math. Soc.*, **347** (1995), 3003–3015.

[15] E.V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Mathematica*, **105** (1997), 79–94.

[16] E.V. Flynn and N.P. Smart. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arith.*, **79** (1997), 333–352.

[17] E.V. Flynn and J.L. Wetherell. Finding rational points on bielliptic genus 2 curves. *Manuscripta Math.*, **100** (1999), 519–533.

[18] E.V. Flynn. On Q-derived polynomials. *Proc. Edinburgh Math. Soc.* **44** (2001), 103–110.

[19] E.V. Flynn and J.L. Wetherell. Covering collections and a challenge problem of Serre. *Acta Arithmetica* **XCVIII.2** (2001), 197–205.

[20] The Magma Computational Algebra System. Available from http://magma.maths.usyd.edu.au/magma/

[21] W.G. McCallum. On the method of Coleman and Chabauty. *Math. Ann.* **299** (1994), no. 3, 565–596.

[22] B. Poonen and M. Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math.* (2) **150** (1999), no. 3, 1109–1149.

[23] V. Scharaschkin. Local Global Problems and the Brauer-Manin Obstruction. PhD Thesis, University of Michigan, 1999.

[24] V. Scharaschkin. The Brauer-Manin obstruction for 0-cycles. Manuscript, 2003.

[25] S. Siksek. On the Brauer-Manin obstruction to the Hasse principle for curves of split Jacobians. Preprint, 2003.

[26] S. Siksek and A.N. Skorobogatov. On a Shimura curve that is a counterexample to the Hasse principle. *Bull. London Math. Soc.*, **35** (2003), no. 3, 409–414.

[27] A.N. Skorobogatov. *Torsors and rational points.* CTM **144**. Cambridge Univ. Press, 2001.

[28] M. Stoll. Two simple 2-dimensional abelian varieties defined over $\mathbb{Q}$ with Mordell-Weil rank at least 19. *C. R. Acad. Sci. Paris, Série I*, **321** (1995), 1341–1344.

[29] M. Stoll. On the height constant for curves of genus two. *Acta Arith.* **90** (1999), 183–201.

[30] M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.* **98** (2001), 245–277.

[31] M. Stoll. On the height constant for curves of genus two, II. *Acta Arith.* **104** (2002), 165–182.

[32] H.P.F. Swinnerton-Dyer. Arithmetic of diagonal quartic surfaces, II. *Proc. London Math. Soc.*, **80** (2000), 513–544.

[33] A. Weil. *Variétés abeliennes et courbes algébriques.* Hermann & Cie, Paris (1948).

[34] J.L. Wetherell. Bounding the number of rational points on certain curves of high rank. PhD Dissertation, University of California at Berkeley, 1997.

Mathematical Institute, 24–29 St. Giles, Oxford OX1 3LB, United Kingdom
E-mail address: flynn@maths.ox.ac.uk