The Arithmetic of Hyperelliptic Curves

E. V. Flynn*, Mathematical Institute, University of Oxford

Abstract

We summarise recent advances in techniques for solving Diophantine problems on hyperelliptic curves; in particular, those for finding the rank of the Jacobian, and the set of rational points on the curve.

§0. Introduction

The constructive theory of hyperelliptic curves has been advanced significantly during the last year. It is intended to give here an indication of the current level of progress, and an outline of the main methods employed. The emphasis in Sections 1 to 4 will be on the group of rational points on the Jacobian of a hyperelliptic curve. Section 5 will concern itself with the use of the Jacobian to help to determine the rational points on the curve itself.

§1. The group law and formal group on the Jacobian

Let $\mathcal{C}$ be a hyperelliptic curve of genus g:

$$\mathcal{C} : Y^2 = F(X), \text{ where } deg(F) = 2g+1 \text{ or } 2g+2 \text{ and } F \text{ has non-zero discriminant.} \quad (1)$$

We shall assume that $\mathcal{C}$ is *defined over* $\mathbb{Q}$; that is, the coefficients of F are in $\mathbb{Q}$. By a *divisor* of $\mathcal{C}$ we shall mean (with slight abuse of notation and uniqueness) an unordered set of g points on the curve, where multiplicities are permitted. When $deg(F) = 2g+1$, we include ∞ as a point on $\mathcal{C}$, and denote $\{\infty, \ldots, \infty\} = \{g \cdot \infty\}$ by $\mathcal{O}$. When $deg(F) = 2g+2$ and g is even, we must include ∞^+ and ∞^- (the branches of the singularity at infinity) as separate points on $\mathcal{C}$, and we take $\mathcal{O} = \{g/2 \cdot \infty^+, g/2 \cdot \infty^-\}$. When $deg(F) = 2g+2$ and g is odd, then such an $\mathcal{O}$ is not defined over $\mathbb{Q}$ – however this technicality need not concern us here, as our examples will avoid that situation. Given a point $P = (x, y)$ on $\mathcal{C}$, its *flip* $\overline{P} = (x, -y)$. The inverse of a divisor $\{P_1, \ldots, P_g\}$ will then be $\{\overline{P_1}, \ldots, \overline{P_g}\}$.

* The author thanks SERC for financial support.

We shall say that three such divisors D_1, D_2, D_3 sum to $\mathcal{O}$ if there exists a function of the form

$$R(X) \cdot Y - S(X), \text{ where } deg(R) \leqslant g/2 - 1, \text{ and } deg(S) \leqslant 3g/2 \tag{2}$$

which is satisfied by the $3g$ points contained in the sets D_1, D_2, D_3. We let $\mathcal{J} = \mathcal{J}(\mathcal{C})$, the *Jacobian of* $\mathcal{C}$, denote all such sets of g points; then the above laws give $\mathcal{J}$ the structure of an abelian group, with identity $\mathcal{O}$, which generalises the usual group law on an elliptic curve (the case $g = 1$). A divisor $D = \{P_1, \ldots P_g\} = \{(x_1, y_1), \ldots (x_g, y_g)\}$ in $\mathcal{J}$ is *rational* if there exist polynomials ϕ and ψ of degree g, with coefficients in $\mathbb{Q}$, such that:

$$\phi(X) = \prod_{i=1}^{n} (X - x_i) \text{ and } y_i = \psi(x_i), \text{ for all } i. \tag{3}$$

The rational divisors form a subgroup of $\mathcal{J}$, denoted $\mathcal{J}(\mathbb{Q})$. A divisor D in $\mathcal{J}$ is of *finite order* (or *torsion*) if there exists a positive integer N such that $ND = \mathcal{O}$; the smallest such N is the *order* of D. It is well known that the subgroup of rational torsion divisors, $\mathcal{J}_{tors}(\mathbb{Q})$, is finite. It is also well known that $\mathcal{J}(\mathbb{Q})$ is finitely generated, and so there exists a non-negative integer r such that $\mathcal{J}(\mathbb{Q}) \cong \mathcal{J}_{tors}(\mathbb{Q}) \times \mathbb{Z}^r$. This integer r is the *rank* of the Jacobian. One of main aims of techniques developed during the last five years, has been – given a hyperelliptic curve – to find a set of generators for $\mathcal{J}(\mathbb{Q})$.

As well as being an abelian group, the Jacobian can also be given the structure of a smooth projective variety. By a theorem of Lefschetz ([15], p.105), we can find an embedding into $\mathbb{P}^{4^g-1}$.

Theorem 1.1. *Let $\mathcal{C}$ be a hyperelliptic curve of genus g, with coefficients in $\mathbb{Q}$. Then there is an embedding of $\mathcal{J}$ into $\mathbb{P}^{4^g-1}$ (which maps $\mathcal{J}(\mathbb{Q})$ into $\mathbb{P}^{4^g-1}(\mathbb{Q})$) as a smooth variety of dimension g, with defining equations given by quadratic forms, and the group law given by a biquadratic map. Further, the Kummer variety, obtained by taking the quotient of the Jacobian by ±, may be embedded into $\mathbb{P}^{2^g-1}$, with the duplication law given by quartic forms on both the Jacobian and Kummer varieties.* □

In practice, it is difficult to compute a set of defining equations for the Jacobian, due to the sheer size of the expressions involved. In the case of genus 2, however, the equations have been derived explicitly with the help of the computer algebra package Maple (see [3],[6],[8]).

Theorem 1.2. *Let* $\mathbf{a} = (a_0 \dots a_{15})$ *be the 16 functions given in [8]. Then these provide an embedding of the Jacobian into* $\mathbb{P}^{15}$*, with defining equations given by the 72 quadratic forms given in Appendix A of [6].* □

When considering local properties of the Jacobian (viewed over $\mathbb{Q}_p$) "near" $\mathcal{O}$, it is convenient to work with a power series description of the group law. It is necessary to find a basis of local parameters $\mathbf{s} = (s_1, \dots s_g)$, which are expressed in terms of the coordinate functions of the projective embedding of the Jacobian. A set of local parameters must have the property that they uniquely determine any $D \in \mathcal{J}$ which is sufficiently close to $\mathcal{O}$. There exists an associated vector $\mathcal{F} = (\mathcal{F}_1, \dots \mathcal{F}_g)$, where each $\mathcal{F}_i = \mathcal{F}_i(s_1, \dots s_g, t_1, \dots t_g)$ is a power series in $2g$ variables. Let $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathcal{J}(\mathbb{Q}_p)$ have local parameters $\mathbf{s}, \mathbf{t}, \mathbf{u}$, respectively; then, in a neighbourhood of $\mathcal{O}$, we have $\mathbf{u} = \mathcal{F}(\mathbf{s}, \mathbf{t})$. For the genus 2 case, a pair of local parameters is given by $s_1 = a_1/a_0, s_2 = a_2/a_0$, where $\mathbf{a}$ is as in Theorem 1.2. In this case, a method for deriving terms of the formal group is described in [6], [8].

In the case when a curve of genus 2 can be written over $\mathbb{Q}$ in the form $Y^2 =$ *quintic in* X, then the variety describing the Jacobian may be embedded into $\mathbb{P}^8$ rather than $\mathbb{P}^{15}$. The resulting algebra is considerably simpler, both for computing the defining equations of the Jacobian, and the terms of the formal group. This situation has been considered in detail in [13].

§2. Rational torsion sequences

In the case of an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$, the possible torsion groups $\mathcal{E}_{tors}(\mathbb{Q})$ which can occur have been completely determined by Mazur in [18].

Theorem 2.1. *Let* $\mathcal{E}$ *be an elliptic curve defined over* $\mathbb{Q}$*. Then the torsion subgroup* $\mathcal{E}_{tors}(\mathbb{Q})$ *is one of the fifteen groups:* $\mathbb{Z}/N\mathbb{Z}$ *for* $N = 1, \dots 10, 12$*, or* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ *for* $N = 1, \dots 4$. □

A result which applies to elliptic curves over a number field K has recently been found by Merel in [21], where it is shown that any prime torsion order p must be bounded by d^{3d^2}, where d is the degree of K over $\mathbb{Q}$. No result along these lines has been found for Jacobians of curves of higher genus, and it is a natural question to ask what new torsion orders can occur in $\mathcal{J}_{tors}(\mathbb{Q})$ as the genus increases.

In order to derive hyperelliptic curves for which the torsion orders in $\mathcal{J}(\mathbb{Q})$ increase quickly with respect to the genus, the strategy is to choose sequences of curves of genus g with rational points $P_1, \ldots, P_n$, so that n different functions meet the curve only at these points. If these functions induce n $\mathbb{Z}[g]$-linear conditions given by:

$$A \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \vdots \\ \mathcal{O} \end{pmatrix} \tag{4}$$

where $A \in M_n[\mathbb{Z}[g]]$, then it is immediate (on multiplying both sides on the left by $\det(A) \cdot A^{-1} \in M_n[\mathbb{Z}[g]]$) that

$$\det(A) \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \vdots \\ \mathcal{O} \end{pmatrix} \tag{5}$$

so that, for $i = 1, \ldots, n$, $\det(A) \cdot P_i = \mathcal{O}$ (where, as always, everything is up to linear equivalence). This provides a divisor of order dividing $\det(A)$, which can often be shown to have order exactly $\det(A)$.

For the purpose of deriving quadratic sequences, we require only two such points and two such functions. We have used this technique in [7] to find the following sequences.

Result 2.2. *The 1-parameter space of curves of genus g ($t \neq 0$):*

$$\mathcal{C} : Y^2 = -tX^{g-r}(X-1)^{g+r+1} + \psi(X)^2$$

where $0 \leqslant r \leqslant g-1$, and $\psi(X) = X^{g+1} - t(X-1)^g - X^{g-r}(X-1)^{r+1}$ (degree g in X), has a divisor of positive torsion order dividing: $2g^2 + 2g + r + 1$. In particular, when $r = 0$, the divisor $D = \{(1,1), (g-1) \cdot \infty\}$ has exact order $2g^2 + 2g + 1$. □

Result 2.3. *In even genus g, there exists $\mathbb{Q}$ rational torsion divisors of all orders in the interval $[g^2 + 2g + 1, g^2 + 3g + 1]$. Explicitly, the 1-parameter space of curves of genus g (g even, $t \neq 0$):*

$$\mathcal{C} : Y^2 = \big(\psi(X)\big)^2 - 2t(X^{g+2} + X^{r+1}) + t^2(X-1)^2$$

where $0 \leqslant r \leqslant g$, and $\psi(X) = \sum_{i=1}^{g-r+1} X^{r+i} = (X^{g+2} - X^{r+1})/(X-1)$, has a divisor of exact order $g^2 + 3g + 1 - r$. □

More recently, Leprévost in [16],[17] has improved Result 2.2 to find sequences of the form: $2g^2 + kg + 1$, for $k = 2, 3, 4$.

§3. Complete 2-descent and descent via isogeny

An intermediary step towards resolving $\mathcal{J}(\mathbb{Q})$ is to find $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, which is known to be finite. For a hyperelliptic curve $Y^2 = F(X)$ defined over $\mathbb{Q}$, let $F(X) = F_1(X)\ldots F_n(X)$ be the irreducible factorisation of $F(X)$ over $\mathbb{Q}$ and, for each i, let $K_i = \mathbb{Q}(\theta_i)$, where θ_i is a root of $F_i(X)$. Then, there is a well known [2] finite group M, which can be given as a subgroup of $K_1^*/(K_1^*)^2 \times \ldots \times K_n^*/(K_n^*)^2$, and an injection $\psi : \mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \longrightarrow M$. The construction of M and ψ guarantees that $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ is finite and provides an upper bound for its size, but does not guarantee that $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ can be found completely. The standard technique is to make use of the commutative diagram:

$$\begin{tikzcd}
\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \arrow[r, "\psi"] \arrow[d, "i_p"] & M \arrow[d, "j_p"] \\
\mathcal{J}(\mathbb{Q}_p)/2\mathcal{J}(\mathbb{Q}_p) \arrow[r, "\psi_p"] & M_p
\end{tikzcd} \tag{6}$$

where the bottom row is constructed in the same way as the top row, but with respect to $\mathbb{Q}_p$, the p-adic numbers. The maps i_p and j_p are natural maps on the quotient induced by the inclusion map from $\mathbb{Q}$ into $\mathbb{Q}_p$ (note that i_p and j_p are not injective in general). It turns out that, for any p, it is straightforward to compute $\mathcal{J}(\mathbb{Q}_p)$, ψ_p and M_p completely. The preimage of M_p under j_p can then be used to bound the image of ψ. We define the *Selmer group*, S, by:

$$S = \bigcap_p j_p^{-1}\big(im(\psi_p)\big).$$

The group S may be viewed as those members of M which cannot be discarded as potential members of $im\,\psi$ merely by "congruence" arguments. Clearly $im\,\psi \leqslant S$. It may turn out that $im\,\psi = S$, in which case the above method determines $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, and hence the rank of $\mathcal{J}(\mathbb{Q})$, completely. The extent to which S fails to determine $im\,\psi$ completely is described by a portion of a strucure called the *Tate-Shafarevich group.* The method is not an algorithm, since there is no known effective procedure for determining the Tate-Shafarevich group.

The above methodology has long been employed to find ranks of elliptic curves (the case $g = 1$). It is only very recently that non-trivial examples have been computed on Jacobians of curves of higher genus. The first successful method (complete 2-descent) was due to Gordon and Grant [12], which applies to curves of genus 2 which split completely over $\mathbb{Q}$:

$$Y^2 = (X - a_1)(X - a_2)(X - a_3)(X - a_4)(X - a_5),\ a_i \in \mathbb{Q}.$$

Note that, for a general curve of genus 2, given by $Y^2 = F(X)$, the 2-torsion subgroup of $\mathcal{J}$ is given by $\mathcal{O}$ and divisors of the form $\{(x_1, 0), (x_2, 0)\}$, where x_1, x_2 are distinct roots of $F(X)$. This gives a 2-torsion group of size 16 in $\mathcal{J}$, when viewed over $\mathbb{C}$. The above condition imposed by Gordon and Grant guarantees that all points of order 2 in $\mathcal{J}$ lie in $\mathcal{J}(\mathbb{Q})$, which simplifies the construction of the finite group M above (which lies inside products of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$). For each $d \in M$, they construct homogeneous spaces $\mathcal{J}_d$, which have the property that $d \in im\,\psi \iff \mathcal{J}_d(\mathbb{Q}) \neq \emptyset$. For each $\mathcal{J}_d$, one then tries either to find a rational point, or to find a contradiction in some $\mathbb{Q}_p$. Two examples were computed by this method in [12].

Example 3.1. *Let C be the curve $y^2 = x(x-1)(x-2)(x-5)(x-6)$. Then $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ is generated by the 2-torsion divisors, and the divisor $\{(3, 6), \infty\}$, which has infinite order. It follows that $\mathcal{J}(\mathbb{Q})$ has rank* 1, □

Example 3.2. *Let C be the curve $y^2 = x(x-3)(x-4)(x-6)(x-7)$. Then $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ is generated by the 2-torsion divisors, and $\mathcal{J}(\mathbb{Q})$ has rank* 0. □

Note that, in Example 3.1, the rank of $\mathcal{J}(\mathbb{Q})$ was deduced from the size of $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, by first finding the image of $\mathcal{J}_{tors}(\mathbb{Q})$ on $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, and then using the fact that each independent divisor of infinite order on $\mathcal{J}(\mathbb{Q})$ contributes precisely one to the nuumber generators of $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$. Therefore, the rank has been determined, without any guarantee that the divisors found are actual generators for $\mathcal{J}(\mathbb{Q})$. We will return to this point in Section 4.

A second method was developed by the author in [9], which applies to the more general class of curves of genus 2 which may be written in the form: $\mathcal{C} : Y^2 = q_1(X)q_2(X)q_3(X)$, where each $q_i(X)$ is a quadratic defined over $\mathbb{Q}$. In this case, the 2-torsion group of $\mathcal{J}(\mathbb{Q})$ must have size at least 4, including $\mathcal{O}$ and the 3 rational divisors of order 2, each given by a conjugate pair of roots to $q_i(X)$. This group of size 4 can be taken to be the kernel of a homomorphism (an *isogeny* of degree 4) to the Jacobian of an associated curve [1].

Definition 3.3. Let $\mathcal{C}$ be the curve of genus 2 defined over $\mathbb{Q}$ as:

$$\mathcal{C} : Y^2 = q_1(X)q_2(X)q_3(X) = (f_1X^2+g_1X+h_1)(f_2X^2+g_2X+h_2)(f_3X^2+g_3X+h_3). \quad (7)$$

For any two polynomials $p(X)$, $q(X)$, let $[p, q]$ denote $p'q - pq'$. Define $\widehat{\mathcal{C}}$ by:

$$\widehat{\mathcal{C}} : \Delta Y^2 = \hat{q}_1(X)\hat{q}_2(X)\hat{q}_3(X) = [q_2, q_3][q_3, q_1][q_1, q_2], \text{ where } \Delta = \begin{vmatrix} h_1 & g_1 & f_1 \\ h_2 & g_2 & f_2 \\ h_3 & g_3 & f_3 \end{vmatrix}.$$

Denote $b_{ij} = \text{resultant}(q_i, q_j)$, $b_i = b_{ij}b_{ik}$, $\hat{b}_{ij} = \text{resultant}(\hat{q}_i, \hat{q}_j)$, $\hat{b}_i = \hat{b}_{ij}\hat{b}_{ik}$. Let $\mathcal{J}$, $\widehat{\mathcal{J}}$ be the Jacobians of $\mathcal{C}$ and $\widehat{\mathcal{C}}$, and let α_i denote the point of order 2 in $\mathcal{J}(\mathbb{Q})$ corresponding to $q_i(X)$; similarly for $\hat{\alpha}_i$.

It has been shown in [1] that $\mathcal{J}$, $\widehat{\mathcal{J}}$ are isogenous. There exists isogenies: $\phi : \mathcal{J} \to \widehat{\mathcal{J}}$ with kernel $\{\mathcal{O}, \alpha_1, \alpha_2, \alpha_3\}$ and $\hat{\phi} : \widehat{\mathcal{J}} \to \mathcal{J}$ with kernel $\{\widehat{\mathcal{O}}, \hat{\alpha}_1, \hat{\alpha}_2, \hat{\alpha}_3\}$, such that $\hat{\phi}\circ\phi = [2]$, the duplication map on $\mathcal{J}$. As with elliptic curves, there is a natural injection [9] from $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$ into a known finite group which provides the foundation for descent via isogeny.

Theorem 3.4. *Let $\mathcal{C}, \widehat{\mathcal{C}}$ be as in Definition 1.1, and let $\mathbf{w} \in \widehat{\mathcal{J}}(\mathbb{Q})$. Then there exists a unique pair $(d_1, d_2) \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$ such that for every $\mathbf{v} \in \phi^{-1}(\mathbf{w})$, the sets $\{\mathbf{v}\}$, $\{\mathbf{v}, \mathbf{v}+\alpha_i\}$, $\{\mathbf{v}, \mathbf{v}+\alpha_1, \mathbf{v}+\alpha_2, \mathbf{v}+\alpha_3\}$ are defined over $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, $\mathbb{Q}(\sqrt{d_i})$, $\mathbb{Q}$, respectively ($i = 1, 2, 3$, $d_3 = d_1d_2$). Let $\psi^\phi : \widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q})) \mapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 : \mathbf{w} \mapsto (d_1, d_2)$. Then ψ^ϕ is a well defined injective homomorphism. Let $\mathcal{S} = \{p : p \mid \Delta b_1b_2b_3\hat{b}_1\hat{b}_2\hat{b}_3\} \cup \{2\} = \{p_1 \dots p_r\}$, and $\mathbb{Q}(\mathcal{S}^\phi) = \{\pm p_1^{e_1} \dots p_r^{e_r}\} \leqslant \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then im $\psi^\phi \leqslant \mathbb{Q}(\mathcal{S}) \times \mathbb{Q}(\mathcal{S})$.*

□

The problem of finding $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$ is therefore reduced to that of determining, for each member of $\mathbb{Q}(\mathcal{S}) \times \mathbb{Q}(\mathcal{S})$, whether a preimage exists under ψ^ϕ. As before, we use a commutative diagram similar to equation (6), except with $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ replaced by $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$, and with $\mathbb{Q}(\mathcal{S}) \times \mathbb{Q}(\mathcal{S})$ performing the role of the finite group M. We again hope that the image of ψ^ϕ is completely determined by p-adic considerations. Having found $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$, we then perform the same process with respect to the dual isogeny to find $\mathcal{J}(\mathbb{Q})/\hat{\phi}(\mathcal{J}(\mathbb{Q}))$. Then the exact sequence

$$0 \longrightarrow \{\widehat{\mathcal{O}}, \hat{\alpha}_1, \hat{\alpha}_2, \hat{\alpha}_3\} \longrightarrow \widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q})) \xrightarrow{\hat{\phi}} \mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \longrightarrow \mathcal{J}(\mathbb{Q})/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q})) \longrightarrow 0$$

may be used to give generators for $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, and hence the rank of $\mathcal{J}(\mathbb{Q})$ as before.

Descent via isogeny can be viewed as breaking the work of finding $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ into 2 easier pieces. It has the considerable advantage that the computations are performed over number fields of smaller degree than if a complete 2-descent were attempted. In [9], 12 worked examples were given of the following type.

Example 3.5. *Let $\mathcal{C}$, $\widehat{\mathcal{C}}$ be as follows:*

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

$$\widehat{\mathcal{C}} : Y^2 = (X^2 - 2X - 5)(X^2 + 2X - 1)(X^2 + 6X + 11).$$

Then $\mathcal{J}(\mathbb{Q})$ and $\widehat{\mathcal{J}}(\mathbb{Q})$ have rank 2. □

Recent improvements have significantly improved the speed of both methods. For example, Schaefer [22] has computer the following genus 3 example.

Example 3.6. *Let $\mathcal{C}$ be the curve:*

$$Y^2 = X(X - 2)(X - 3)(X - 4)(X - 5)(X - 7)(X - 10)$$

.

Then $\mathcal{J}(\mathbb{Q})$ has rank 2. □

Inprovements to the technique of descent via isogeny are described in [11], in which further ranks are computed. So far, the various techniques have computed over 100 ranks, and it hoped that rank tables will soon be made available by anonymous ftp.

§4. Height functions on the Kummer variety

It was observed in Section 3 that the methods for finding $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ found the rank of $\mathcal{J}(\mathbb{Q})$, but did not provide a way of showing that the divisors generating $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ also generate $\mathcal{J}(\mathbb{Q})$. A possible route from $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ to generators of $\mathcal{J}(\mathbb{Q})$ is via a height function defined on $\mathcal{J}(\mathbb{Q})$. We first define a height function on a general abelian group.

Definition 4.1. Let G be an abelian group. A *height function* H is a map $H : G \mapsto \mathbb{R}^+$ satisfying:

(1). There exists a constant C_1 such that, for all $P, Q \in G$, $H(P + Q)H(P - Q) \leqslant C_1 H(P)^2 H(Q)^2$.

(2). There exists a constant C_2 such that, for all $P \in G$, $H(2P) \geqslant H(P)^4/C_2$.

(3). For any constant C_3, the set $\{P \in G : H(P) \leqslant C_3\}$ is finite.

The constants C_1, C_2 depend only on the group G and the height function H, and we shall refer to them as the *height constants*.

The following property of abelian groups with a height function is proved in [23], p.199.

Lemma 4.2. *Let G be an abelian group with height function H, such that $G/2G$ is a finite set: $\{Q_1, \ldots, Q_n\}$, say. Then G is finitely generated. Explicitly, if $\epsilon = min\{H(P) : P \in G\}$, and $C_1' = max\{H(Q_i)^2 : 1 \leqslant i \leqslant n\} \cdot C_1/\epsilon$, then G is generated by the finite set: $\{P \in G : H(P) \leqslant \sqrt{C_1' C_2}\} \cup \{Q_1, \ldots, Q_n\}$.* □

In general, if $G/2G$ has already been computed, and if there is a height function on G, then the above Lemma reduces the task of finding generators for G to a finite computation. This is precisely the situation we have after the techniques for Section 3 have been successfully applied. In principle, therefore, it is sufficient to define a height function on $\mathcal{J}(\mathbb{Q})$. Such a function may be found by first embedding the Jacobian variety into $\mathbb{P}^{4^g-1}$, and the Kummer variety into $\mathbb{P}^{2^g-1}$, as in Theorem 1.1., and then taking the standard height of the resulting point in $\mathbb{P}^{2^g-1}(\mathbb{Q})$.

Definition 4.3. Let $\kappa : \mathcal{J}(\mathbb{Q}) \longrightarrow \mathbb{P}^{2^g-1}(\mathbb{Q})$ be an embedding of the Kummer surface. For any $D \in \mathcal{J}(\mathbb{Q})$, let $\kappa(D) = (v_0, \ldots, v_{2^g-1}) \in \mathbb{P}^{2^g-1}(\mathbb{Q})$. We may choose $v_0, \ldots, v_n$ to be integers with no common factor. Now define, $H_\kappa(D) = \max_i |v_i|$.

This is the natural generalisation of the usual x-coordinate height function on an elliptic curve, for which $H_\kappa(\{(x, y)\}) = \max(v_0, v_1)$, where $x = v_1/v_0$, with v_0, v_1 coprime integers.

In any genus, it is straightforward to show that H_κ is a height function. In genus 2, the height constant C_1 is easy to compute. However, the constant C_2 is more difficult. In principle, C_2 can be found by applying Hilbert's Nullstellensatz to the non-degenerate quartics which define the duplication map. In practice, this is not computationally viable even for curves with small coefficients. An improvement has been found [10], in which the duplication law on the Kummer variety is factored as:

$$\kappa(2D) = W_1 \tau W_2 \tau W_3 \kappa(D),$$

where $\tau : (v_0, \ldots, v_{2^g-1}) \mapsto (v_0^2, \ldots, v_{2^g-1}^2)$ and where W_1, W_2, W_3 are linear maps. The derivation of the equations describing W_1, W_2, W_3 makes use of the isogeny of Definition 3.3. A vastly smaller value of the constant C_2 may then be expressed in terms of the entries of the matrices for W_1, W_2, W_3.

Example 4.4. *Let C be the curve $y^2 = x(x-1)(x-2)(x-5)(x-6)$, as in Example 3.1. Then $\mathcal{J}(\mathbb{Q})$ is generated by the 2-torsion divisors, and the divisor $\{(3,6), \infty\}$.* □

Several other examples have been computed in [10]. However, it should be emphasised that this approach will become too slow as the size of the coefficients of $\mathcal{C}$ increases, and considerable work needs to be done before there is a viable, widely applicable method for finding generators for $\mathcal{J}(\mathbb{Q})$.

§5. Implementing theorems of Coleman

The following classical result of Chabauty [4] gives a way of deducing information about a curve from its Jacobian.

Proposition 5.1. *Let $\mathcal{C}$ be a curve of genus g defined over a number field K, whose Jacobian has Mordell-Weil rank $\leqslant g-1$. Then $\mathcal{C}$ has only finitely many K-rational points.*

This is a strictly weaker result than Falting's theorem (which gives the same result unconditionally); however it has been shown by Coleman [5] that Chabauty's method – when applicable – can be used in many situations to give good bounds for the number of points on a curve. In particular, there are two potential genus 2 applications [5], [14].

Proposition 5.2. *Let $\mathcal{C}$ be a curve of genus 2 defined over $\mathbb{Q}$, and $p \geqslant 4$ be a prime of good reduction. If the Jacobian of $\mathcal{C}$ has rank at most 1 and $\widetilde{\mathcal{C}}$ is the reduction of $\mathcal{C}$ mod p then $\#\mathcal{C}(\mathbb{Q}) \leqslant \#\widetilde{\mathcal{C}}(\mathbb{F}_p) + 2$.* □

Proposition 5.3. *Let $\mathcal{C}$ be a curve of genus 2 defined over $\mathbb{Q}$ with 4 rational branch points and good reduction at 3, whose Jacobian has rank at most 1. Then $\#\mathcal{C}(\mathbb{Q}) \leqslant 6$.* □

If the the rational branch points of the curve in Proposition 0.3 are mapped to $(0,0), (1,0), (-1,0), (1/\lambda, 0)$, then there is the following situation for which Coleman's method is guaranteed to determine $\mathcal{C}(\mathbb{Q})$ completely.

Proposition 5.4. *Let $\mathcal{C}$ be the curve of genus 2:*

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

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

There is only one non-trivial application of Proposition 5.2 in the literature, which is the curve already given as Example 3.1, due to Gordon and Grant [14].

Example 5.5. *Let $\mathcal{C}$ be the curve $Y^2 = X(X-1)(X-2)(X-5)(X-6)$ defined over $\mathbb{Q}$. Then $\#\mathcal{C}(\mathbb{Q}) = \#\widetilde{\mathcal{C}}(\mathbb{F}_7) + 2 = 10$.* □

It seems unlikely that there will be many direct applications of Proposition 5.2, which will resolve $\#\mathcal{C}(\mathbb{Q})$ completely, since one has to be fortunate for the bound $\#\widetilde{\mathcal{C}}(\mathbb{F}_p) + 2$ to be attained. However, there have recently been applications of Proposition 5.4 in [11], such as the following example.

Example 5.6. *The Jacobian of the curve: $Y^2 = X(X^2-1)(X - \frac{1}{9})(X^2 - 18X + 1)$ has rank 1 over $\mathbb{Q}$. Hence, by Proposition 5.4, there are no $\mathbb{Q}$-rational points on the curve apart from the points $(0,0), (1,0), (-1,0), (1/9, 0)$ and the 2 rational points at infinity.* □

We also refer the reader to the work of McCallum [19],[20], who makes use of Coleman's version of Chabauty's Theorem to obtain conditional bounds on the number of rational points on the Fermat curves.

§6. Work in progress

Work currently in progress emphasises enhancements of the techniques described in Section 3 (computing the rank of $\mathcal{J}(\mathbb{Q})$) and Section 5 (applying the theorems of Chabauty and Coleman).

The main impediment to a fast and widely applicable implementation of the descent procedures of Section 3 is the difficulty in explicitly describing generators of the finite group M into which $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ injects. This is the main step which requires genuine work in a number field. An example of a key slow step is the following: *Given α in the* *ring of integers of a number field K, find all irreducibles which divide α.* This type of problem is straightforward when K has class number 1, but otherwise can quickly become time consuming. Any progress with this slow step would have a dramatic effect on the speed at which ranks of Jacobians could be computed.

Techniques for applying Chabauty's theorem are rapidly being made more flexible and widely applicable beyond the special cases indicated in Section 5. The formal group of the Jacobian (mentioned at the end of Section 1) is being used to construct formal power series, defined over $\mathbb{Q}_p$ (for some choice of p), which must be satisfied by n, where n is the number of $\mathbb{Q}$-rational points on the original curve. This power series induces a bound on n which experimentally appears very sharp. In the 20 examples computed so far, the bound was attained in 17 cases (finding $\mathcal{C}(\mathbb{Q})$ completely), and in the 3 remaining cases, the bound was only 1 greater than the number of known rational points on the curve.

REFERENCES

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

[2] Cassels, J. W. S. *The Mordell-Weil Group of Curves of Genus 2.* Arithmetic and Geometry papers dedicated to I. R. Shafarevich on the occasion of his sixtieth birthday, Vol. **1.** Arithmetic, 29-60, Birkhäuser, Boston (1983).

[3] Cassels, J. W. S. *Arithmetic of curves of genus 2.* Number Theory and Applications (ed. R.A. Mollin), 27-35. NATO ASI Series C,265. Kluwer Academic Publishers, 1989.

[4] Chabauty C. *Sur les points rationels des variétés algébriques dont l'irregularité et supérieur á la dimension.* Comptes Rendus, Paris **212** (1941), 882-885.

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

[6] Flynn, E. V. *The Jacobian and Formal Group of a Curve of Genus 2 over an Arbitrary Ground Field.* Math. Proc. Camb. Phil. Soc. **107** (1990), 425-441.

[7] Flynn, E. V. *Sequences of rational torsions on abelian varieties.* Inventiones Math. **106** (1991), 433-442.

[8] Flynn, E. V. *The group law on the Jacobian of a curve of genus 2.* J. Reine Angew. Math. **439** (1993), 45-69.

[9] Flynn, E. V. *Descent via isogeny on the Jacobian of a curve of genus 2.* Acta Arithmetica LXVII.1 (1994), 23-43.

[10] Flynn, E. V. *An explicit theory of heights in dimension 2.* Preprint, February 1994.

[11] Flynn, E. V. *On a Theorem of Coleman.* Preprint, April 1994,

[12] Gordon, D.M. and Grant, D. *Computing the Mordell-Weil rank of Jacobians of curves of genus 2.* Trans. A.M.S., **337**, Number 2, (1993), 807-824.

[13] Grant, D. *Formal Groups in Genus 2.* J. Reine Angew. Math. **411** (1990), 96-121.

[14] Grant, D. *A curve for which Coleman's Chabauty bound is sharp.* Preprint, 1991.

[15] Lang, S. *Introduction to Algebraic and Abelian Functinos,* 2nd edition. Graduate Texts in Math. no. 89 (Springer-Verlag, 1982).

[16] Leprévost, F. *Torsion sur des familles de courbes de genre g.* Manuscripta math. **75** (1992), 303-326.

[17] Leprévost, F. *Famille de Courbes Hyperelliptiques de Genre g munies d'une Classe de Diviseurs Rationnels d'Ordre* $2g^2 + 4g + 1$. Preprint, 1993.

[18] Mazur, B. *Rational points of modular curves*, Modular Functions of One Variable, V, Lecture Notes in Math. **601** (1977), 107-148.

[19] McCallum, W.G. *On the Shafarevich-Tate group of the Jacobian of a quotient of the Fermat curve.* Invent. Math. **93** (1988), 637-666.

[20] McCallum, W.G. *The Arithmetic of Fermat Curves.* Math. Ann. **294** (1992), 503-511.

[21] Merel, L. *Bornes pours la torsion des courbes elliptiques sur les corps de nombres.* Preprint, 1994.

[22] Schaefer, E.F. *2-descent on the Jacobians of hyperelliptic curves.* J. Number Theory (to appear).

[23] Silverman, J. H. *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York (1986).