Solving Diophantine Problems on Curves via Descent on the Jacobian

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

§0. Introduction

The theory of Jacobians of curves has largely been developed in a vacuum, with little computational counterpart to the abstract theory. A recent development has been the explicit construction of Jacobians & formal groups, and workable methods of descent [6],[7] to find the rank. We suggest that the following plan will provide a powerful tool for finding the set of $\mathbb{Q}$-rational points $\mathcal{C}(\mathbb{Q})$ on a curve $\mathcal{C}$ of genus > 1:

(1). Find $J(\mathbb{Q})/2J(\mathbb{Q})$ via descent on J, the Jacobian of $\mathcal{C}$.

(2). Deduce generators for $J(\mathbb{Q})$ via an explicit theory of heights.

(3). Apply local techniques to try to deduce $\mathcal{C}(\mathbb{Q})$ via an embedding of $\mathcal{C}(\mathbb{Q})$ inside $J(\mathbb{Q})$.

We describe work just completed, which gives versions of (1),(2),(3) which are often workable in practice for genus 2, and outline the potential for a computationally viable generalisation. We note that (1),(2),(3) (quite aside from being part of this plan) have their own independent applications to other branches of the Mathematics of Computation, such as the search for large rank, the higher dimensional testing of well known conjectures [8], and algorithms for symbolic integration.

§1. Rank of the Mordell-Weil group using descent by isogeny.

It should first be mentioned that, in principle, there already exists a technique due to Gordon and Grant [7] which computes the Mordell-Weil group $J(\mathbb{Q})$ by complete 2-descent for the highly special case when the curve of genus 2 has all of its Weierstrass points defined over $\mathbb{Q}$. Such curves can be written in the form: $Y^2 = \Pi_{i=1}^{5}(X - \alpha_i)$, $\alpha_i \in \mathbb{Z}$. The problem here is that only a tiny handful of such curves have 3 or less primes of bad reduction, and so there will typically be a large number of homogeneous spaces to be checked. We have recently completed theory which fills this gap in the genus 2 situation; namely: a method of descent by isogeny likely to yield rank tables for large numbers of curves. A helpful feature recently publicised by Bost & Mestre in [1] (originally due to Richelot) is that there are natural underlying pairs of curves whose Jacobians are isogenous; specifically, there is an isogeny from the Jacobian of $\mathcal{C}$ to that of $\widehat{\mathcal{C}}$, where:

$$\mathcal{C} : Y^2 = g(X)h(X)i(X) = (g_2X^2 + g_1X + g_0)(h_2X^2 + h_1X + h_0)(i_2X^2 + i_1X + i_0) \quad (*)$$

$$\widehat{\mathcal{C}} : \Delta Y^2 = \big(h'(x)i(X) - h(X)i'(X)\big)\big(i'(x)g(X) - i(X)g'(X)\big)\big(g'(x)h(X) - g(X)h'(X)\big)$$

$$\text{where } \Delta = \det \begin{pmatrix} g_0 & g_1 & g_2 \\ h_0 & h_1 & h_2 \\ i_0 & i_1 & i_2 \end{pmatrix}.$$

Bost & Mestre investigate the geometry behind the isogeny, work over $\mathbb{R}$ rather than $\mathbb{Q}$, and do not make any use of the Jacobian as a variety. Our first task was to develop the isogeny explicitly from J to $\widehat{J}$, the Jacobians of $\mathcal{C}$ and $\widehat{\mathcal{C}}$, respectively, each embedded into $\mathbf{P}^{15}$. We have found the quadratic map over the ground field $\phi : J \mapsto \widehat{J}$ which defines the isogeny, and have performed a similar computation for the dual isogeny $\hat{\phi} : \widehat{J} \mapsto J$.

The computation of $\widehat{J}(\mathbb{Q})/\phi(J(\mathbb{Q}))$ is equivalent to determining, for a finite set of pairs $(d_1, d_2) \in \left(\mathbb{Q}^*/(\mathbb{Q}^*)^2\right)^2$, whether the *homogeneous spaces* C_{d_1,d_1} has a rational point. The space C_{d_1,d_2} is defined by a set of 72 equations over $\mathbb{Q}$, which are twists of the defining equations of the Jacobian. The symbolic algebra package Maple was essential for constructing the defining equations of C_{d_1,d_2}, as described in [6]. By applying the dual isogeny, $J(\mathbb{Q})/\phi(\widehat{J}(\mathbb{Q}))$ may also be found, giving $J(\mathbb{Q})/2J(\mathbb{Q})$, and hence the rank of $J(\mathbb{Q})$. We can show (for example) that the Jacobian of the curve:

$$\mathcal{C}^{(k)} : Y^2 = k(X^2+1)(X^2+2)(X^2+X+1)$$

has rank 1 when $k = 1, 2, 6$. Note that there are at least 60 curves of the form $(*)$ with small integer coefficients and only two primes (including $p = 2$) of bad reduction (which would not have been possible in the completely split situation), and a much larger number of curves available with three such primes. Even from these curves alone, We expect quickly to have about 60 ranks calculated and considerably more to follow. Quite aside from the applicability to solving Diophantine problems on curves (as will be described), it is to be hoped that such rank calculations will also lay the eventual foundation for testing and motivating higher dimensional analogues of conjectures [8] currently only tested for elliptic curves, such as the conjectures of Birch and Swinnerton-Dyer.

§2. Explicit theory of heights.

For the theory of heights, We consider $\mathbf{a} = (a_0, \ldots a_{15}) \in J(\mathbb{Q})$, where J is the embedding of the Jacobian in $\mathbf{P}^{15}$ mentioned in §1. Any such $\mathbf{a}$ can be written so that each $a_i \in \mathbb{Z}$ and $\gcd(a_0, \ldots, a_{15}) = 1$. By analogy with elliptic curves, let:

$$H(\mathbf{a}) = \max(|a_0|, \ldots, |a_{15}|).$$

which defines a height function. We have expressed the relevant constants in terms of the coefficients of the original curve. That is to say, for $\mathcal{C} : Y^2 = f_6X^6 + \ldots + f_0$ and for any

fixed $\mathbf{b} \in J(\mathbb{Q})$, We have found $k_1 = k_1(f_0, \ldots, f_6, \mathbf{b})$ and $k_2 = k_2(f_0, \ldots, f_6)$, expressed in terms of absolute values of expressions in $\mathbb{Z}[f_0, \ldots, f_6]$, such that for any $\mathbf{a} \in J(\mathbb{Q})$:

$$H(\mathbf{a} + \mathbf{b}) \leqslant k_1 H(\mathbf{a})^2, \;\; H(2\mathbf{a}) \geqslant k_2 H(\mathbf{a})^4.$$

This form of k_1 follows from the biquadratic forms defining the group law in [5]. The constant k_2 required considerably more symbolic computation (again, using Maple). It required the application of many resultant calculations to the duplication law on the Jacobian and Kummer surface (given by quartic forms). We have used this theory to show that, for the curves in [6], [7], the given generators of $J(\mathbb{Q})/2J(\mathbb{Q})$ are also generators of $J(\mathbb{Q})$. This represents the first non-trivial calculation of this type in dimension > 1. My intention is to do the same for those curves whose ranks are determined by my method of descent by isogeny. This should be facilitated by enhancements in progress using the restriction of the height function to the Kummer surface. There are also immediate applications of our explicit theory of heights to algorithms for finding the torsion subgroup of $J(\mathbb{Q})$; these, in turn, are relevant to the theory of computer integration of algebraic functions [4].

§3. Local techniques to find $\mathcal{C}(\mathbb{Q})$.

We have also investigated a theorem of Chabauty ([2],[3]) which states that a curve has only finitely many rational points when its Jacobian has rank less than the genus of the curve. This theorem was established (in 1941) long before Falting's Theorem, and it is an eccentric feature of the literature that there has been virtually no opportunity during the intervening 50 years to apply it non-trivially to Diophantine problems, due to the lack of rank calculations for genus > 1 (for elliptic curves, the result merely asserts in rank 0 that there are finitely many rational torsion points). This result can be interpreted in genus 2 (with rank 1 Jacobian) in a form amenable to practical computation. One first finds the first few terms of the formal group law, a calculation greatly facilitated by the form of the global group law in [5]. One can then, for any prime p of good reduction, use the generators of $J(\mathbb{Q})$ (determined by the descent techniques already described) to obtain a power series over $\mathbb{Q}_p$ which has at least as many solutions as $\mathbb{Q}$-rational points on the original curve. Bounds on the p-adic values of the coefficients together with Strassman's theorem then gives an upper bound on the p-adic solutions to the power series, and hence on the number of $\mathbb{Q}$-rational point on the curve. Should this bound be attained by the number of known $\mathbb{Q}$-rational points then $\mathcal{C}(\mathbb{Q})$ is determined completely. Otherwise, one can repeat the process for different values of p, and hope that the bound is attained for some p. It is not claimed that this is an effective procedure, merely a workable tool which appears almost always to resolve $\mathcal{C}(\mathbb{Q})$. We have applied it to a number of curves of genus 2 of rank 1, and found that the bound is attained in each case.

§4. Potential future progress.

The ideas of §1 are highly amenable to generalisation; there are already signs that descent procedures to find $J(\mathbb{Q})/2J(\mathbb{Q})$, and hence the rank of $J(\mathbb{Q})$, are being made viable at least for hyperelliptic curves of genus 3 [9], and possibly higher. The material of §2 and §3 should in principle be amenable to generalisation, although the search area in the heights computation may increase quickly with respect to genus.

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] Chabauty, C. *Sur les points rationels des courbes algébriques de genre supérieur á l'unité.* Comptes rendus, Paris **212** (1941), 882-885.

[3] Coleman, R. F. *Effective Chabauty.* Duke Math. J. **52** (1985), 765-770.

[4] Davenport, J. H. *On the Integration of Algebraic Functions*, Springer Lecture Notes in Computer Science **102**, Springer-Verlag (1981).

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

[6] Flynn, E. V. *Descent via isogeny in dimension 2.* To appear in Acta Arith.

[7] Gordon, D.M. and Grant, D. *Computing the Mordell-Weil rank of Jacobians of curves of genus 2.* Transactions of the American Mathematical Society. To appear.

[8] Hulsbergen, W.W.J. *Conjectures in arithmetic algebraic geometry: a survey*, Aspects of Mathematics **18**, Vieweg (1992).

[9] Schaefer, E.F. *2-descent on the Jacobians of hyperelliptic curves.* Draft manuscript, Dec. 1992.